TP 1 : Tests d'intrusions sur les équipements Cisco

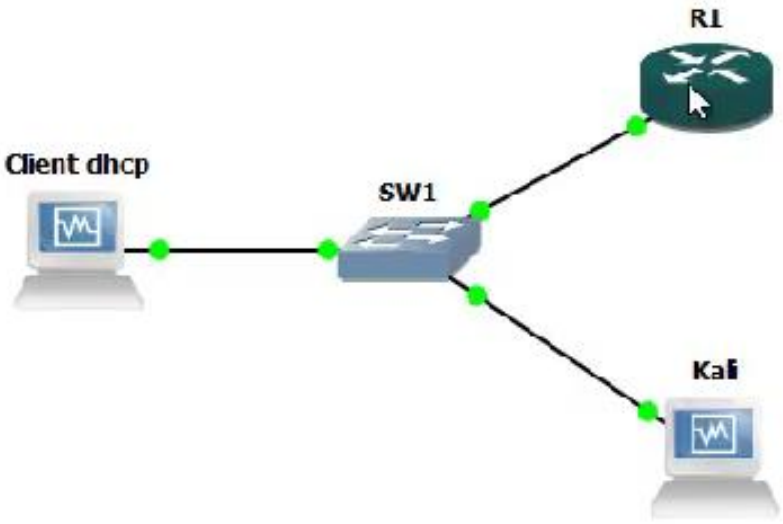
1- Objectif du TP: Le but de ce TP est de simuler des tests d'intrusion et des attaques en simulant un réseau sous GNS3 et en utilisant les outils Cisco Tools (https://www.kali.org/tools/) intégrés dans Kali Linux.

2- Prérequis : Pour pouvoir suivre ce TP, les connaissances suivantes sont requises :

- Script et commandes Bash Linux.
- Commandes IOS Cisco.
- Maitrise des protocoles de la pile TCP/IP. Exemples: DHCP, DNS, HTTP, UDP, …

3- Laboratoire GNS3 :

- Installer GNS3 sur votre machine Linux via le lien GNS3 | The software that empowers network professionals
- La topologie à construire est la suivante, pour cela :
  - Installer une image IOS d'un routeur CISCO. Par exemple un C3725 via Cisco 3725 | GNS3 ou un C7200 via le lien X-Files (lagout.org) . Ce routeur sera le serveur DHCP.
  - Ajouter un Hôte qui sera le client DHSCP
  - Ajouter Kali Linux à ce Lab sans pour autant importer la machine kali sur GNS3, dans le but de faire d tests d'intrusions sur les équipements Cisco. Pour cela, il faut suivre les instructions du lien https://medium.com/@ngommouhamad/ajouter-kali-linux-dans-un-lab-gns3-49d3b28e360d



4- Simulations d'intrusions:

Le but de cette partie est de dérouler les scénarii d'intrusions décrits par les liens suivants :

- fr gillette intimate video 6s 1920x1080 JFM24 (youtube.com)
- **https://www.youtube.com/watch?v=QTWk0Ckl00I**

