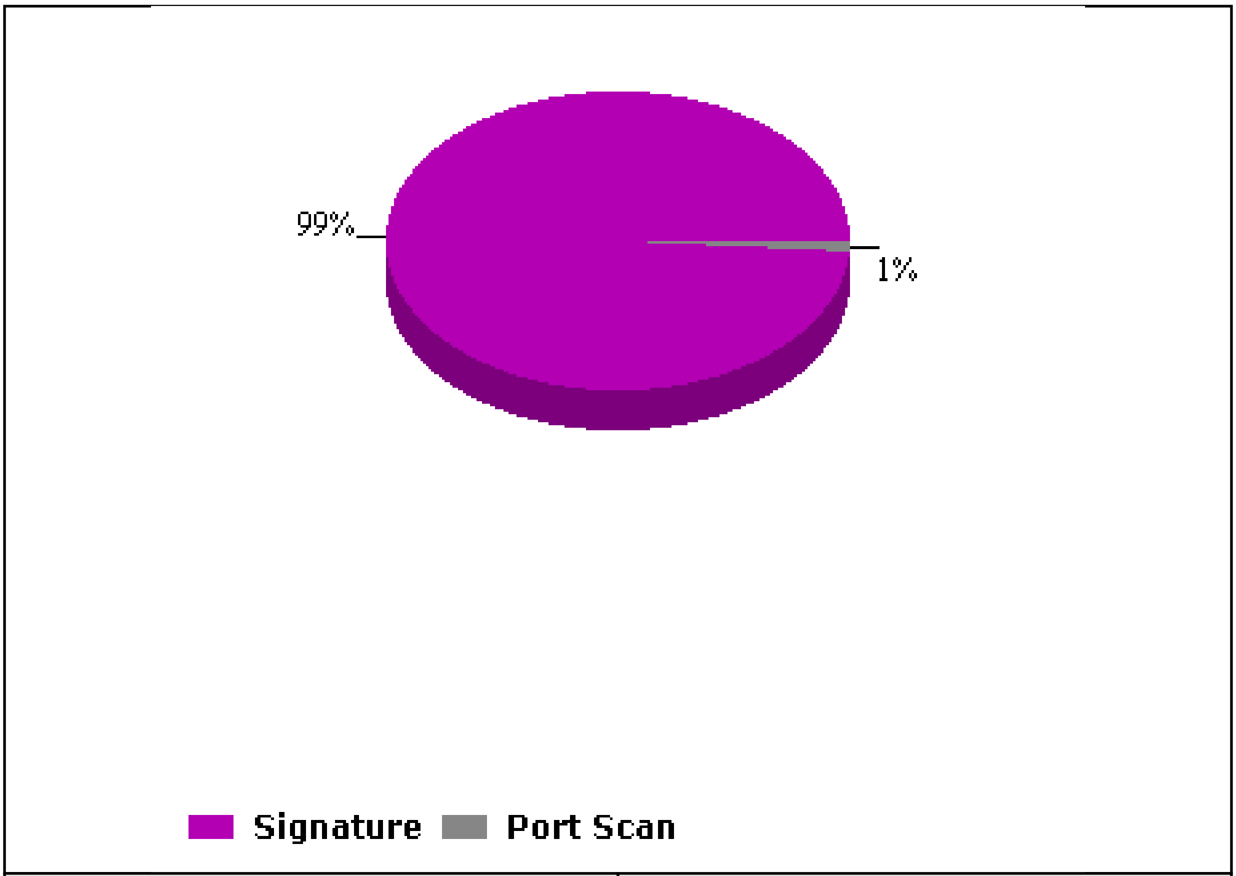
IntruShield™ IDS Report

EXECUTIVE SUMMARY REPORT

Admin Domain:	/eWEEK OpenHack 4 all
Sensor:	I2600
Alert Severity:	Low, Medium, High
Alert State:	All Alerts
Start Date:	Sat Nov 02 00:00:00 PST 2002
End Date:	Sat Nov 02 23:59:59 PST 2002

