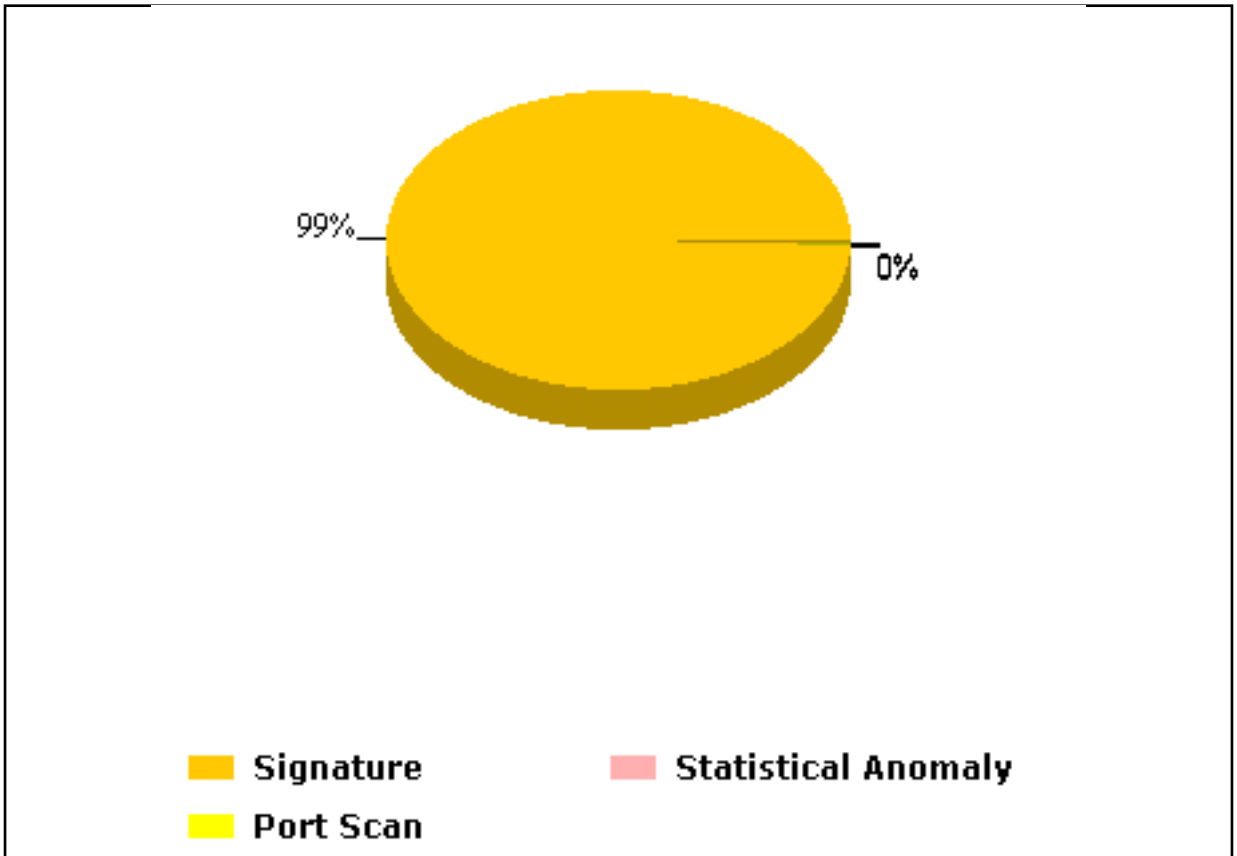
IntruShield™ IDS Report

EXECUTIVE SUMMARY REPORT

Admin Domain:	/eWEEK OpenHack 4 all
Sensor:	I2600
Alert Severity:	Low, Medium, High
Alert State:	All Alerts
Start Date:	Fri Oct 25 00:00:00 PDT 2002
End Date:	Fri Oct 25 23:59:59 PDT 2002

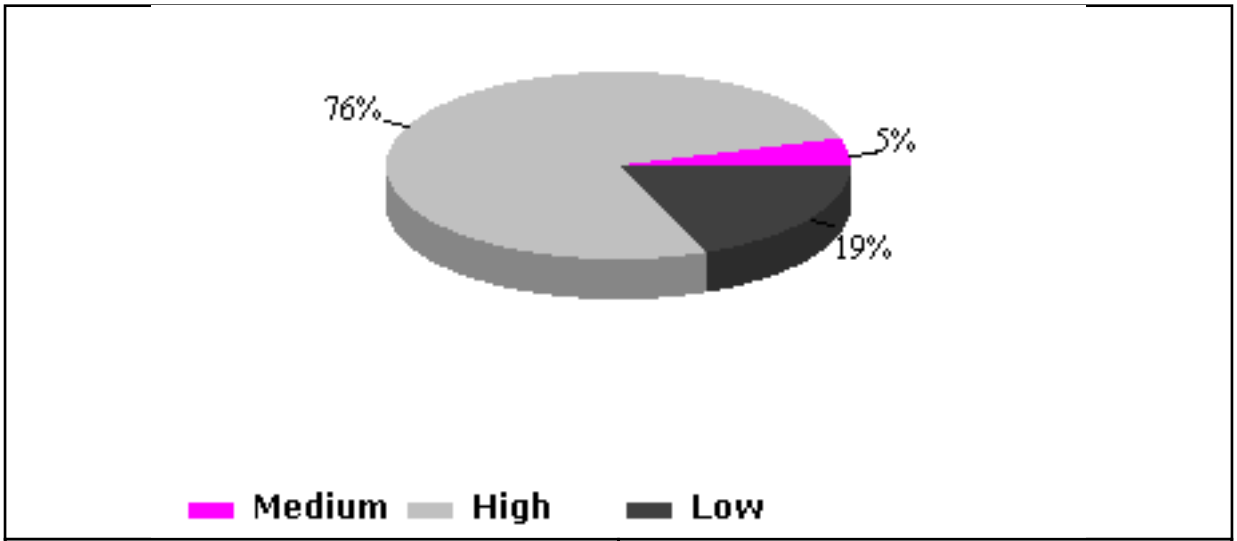
Total alerts detected by the sensor: 8993

