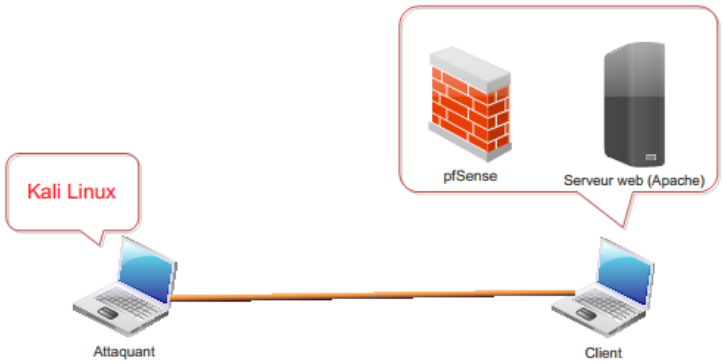
Travail pratique 3 LMD – SI

Module : Sécurité Informatique

Topologie :



Matériels : 2 PCs + câble

Logiciels :

1. Virtualbox
2. Wireshark
3. **Victime** : Serveur web s'exécutant sous Winows/ Linux
4. **Pare-feu** : pfsense
5. **Attaquant :** Kali Linux

Objectif : le but du TP est de simuler une attaque contre un serveur web et de montrer comment le pare-feu peut arrêter l'attaque.

Etapes :

1. Configurez pfsense de sorte à autoriser l'accès depuis l'extérieur au serveur web
   a. Vérification : l'attaquant doit pouvoir accéder la page par défaut du serveur
   b. Notez les performances de la machine cliente (taux d'utilisation de la CPU)
2. A partir de la machine de l'attaquant lancer une attaque contre le serveur web
   a. Utilisez Metasploit sous Kali linux pour lancer l'attaque
   b. Analysez le trafic sur la machine cliente pendant l'attaque en utilisant Wireshark
   c. Notez les performances de la machine cliente (CPU) pendant l'attaque, qu'est-ce que vous remarquez ?
3. Configurez pfsense de telle sorte à n'autoriser qu'une seule connexion par adresse IP (une machine ne pourra pas établir plus d'une connexion avec le serveur web)
   a. Relancez l'attaque
   b. Analysez le trafic sur la machine cliente pendant l'attaque en utilisant Wireshark, qu'est-ce que vous remarquez ?
   c. Notez les performances de la machine cliente, qu'est-ce que vous remarquez ?

Remarques :

- Un rapport détaillé (contenant la configuration, les commandes utilisées, et les réponses aux questions et l'explication) doit être fourni le jour de la validation.
- Vous avez le choix de travailler en monôme ou en binôme.

Les attaques informatique à lancer sont les suivants :

Les attaques	Les outils
1. NTP 2. DNS 3. LDAP 4. MSSQL 5. NetBIOS 6. SNMP 7. SSDP 8. UDP 9. UDP-Lag 10. WebDDoS 11. SYN 12. TFTP 13. Bruteforce attack 14. Web attack 15. Infiltration attack 16. Botnet attack 17. DDoS+PortScan	1. FTP – Patator 2. SSH – Patator 3. Hulk, GoldenEye, 4. Slowloris, Slowhttptest 5. Heartleech 6. Damn Vulnerable Web App (DVWA) 7. In-house selenium framework (XSS and Brute-force) 8. Nmap and portscan 9. Ares (developed by Python): remote shell, file upload/download, capturing 10. screenshots and key logging 11. Low Orbit Ion Canon (LOIC) for UDP, TCP, or HTTP requests