6 Test Results

The results of each of the sixteen test runs were recorded according to the Result Forms from Appendices F, G, H and I. A table summarising the results of each test data set follows each results table. For example, Table 6.1 presents test results from test data set 1, this is followed-up with Table 6.2 that presents a summary of the results from table 6.1. Finally, an overall results table (Table 6.9) is presented.

6.1 Test Data Set 1 (1998 Learning Data Week 6)

Table 6.1 presents the results of running test data set 1 through the four configurations of Snort.

Table 6.1: Results of Testing the Snort Configurations with Test Data Set 1

Week	Day	Attack Category	Attack Name	Snort 1.7 Full	Snort 1.7 Custom	Snort 1.8 Full	Snort 1.8 Custom
6	Mon	R2L	Phf	N	N	Y	Y
6	Mon	Probe	Satan	N	N	Y	Y
6	Mon	DoS	Neptune	N	N	N	N
6	Tues	Probe	Portsweep	N	N	N	N
6	Tues	DoS	Pod	Y	Y	Y	Y
6	Tues	DoS	Land	N	N	Y	Y
6	Wed	Probe	Ipsweep	Y	N	Y	Y
6	Wed	DoS	Neptune	N	N	N	N
6	Wed	DoS	Back	N	N	Y	Y
6	Thurs	Probe	Ipsweep	Y	N	Y	Y
6	Thurs	Probe	Ipsweep	Y	N	Y	Y
6	Thurs	U2R	Eject	N	N	N	N
6	Thurs	U2R	Ffb	N	N	N	N
6	Thurs	U2R	Eject	N	N	N	N
6	Thurs	U2R	Eject	N	N	N	N
6	Thurs	U2R	Eject	N	N	N	N
6	Thurs	DoS	Pod	Y	Y	Y	Y
6	Thurs	DoS	Pod	Y	Y	Y	Y
6	Thurs	DoS	Pod	Y	Y	Y	Y
6	Thurs	R2L	Dict	N	N	N	N

Week	Day	Attack Category	Attack Name	Snort 1.7 Full	Snort 1.7 Custom	Snort 1.8 Full	Snort 1.8 Custom
5	*Thurs*	*Probe*	*Ipsweep*	Y	N	Y	Y
5	Thurs	R2L	Phf	N	N	Y	Y
5	Thurs	DoS	Neptune	N	N	N	N
5	Thurs	Probe	Portsweep	Y	N	Y	Y
5	Thurs	U2R	Eject	N	N	N	N
5	Thurs	Probe	Portsweep	Y	N	Y	Y
5	Thurs	DoS	Smurf	Y	N	Y	Y
5	Thurs	DoS	Land	N	N	Y	Y
5	Thurs	DoS	Neptune	N	N	N	N
5	Thurs	DoS	Teardrop	Y	Y	Y	Y
5	Thurs	Probe	Satan	Y	N	Y	Y
5	Thurs	Probe	Ipsweep	Y	N	Y	Y
5	Thurs	U2R	Eject	N	N	N	N
5	Thurs	Probe	Portsweep	Y	N	Y	Y
5	Thurs	U2R	Ffb	N	N	N	N
5	Thurs	Probe	Ipsweep	Y	N	Y	Y
5	Thurs	DoS	Land	N	N	N	N
5	Thurs	DoS	Teardrop	Y	Y	Y	Y
5	Thurs	DoS	Pod	Y	Y	Y	Y
5	Thurs	DoS	Pod	Y	Y	Y	Y
5	Thurs	U2R	Perlmagic	N	N	N	N
5	Thurs	Probe	Satan	N	N	Y	Y
5	Thurs	U2R	Perlmagic	N	N	N	N
5	Thurs	U2R	Eject	N	N	N	N
5	Thurs	DoS	Smurf	Y	Y	Y	Y
5	Thurs	U2R	Eject	N	N	N	N
5	Thurs	U2R	Ffb	N	N	N	N
5	Thurs	U2R	Eject	N	N	N	N
5	Thurs	U2R	Eject	N	N	N	N
5	Thurs	U2R	Eject	N	N	N	N
5	Fri	DoS	Teardrop	N	N	N	N
5	Fri	DoS	Neptune	N	N	N	N
5	Fri	DoS	Smurf	Y	Y	Y	Y

6.1.1 Summary of Results from Test Data Set 1

Table 6.2 summarises the test results from running Snort against test data set 1.

