|  |  |  |
| --- | --- | --- |
| *feature name* | *description* | *type* |
| duration | length (number of seconds) of the connection | continuous |
| protocol\_type | type of the protocol, e.g. tcp, udp, etc. | discrete |
| service | network service on the destination, e.g., http, telnet, etc. | discrete |
| src\_bytes | number of data bytes from source to destination | continuous |
| dst\_bytes | number of data bytes from destination to source | continuous |
| flag | normal or error status of the connection | discrete |
| land | 1 if connection is from/to the same host/port; 0 otherwise | discrete |
| wrong\_fragment | number of ``wrong'' fragments | continuous |
| urgent | number of urgent packets | continuous |
| Table 1: Basic features of individual TCP connections. | | |
| *feature name* | *description* | *type* |
| hot | number of ``hot'' indicators | continuous |
| num\_failed\_logins | number of failed login attempts | continuous |
| logged\_in | 1 if successfully logged in; 0 otherwise | discrete |
| num\_compromised | number of ``compromised'' conditions | continuous |
| root\_shell | 1 if root shell is obtained; 0 otherwise | discrete |
| su\_attempted | 1 if ``su root'' command attempted; 0 otherwise | discrete |
| num\_root | number of ``root'' accesses | continuous |
| num\_file\_creations | number of file creation operations | continuous |
| num\_shells | number of shell prompts | continuous |
| num\_access\_files | number of operations on access control files | continuous |
| num\_outbound\_cmds | number of outbound commands in an ftp session | continuous |
| is\_hot\_login | 1 if the login belongs to the ``hot'' list; 0 otherwise | discrete |
| is\_guest\_login | 1 if the login is a ``guest''login; 0 otherwise | discrete |
| Table 2: Content features within a connection suggested by domain knowledge. | | |
| *feature name* | *description* | *type* |
| count | number of connections to the same host as the current connection in the past two seconds | continuous |
|  | *Note: The following  features refer to these same-host connections.* |  |
| serror\_rate | % of connections that have ``SYN'' errors | continuous |
| rerror\_rate | % of connections that have ``REJ'' errors | continuous |
| same\_srv\_rate | % of connections to the same service | continuous |
| diff\_srv\_rate | % of connections to different services | continuous |
| srv\_count | number of connections to the same service as the current connection in the past two seconds | continuous |
|  | *Note: The following features refer to these same-service connections.* |  |
| srv\_serror\_rate | % of connections that have ``SYN'' errors | continuous |
| srv\_rerror\_rate | % of connections that have ``REJ'' errors | continuous |
| srv\_diff\_host\_rate | % of connections to different hosts | continuous |
| Table 3: Traffic features computed using a two-second time window. | | |

**Flags Info**

* S0: Connection attempt seen, no reply.
* S1: Connection established, not terminated.
* SF: Normal establishment and termination. Note that this is the same symbol as for state S1. You can tell the two apart because for S1 there will not be any byte counts in the summary, while for SF there will be.
* REJ: Connection attempt rejected.
* S2: Connection established and close attempt by originator seen (but no reply from responder).
* S3: Connection established and close attempt by responder seen (but no reply from originator).
* RSTO: Connection established, originator aborted (sent a RST).
* RSTR: Responder sent a RST.
* RSTOS0: Originator sent a SYN followed by a RST, we never saw a SYN-ACK from the responder.
* RSTRH: Responder sent a SYN ACK followed by a RST, we never saw a SYN from the (purported) originator.
* SH: Originator sent a SYN followed by a FIN, we never saw a SYN ACK from the responder (hence the connection was “half” open).
* SHR: Responder sent a SYN ACK followed by a FIN, we never saw a SYN from the originator.
* OTH: No SYN seen, just midstream traffic (one example of this is a “partial connection” that was not later closed).