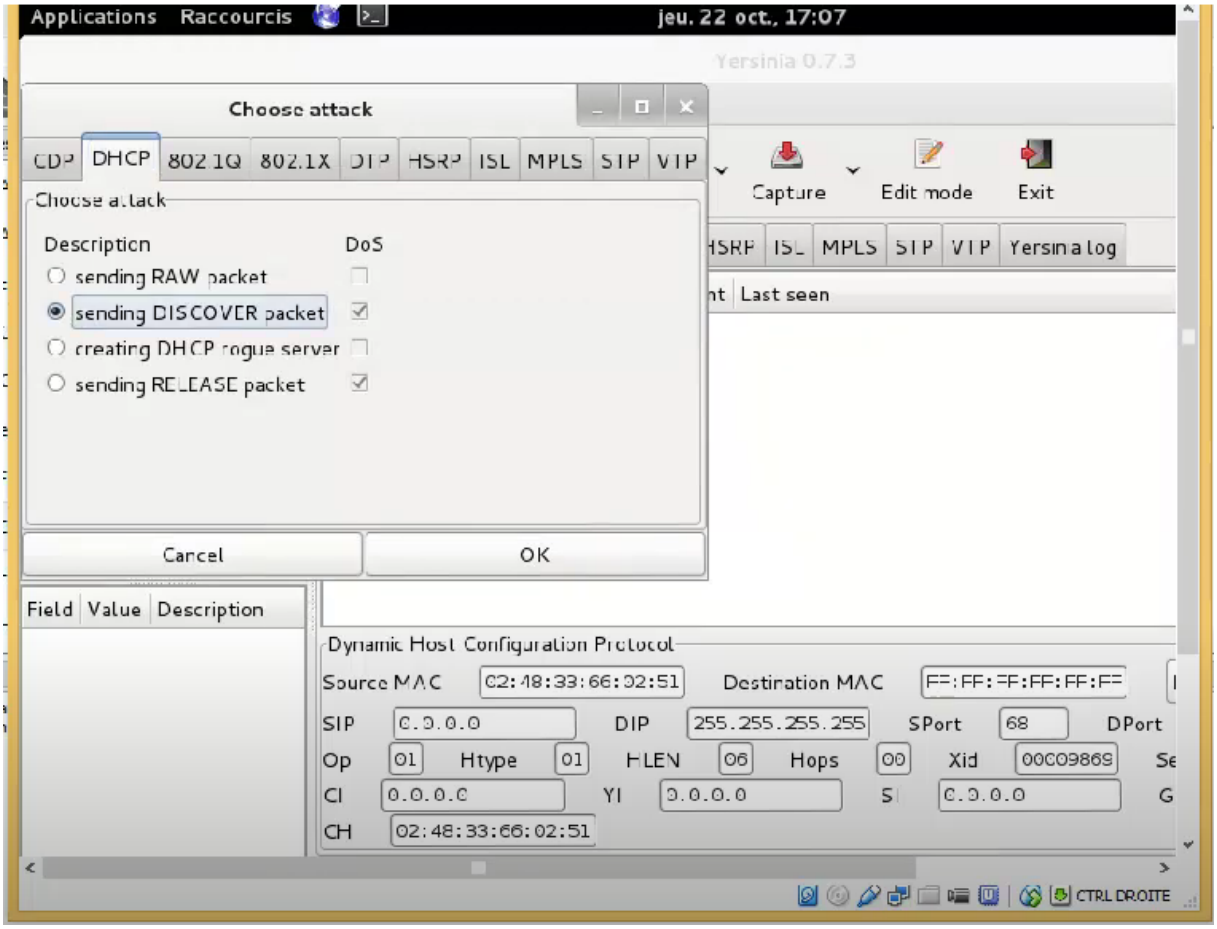
4-1 Avant ça vous devez :

- Commencer par configurer le service DHCP sur le routeur R1 pour attribuer des adresses IP dans le réseau 10.0.0.0/8
- Reporter sur le CR de votre TP les commandes CISCO utilisées pour configurer le DHCP (Screenshot autorisés).
- Vérifier le bon fonctionnement du serveur SHCP en consultant la configuration IP du client dhcp (attribution d'une @IP dans la plage 10.0.0.0/8. Screenshot autorisé.

4-2 Saturation du serveur DHCP via le script Kali Linux Yersinia :

- Lancer l'outil Yersinia à partir de la VM Kali Linux déjà installée et en exécutant la commande **yersinia -G**

