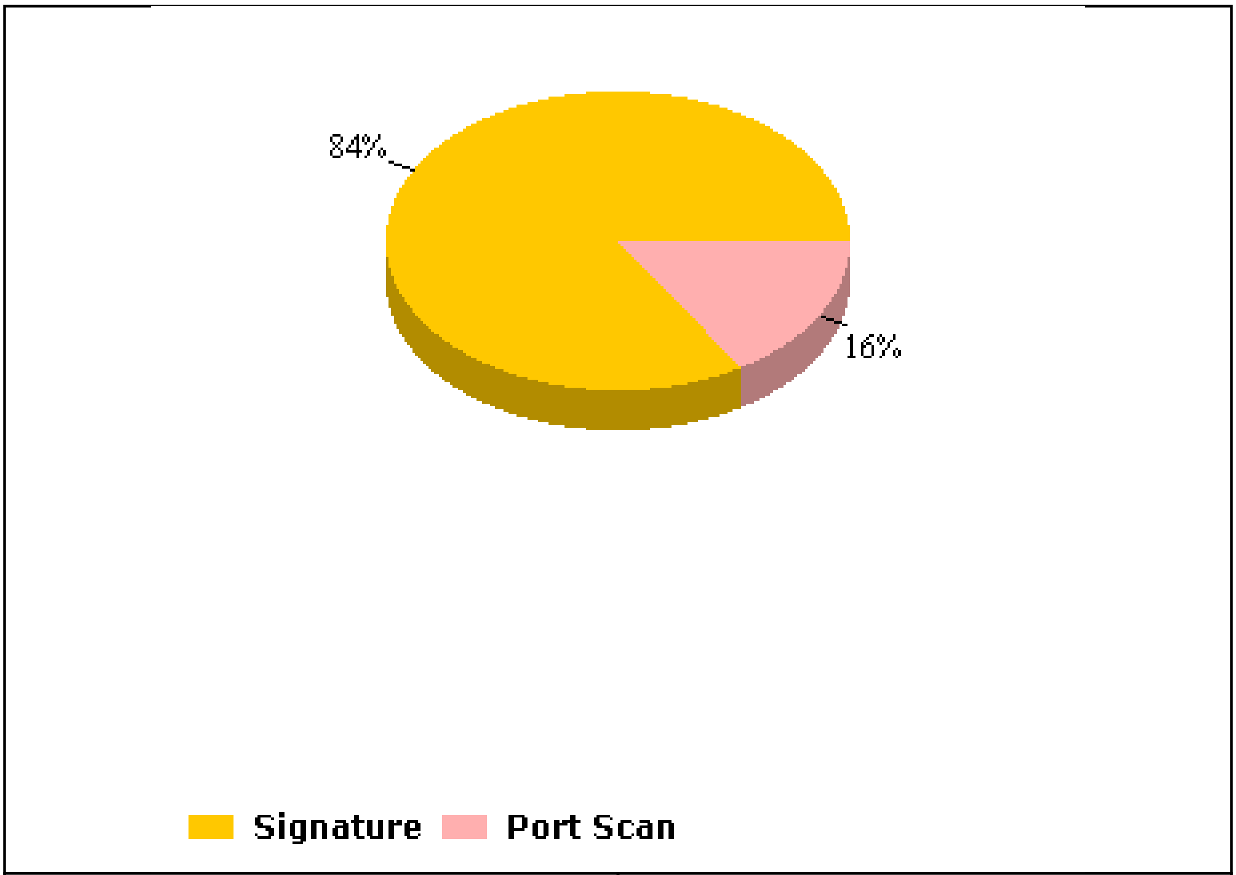
IntruShield™ IDS Report

EXECUTIVE SUMMARY REPORT

Admin Domain:	/eWEEK OpenHack 4 all
Sensor:	I2600
Alert Severity:	Low, Medium, High
Alert State:	All Alerts
Start Date:	Mon Oct 28 00:00:00 PST 2002
End Date:	Mon Oct 28 23:59:59 PST 2002

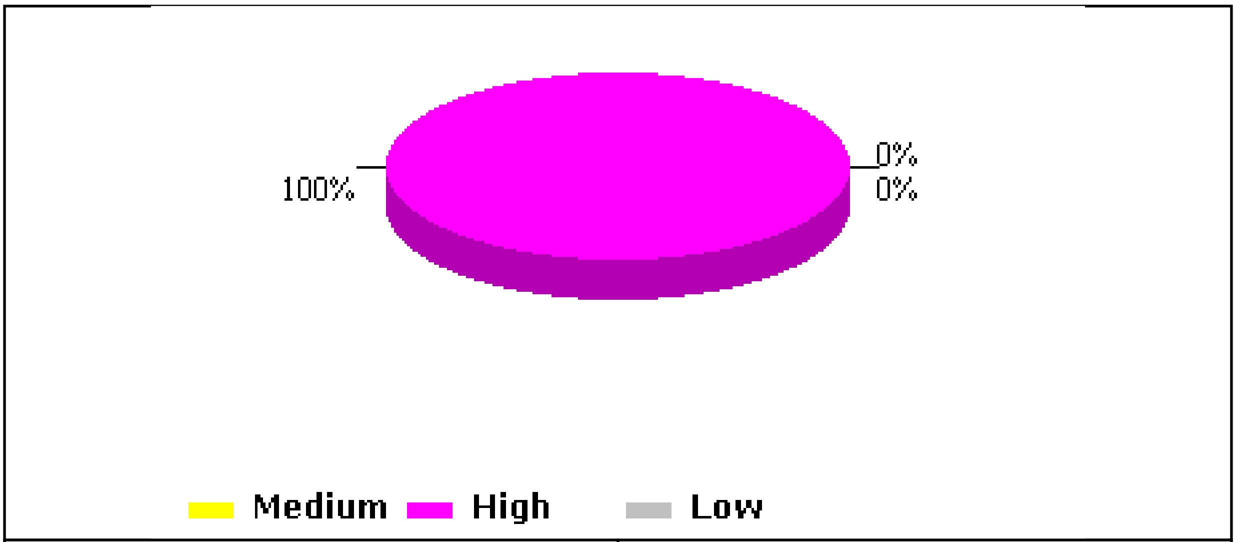
Total alerts detected by the sensor: 935