Total Alerts Per Alert Type



Alert Type	Alerts Detected
Signature	8941
Statistical Anomaly	13
Port Scan	39

Total Alerts Per Severity



Attack Severity	Alerts Detected
Medium	432
High	6871
Low	1690

Top '20' Alert Details

Alert Name	Alert Type	Severity	Count	Last Detected
HTTP: IIS CMD.EXE Execution	Signature	High	1639	10-31-2002 8:16:6
HTTP: IIS Command Execution	Signature	High	1624	10-31-2002 8:16:6
SNMP: Read Other Default Community String	Signature	Low	1389	10-30-2002 22:9:47
HTTP: CGI EscapeCharacter DirectoryTraversal	Signature	High	1369	10-31-2002 7:3:23
unicode-utf8-too-long-encoding	Signature	High	815	10-31-2002 8:16:6
HTTP: Nimda Worm - IIS Extended Unicode Directory Travesal Attack	Signature	High	642	10-31-2002 8:16:6
SNMP: Cisco IOS Undocumented Community String	Signature	Medium	131	10-30-2002 19:55:7
HTTP: Cross Site Script Attack	Signature	High	90	10-31-2002 3:17:17
HTTP: IIS 4.0 idc path disclosure	Signature	Low	62	10-31-2002 7:55:59
RPC: Portmap Dump Request	Signature	Medium	59	10-25-2002 11:47:32
HTTP: Test Cgi DirectoryListing	Signature	Medium	49	10-31-2002 3:8:13
HTTP: Phf Execute Arbitary Command	Signature	High	48	10-31-2002 7:56:3
TCP-Illegal-FIN-Probe	Signature	Low	46	10-31-2002 10:47:15
DNS: Invalid Field Value	Signature	Low	46	10-31-2002 7:57:13
Scan: Amanda Client Version Probe	Signature	Low	36	10-30-2002 20:3:2
HTTP: IIS multiple sample ASP script View File Attempt	Signature	Medium	33	10-31-2002 3:17:48
HTTP: URI Too Long	Signature	Medium	33	10-30-2002 6:23:18
TCP SYN port scan	Port Scan	Medium	30	10-31-2002 10:48:3
HTTP: Interpreter AccessAttempt	Signature	Medium	30	10-31-2002 7:56:9
Scan: SYN FIN Based Probes	Signature	Low	28	10-31-2002 10:47:15

Top '20' Source IP Details

Source IP	Count
24.91.27.101	4072
67.96.113.140	2304
200.181.177.214	1207
172.155.92.14	327
216.232.11.49	169
208.156.111.3	164
24.130.76.111	148
209.103.231.34	86
217.121.2.55	78
67.84.155.168	47
159.215.52.124	34
24.242.49.201	30
68.69.0.166	24
65.69.58.203	24
217.134.15.134	22
66.156.35.110	20
24.29.57.42	19
80.116.115.113	19
149.156.208.100	17
170.215.75.101	14

Top '20' Destination IP Details

Destination IP	Count
209.20.153.101	7288
209.20.153.105	1018
209.20.153.110	626
*	13
209.20.153.100	7
209.20.130.35	6
209.20.153.99	4
209.20.153.102	4
209.20.153.104	4
209.20.153.106	4
209.20.153.107	4
209.20.153.108	4
209.20.153.109	4
64.4.12.138	3
0.0.0.0	2
209.20.153.98	2

Top '20' Source/Destination IP Pair Details

Source IP	Destination IP	Count
24.91.27.101	209.20.153.101	4072
67.96.113.140	209.20.153.101	2304
200.181.177.214	209.20.153.105	608
200.181.177.214	209.20.153.110	599
172.155.92.14	209.20.153.101	327
216.232.11.49	209.20.153.105	169
208.156.111.3	209.20.153.101	164
24.130.76.111	209.20.153.101	148
209.103.231.34	209.20.153.101	86
217.121.2.55	209.20.153.101	78
67.84.155.168	209.20.153.105	47
159.215.52.124	209.20.153.105	34
24.242.49.201	209.20.153.105	30
68.69.0.166	209.20.153.105	24
80.116.115.113	209.20.153.105	19
24.29.57.42	209.20.153.101	19
170.215.75.101	209.20.153.101	14
*	*	13
211.161.246.9	209.20.153.105	13
64.208.104.215	209.20.153.110	13

NOTE: The red asterisk indicates a non-existent value. For instance, Statistical and Threshold anomaly alerts do NOT have either the source OR destination IP address fields populated. Host sweep alerts MAY OR MAY NOT have the destination IP address field populated, AND Throttle summary alerts MAY OR MAY NOT have either the source OR destination IP address fields populated.