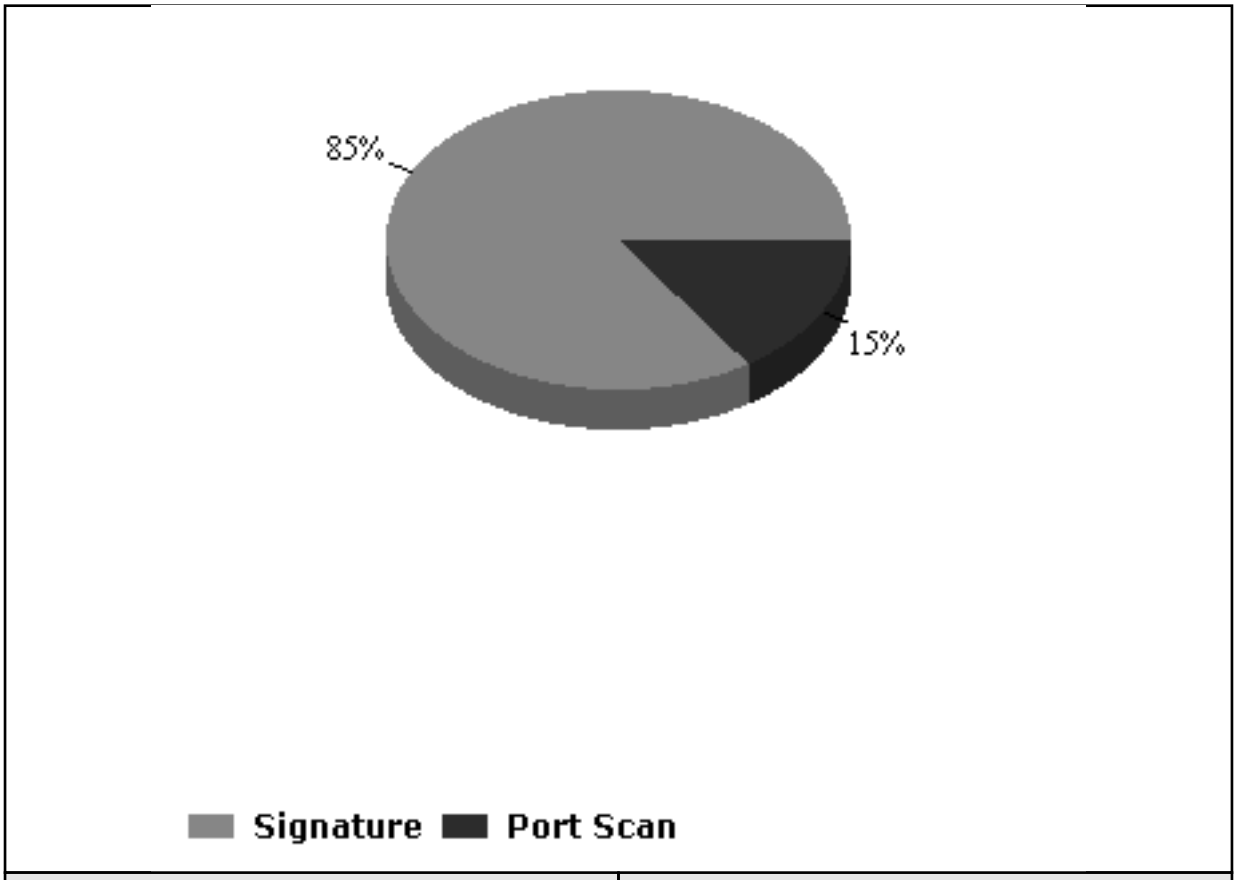
IntruShield™ IDS Report

EXECUTIVE SUMMARY REPORT

Admin Domain:	/eWEEK OpenHack 4 all
Sensor:	I2600
Alert Severity:	Low, Medium, High
Alert State:	All Alerts
Start Date:	Mon Nov 04 00:00:00 PST 2002
End Date:	Mon Nov 04 23:59:59 PST 2002

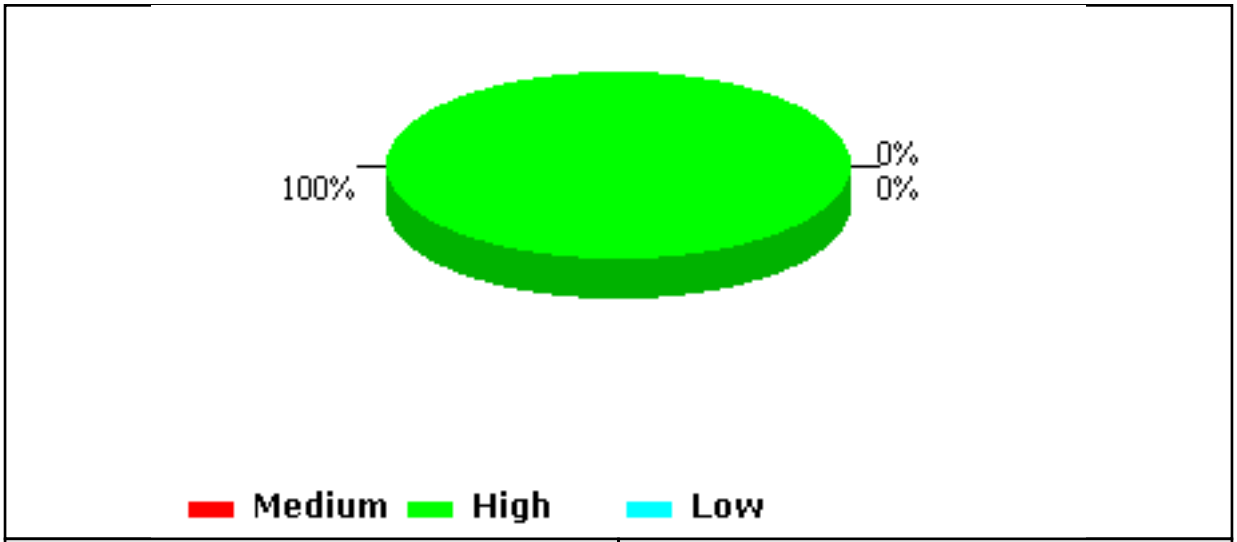
Total alerts detected by the sensor: 317