Total Alerts Per Alert Type



Alert Type	Alerts Detected
Signature	785
Port Scan	150

Total Alerts Per Severity



Attack Severity	Alerts Detected
Medium	0
High	935
Low	0

Top '20' Alert Details

Alert Name	Alert Type	Severity	Count	Last Detected
TCP SYN port scan	Port Scan	Medium	147	10-31-2002 14:24:24
HTTP: CGI EscapeCharacter DirectoryTraversal	Signature	High	102	10-31-2002 14:23:42
HTTP: IIS Command Execution	Signature	High	101	10-31-2002 8:16:6
SNMP: Read Other Default Community String	Signature	Low	100	10-30-2002 22:9:47
HTTP: IIS CMD.EXE Execution	Signature	High	59	10-31-2002 8:16:6
SNMP: Read Public Community String	Signature	&nbsp;	35	10-31-2002 9:35:10
HTTP: Abnomal %00 in Parameter	Signature	Low	34	10-31-2002 3:18:56
HTTP: IIS 4.0 idc path disclosure	Signature	Low	26	10-31-2002 7:55:59
TCP-Illegal-FIN-Probe	Signature	Low	19	10-31-2002 10:47:15
IPHdr-SrcDstInvalidAddress	Signature	Low	19	10-31-2002 7:11:12
HTTP: Interpreter AccessAttempt	Signature	Medium	18	10-31-2002 7:56:9
HTTP: Cross Site Script Attack	Signature	High	16	10-31-2002 3:17:17
HTTP: Nimda Worm - IIS Extended Unicode Directory Travesal Attack	Signature	High	16	10-31-2002 8:16:6
unicode-utf8-too-long-encoding	Signature	High	12	10-31-2002 8:16:6
HTTP: ExpressionCalculator InputValidation	Signature	Medium	12	10-31-2002 3:9:1
Scan: SYN FIN Based Probes	Signature	Low	11	10-31-2002 10:47:15
SNMP: Cisco IOS Undocumented Community String	Signature	Medium	11	10-30-2002 19:55:7
HTTP: FUDforum script exploit	Signature	High	8	10-31-2002 3:18:37
NMAP XMAS Probe	Signature	Medium	8	10-29-2002 17:3:41
HTTP: IIS Root.exe Execute Command	Signature	High	8	10-30-2002 13:5:10

Top '20' Source IP Details

Source IP	Count
213.97.20.166	395
66.68.87.36	82
193.252.24.77	64
200.40.94.215	48
211.141.206.44	42
209.244.95.202	42
208.47.211.5	30
67.80.229.14	27
202.41.10.26	22
12.163.89.1	21
64.19.154.147	17
209.123.101.203	16
193.110.121.9	16
67.114.20.58	12
65.94.228.214	12
208.14.6.170	12
64.225.138.225	11
209.247.140.173	10
220.75.249.42	8
211.228.46.39	5

Top '20' Destination IP Details

Destination IP	Count
209.20.153.101	627
209.20.153.105	235
209.20.153.110	39
209.20.153.106	6
209.20.153.107	6
209.20.153.108	6
209.20.153.100	4
209.20.153.102	4
209.20.153.104	4
209.20.153.98	2
209.20.153.99	2

Top '20' Source/Destination IP Pair Details

Source IP	Destination IP	Count
213.97.20.166	209.20.153.101	395
66.68.87.36	209.20.153.105	82
193.252.24.77	209.20.153.101	64
200.40.94.215	209.20.153.105	48
211.141.206.44	209.20.153.101	42
209.244.95.202	209.20.153.101	42
67.80.229.14	209.20.153.105	27
208.47.211.5	209.20.153.105	22
12.163.89.1	209.20.153.105	21
193.110.121.9	209.20.153.110	16
209.123.101.203	209.20.153.101	16
208.14.6.170	209.20.153.105	12
65.94.228.214	209.20.153.110	12
209.247.140.173	209.20.153.101	10
67.114.20.58	209.20.153.105	9
220.75.249.42	209.20.153.101	8
211.228.46.39	209.20.153.101	5
213.66.43.145	209.20.153.101	4
65.211.58.5	209.20.153.101	4
220.82.1.136	209.20.153.101	4