Table 6.2: Summary of Results from Testing Snort with Test Data Set 1

		Snort 1.7 Full		Snort 1.7 Custom		Snort 1.8 Full		Snort 1.8 Custom	
ck	No. of Attacks	No. Detected	Detection Rate	No. Detected	Detection Rate	No. Detected	Detection Rate	No. Detected	Detection Rate
S	21	11	52%	10	48%	14	67%	14	67%
R	16	0	0%	0	0%	0	0%	0	0%
L	3	0	0%	0	0%	2	67%	2	67%
obe	13	10	77%	0	0%	12	92%	12	92%
ta	0	N/a*	N/a*	N/a*	N/a*	N/a*	N/a*	N/a*	N/a*

*N/a – not applicable as there were no attacks in this category

As can be seen from table 6.2, there were 21 instances of Denial of Service attacks, 16 instances of User to Root attacks, 3 instances of Remote to Local attacks, 13 instances of Probe attacks and no instances of Data attacks in test data set 1. The majority of the attacks were from the Denial of Service category.

The attack category that was easiest to detect was the Probe category. Snort 1.8 Full and Snort 1.8 Custom detected 92% of the total Probe attacks while Snort 1.7 Full detected 77% of the attacks in this category. All the four configurations performed fairly well in detecting the Denial of Service attack where the detection rates for Snort 1.7 Full, Snort 1.7 Custom, Snort 1.8 Full and Snort 1.8 Custom were 52%, 48%, 67% and 67% respectively. The detection rates were identical for Snort 1.8 Full and Snort 1.8 Custom in all attack categories.

6.2 *Test Data Set 2 (1998 Learning Data Week 7)*

Table 6.3 presents the results of running test data set 2 through the four configurations of Snort.

Table 6.3: Results of Testing the Snort Configurations with Test Data Set 2

Week	Day	Attack Category	Attack Name	Snort 1.7 Full	Snort 1.7 Custom	Snort 1.8 Full	Snort 1.8 Custom
7	Mon	Probe	Satan	Y	N	N	N
7	Mon	DoS	Syslog	N	N	N	N
7	Mon	R2L	Phf	N	N	Y	Y
7	Mon	DoS	Land	Y	N	Y	Y
7	Tues	Probe	Portsweep	N	N	Y	Y
7	Tues	DoS	Pod	Y	Y	Y	Y
7	Tues	U2R	Ffb	N	N	N	N
7	Tues	U2R	Eject	N	N	N	N
7	Wed	R2L	Phf	N	N	Y	Y
7	Thurs	U2R	Loadmodule	N	N	N	N
7	Thurs	DoS	Teardrop	Y	Y	Y	Y
7	Thurs	Probe	Ipsweep	Y	N	Y	Y
7	Thurs	Probe	Portsweep	N	N	N	N
7	Thurs	DoS	Smurf	Y	N	Y	Y
7	Thurs	Probe	Satan	Y	N	Y	Y
7	Thurs	U2R	Perlmagic	N	N	N	N
7	Thurs	Probe	Ipsweep	Y	N	Y	Y
7	Thurs	DoS	Neptune	N	N	Y	Y
7	Thurs	DoS	Smurf	N	N	N	N
7	Thurs	DoS	Neptune	N	N	Y	Y
7	Thurs	DoS	Back	N	N	Y	Y

6.2.1 Summary of Results from Test Data Set 2

Table 6.4 summarises the test results from running Snort against test data set 2.

