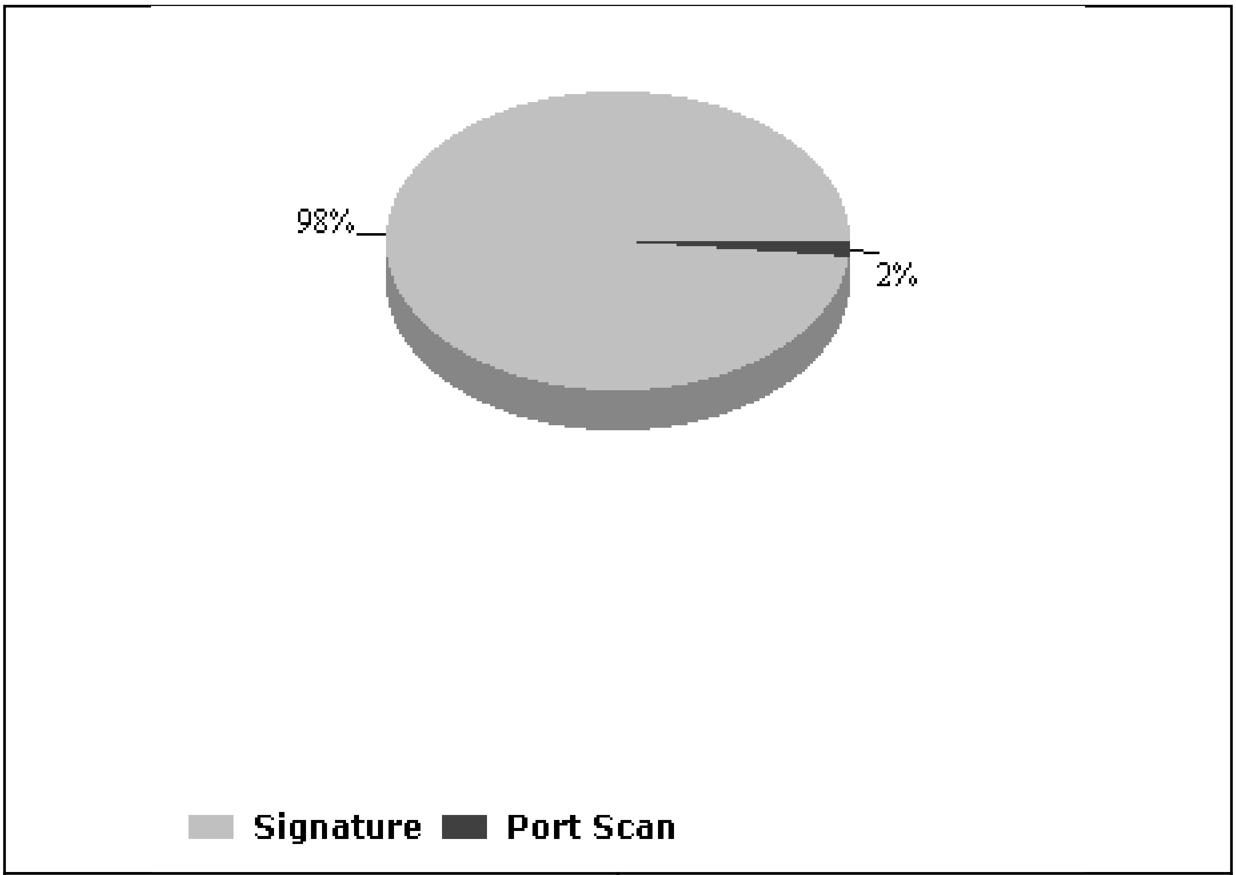
IntruShield™ IDS Report

EXECUTIVE SUMMARY REPORT

Admin Domain:	/eWEEK OpenHack 4 all
Sensor:	I2600
Alert Severity:	Low, Medium, High
Alert State:	All Alerts
Start Date:	Sun Nov 03 00:00:00 PST 2002
End Date:	Sun Nov 03 23:59:59 PST 2002

