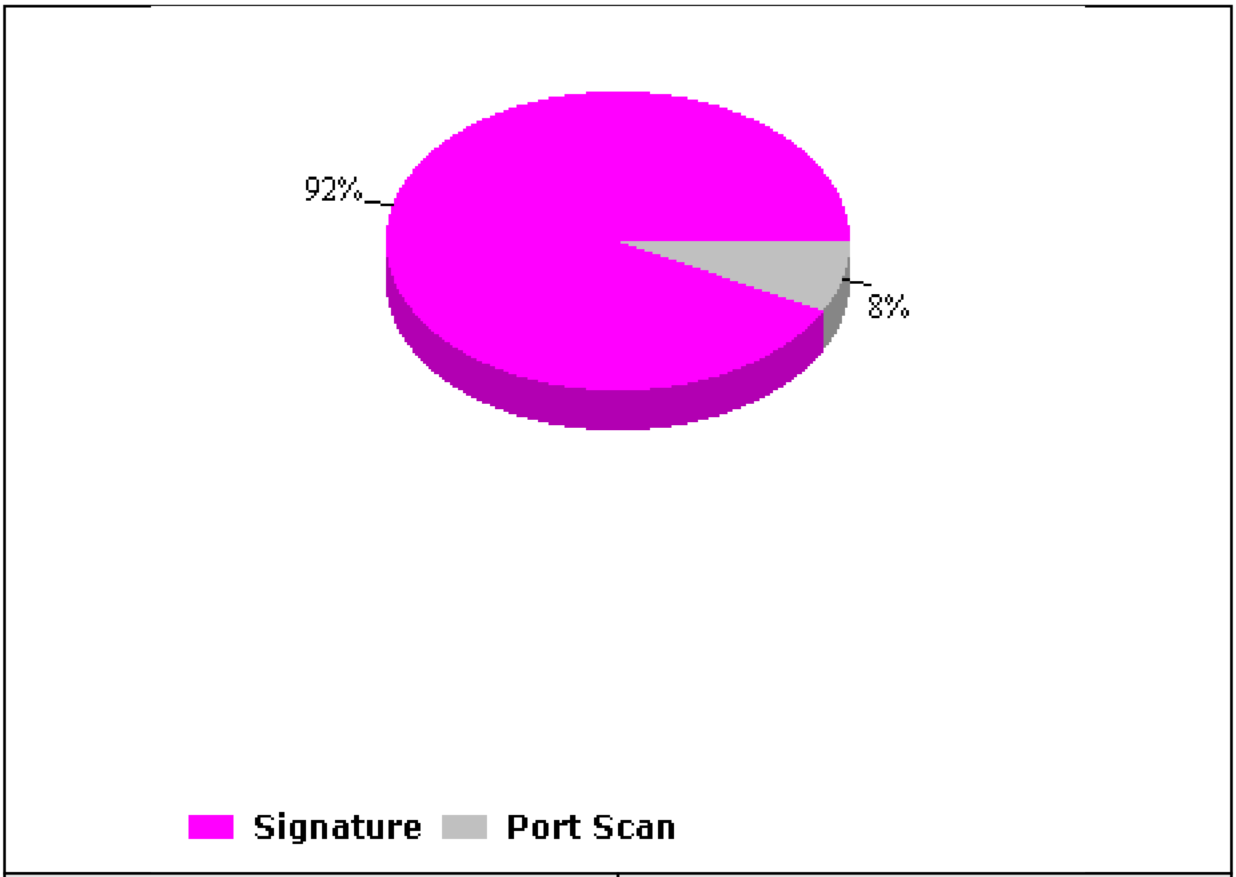
IntruShield™ IDS Report

EXECUTIVE SUMMARY REPORT

Admin Domain:	/eWEEK OpenHack 4 all
Sensor:	I2600
Alert Severity:	Low, Medium, High
Alert State:	All Alerts
Start Date:	Fri Nov 01 00:00:00 PST 2002
End Date:	Fri Nov 01 23:59:59 PST 2002

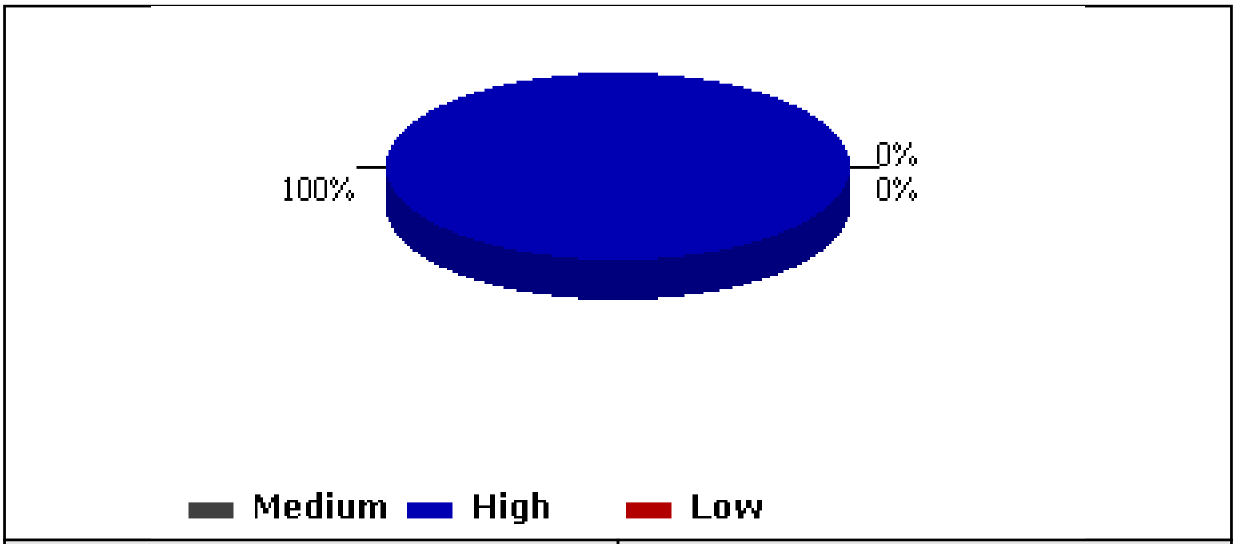
Total alerts detected by the sensor: 484