Table 6.4: Summary of Results from Testing Snort with Test Data Set 2

		Snort 1.7 Full		Snort 1.7 Custom		Snort 1.8 Full		Snort 1.8 Custom	
Attack Cat.	No. of Attacks	No. Detected	Detection Rate	No. Detected	Detection Rate	No. Detected	Detection Rate	No. Detected	Detection Rate
DoS	9	4	44%	2	22%	7	78%	7	78%
U2R	4	0	0%	0	0%	0	0%	0	0%
R2L	2	0	0%	0	0%	2	100%	2	100%
Probe	6	4	67%	0	0%	4	67%	4	67%
Data	0	N/a*	N/a*	N/a*	N/a*	N/a*	N/a*	N/a*	N/a*

*N/a – not applicable as there were no attacks in this category

As can be seen from table 6.4, there were 9 instances of Denial of Service attacks, 4 instances of User to Root attacks, 2 instances of Remote to Local attacks, 6 instances of Probe attacks and no instances of Data attacks in test data set 2. Test data set 2 is the smallest of the four test data sets. The majority of the attacks were from the Denial of Service category.

The attack category that was easiest to detect by both the Snort 1.8 configurations was the Remote to Local category. Both the Snort 1.8 configurations recorded 100% detection rate for this type of attack. In the Probe category, Snort 1.8 Full, Snort 1.8 Custom and Snort 1.7 Full detected 67% of the attacks. All the four configurations detected at least some of the Denial of Service attack. The detection rates for Snort 1.7 Full, Snort 1.7 Custom, Snort 1.8 Full and Snort 1.8 Custom in this category (DoS) were 44%, 22%, 78% and 78% respectively. The detection rates were identical for Snort 1.8 Full and Snort 1.8 Custom in all attack categories.

6.3 Test Data Set 3 (1999 Test Data Week 1)

Table 6.5 presents the results of running test data set 3 through the four configurations of Snort.

Table 6.5: Results of Testing the Snort Configurations with Test Data Set 3

Week	Day	Attack Category	Attack Name	Snort 1.7 Full	Snort 1.7 Custom	Snort 1.8 Full	Snort 1.8 Custom
1	Mon	U2R	Ps	N	N	N	N
1	Mon	R2L	Sendmail	N	N	N	N
1	Mon	U2R	Ntfsdos	N	N	N	N
1	Mon	Probe	Portsweep	Y	N	Y	Y
1	Mon	R2L	Sshtrojan	N	N	N	N
1	Mon	Probe	Portsweep	Y	N	Y	Y
1	Mon	R2L	Xsnoop	N	N	N	Y

Week	Day	Attack Category	Attack Name	Snort 1.7 Full	Snort 1.7 Custom	Snort 1.8 Full	Snort 1.8 Custom
1	Mon	R2L	Snmpget	N	N	N	N
1	Mon	R2L	Guesstelnet	N	N	N	N
1	Mon	Probe	Portsweep	Y	N	Y	Y
1	Mon	R2L	Guessftp	N	N	Y	N
1	Mon	R2L	Ftpwrite	N	N	Y	Y
1	Mon	U2R	Yaga	N	N	Y	Y
1	Mon	DoS	Crashii	N	N	N	N
1	Mon	Probe	Portsweep	N	N	Y	N
1	Mon	Data	Secret	N	N	N	N
1	Mon	DoS	Smurf	N	N	N	N
1	Tues	R2L	Httptunnel	N	N	N	N
1	Tues	R2L	Phf	N	N	Y	Y
1	Tues	U2R	Loadmod	N	N	N	N
1	Tues	U2R	Ps	N	N	N	N
1	Tues	U2R	Ntfsdos	N	N	N	N
1	Tues	Data	Secret	N	N	N	N
1	Tues	R2L	Sqlattack	N	N	N	N
1	Tues	U2R	Sechole	N	N	N	N
1	Tues	DoS	Land	N	N	Y	Y
1	Tues	DoS	Mailbomb	N	N	N	N
1	Tues	DoS	Processtable	N	N	N	N
1	Tues	DoS	Crashii	N	N	Y	Y
1	Weds	Probe	Satan	Y	N	Y	Y
1	Weds	R2L	Netcat	N	N	Y	Y
1	Weds	R2L	Imap	N	N	Y	Y
1	Weds	R2L	Ppmacro	N	N	N	N
1	Weds	DoS	Processtable	N	N	N	N
1	Weds	U2R	Fdformat	N	N	N	N
1	Weds	R2L	Nc-breakin	N	N	Y	Y
1	Weds	DoS	Warez	N	N	N	N
1	Weds	Probe	Arppoison	N	N	N	N
1	Weds	R2L	Ncftp	N	N	Y	Y
1	Weds	Data	Secret	N	N	N	N
1	Weds	R2L	Named	N	N	N	N
1	Weds	R2L	Guessftp	N	N	Y	Y
1	Weds	DoS	Smurf	N	N	N	N
1	Weds	R2L	Guest	N	N	N	N
1	Weds	Probe	Portsweep	Y	N	N	N
1	Weds	DoS	Mailbomb	Y	N	N	N
1	Weds	R2L	Guesstelnet	Y	N	Y	Y
1	Weds	R2L	Snmpget	N	N	N	N
1	Thurs	DoS	Teardrop	Y	Y	Y	Y