- Saturer le serveur avec une tempête DoS de message dhcp DISCOVER



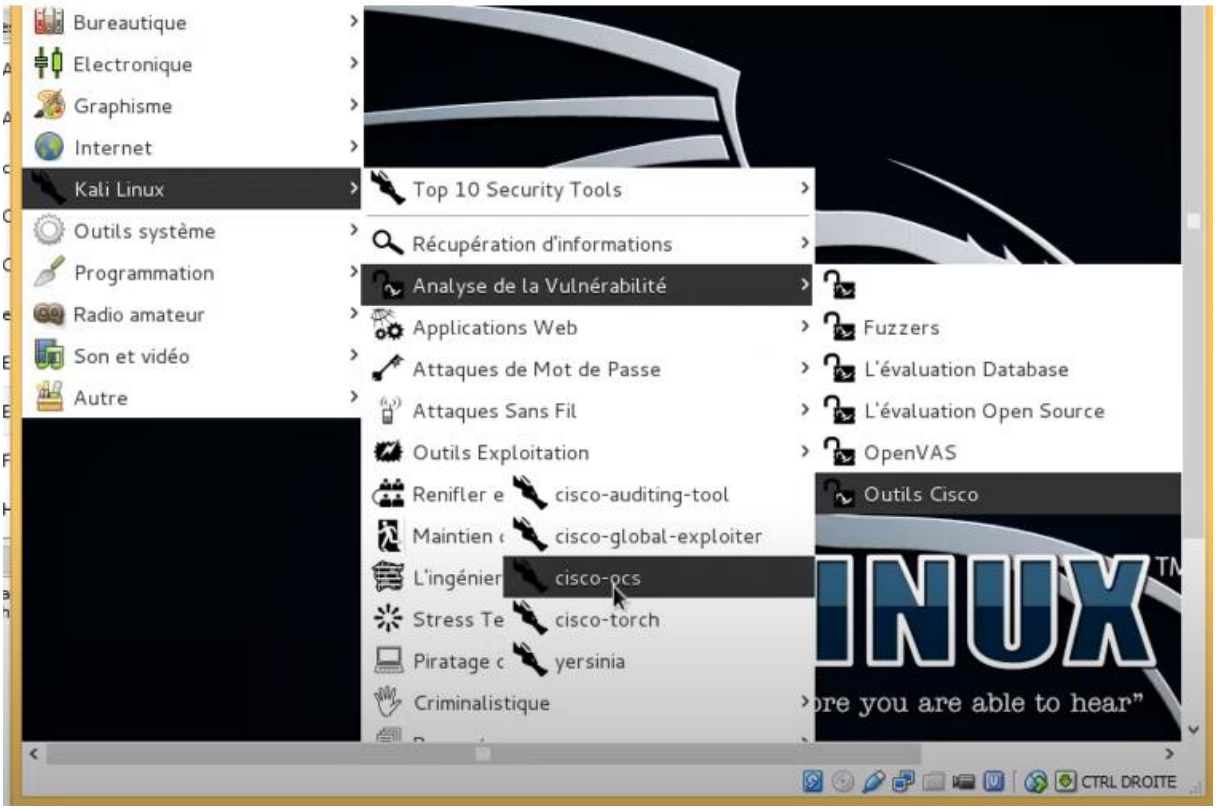
- Observer avec Wireshark les messages DHCP DISCOVER sur le lien entre Kali et le switch. –
  - Reporter sur votre compte rendu un screen shot
  - Quel est le port transport utilisé pour ses messages dhcp discover ?
  - Quelle est la taille du message dhcp discover ?
- Laisser tourner le script yersinia et la tempête dhcp et vérifier maintenant que le client n'a plus d'adresse IP valide. Reporter le screenshot sur votre compte rendu.
- Arrêter maintenant le script avec la commande **yersinia -I**

4-3 Récupération de mot de passe root :

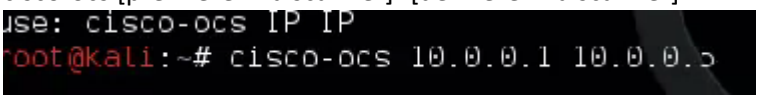
- En suivant les commandes CISCO de l'annexe, mettre en place un mot de passe non robuste « cisco » sur le routeur R1.
- Tester le mot de passe grâce à la commande suivante : telnet @IP routeur 23, où le 23 est le port telnet par défaut.

```
*Mar  1 00:15:31.019: %SYS-5-CONFIG_I: Configured from con
sole by console
R1#
R1#
R1#
R1#telnet 10.0.0.1 23
Trying 10.0.0.1 ...
```

- Lancer l'outil **cisco-ocs** à partir de Kali Linux.
-



- Lancer un scan des mots de passe via la commande suivante sur la console Kali
  cisco-ocs [première IP à scanner]- [dernière IP à scanner]



- Reporter le résultat du scan obtenu et commenter le. Avez-vous trouvé un équipement avec un mot de passe par défaut ; donner @IP de cet équipement ? et quel seraient le login et le mot de mot de passe par défaut?
- Tester à partir de kali , l'accès à distance à cet équipement (Routeur R1), avec la commande telnet.
- Reporter le screenshot d'intrusion telnet à partir de kali sur le routeur R1.

Annexe : Commandes CISCO

Scénario 1: Commandes Cisco pour mettre en place le service DHCP.

```
R1(config-if)#ip add
R1(config-if)#ip address 10.0.0.1 255.0.0.0
R1(config-if)#no shu
R1(config-if)#no shutdown
R1(config-if)#
```

```
R1(config)#service dhcp
R1(config)#ip dhcp pool mon-pool
R1(dhcp-config)#netw
R1(dhcp-config)#network 10.0.0.0
R1(dhcp-config)#
```

```
R1(dhcp-config)#network 10.0.0.0
R1(dhcp-config)#def
R1(dhcp-config)#default-router 10.0.0.1
R1(dhcp-config)#lease 1
R1(dhcp-config)#exit
R1(config)#
```

```
R1(config)#ip dhcp ex
R1(config)#ip dhcp excluded-address 10.0.0.1
```

Scénario 2: Commandes Cisco pour mettre en place un mot de passe

```
R1(config)#line vty 00
R1(config-line)#pass
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#enable secret
```

```
R1(config)#enable secret cisco
```