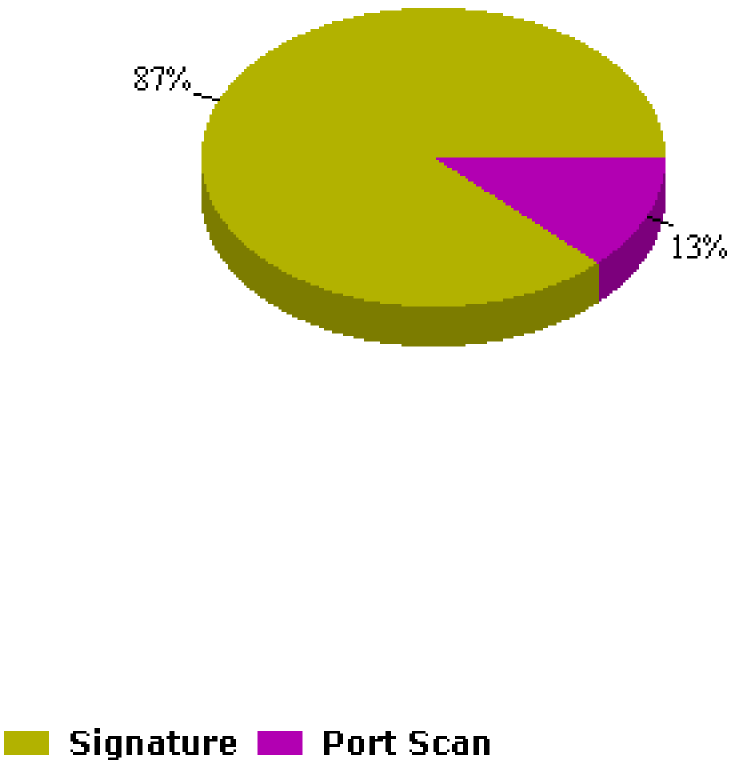
IntruShield™ IDS Report

EXECUTIVE SUMMARY REPORT

Admin Domain:	/eWEEK OpenHack 4 all
Sensor:	I2600
Alert Severity:	Low, Medium, High
Alert State:	All Alerts
Start Date:	Sat Oct 26 00:00:00 PDT 2002
End Date:	Sat Oct 26 23:59:59 PDT 2002

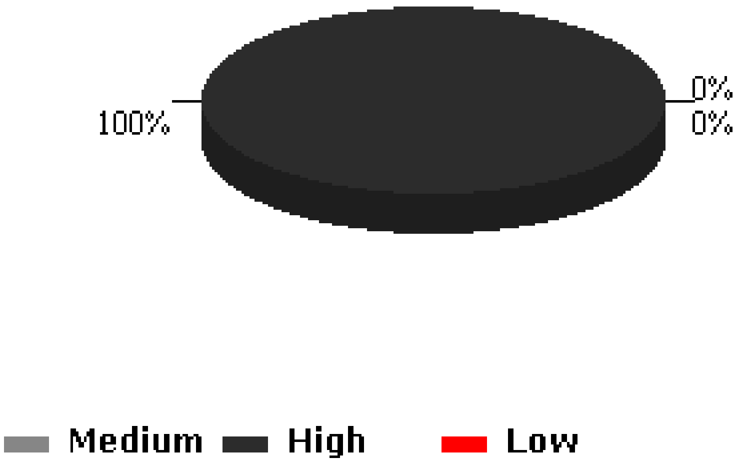
Total alerts detected by the sensor: 2042

Total Alerts Per Alert Type



Alert Type	Alerts Detected
Signature	1786
Port Scan	256

Total Alerts Per Severity



Attack Severity	Alerts Detected
Medium	0
High	2042
Low	0

Top '20' Alert Details

Alert Name	Alert Type	Severity	Count	Last Detected
Scan: NULL Probe	Signature	Low	749	10-31-2002 10:47:15
TCPHdr-Ports-EqualZero	Signature	Low	742	10-30-2002 19:58:52
TCP SYN port scan	Port Scan	Medium	247	10-31-2002 10:48:3
NMAP XMAS Probe	Signature	Medium	108	10-29-2002 17:3:41
HTTP: IIS CMD.EXE Execution	Signature	High	19	10-31-2002 8:16:6
HTTP: CGI EscapeCharacter DirectoryTraversal	Signature	High	18	10-31-2002 7:3:23
HTTP: IIS Command Execution	Signature	High	18	10-31-2002 8:16:6
ICMP: Netmask Request	Signature	Low	13	10-31-2002 9:35:12
ICMP: Timestamp Probe	Signature	Low	13	10-31-2002 9:35:12
TCPHdr-Flags-URGNoACK	Signature	Low	12	10-31-2002 10:47:15
TCP-Illegal-FIN-Probe	Signature	Low	12	10-31-2002 10:47:15
Scan: SYN FIN Based Probes	Signature	Low	12	10-31-2002 10:47:15
NMAP XMAS with SYN Probe	Signature	Medium	7	10-31-2002 10:47:15
IPHdr-SrcDstInvalidAddress	Signature	Low	7	10-31-2002 7:11:12
unicode-utf8-too-long-encoding	Signature	High	6	10-31-2002 8:16:6
SNMP: Cisco IOS Undocumented Community String	Signature	Medium	6	10-30-2002 19:55:7
Fingerprinting NMAP	Port Scan	Medium	5	10-31-2002 10:47:16
HTTP: Nimda Worm - IIS Extended Unicode Directory Travesal Attack	Signature	High	5	10-31-2002 8:16:6
UDP port scan	Port Scan	Medium	4	10-29-2002 20:46:0
HTTP: Cross Site Script Attack	Signature	High	3	10-31-2002 3:17:17

Top '20' Source IP Details

Source IP	Count
151.24.188.80	1489
65.35.244.25	169
217.134.39.19	151
81.12.239.2	38
12.235.124.63	38
200.165.191.136	36
66.68.87.36	23
211.147.22.79	12
151.26.82.240	12
66.12.249.22	11
141.150.122.154	8
68.32.80.64	6
200.63.188.146	6
67.234.27.206	5
193.253.55.236	4
220.76.92.23	4
220.76.163.145	3
62.64.232.164	3
62.83.46.177	3
217.85.151.223	2

Top '20' Destination IP Details

Destination IP	Count
209.20.153.105	1730
209.20.153.101	180
209.20.153.110	41
209.20.153.100	17
209.20.153.99	13
209.20.153.102	12
209.20.153.108	12
209.20.153.98	12
209.20.153.104	8
209.20.153.106	8
209.20.153.107	8
209.20.130.34	1

Top '20' Source/Destination IP Pair Details

Source IP	Destination IP	Count
151.24.188.80	209.20.153.105	1489
65.35.244.25	209.20.153.105	169
81.12.239.2	209.20.153.101	38
12.235.124.63	209.20.153.101	38
200.165.191.136	209.20.153.101	36
217.134.39.19	209.20.153.110	34
66.68.87.36	209.20.153.105	23
217.134.39.19	209.20.153.100	16
217.134.39.19	209.20.153.105	16
217.134.39.19	209.20.153.99	13
217.134.39.19	209.20.153.108	12
217.134.39.19	209.20.153.98	12
217.134.39.19	209.20.153.101	12
217.134.39.19	209.20.153.102	12
151.26.82.240	209.20.153.101	12
211.147.22.79	209.20.153.101	12
217.134.39.19	209.20.153.107	8
217.134.39.19	209.20.153.104	8
66.12.249.22	209.20.153.105	8
217.134.39.19	209.20.153.106	8