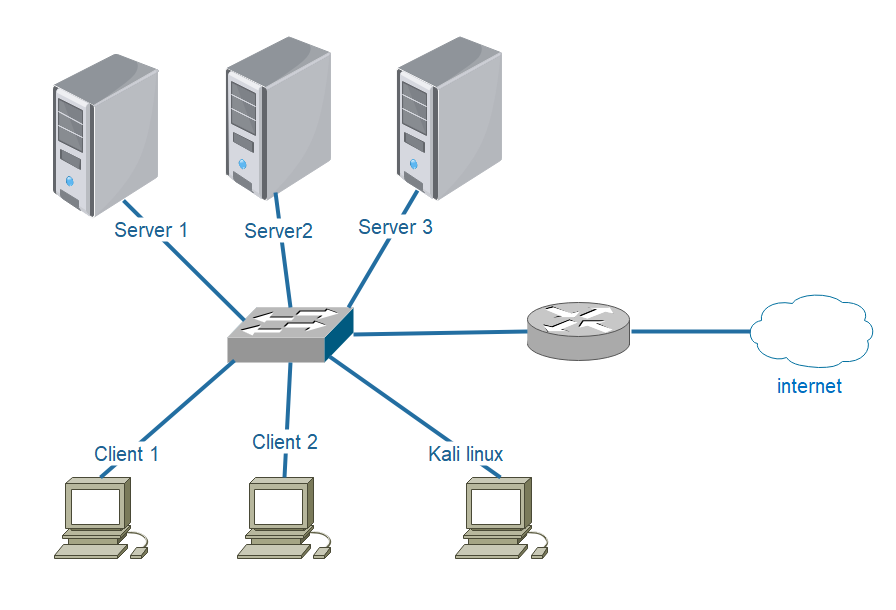
**Projet 3: Sniffers (HACKING DHCP & DNS)**



**Tâche 1 : Préparer le réseau**

Préparer le réseau selon le tableau suivant :

|  |  |  |
| --- | --- | --- |
| L’ordinateur | Le système d’exploitation | Configuration requise |
| Server 1 | Windows 2012 | Active directory  DNS |
| Server 2 | Windows 2012 | WEB  FTP  DHCP  TELNET  RDS |
| Server 3 | CentOS | WEB  SSH |
| Client 1 | Windows 7 | Membre du domaine |
| Client 2 | Windows 10 | Membre du Workgroups |
| Kali linux | Kali linux |  |

**Tâche 2 : Sniffers**

Un renifleur de paquets est un type de programme qui surveille tout morceau d'information entrant ou sortant d'un réseau. C'est un type d'appareil attaché à un ordinateur qui écoute sur le trafic réseau.

**Scenario :**

Le reniflage "sniffing" est une technique utilisée pour intercepter la sécurité des données, où de nombreux outils utilisés pour sécuriser le réseau peuvent également être utilisés par des attaquants pour exploiter et compromettre le même réseau. L'objectif principal du sniffing est de dérober des données, telles que des informations sensibles, des courriels, etc.

Le reniflage de réseau implique l'interception du trafic réseau entre deux nœuds de réseau cible et la capture de paquets réseau échangés entre des nœuds. Un renifleur de paquets est également appelé un moniteur réseau qui est utilisé légitimement par un administrateur réseau pour surveiller le réseau à la recherche de vulnérabilités en capturant le trafic réseau et, en cas de problème, procède à un dépannage de celui-ci.

De même, les outils de sniffing peuvent être utilisés par les attaquants pour capter et analyser tout le trafic réseau. Une fois que les pirates ont capturé le trafic réseau, ils peuvent analyser les paquets de puces et voir les informations de nom d'utilisateur et de mot de passe sur un réseau donné, puisque cette information est transmise en un format de texte clair. Un attaquant peut facilement entrer dans un réseau en utilisant des informations de connexion et compromettre des systèmes plus performants sur le réseau.

Par conséquent, il est très important qu'un administrateur réseau soit familier avec les analyseurs de trafic réseau et qu'il puisse maintenir et surveiller un réseau pour détecter les renifleurs de paquets, attaques MAC, attaques DHCP, empoisonnements ARP, usurpation d'identité ou empoisonnement DNS. et connaissez les types d'informations pouvant être détectées à partir des données capturées et utilisez les informations pour que le réseau fonctionne correctement.

**Objectifs de projet**

L'objectif de ce projet est de détecter un réseau et d'analyser les paquets pour toute attaque sur le réseau.

Les principaux objectifs de ce laboratoire sont :

■ Renifler le réseau

■ Analyser les paquets entrants et sortants

■ Résoudre les problèmes de performance du réseau

**Travail demandé :**

1. Attaquer la disponibilité du serveur DHCP
2. Créer un faux serveur DHCP
3. Vérifier que les victimes ont récupéré la configuration IP auprès du faux serveur
4. Lancer un sniffer réseau
5. Récupérer les informations des victimes

**Tâche 3 : Contremesures**

Proposer les différentes contremesures à mettre en place pour sécuriser notre système contre le hacking des services réseaux.