Total Alerts Per Alert Type



Alert Type	Alerts Detected
Signature	447
Port Scan	37

Total Alerts Per Severity



Attack Severity	Alerts Detected
Medium	0
High	484
Low	0

Top '20' Alert Details

Alert Name	Alert Type	Severity	Count	Last Detected
HTTP: IIS Command Execution	Signature	High	91	11-6-2002 19:22:44
HTTP: IIS CMD.EXE Execution	Signature	High	83	11-6-2002 20:13:16
TCP SYN port scan	Port Scan	Medium	37	11-6-2002 21:13:20
HTTP: CGI EscapeCharacter DirectoryTraversal	Signature	High	33	11-6-2002 20:14:31
HTTP: Nimda Worm - IIS Extended Unicode Directory Travesal Attack	Signature	High	32	11-6-2002 19:22:35
SNMP: Read Public Community String	Signature	&nbsp;	31	11-6-2002 11:39:27
ICMP: Netmask Request	Signature	Low	28	11-5-2002 19:44:42
ICMP: Timestamp Probe	Signature	Low	28	11-5-2002 19:44:42
unicode-utf8-too-long-encoding	Signature	High	27	11-6-2002 19:22:35
HTTP: IIS multiple sample ASP script View File Attempt	Signature	Medium	8	11-6-2002 20:13:21
HTTP: IIS Root.exe Execute Command	Signature	High	8	11-6-2002 19:22:12
HTTP: IIS 4.0 idc path disclosure	Signature	Low	8	11-6-2002 20:14:52
IPHdr-SrcDstInvalidAddress	Signature	Low	6	11-7-2002 3:16:36
HTTP: IIS iisadmpwd Proxied Password Attack Attempt	Signature	Medium	5	11-6-2002 20:14:4
HTTP: ExpressionCalculator InputValidation	Signature	Medium	4	11-6-2002 20:13:27
HTTP: CodeRed Worm	Signature	High	4	11-1-2002 14:40:32
HTTP: Possible Authentication Buffer Overflow	Signature	High	4	11-1-2002 14:40:33
HTTP: IIS htr Obtain Code	Signature	Medium	3	11-5-2002 21:16:14
HTTP: Abnomal %00 in Parameter	Signature	Low	3	11-5-2002 21:18:12
HTTP: IIS Dvwssri View File	Signature	Medium	3	11-6-2002 20:14:38

Top '20' Source IP Details

Source IP	Count
200.151.199.239	297
195.146.51.101	69
209.170.112.107	42
65.31.90.117	21
168.226.122.34	13
209.45.44.133	10
220.82.1.136	6
151.24.139.210	5
67.8.104.6	5
80.116.112.73	4
80.35.108.44	2
193.201.200.130	2
206.46.23.164	2
66.56.210.174	2
206.37.248.254	1
62.36.143.9	1
62.37.145.136	1
64.246.16.46	1

Top '20' Destination IP Details

Destination IP	Count
209.20.153.101	374
209.20.153.105	39
209.20.153.110	14
209.20.153.100	12
209.20.153.98	9
209.20.153.99	9
209.20.153.102	9
209.20.153.104	9
209.20.153.107	3
209.20.153.108	3
209.20.153.106	3

Top '20' Source/Destination IP Pair Details

Source IP	Destination IP	Count
200.151.199.239	209.20.153.101	297
209.170.112.107	209.20.153.101	42
65.31.90.117	209.20.153.105	21
209.45.44.133	209.20.153.101	10
195.146.51.101	209.20.153.102	9
195.146.51.101	209.20.153.104	9
195.146.51.101	209.20.153.105	9
195.146.51.101	209.20.153.100	9
195.146.51.101	209.20.153.101	9
220.82.1.136	209.20.153.101	6
195.146.51.101	209.20.153.99	6
195.146.51.101	209.20.153.98	6
151.24.139.210	209.20.153.105	5
67.8.104.6	209.20.153.110	5
80.116.112.73	209.20.153.110	4
168.226.122.34	209.20.153.101	4
168.226.122.34	209.20.153.98	3
168.226.122.34	209.20.153.99	3
168.226.122.34	209.20.153.100	3
195.146.51.101	209.20.153.106	3