Total Alerts Per Alert Type



Alert Type	Alerts Detected
Signature	268
Port Scan	49

Total Alerts Per Severity



Attack Severity	Alerts Detected
Medium	0
High	317
Low	0

Top '20' Alert Details

Alert Name	Alert Type	Severity	Count	Last Detected
ip-too-many-small-fragments	Signature	High	72	11-4-2002 21:44:30
TCP SYN port scan	Port Scan	Medium	40	11-6-2002 21:13:20
HTTP: IIS Command Execution	Signature	High	26	11-6-2002 19:22:44
HTTP: IIS CMD.EXE Execution	Signature	High	24	11-6-2002 20:13:16
HTTP: IIS iisadmpwd Proxied Password Attack Attempt	Signature	Medium	13	11-6-2002 20:14:4
HTTP: IIS 4.0 idc path disclosure	Signature	Low	13	11-6-2002 20:14:52
SNMP: Read Other Default Community String	Signature	Low	11	11-4-2002 11:36:7
TCP ACK port scan	Port Scan	Medium	9	11-4-2002 15:26:32
HTTP: CGI EscapeCharacter DirectoryTraversal	Signature	High	8	11-6-2002 20:14:31
HTTP: IIS JET VBA Run Command Attempt	Signature	High	7	11-6-2002 20:14:15
IPHdr-SrcDstInvalidAddress	Signature	Low	7	11-7-2002 3:16:36
HTTP: Phf Execute Arbitary Command	Signature	High	6	11-6-2002 20:12:53
HTTP: Nimda Worm - IIS Extended Unicode Directory Travesal Attack	Signature	High	5	11-6-2002 19:22:35
HTTP: IIS multiple sample ASP script View File Attempt	Signature	Medium	4	11-6-2002 20:13:21
HTTP: Uploader.exe Execute Program	Signature	Medium	3	11-6-2002 20:13:10
HTTP: Faxsurvey Execute Command	Signature	High	3	11-6-2002 20:12:57
HTTP: Cobalt Raq Apache .htaccess Disclosure	Signature	Medium	3	11-6-2002 20:14:11
HTTP: PageService Directory Disclosure	Signature	Medium	3	11-6-2002 20:13:33
HTTP: Siteserver site.csc File Read	Signature	Medium	3	11-6-2002 20:14:12
HTTP: Test Cgi DirectoryListing	Signature	Medium	3	11-6-2002 20:14:33

Top '20' Source IP Details

Source IP	Count
38.168.118.3	120
0.0.0.0	76
209.11.163.69	42
166.127.243.181	17
206.20.97.134	15
216.34.199.30	12
66.122.63.68	9
66.67.34.170	5
220.82.1.136	3
148.100.222.235	3
63.162.160.98	3
216.63.39.245	2
217.225.208.200	2
63.202.95.110	2
209.244.107.146	2
195.68.124.50	2
213.1.191.181	1
80.35.108.44	1

Top '20' Destination IP Details

Destination IP	Count
209.20.153.101	217
0.0.0.0	72
209.20.153.105	16
209.20.153.110	4
209.20.153.107	2
209.20.153.106	2
209.20.153.108	2
209.20.153.102	1
209.20.153.104	1

Top '20' Source/Destination IP Pair Details

Source IP	Destination IP	Count
38.168.118.3	209.20.153.101	103
0.0.0.0	0.0.0.0	72
209.11.163.69	209.20.153.101	42
166.127.243.181	209.20.153.101	17
206.20.97.134	209.20.153.101	15
216.34.199.30	209.20.153.101	12
66.122.63.68	209.20.153.101	9
38.168.118.3	209.20.153.105	9
66.67.34.170	209.20.153.101	5
63.162.160.98	209.20.153.105	3
220.82.1.136	209.20.153.101	3
148.100.222.235	209.20.153.101	3
0.0.0.0	209.20.153.110	2
38.168.118.3	209.20.153.107	2
38.168.118.3	209.20.153.106	2
38.168.118.3	209.20.153.108	2
38.168.118.3	209.20.153.110	2
63.202.95.110	209.20.153.101	2
216.63.39.245	209.20.153.101	2
209.244.107.146	209.20.153.101	2