Week	Day	Attack Category	Attack Name	Snort 1.7 Full	Snort 1.7 Custom	Snort 1.8 Full	Snort 1.8 Custom
1	Thurs	R2L	Netbus	N	Y	Y	N
1	Thurs	R2L	Sshtrojan	N	N	N	N
1	Thurs	DoS	Dosnuke	N	N	Y	Y
1	Thurs	R2L	Ncftp	N	N	N	N
1	Thurs	R2L	Ppmarco	N	N	N	N
1	Thurs	R2L	Guest	N	N	N	N
1	Thurs	R2L	Xlock	N	N	N	N
1	Thurs	R2L	Guesspop	N	N	N	N
1	Thurs	R2L	Phf	N	N	Y	Y
1	Thurs	DoS	Processtable	N	N	N	N
1	Thurs	DoS	Mailbomb	N	N	N	N
1	Thurs	R2L	Sqlattack	N	N	N	N
1	Fri	DoS	Smurf	N	N	N	N
1	Fri	Probe	Arppoison	N	N	N	N
1	Fri	R2L	Sshtrojan	N	N	N	N
1	Fri	Probe	Ipsweep	Y	N	Y	Y
1	Fri	R2L	Xlock	N	N	N	N
1	Fri	R2L	Named	N	N	N	N
1	Fri	Probe	Portsweep	Y	N	Y	Y
1	Fri	R2L	Ncftp	Y	N	N	N
1	Fri	R2L	Netbus	N	N	Y	N
1	Fri	DoS	Mailbomb	N	N	N	N
1	Fri	Probe	Ipsweep	Y	N	Y	Y
1	Fri	U2R	Loadmod	N	N	N	N
1	Fri	U2R	Sechole	N	N	N	N
1	Fri	Probe	Portsweep	Y	N	Y	Y
1	Fri	Probe	Ipsweep	Y	N	Y	Y
1	Fri	Data	Secret	N	N	N	N

6.3.1 Summary of Results from Test Data Set 3

Table 6.6 summarises the test results from running Snort against test data set 3.

Table 6.6: Summary of Results from Testing Snort with Test Data Set 3

		Snort 1.7 Full		Snort 1.7 Custom		Snort 1.8 Full		Snort 1.8 Custom	
Attack Cat.	No. of Attacks	No. Detected	Detection Rate	No. Detected	Detection Rate	No. Detected	Detection Rate	No. Detected	Detection Rate
DoS	16	2	13%	1	6%	4	25%	4	25%
U2R	10	0	0%	0	0	0	0%	0	0%
R2L	34	1	3%	0	0	12	35%	9	26%
Probe	13	7	54%	0	0	10	77%	9	69%
Data	4	0	0%	0	0	0	0%	0	0%

As can be seen from table 6.6, there were 16 instances of Denial of Service attacks, 10 instances of User to Root attacks, 34 instances of Remote to Local attacks, 13 instances of Probe attacks and 4 instances of Data attacks in test data set 3. The majority of the attacks were from the Remote to Local category.

The attack category that was easiest to detect was the Probe category. Although Snort 1.7 Custom did not detect any probe attacks, but the detection rate for this category was the highest. In this category, the detection rates for Snort 1.8 Full, Snort 1.8 Custom and Snort 1.7 Full were 77%, 69% and 54% respectively. In the Denial of Service category, all the four configurations detected at least some of this type of attack. The detection rates for Snort 1.7 Full, Snort 1.7 Custom, Snort 1.8 Full and Snort 1.8 Custom in this category were 13%, 6%, 25% and 25% respectively.

