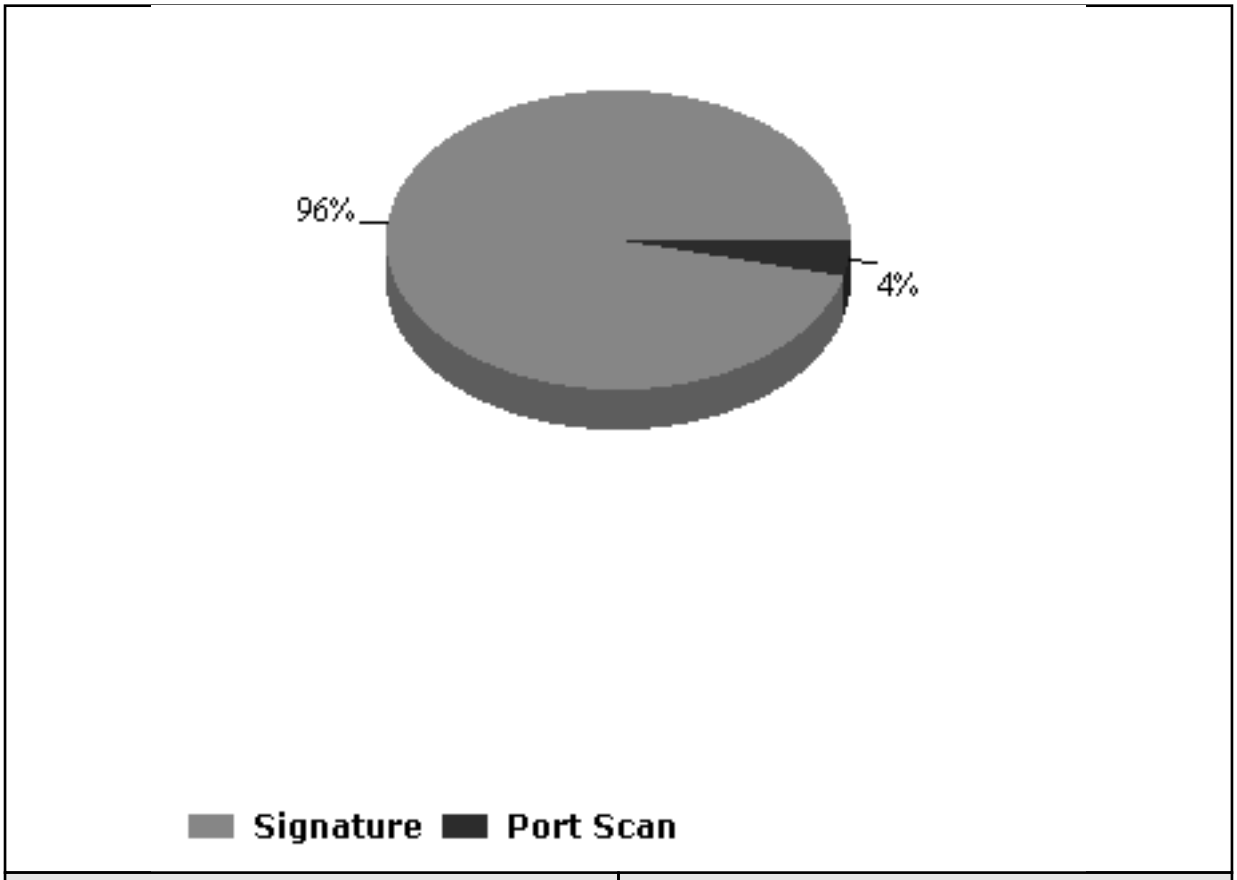
IntruShield™ IDS Report

EXECUTIVE SUMMARY REPORT

Admin Domain:	/eWEEK OpenHack 4 all
Sensor:	I2600
Alert Severity:	Low, Medium, High
Alert State:	All Alerts
Start Date:	Fri Nov 08 00:00:00 PST 2002
End Date:	Fri Nov 08 23:59:59 PST 2002