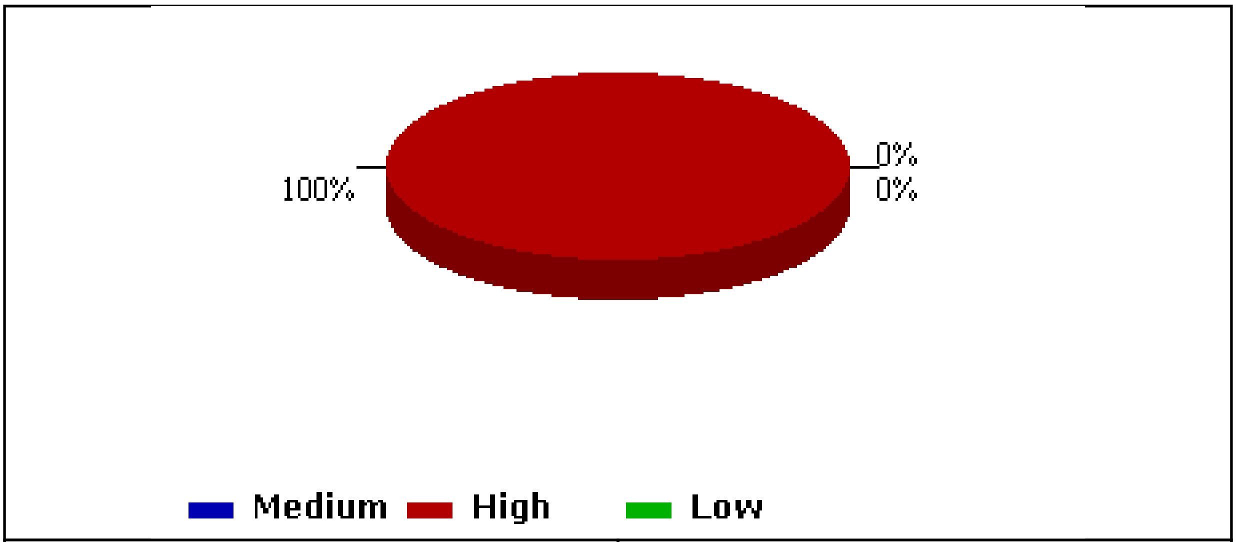
Total alerts detected by the sensor: 572

Total Alerts Per Alert Type



Alert Type	Alerts Detected
Signature	563
Port Scan	9

Total Alerts Per Severity



Attack Severity	Alerts Detected
Medium	0
High	572
Low	0

Top '20' Alert Details

Alert Name	Alert Type	Severity	Count	Last Detected
HTTP: CGI EscapeCharacter DirectoryTraversal	Signature	High	94	11-6-2002 20:14:31
HTTP: IIS Command Execution	Signature	High	66	11-6-2002 19:22:44
HTTP: Nimda Worm - IIS Extended Unicode Directory Travesal Attack	Signature	High	35	11-6-2002 19:22:35
unicode-utf8-too-long-encoding	Signature	High	30	11-6-2002 19:22:35
HTTP: Abnomal %00 in Parameter	Signature	Low	29	11-5-2002 21:18:12
HTTP: IIS CMD.EXE Execution	Signature	High	21	11-6-2002 20:13:16
HTTP: IIS iisadmpwd Proxied Password Attack Attempt	Signature	Medium	17	11-6-2002 20:14:4
HTTP: IIS 4.0 idc path disclosure	Signature	Low	17	11-6-2002 20:14:52
HTTP: Phf Execute Arbitary Command	Signature	High	16	11-6-2002 20:12:53
IPHdr-SrcDstInvalidAddress	Signature	Low	15	11-7-2002 3:16:36
HTTP: ExpressionCalculator InputValidation	Signature	Medium	14	11-6-2002 20:13:27
HTTP: IIS multiple sample ASP script View File Attempt	Signature	Medium	13	11-6-2002 20:13:21
HTTP: Cobalt Raq Apache .htaccess Disclosure	Signature	Medium	11	11-6-2002 20:14:11
TCP SYN port scan	Port Scan	Medium	9	11-6-2002 21:13:20
HTTP: IIS JET VBA Run Command Attempt	Signature	High	8	11-6-2002 20:14:15
HTTP: Read Password File Attempt	Signature	Medium	7	11-5-2002 21:19:39
DNS: HINFO Query	Signature	Medium	7	11-6-2002 13:49:38
HTTP: Finger Leak User Info	Signature	Medium	6	11-6-2002 20:13:2
HTTP: nph-test-cgi Browse Filesystem	Signature	Medium	6	11-6-2002 20:12:54
HTTP: IIS3 ASP Dot Bug	Signature	Medium	6	11-6-2002 20:14:31

Top '20' Source IP Details

Source IP	Count
63.206.195.138	344
195.174.56.103	188
206.13.29.42	5
67.8.104.6	5
66.75.145.149	4
220.76.134.172	4
220.77.140.35	4
220.82.1.136	3
220.78.130.214	3
64.109.57.34	2
140.118.122.143	2
65.191.143.93	2
192.117.238.185	2
206.13.29.43	1
0.0.0.0	1
68.98.160.96	1
64.29.214.250	1

Top '20' Destination IP Details

Destination IP	Count
209.20.153.101	559
209.20.153.100	7
209.20.153.110	6

Top '20' Source/Destination IP Pair Details

Source IP	Destination IP	Count
63.206.195.138	209.20.153.101	344
195.174.56.103	209.20.153.101	188
206.13.29.42	209.20.153.100	5
67.8.104.6	209.20.153.110	5
66.75.145.149	209.20.153.101	4
220.76.134.172	209.20.153.101	4
220.77.140.35	209.20.153.101	4
220.82.1.136	209.20.153.101	3
220.78.130.214	209.20.153.101	3
65.191.143.93	209.20.153.101	2
192.117.238.185	209.20.153.101	2
64.109.57.34	209.20.153.101	2
140.118.122.143	209.20.153.101	2
64.29.214.250	209.20.153.100	1
206.13.29.43	209.20.153.100	1
68.98.160.96	209.20.153.101	1
0.0.0.0	209.20.153.110	1