CASE STUDY

**Background**

The dataset to be audited was provided which consists of a wide variety of intrusions simulated in a military network environment. It created an environment to acquire raw TCP/IP dump data for a network by simulating a typical US Air Force LAN. The LAN was focused like a real environment and blasted with multiple attacks. A connection is a sequence of TCP packets starting and ending at some time duration between which data flows to and from a source IP address to a target IP address under some well-defined protocol. Also, each connection is labelled as either normal or as an attack with exactly one specific attack type. Each connection record consists of about 100 bytes.

For each TCP/IP connection, 41 quantitative and qualitative features are obtained from normal and attack data (3 qualitative and 38 quantitative features) . The class variable has two categories:

* Normal
* Anomalous

Data basically represents the packet data for a time duration of 2 seconds.

1-9 Columns: basic features of packet (type 1)

10-22 columns: employ the content features (type 2)

23-31 columns: employ the traffic features with 2 seconds of time window (type 4)

32-41 columns: employ the host based features

C: Continuous data

D: Discrete data

|  |  |  |  |
| --- | --- | --- | --- |
| **Feature name** | **Variable type** | **Type** | **Description** |
| Duration | C | 1 | No. of seconds of the connection |
| Protocol\_type | D | 1 | Type of protocol  E.g.: TCP,UDP ,ICMP |
| Service | D | 1 | Network service on the destination E.g.: http, telnet |
| Flag | D | 1 | Normal or error status of the connection |
| src\_bytes | C | 1 | Number of data bytes from source to destination |
| dst\_bytes | C | 1 | Number of data bytes from destination to source |
| Land | D | 1 | 1-connection is from the same host/port:  0-otherwise |
| Wrong\_fragment | C | 1 | No. of ‘wrong’ fragments |
| Urgent | C | 1 | No of urgent fragments |
| Hot | C | 2 | The count of access to system directories, creation and execution of programs |
| Num\_failed\_logins | C | 2 | No. of failed login attempts |
| Logged\_in | D | 2 | 1-successfully logged in  0-otherwise |
| num\_compromised | C | 2 | No. of compromised conditions |
| Root\_shell | C | 2 | 1-root shell is obtained;0 otherwise |
| Su\_attempted | C | 2 | 1-‘su root’ command attempted;0 otherwise |
| Num\_root | C | 2 | No .of root accesses |
| num\_file\_creations | C | 2 | Number of file creation operations |
| Num\_shells | C | 2 | No of shell prompts |
| Num\_access\_files | C | 2 | No. of write ,delete and create operations on access control files |
| Num\_outbound\_cmds | C | 2 | No. of outbound commands in an ftp session |
| Is\_hot\_login | D | 2 | 1-the login belongs to the ‘hot’ list  0: otherwise |
| Count | C | 3 | No. of connections to the same host as the current connection in the past seconds |
| Srv\_count | C | 3 | No of connections to the same host as the current connection in the past 2 seconds |
| serror\_rate | C | 3 | % of connections that have ‘SYN’ errors to the same host |
| Srv\_serror\_rate | C | 3 | % of connections that have ‘SYN’ errors to the same service |
| Rerror\_rate | C | 3 | % of connections that have ‘REJ’ errors to the same host |
| Srv\_diff\_host\_rate | C | 3 | % of connections to different services and to the same host |
| Dst\_host\_count | C | 3 | No of connections to the same host to the destination host as the current connection in the past 2 seconds |
| Dst\_host\_srv\_count | C | 3 | No of connections from the same service to the destination host as the current connection in the past 2 seconds |
| dst\_host\_srv\_count | C | 3 | No. of connections from the same service to the destination host as the current connection in the past 2 seconds |
| Dst\_host\_srv\_count | C | 3 | No. of connections from the same service to the destination host as the current connection in the past 2 seconds |
| Dst\_host\_same\_srv\_rate | C | 3 | % of connections from the same service to the destination host |
| Dst\_host\_diff\_srv\_rate | C | 3 | % of connections from the different services to the destination host |
| Dst\_host\_same\_src\_port\_rate | C | 3 | % of connections from the port services to the destination host |
| Dst\_host\_srv\_diff\_host\_rate | C | 3 | % of connections from the different hosts from the same service to destination host |
| Dst\_host\_serror\_rate | C | 3 | % of connections that have ‘SYN” errors to same host to the destination host |
| dst\_host\_srv\_serror\_rate | C | 3 | % of connections that have ‘SYN’ errors from the same service to the destination host |
| Dst\_host\_rerror\_rate | C | 3 | % of connections that have ‘REJ’ errors from the same host to destination host |
| Dst\_host\_srv\_rerror\_rate | C | 3 | % of connections that have ‘REJ’ errors from the same service to the destination host |