6.4 *Test Data Set 4 (1999 Test Data Week 2)*

Table 6.7 presents the results of running test data set 4 through the four configurations of Snort.

Table 6.7: Results of Testing the Snort Configurations with Test Data Set 4

Week	Day	Attack Category	Attack Name	Snort 1.7 Full	Snort 1.7 Custom	Snort 1.8 Full	Snort 1.8 Custom
2	Mon	DoS	Pod	Y	Y	Y	Y
2	Mon	Probe	portsweep	Y	N	Y	Y
2	Mon	DoS	Pod	Y	N	Y	Y
2	Mon	DoS	Pod	Y	N	Y	Y
2	Mon	DoS	Warezclient	N	N	N	N
2	Mon	DoS	Smurf	N	N	Y	Y
2	Mon	Probe	Portsweep	Y	N	Y	Y
2	Mon	DoS	Apache2	N	N	N	N
2	Mon	R2L	Guesstelnet	N	N	N	N
2	Mon	DoS	Dosnuke	N	N	Y	Y
2	Mon	U2R	Loadmodule	N	N	N	N
2	Mon	U2R	Ffbconfig	N	N	N	N
2	Mon	DoS	Smurf	N	N	Y	Y
2	Mon	DoS	Arppoison	N	N	N	N
2	Mon	DoS	Apache2	N	N	N	N
2	Mon	DoS	Pod	Y	N	Y	Y
2	Mon	R2L	Imap	N	N	Y	Y
2	Mon	Probe	Ipsweep	N	N	Y	Y
2	Mon	R2L	Dict	N	N	N	N
2	Mon	DoS	Syslogd	N	N	N	N
2	Mon	DoS	Neptune	N	N	Y	Y
2	Mon	DoS	Crashiis	N	N	Y	Y
2	Mon	Probe	Ls	N	N	N	N
2	Mon	Dos	Dosnuke	N	N	Y	Y
2	Mon	DoS	Udpstorm	N	N	N	N
2	Mon	DoS	Selfping	N	N	Y	Y
2	Mon	R2L	Ncftp	N	N	Y	Y
2	Tues	DoS	Tcpreset	N	N	N	N
2	Tues	DoS	Teardrop	Y	Y	Y	Y
2	Tues	U2R	Casesen	N	N	N	N
2	Tues	R2L	Xsnoop	N	N	N	N
2	Tues	DoS	Selfping	N	N	N	N
2	Tues	U2R	Xterm	N	N	N	N
2	Tues	R2L	Ftpwrite	N	N	Y	Y
2	Tues	DoS	Back	N	N	Y	Y
2	Tues	U2R	Ps	N	N	N	N
2	Tues	DoS	Neptune	N	N	Y	Y
2	Tues	R2L	Httptunnel	N	N	N	N
2	Tues	U2R	Eject	N	N	N	N
2	Tues	DoS	Pod	Y	Y	Y	Y
2	Tues	U2R	Yaga	N	N	N	N

