**Pytbull**

|  |  |
| --- | --- |
| **DESC** | |
| Testeur d’IDS | |
| **FILES** | |
|  |  |
| **QUICK START** | |
|  | |

**Généralités :**

* 300 tests regroupés dans 11 modules :

|  |  |
| --- | --- |
| **Module** | **Comments** |
| badTraffic | Trames non RFC |
| bruteForce | Sur FTP ou autre |
| clientSideAttacks | Utilisation d’un reverse shell pour downloader un fichier malicieux |
| denialOfService | DOS |
| evasionTechniques | Détection d’évasion |
| fragmentedPackets | Détection d’attaques fragmentées |
| ipReputation | Détection d’IPs compromises |
| normalUsage | Voir les FP |
| pcapReplay | Replay de fichiers PCAP |
| shellCodes | Détection de shellcodes sur le port 21 |
| testRules | **Test** de règles basiques |

|  |  |
| --- | --- |
| **Test** | **Comments** |
| socket | Envoie de données sur un port |
| command | Envoie d’une commande via subprocess.call() de Python |
| scapy | Envoie de payloads sur mesure via la syntaxe Scapy |
| Client side attacks | Utilisation d’un reverse shell (ex wget) |
| Pcap replay | Envoie d’un trafic basé sur un fichier PCAP |