Description of the KDD Cup 1999 Data

A connection is a sequence of TCP packets starting and ending at some well-defined times, between which data flows to and from a source IP address to a target IP address under some well-defined protocol. Each connection is labeled as either normal, or as an attack, with exactly one specific attack type. It is important to note that the testing set includes specific attack types not in the training set.

|  |  |  |
| --- | --- | --- |
| Attack Class | Description | Attack Name |
| DoS (Denial-of-service) | Attack in which attacker makes computing/memory resources too busy to handle legitimate requests | smurf, pod, teardrop, neptune, back |

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Feature Name | Description | Type |
| 1 | duration | Length (number of seconds) of the connection | Continuous |
| 2 | protocol\_type | Type of the protocol (e.g. tcp, udp) | Discrete |
| 3 | service | Network service on the destination (e.g. http, telnet) | Discrete |
| 4 | src\_bytes | Number of data bytes from source to destination | Continuous |
| 5 | dst\_bytes | Number of data bytes from destination to source | Continuous |
| 6 | hot | Number of ‘hot’ indicators | Continuous |
| 7 | num\_failed\_logins | Number of failed login attempts | Continuous |
| 8 | logged\_in | “1” if successfully logged in; “0” otherwise | Discrete |
| 9 | num\_compromised | Number of ‘compromised’ conditions | Continuous |
| 10 | root\_shell | “1” if root shell is obtained, “0” otherwise | Discrete |
| 11 | su\_attempted | “1” if ‘su root’ command attempted; “0” otherwise | Discrete |
| 12 | num\_root | Number of ‘root’ access | Continuous |
| 13 | is\_guest\_login | “1” if the login is a ‘guest’ login; “0” otherwise | Discrete |
| 14 | count | Number of connections to the same host as the current connection in the past two seconds | Continuous |
| 15 | srv\_count | Number of connections to the same service as the current connection in the past two seconds | Continuous |
| 16 | serror\_rate | % of connections that have the ‘SYN’ error | Continuous |
| 17 | rerror\_rate | % of connections that have the ‘REJ’ error | Continuous |
| 18 | same\_srv\_rate | % of connections to the same service | Continuous |
| 19 | diff\_srv\_rate | % of connections to different services | Continuous |
| 20 | dst\_host\_count | Count of connections having the same destination host | Continuous |
| 21 | dst\_host\_srv\_count | Count of connections having the same destination host and the same service | Continuous |
| 22 | dst\_host\_same\_srv\_rate | % of connections having the same destination host and using the same service | Continuous |
| 23 | dst\_host\_diff\_srv\_rate | % of different services on the current host | Continuous |
| 24 | dst\_host\_srv\_serror\_rate | % of connections to the current host and specified service that have an S0 error | Continuous |
| 25 | dst\_host\_srv\_rerror\_rate | % of connections to the current host that have an RST error | Continuous |
| 26 | outcome | The assigned class to the connection, whether it was an attack or a normal connection | Discrete |