Week	Day	Attack Category	Attack Name	Snort 1.7 Full	Snort 1.7 Custom	Snort 1.8 Full	Snort 1.8 Custom
2	Tues	DoS	Crashiis	N	N	N	N
2	Tues	R2L	Ppmacro	N	N	N	N
2	Tues	DoS	Syslog	N	N	N	N
2	Tues	U2R	Perl	N	N	N	N
2	Tues	U2R	Fdformat	N	N	N	N
2	Tues	Data	Secret	N	N	N	N
2	Tues	Probe	Queso	N	N	N	N
2	Tues	DoS	Neptune	N	N	Y	Y
2	Tues	DoS	Dosnuke	N	N	Y	Y
2	Tues	Probe	Portsweep	Y	N	Y	Y
2	Tues	R2L	Ncftp	N	N	N	N
2	Wed	DoS	Udpstorm	N	N	N	N
2	Wed	DoS	Selfping	N	N	N	N
2	Wed	R2L	Xlock	N	N	N	N
2	Wed	R2L	Phf	N	N	Y	Y
2	Wed	DoS	tcpreset	N	N	N	N
2	Wed	R2L	Netbus	N	N	N	N
2	Wed	DoS	Back	N	N	N	N
2	Wed	R2L	Netcat	N	N	N	N
2	Wed	Probe	Queso	N	N	Y	Y
2	Wed	Probe	Portsweep	Y	N	Y	Y
2	Wed	U2R	Perl	N	N	N	N
2	Wed	Probe	Queso	N	N	N	N
2	Wed	R2L	Snmpget	N	N	N	N
2	Wed	DoS	Processtable	N	N	N	N
2	Wed	DoS	Back	N	N	N	N
2	Wed	U2R	Ffbconfig	N	N	N	N
2	Wed	DoS	Apache2	N	N	N	N
2	Wed	Probe	Portsweep	Y	N	N	N
2	Thurs	U2R	Ps	N	N	N	N
2	Thurs	R2L	Phf	N	N	Y	Y
2	Thurs	U2R	Casesen	N	N	N	N
2	Thurs	U2R	Ntfsdos	N	N	N	N
2	Thurs	Probe	Portsweep	Y	N	Y	Y
2	Thurs	Probe	Ntinfoscan	N	N	N	N
2	Thurs	U2R	Yaga	N	N	N	N
2	Thurs	DoS	Crashiis	N	N	Y	Y
2	Thurs	R2L	Httptunnel	N	N	N	N
2	Thurs	U2R	Fdformat	N	N	N	N
2	Thurs	Probe	Satan	N	N	Y	Y
2	Thurs	DoS	Teardrop	Y	Y	Y	Y
2	Thurs	U2R	Sechole	N	N	N	N

Week	Day	Attack Category	Attack Name	Snort 1.7 Full	Snort 1.7 Custom	Snort 1.8 Full	Snort 1.8 Custom
2	Thurs	Probe	Resetscan	N	N	N	N
2	Thurs	Probe	Ipsweep	Y	N	Y	Y
2	Thurs	R2L	Snmpget	N	N	N	N
2	Thurs	Probe	Ntinfoscan	N	N	N	N
2	Thurs	Probe	Ls	N	N	N	N
2	Thurs	DoS	Warezclient	N	N	N	N
2	Thurs	Probe	Mscan	Y	N	Y	Y
2	Thurs	DoS	Arppoison	N	N	N	N
2	Fri	Probe	Portsweep	N	N	Y	Y
2	Fri	R2L	Xsnoop	N	N	N	N
2	Fri	DoS	Crashiis	N	N	Y	Y
2	Fri	Probe	Insidesniffer	N	N	Y	Y
2	Fri	R2L	Netcat	N	N	Y	Y
2	Fri	U2R	Xterm	N	N	N	N
2	Fri	Probe	Portsweep	Y	N	N	N
2	Fri	U2R	Anypw	N	N	N	N
2	Fri	R2L	Guest	N	N	N	N
2	Fri	DoS	Tcpreset	N	N	N	N
2	Fri	U2R	Perl	N	N	N	N
2	Fri	R2L	Framespoofer	N	N	N	N
2	Fri	Probe	Portsweep	N	N	Y	Y
2	Fri	R2L	Sqlattack	N	N	N	N
2	Fri	U2R	Yaga	N	N	N	N
2	Fri	DoS	Crashiis	N	N	Y	Y
2	Fri	R2L	Guesstelnet	N	N	N	N
2	Fri	DoS	Crashiis	N	N	Y	Y
2	Fri	DoS	Syslogd	N	N	N	N
2	Fri	U2R	Eject	N	N	N	N
2	Fri	DoS	Land	N	N	Y	Y
2	Fri	DoS	Syslogd	N	N	N	N
2	Fri	R2L	Sendmail	N	N	N	N
2	Fri	U2R	Xterm	N	N	N	N
2	Fri	DoS	Neptune	N	N	Y	Y
2	Fri	U2R	Perl	N	N	N	N
2	Fri	DoS	Warezclient	N	N	N	N
2	Fri	Probe	Queso	Y	N	N	N
2	Fri	U2R	Casesen	N	N	N	N
2	Fri	Data	Secret	N	N	N	N

6.4.1 Summary of Results from Test Data Set 4

Table 6.8 summarises the test results from running Snort against test data set 4.

