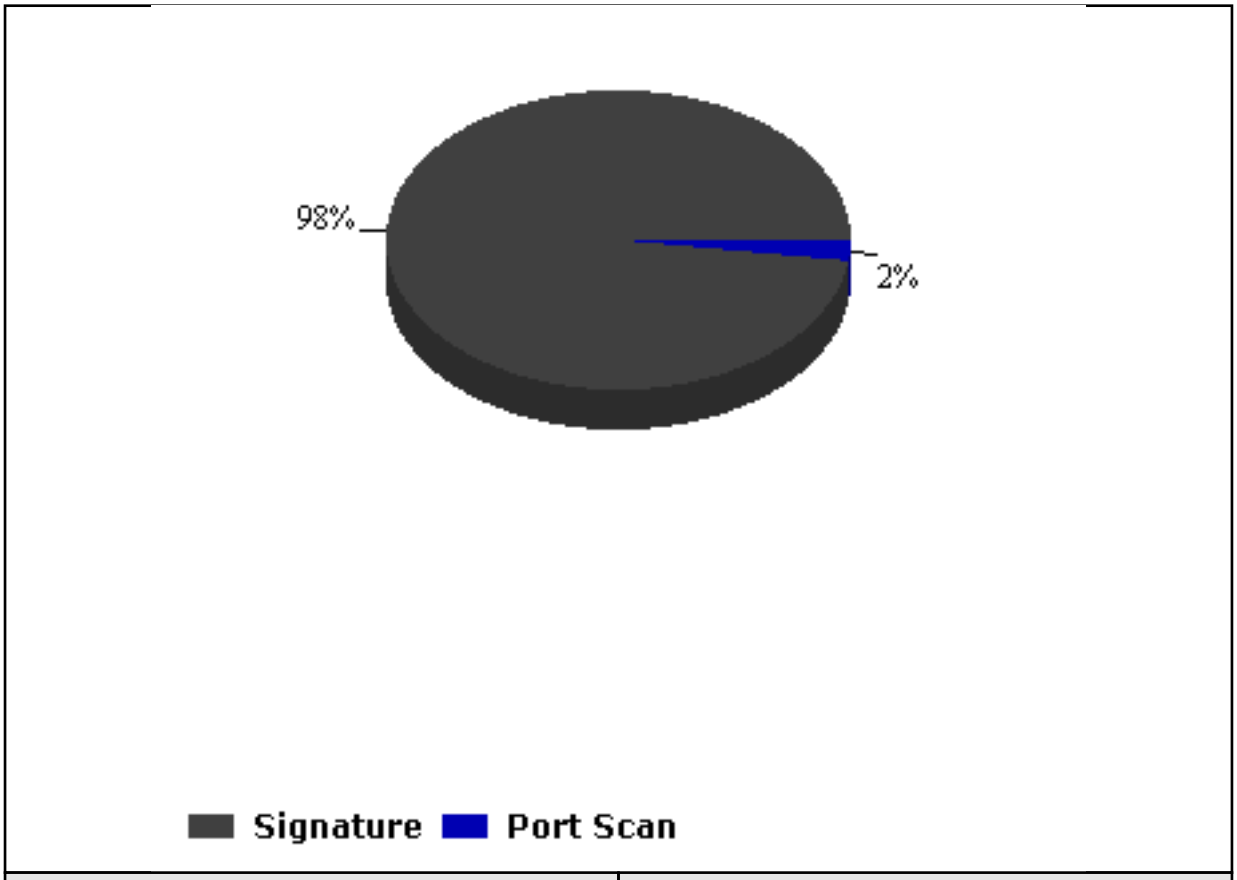
IntruShield™ IDS Report

EXECUTIVE SUMMARY REPORT

Admin Domain:	/eWEEK OpenHack 4 all
Sensor:	I2600
Alert Severity:	Low, Medium, High
Alert State:	All Alerts
Start Date:	Tue Nov 05 00:00:00 PST 2002
End Date:	Tue Nov 05 23:59:59 PST 2002

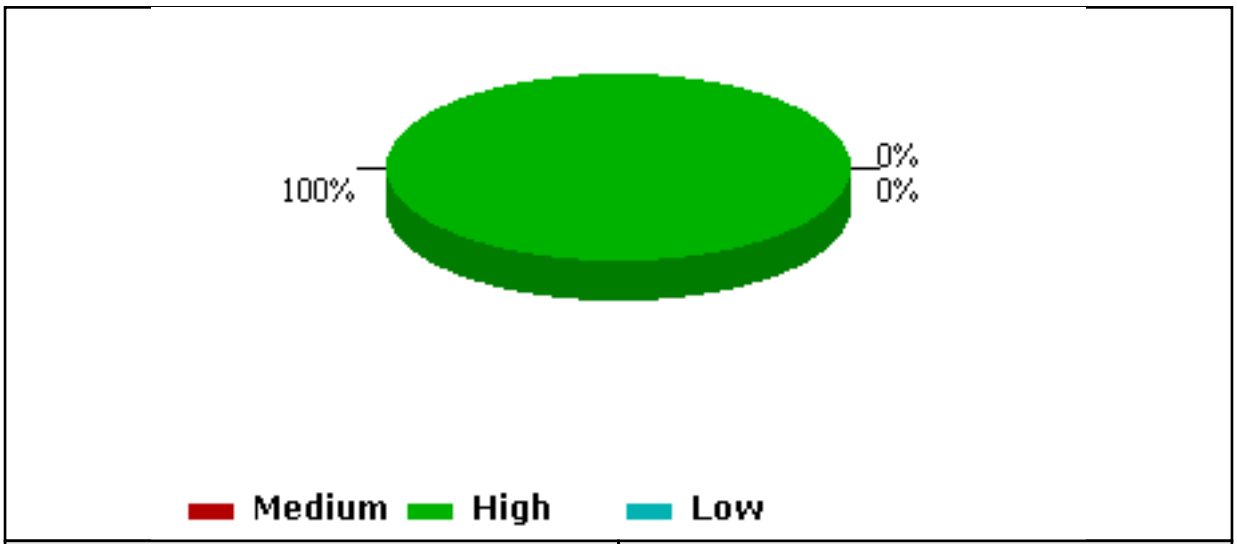
Total alerts detected by the sensor: 1264

