The data file contains the following independent attributes.

Field Names

duration: continuous.
protocol_type: symbolic.
service: symbolic.
flag: symbolic.
src_bytes: continuous.
dst_bytes: continuous.
land: symbolic.
wrong_fragment: continuous.
urgent: continuous.
hot: continuous.
num_failed_logins: continuous.
logged_in: symbolic.
num_compromised: continuous.
root_shell: continuous.
su_attempted: continuous.
num_root: continuous.
num_file_creations: continuous.
num_shells: continuous.
num_access_files: continuous.
num_outbound_cmds: continuous.
is_host_login: symbolic.
is_guest_login: symbolic.
count: continuous.
srv_count: continuous.
serror_rate: continuous.
srv_serror_rate: continuous.
rerror_rate: continuous.
srv_rerror_rate: continuous.
same_srv_rate: continuous.
diff_srv_rate: continuous.
srv_diff_host_rate: continuous.
dst_host_count: continuous.
dst_host_srv_count: continuous.
dst_host_same_srv_rate: continuous.
dst_host_diff_srv_rate: continuous.
dst_host_same_src_port_rate: continuous.
dst_host_srv_diff_host_rate: continuous.
dst_host_serror_rate: continuous.
dst_host_srv_serror_rate: continuous.
dst_host_rerror_rate: continuous.
dst_host_srv_rerror_rate: continuous.

In addition, there is a target attribute named “attack_type”, which is a categorical variable with 22 different values. Before using this as a target variable, this one needs to be mapped into four types (dos, u2r, r2l and probe), as mentioned in Table 3 of the article, using following mapping table. This modified target attribute should be used for answering all the questions.

S/N	Name	Type
1.	Back	dos
2.	buffer_overflow	u2r
3.	ftp_write	r2l
4.	guess_passwd	r2l
5.	imap	r2l
6.	ipsweep	probe
7.	land	dos
8.	loadmodule	u2r
9.	multihop	r2l
10.	neptune	dos
11.	nmap	probe
12.	perl	u2r
13.	phf	r2l
14.	pod	dos
15.	portsweep	probe
16.	rootkit	u2r
17.	satan	probe
18.	smurf	dos
19.	spy	r2l
20.	teardrop	dos

21.	warezclient	r2l
22.	warezmaster	r2l