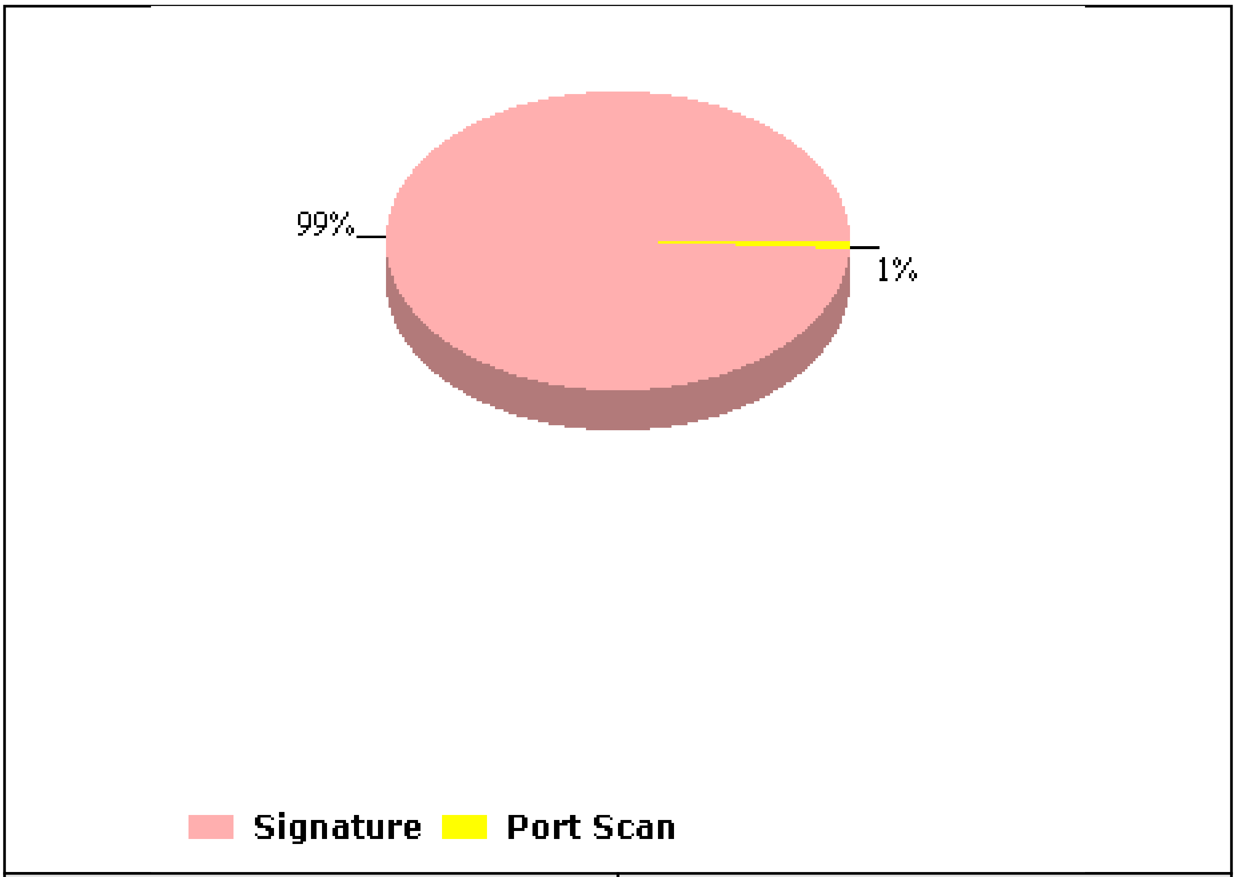
IntruShield™ IDS Report

EXECUTIVE SUMMARY REPORT

Admin Domain:	/eWEEK OpenHack 4 all
Sensor:	I2600
Alert Severity:	Low, Medium, High
Alert State:	All Alerts
Start Date:	Wed Oct 30 00:00:00 PST 2002
End Date:	Wed Oct 30 23:59:59 PST 2002

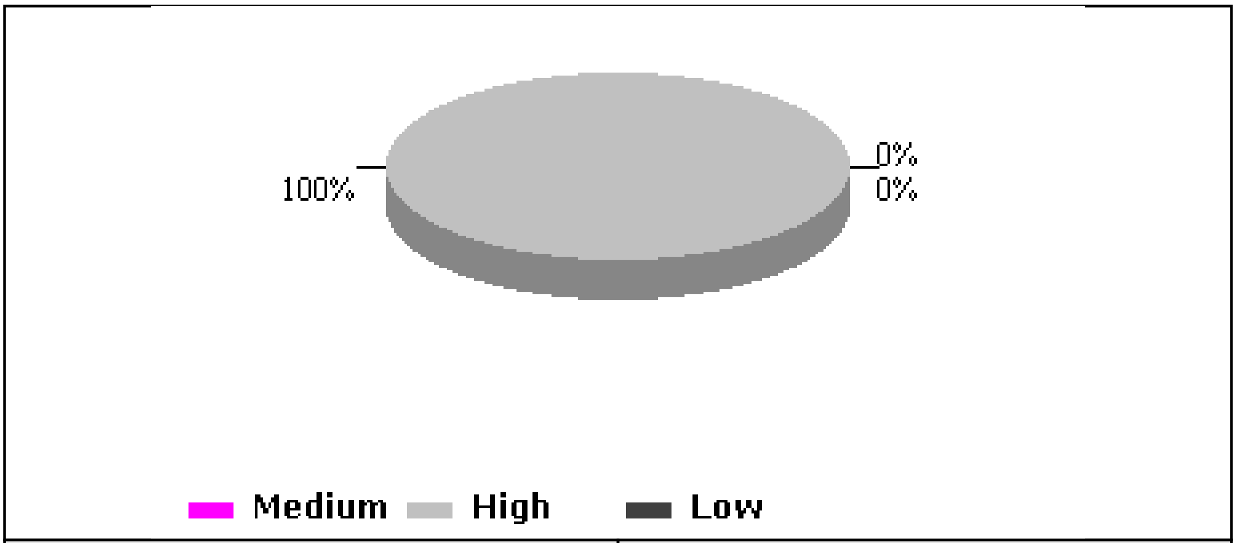
Total alerts detected by the sensor: 6252