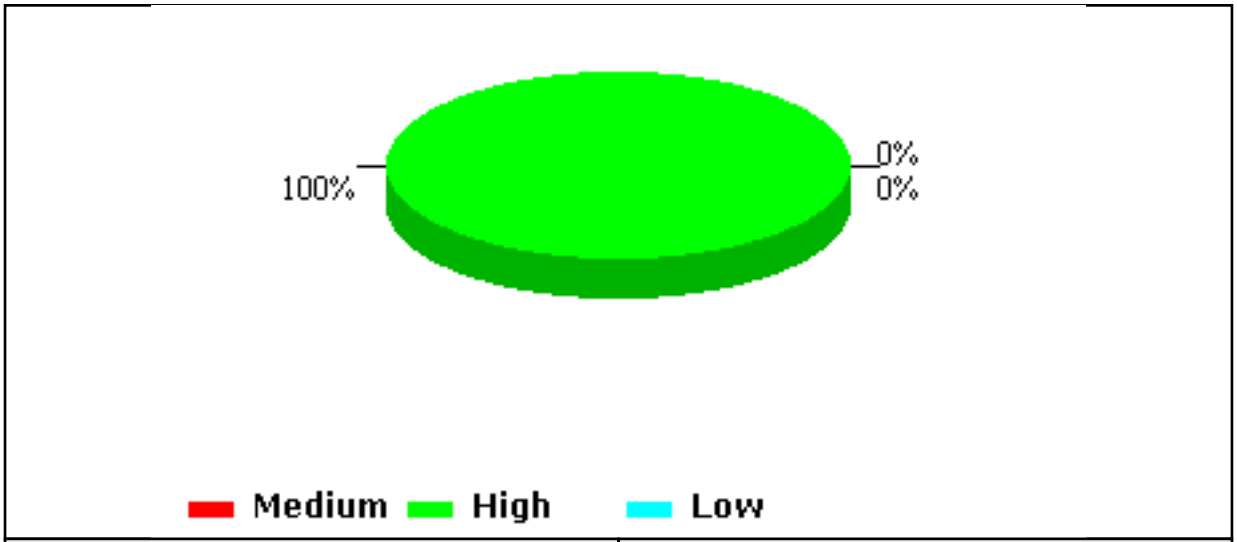
Total alerts detected by the sensor: 749

Total Alerts Per Alert Type



Alert Type	Alerts Detected
Signature	719
Port Scan	30

Total Alerts Per Severity



Attack Severity	Alerts Detected
Medium	0
High	749
Low	0

Top '20' Alert Details

Alert Name	Alert Type	Severity	Count	Last Detected
SNMP: Read Other Default Community String	Signature	Low	540	11-8-2002 8:23:3
SNMP: Cisco IOS Undocumented Community String	Signature	Medium	60	11-8-2002 8:17:41
SNMP: Read Public Community String	Signature		38	11-8-2002 23:38:4
RPC: Portmap Dump Request	Signature	Medium	30	11-8-2002 8:13:42
TCP SYN port scan	Port Scan	Medium	29	11-9-2002 0:2:47
IPHdr-SrcDstInvalidAddress	Signature	Low	11	11-8-2002 11:47:54
DNS: Invalid Field Value	Signature	Low	10	11-8-2002 8:14:2
ICMP: Netmask Request	Signature	Low	7	11-8-2002 23:38:11
ICMP: Timestamp Probe	Signature	Low	7	11-8-2002 23:38:11
HTTP: IIS CMD.EXE Execution	Signature	High	6	11-8-2002 14:43:14
HTTP: IIS Command Execution	Signature	High	6	11-8-2002 14:43:14
HTTP: Read Password File Attempt	Signature	Medium	1	11-8-2002 18:40:33
HTTP: IIS 4.0 idc path disclosure	Signature	Low	1	11-8-2002 19:19:14
HTTP: CodeRed Worm	Signature	High	1	11-8-2002 19:19:14
TCP-Illegal-FIN-Probe	Signature	Low	1	11-8-2002 8:15:27
Fingerprinting Queso	Port Scan	High	1	11-8-2002 8:15:29

Top '20' Source IP Details

Source IP	Count
200.181.177.193	670
198.77.21.66	25
209.47.206.43	10
12.235.20.80	9
12.230.172.110	6
220.81.57.36	6
220.74.26.90	5
148.100.208.103	4
216.53.183.123	2
216.234.205.179	2
200.161.142.173	2
212.163.163.65	2
207.46.137.253	1
66.67.34.170	1
66.67.34.108	1
207.46.137.8	1
193.152.208.169	1
131.107.3.79	1

Top '20' Destination IP Details

Destination IP	Count
209.20.153.105	344
209.20.153.110	343
209.20.153.101	29
209.20.153.100	27
10.0.10.10	2
10.0.5.10	2
209.20.153.106	1
209.20.153.107	1

Top '20' Source/Destination IP Pair Details

Source IP	Destination IP	Count
200.181.177.193	209.20.153.110	335
200.181.177.193	209.20.153.105	335
198.77.21.66	209.20.153.100	25
220.81.57.36	209.20.153.101	6
220.74.26.90	209.20.153.101	5
12.235.20.80	209.20.153.101	5
12.235.20.80	209.20.153.110	3
12.230.172.110	209.20.153.105	3
209.47.206.43	209.20.153.101	2
209.47.206.43	209.20.153.110	2
216.53.183.123	209.20.153.110	2
209.47.206.43	10.0.10.10	2
216.234.205.179	209.20.153.101	2
148.100.208.103	209.20.153.101	2
209.47.206.43	209.20.153.105	2
148.100.208.103	209.20.153.100	2
209.47.206.43	10.0.5.10	2
212.163.163.65	209.20.153.101	2
200.161.142.173	209.20.153.101	2
207.46.137.8	209.20.153.105	1