Table 6.8: Summary of Results from Testing Snort with Test Data Set 4

		Snort 1.7 Full		Snort 1.7 Custom		Snort 1.8 Full		Snort 1.8 Custom	
Attack Cat.	No. of Attacks	No. Detected	Detection Rate	No. Detected	Detection Rate	No. Detected	Detection Rate	No. Detected	Detection Rate
DoS	48	7	15%	3	6%	24	50%	24	50%
U2R	25	0	0%	0	0%	2	8%	2	8%
R2L	24	1	4%	0	0%	4	17%	4	17%
Probe	24	10	42%	0	0%	20	83%	20	83%
Data	2	0	0%	0	0%	0	0%	0	0%

As can be seen from table 6.8, there were 48 instances of Denial of Service attacks, 25 instances of User to Root attacks, 24 instances of Remote to Local attacks, 24 instances of Probe attacks and 2 instances of Data attacks in test data set 4. This is comparatively the largest test data set as it has the most attack instances. The majority of the attacks were from the Denial of Service category.

The attack category that was easiest to detect was the Probe category. Although Snort 1.7 Custom did not detect any probe attacks, but the detection rate for this category was the highest. In this category, the detection rates for Snort 1.8 Full, Snort 1.8 Custom and Snort 1.7 Full were 83%, 83% and 42% respectively. In the Denial of Service category, all the four configurations detected at least some of this type of attack. The detection rates for Snort 1.7 Full, Snort 1.7 Custom, Snort 1.8 Full and Snort 1.8 Custom in this category were 15%, 6%, 50% and 50% respectively.

6.5 Overall Test Result Summary

Table 6.9 presents the overall result of the testing which was summarised from Tables 6.2, 6.4, 6.6 and 6.8:

Table 6.9: Summary of the Overall Test Results

		Snort 1.7 Full		Snort 1.7 Custom		Snort 1.8 Full		Snort 1.8 Custom	
ack .	Total No. of Attacks	Total No. Detected	Overall Detection Rate	Total No. Detected	Overall Detection Rate	Total No. Detected	Overall Detection Rate	Total No. Detected	Overall Detection Rate
S	94	24	26%	16	17%	49	52%	49	52%
R	55	0	0%	0	0%	2	5%	2	5%
L	63	2	3%	0	0%	20	32%	17	27%
be	56	31	55%	0	0%	46	82%	45	80%
ta	6	0	0%	0	0%	0	0%	0	0%
erall	274	57	21%	16	6%	117	43%	113	41%

As can be seen from table 6.9, there were 94 instances of Denial of Service attacks, 55 instances of User to Root attacks, 63 instances of Remote to Local attacks, 56 instances of Probe attacks and 6 instances of Data attacks in total. The majority of the attacks were from the Denial of Service category.

The attack category that had the highest detection rate was the Probe category. Snort 1.8 Full and Snort 1.8 Custom detected at least 80% of the total Probe attacks. All configurations detected some Denial of Service attacks. The detection rates for Snort 1.7 Full, Snort 1.7 Custom, Snort 1.8 Full and Snort 1.8 Custom in the Denial of Service category were 26%, 17%, 52% and 52% respectively. The Data attack was the hardest to detect as none of the four configurations detected it.

The Snort configurations that performed best in all categories were Snort 1.8 Full and Snort 1.8 Custom with the former performing slightly better than the latter in the Probe and Remote to Local categories. The weakest Snort configuration was Snort 1.7

Custom which only detected Denial of Service attacks. The performance of each Snort onfiguration is explained in more detail in chapter 7.

6.6 Summary

This chapter presented the test results from all sixteen test runs. The test results were recorded according to the Result Forms from Appendices F, G, H and I. Results from test data sets 1,2,3 and 4 were presented in Tables 6.1, 6.3, 6.5 and 6.7 respectively. Each of these results tables was followed by a table that summarised their test results. In hese summarised tables (Tables 6.2, 6.4, 6.6 and 6.8), the detection rates for the four configurations of Snort for each attack category were presented. Finally, a table that summarised the overall test result is presented and its contents discussed.