Total Alerts Per Alert Type



Alert Type	Alerts Detected
Signature	1236
Port Scan	28

Total Alerts Per Severity



Attack Severity	Alerts Detected
Medium	0
High	1264
Low	0

Top '20' Alert Details

Alert Name	Alert Type	Severity	Count	Last Detected
HTTP: IIS CMD.EXE Execution	Signature	High	197	11-6-2002 20:13:16
HTTP: IIS Command Execution	Signature	High	166	11-6-2002 19:22:44
HTTP: CGI EscapeCharacter DirectoryTraversal	Signature	High	165	11-6-2002 20:14:31
HTTP: Nimda Worm - IIS Extended Unicode Directory Travesal Attack	Signature	High	86	11-6-2002 19:22:35
unicode-utf8-too-long-encoding	Signature	High	80	11-6-2002 19:22:35
HTTP: IIS 4.0 idc path disclosure	Signature	Low	61	11-6-2002 20:14:52
SNMP: Read Public Community String	Signature		40	11-6-2002 11:39:27
ICMP: Netmask Request	Signature	Low	30	11-5-2002 19:44:42
ICMP: Timestamp Probe	Signature	Low	30	11-5-2002 19:44:42
HTTP: Phf Execute Arbitary Command	Signature	High	28	11-6-2002 20:12:53
HTTP: Abnomal %00 in Parameter	Signature	Low	27	11-5-2002 21:18:12
TCP SYN port scan	Port Scan	Medium	27	11-6-2002 21:13:20
HTTP: Test Cgi DirectoryListing	Signature	Medium	23	11-6-2002 20:14:33
HTTP: Read Password File Attempt	Signature	Medium	16	11-5-2002 21:19:39
HTTP: Cobalt Raq Apache .htaccess Disclosure	Signature	Medium	16	11-6-2002 20:14:11
HTTP: Wwwboard.pl File Access	Signature	Medium	16	11-6-2002 20:12:58
HTTP: nph-test-cgi Browse Filesystem	Signature	Medium	15	11-6-2002 20:12:54
HTTP: Interpreter AccessAttempt	Signature	Medium	14	11-5-2002 21:20:32
HTTP: Finger Leak User Info	Signature	Medium	14	11-6-2002 20:13:2
HTTP: Faxsurvey Execute Command	Signature	High	14	11-6-2002 20:12:57

Top '20' Source IP Details

Source IP	Count
68.46.68.173	1048
65.42.94.255	89
216.226.62.148	64
207.76.125.152	14
207.43.157.129	9
220.74.15.247	7
80.142.179.235	6
12.4.81.145	5
220.82.58.132	5
207.46.225.252	4
213.156.50.136	2
131.107.3.85	2
66.178.157.237	2
24.169.93.17	2
64.168.223.194	2
216.191.171.2	2
4.47.163.97	1

Top '20' Destination IP Details

Destination IP	Count
209.20.153.101	1181
209.20.153.105	23
209.20.153.100	14
209.20.153.102	8
209.20.153.104	8
209.20.153.110	6
209.20.153.106	5
209.20.153.107	5
209.20.153.108	5
209.20.153.99	5
209.20.153.98	4

Top '20' Source/Destination IP Pair Details

Source IP	Destination IP	Count
68.46.68.173	209.20.153.101	1048
216.226.62.148	209.20.153.101	64
65.42.94.255	209.20.153.101	37
65.42.94.255	209.20.153.105	13
65.42.94.255	209.20.153.104	7
220.74.15.247	209.20.153.101	7
80.142.179.235	209.20.153.101	6
207.43.157.129	209.20.153.101	6
207.76.125.152	209.20.153.100	6
220.82.58.132	209.20.153.101	5
65.42.94.255	209.20.153.102	4
207.46.225.252	209.20.153.105	4
65.42.94.255	209.20.153.106	4
65.42.94.255	209.20.153.107	4
65.42.94.255	209.20.153.108	4
65.42.94.255	209.20.153.110	4
65.42.94.255	209.20.153.98	4
65.42.94.255	209.20.153.99	4
65.42.94.255	209.20.153.100	4
207.43.157.129	209.20.153.102	3