Total Alerts Per Alert Type



Alert Type	Alerts Detected
Signature	6198
Port Scan	54

Total Alerts Per Severity



Attack Severity	Alerts Detected
Medium	0
High	6252
Low	0

Top '20' Alert Details

Alert Name	Alert Type	Severity	Count	Last Detected
HTTP: IIS Command Execution	Signature	High	1280	10-31-2002 8:16:6
HTTP: CGI EscapeCharacter DirectoryTraversal	Signature	High	1178	10-31-2002 14:23:42
HTTP: IIS CMD.EXE Execution	Signature	High	1095	10-31-2002 8:16:6
unicode-utf8-too-long-encoding	Signature	High	583	10-31-2002 8:16:6
HTTP: Nimda Worm - IIS Extended Unicode Directory Travesal Attack	Signature	High	486	10-31-2002 8:16:6
SNMP: Read Other Default Community String	Signature	Low	190	10-30-2002 22:9:47
HTTP: IIS 4.0 idc path disclosure	Signature	Low	148	10-31-2002 7:55:59
HTTP: Abnomal %00 in Parameter	Signature	Low	129	10-31-2002 3:18:56
HTTP: ExpressionCalculator InputValidation	Signature	Medium	65	10-31-2002 3:9:1
HTTP: Interpreter AccessAttempt	Signature	Medium	55	10-31-2002 7:56:9
TCP SYN port scan	Port Scan	Medium	52	10-31-2002 14:24:24
HTTP: Cross Site Script Attack	Signature	High	40	10-31-2002 3:17:17
HTTP: Phf Execute Arbitary Command	Signature	High	37	10-31-2002 7:56:3
HTTP: IIS iisadmpwd Proxied Password Attack Attempt	Signature	Medium	37	10-31-2002 3:7:50
HTTP: IIS multiple sample ASP script View File Attempt	Signature	Medium	34	10-31-2002 3:17:48
HTTP: IIS JET VBA Run Command Attempt	Signature	High	34	10-31-2002 3:12:21
HTTP: Cobalt Raq Apache .htaccess Disclosure	Signature	Medium	32	10-31-2002 7:56:11
HTTP: Faxsurvey Execute Command	Signature	High	27	10-31-2002 12:36:1
HTTP: Netscape Directory Indexing Browse Directory	Signature	Medium	25	10-30-2002 11:39:1
IPHdr-SrcDstInvalidAddress	Signature	Low	24	10-31-2002 7:11:12

Top '20' Source IP Details

Source IP	Count
161.109.100.250	4533
218.8.83.130	1160
161.109.100.20	229
149.168.193.43	213
198.151.130.145	36
209.145.216.240	22
62.32.50.186	12
220.82.1.136	11
220.79.6.138	7
62.211.187.250	4
65.58.136.26	3
62.151.47.70	3
220.77.161.159	3
220.75.249.42	3
67.233.134.198	2
209.113.228.27	2
61.174.157.6	2
198.108.1.42	1
204.39.208.194	1
65.66.71.38	1

Top '20' Destination IP Details

Destination IP	Count
209.20.153.101	5993
209.20.153.110	224
209.20.153.105	13
209.20.153.99	7
209.20.153.100	6
209.20.153.104	3
209.20.153.102	2
209.20.153.107	2
209.20.153.108	1
209.20.153.106	1

Top '20' Source/Destination IP Pair Details

Source IP	Destination IP	Count
161.109.100.250	209.20.153.101	4532
218.8.83.130	209.20.153.101	1160
161.109.100.20	209.20.153.101	227
149.168.193.43	209.20.153.110	213
198.151.130.145	209.20.153.101	22
62.32.50.186	209.20.153.101	12
220.82.1.136	209.20.153.101	11
209.145.216.240	209.20.153.105	8
220.79.6.138	209.20.153.101	7
198.151.130.145	209.20.153.99	7
198.151.130.145	209.20.153.110	6
62.211.187.250	209.20.153.105	3
62.151.47.70	209.20.153.101	3
220.75.249.42	209.20.153.101	3
209.145.216.240	209.20.153.101	3
65.58.136.26	209.20.153.110	3
220.77.161.159	209.20.153.101	3
209.145.216.240	209.20.153.104	2
209.113.228.27	209.20.153.101	2
209.145.216.240	209.20.153.102	2