**DNS library Python**

Scapy est un puissant programme interactif de manipulation de paquets basé sur Python et bibliothèque.

Il est capable de forger ou de décoder des paquets d'un grand nombre de protocoles, de les envoyer sur le fil, les capturer, les stocker ou les lire à l'aide de fichiers pcap, faire correspondre les demandes et des réponses, et bien plus encore. Il est conçu pour permettre le prototypage rapide de paquets en en utilisant des valeurs par défaut qui fonctionnent.

Il peut facilement gérer la plupart des tâches classiques telles que la numérisation, le traçage, le sondage, tests unitaires, attaques ou découverte de réseau (il peut remplacer hping, 85% des nmap, arpspoof, arp-sk, arping, tcpdump, wireshark, p0f, etc.). Ça aussi fonctionne très bien dans de nombreuses autres tâches spécifiques que la plupart des autres outils ne peuvent pas gérer, comme envoyer des trames invalides, injecter vos propres trames 802.11, combiner techniques (VLAN hopping+ARP cache poisoning, décodage VoIP sur WEP protégé chaîne, ...), etc.

Scapy prend en charge Python 2.7 et Python 3 (3.4 à 3.9). Il est destiné à être multiplateforme et fonctionne sur de nombreuses plateformes différentes (Linux, OSX, \*BSD et Windows).

NetfilterQueue fournit un accès aux paquets correspondant à une règle iptables dans Linux. Les paquets ainsi mis en correspondance peuvent être acceptés, supprimés, modifiés, réorganisés, ou donné une note.

libnetfilter\_queue (la bibliothèque netfilter, pas ce module) fait partie du [Projet Netfilter](http://netfilter.org/projects/libnetfilter_queue/) .

La version actuelle de NetfilterQueue nécessite Python 3.6 ou version ultérieure. La dernière version prenant en charge Python 2.7 était la 0.9.0.

**Log in IPTABLES**

Dans le contexte de iptables, le terme "log" fait référence à l'action de journaliser le trafic réseau qui correspond à une règle spécifique. Lorsqu'un paquet correspond à une règle avec une cible LOG, iptables créera une entrée de journal avec des informations sur le paquet, telles que ses adresses IP source et destination, son protocole et ses numéros de port. L'entrée de journal peut ensuite être écrite dans un fichier, envoyée à un serveur syslog distant ou affichée sur la console.

Voici un exemple de règle iptables qui journalise le trafic entrant sur le port 22 (SSH) :

css

iptables -A INPUT -p tcp --dport 22 -j LOG --log-prefix "Trafic SSH : "

Cette règle ajoutera une nouvelle entrée dans le journal système pour chaque paquet correspondant à la règle. La chaîne de caractères "Trafic SSH : " sera ajoutée comme préfixe à chaque entrée de journal, ce qui permettra de distinguer facilement le trafic SSH des autres types de trafic dans le journal.