|  |  |  |  |
| --- | --- | --- | --- |
| **Description of Network Features** | | | |
|
|
| **Service profile:** Connection activity | | | |
| **ID** | **Feature** | **Type** | **Description** |
| 1 | ts | Time | Timestamp of connection between flow identifiers |
| 2 | src\_ip | String | Source IP addresses which originate endpoints’ IP addresses |
| 3 | src\_port | Number | Source ports which Originate endpoint’s TCP/UDP ports |
| 4 | dst\_ip | String | Destination IP addresses which respond to endpoint’s IP addresses |
| 5 | dst\_port | Number | Destination ports which respond to endpoint’s TCP/UDP ports |
| 6 | proto | String | Transport layer protocols of flow connections |
| 7 | service | String | Dynamically detected protocols, such as DNS, HTTP and SSL |
| 8 | duration | Number | The time of the packet connections, which is estimated by subtracting ‘time of last packet seen’ and ‘time of first packet seen’ |
| 9 | src\_bytes | Number | Source bytes which are originated from payload bytes of TCP sequence numbers |
| 10 | dst\_bytes | Number | Destination bytes which are responded payload bytes from TCP sequence numbers |
| 11 | conn\_state | String | Various connection states, such as S0 (connection without replay), S1 (connection established), and REJ (connection attempt rejected) |
| 12 | missed\_bytes | Number | Number of missing bytes in content gaps |
|  |  |  |  |
| **Service profile:** Statistical activity | | | |
| **ID** | **Feature** | **Type** | **Description** |
| 13 | src\_pkts | Number | Number of original packets which is estimated from source systems |
| 14 | src\_ip\_bytes | Number | Number of original IP bytes which is the total length of IP header field of source systems |
| 15 | dst\_pkts | Number | Number of destination packets which is estimated from destination systems |
| 16 | dst\_ip\_bytes | Number | Number of destination IP bytes which is the total length of IP header field of destination systems |
|  |  |  |  |
| **Service profile:** DNS activity | | | |
| **ID** | **Feature** | **Type** | **Description** |
| 17 | dns\_query | string | Domain name subjects of the DNS queries |
| 18 | dns\_qclass | Number | Values which specifies the DNS query classes |
| 19 | dns\_qtype | Number | Value which specifies the DNS query types |
| 20 | dns\_rcode | Number | Response code values in the DNS responses |
| 21 | dns\_AA | Bool | Authoritative answers of DNS, where T denotes server is authoritative for query |
| 22 | dns\_RD | Bool | Recursion desired of DNS, where T denotes request recursive lookup of query |
| 23 | dns\_RA | Bool | Recursion available of DNS, where T denotes server supports recursive queries |
| 24 | dns\_rejected | Bool | DNS rejection, where the DNS queries are rejected by the server |
|  |  |  |  |
| **Service profile:** SSL activity | | | |
| **ID** | **Feature** | **Type** | **Description** |
| 25 | ssl\_version | String | SSL version which is offered by the server |
| 26 | ssl\_cipher | String | SSL cipher suite which the server chose |
| 27 | ssl\_resumed | Bool | SSL flag indicates the session that can be used to initiate new connections, where T refers to the SSL connection is initiated |
| 28 | ssl\_established | Bool | SSL flag indicates establishing connections between two parties, where T refers to establishing the connection |
| 29 | ssl\_subject | String | Subject of the X.509 cert offered by the server |
| 30 | ssl\_issuer | String | Trusted owner/originator of SLL and digital certificate (certificate authority) |
|  |  |  |  |
| **Service profile:** HTTP activity | | | |
| **ID** | **Feature** | **Type** | **Description** |
| 31 | http\_trans\_depth | Number | Pipelined depth into the HTTP connection |
| 32 | http\_method | String | HTTP request methods such as GET, POST and HEAD |
| 33 | http\_uri | String | URIs used in the HTTP request |
| 35 | http\_version | String | The HTTP versions utilised such as V1.1 |
| 36 | http\_request\_body\_len | Number | Actual uncompressed content sizes of the data transferred from the HTTP client |
| 37 | http\_response\_body\_len | Number | Actual uncompressed content sizes of the data transferred from the HTTP server |
| 38 | http\_status\_code | Number | Status codes returned by the HTTP server |
| 39 | http\_user\_agent | Number | Values of the User-Agent header in the HTTP protocol |
| 40 | http\_orig\_mime\_types | String | Ordered vectors of mime types from source system in the HTTP protocol |
| 41 | http\_resp\_mime\_types | String | Ordered vectors of mime types from destination system in the HTTP protocol |
|  |  |  |  |
| **Service profile:** Violation activity | | | |
| **ID** | **Feature** | **Type** | **Description** |
| 42 | weird\_name | String | Names of anomalies/violations related to protocols that happened |
| 43 | weird\_addl | String | Additional information is associated to protocol anomalies/violations |
| 44 | weird\_notice | bool | It indicates if the violation/anomaly was turned into a notice |
|  |  |  |  |
| **Service profile:** Data labelling | | | |
| **ID** | **Feature** | **Type** | **Description** |
| 45 | label | Number | Tag normal and attack records, where 0 indicates normal and 1 indicates attacks |
| 46 | type | String | Tag attack categories, such as normal, DoS, DDoS and backdoor attacks, and normal records |