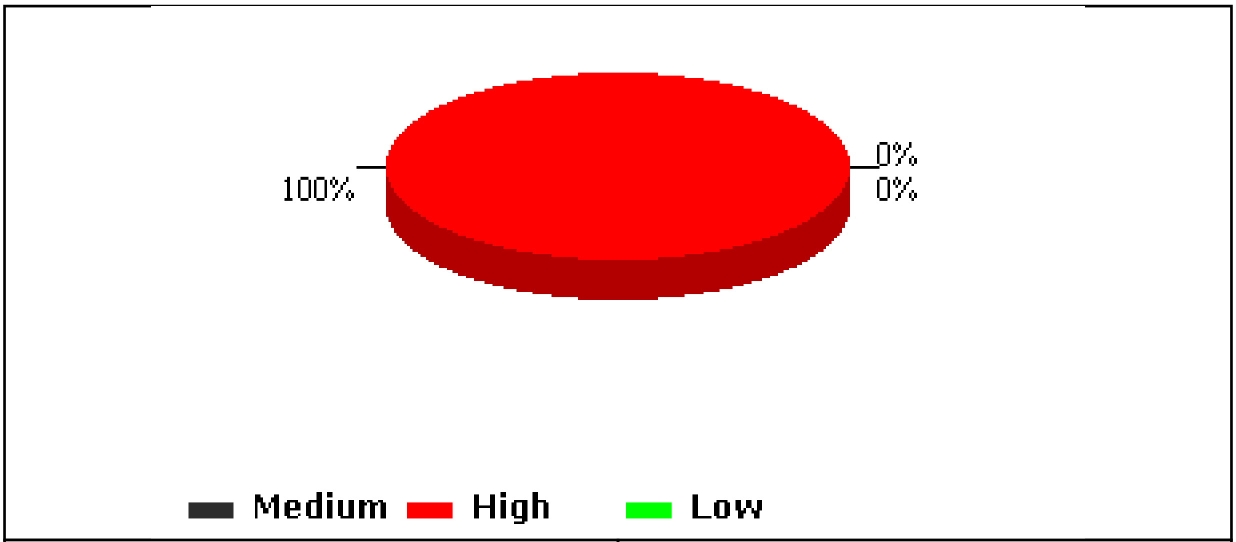
Total alerts detected by the sensor: 708

Total Alerts Per Alert Type



Alert Type	Alerts Detected
Signature	701
Port Scan	7

Total Alerts Per Severity



Attack Severity	Alerts Detected
Medium	0
High	708
Low	0

Top '20' Alert Details

Alert Name	Alert Type	Severity	Count	Last Detected
SNMP: Read Other Default Community String	Signature	Low	540	11-4-2002 11:36:7
SNMP: Cisco IOS Undocumented Community String	Signature	Medium	60	11-4-2002 11:36:7
RPC: Portmap Dump Request	Signature	Medium	30	11-2-2002 16:6:50
SNMP: Read Public Community String	Signature	&nbsp;	30	11-6-2002 11:39:27
IPHdr-SrcDstInvalidAddress	Signature	Low	25	11-7-2002 3:16:36
DNS: Invalid Field Value	Signature	Low	10	11-5-2002 16:45:17
TCP SYN port scan	Port Scan	Medium	6	11-6-2002 21:13:20
HTTP: Phf Execute Arbitary Command	Signature	High	2	11-6-2002 20:12:53
HTTP: IIS CMD.EXE Execution	Signature	High	2	11-6-2002 20:13:16
HTTP: IIS Command Execution	Signature	High	2	11-6-2002 19:22:44
UDP port scan	Port Scan	Medium	1	11-6-2002 21:37:53

Top '20' Source IP Details

Source IP	Count
200.181.177.193	670
220.76.194.163	12
220.74.139.184	10
193.152.255.161	4
220.79.182.175	3
128.148.23.55	2
68.83.30.127	2
207.188.152.178	2
217.134.61.80	2
217.45.38.203	1

Top '20' Destination IP Details

Destination IP	Count
209.20.153.105	337
209.20.153.110	335
209.20.153.101	34
209.20.153.102	2

Top '20' Source/Destination IP Pair Details

Source IP	Destination IP	Count
200.181.177.193	209.20.153.105	335
200.181.177.193	209.20.153.110	335
220.76.194.163	209.20.153.101	12
220.74.139.184	209.20.153.101	10
193.152.255.161	209.20.153.101	3
220.79.182.175	209.20.153.101	3
207.188.152.178	209.20.153.101	2
217.134.61.80	209.20.153.102	2
128.148.23.55	209.20.153.101	2
68.83.30.127	209.20.153.101	2
217.45.38.203	209.20.153.105	1
193.152.255.161	209.20.153.105	1