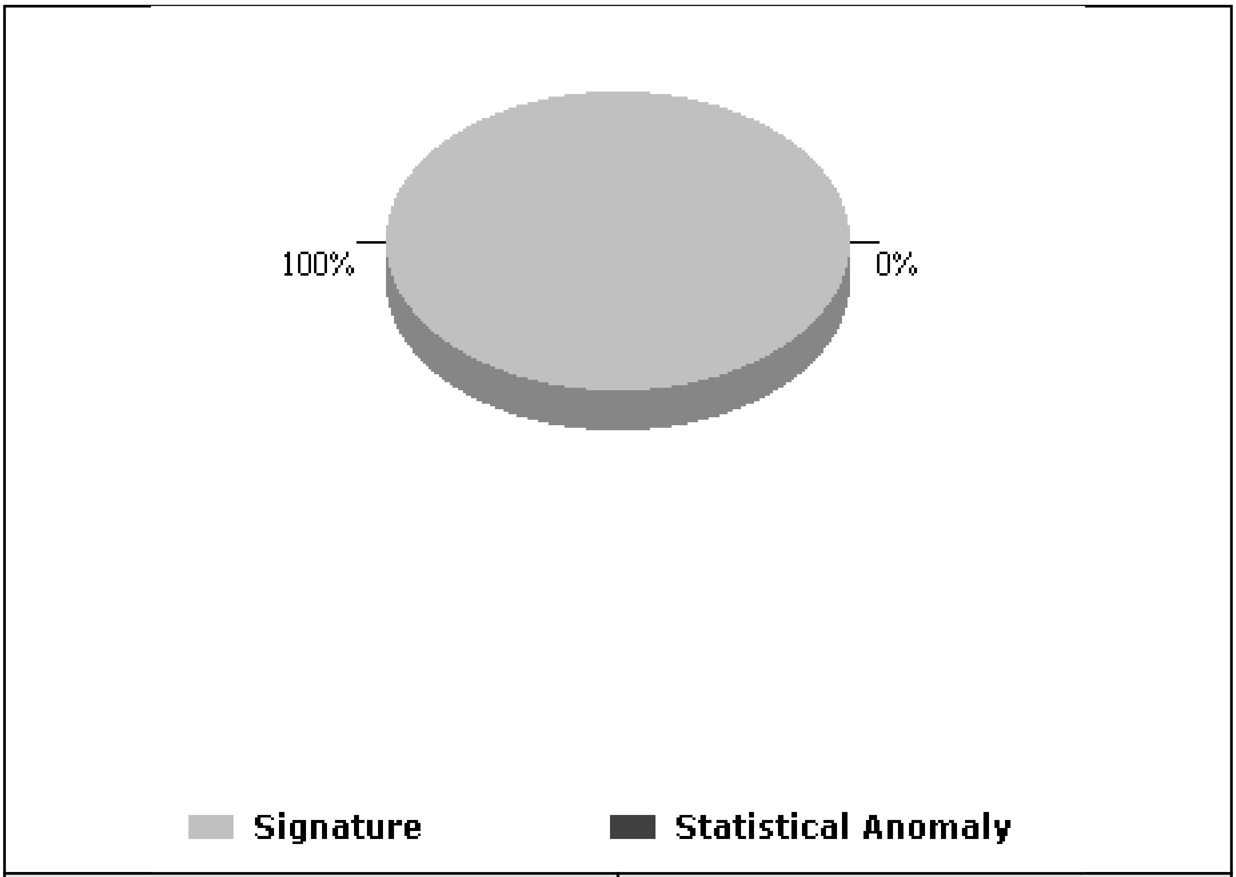
IntruShield™ IDS Report

EXECUTIVE SUMMARY REPORT

Admin Domain:	/eWEEK OpenHack 4 all
Sensor:	I2600
Alert Severity:	Low, Medium, High
Alert State:	All Alerts
Start Date:	Thu Oct 24 00:00:00 PDT 2002
End Date:	Thu Oct 24 23:59:59 PDT 2002

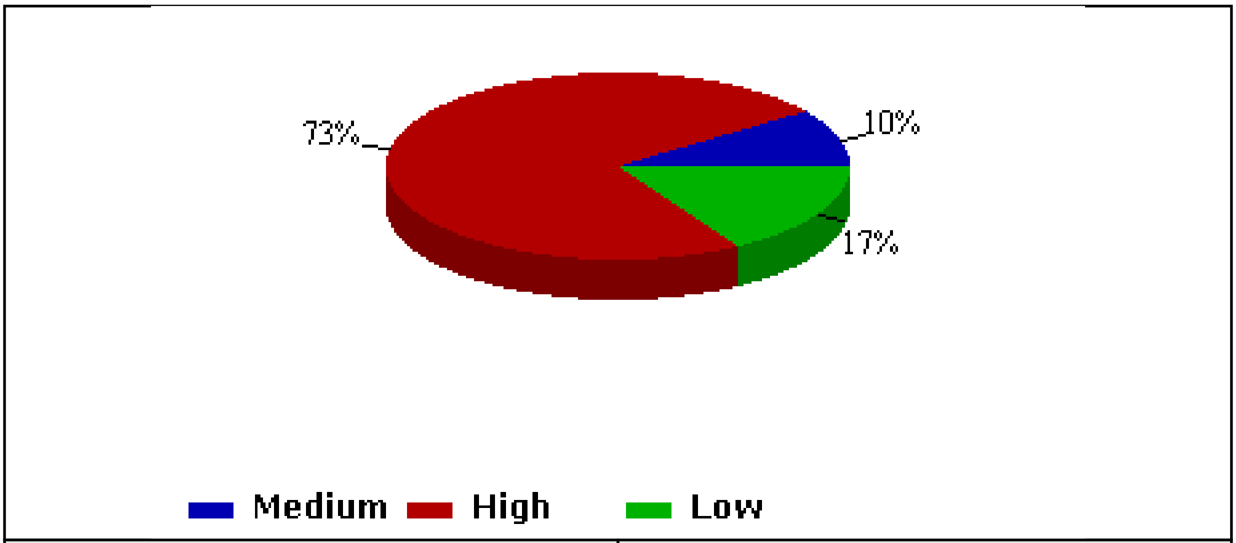
Total alerts detected by the sensor: 14094

Total Alerts Per Alert Type



Alert Type	Alerts Detected
Signature	14093
Statistical Anomaly	1

Total Alerts Per Severity



Attack Severity	Alerts Detected
Medium	1400
High	10359
Low	2335

Top '20' Alert Details

Alert Name	Alert Type	Severity	Count	Last Detected
HTTP: CGI EscapeCharacter DirectoryTraversal	Signature	High	3421	10-25-2002 18:46:39
HTTP: IIS CMD.EXE Execution	Signature	High	2263	10-25-2002 18:45:38
HTTP: IIS Command Execution	Signature	High	2069	10-25-2002 18:45:38
unicode-utf8-too-long-encoding	Signature	High	1268	10-25-2002 18:45:38
HTTP: Nimda Worm - IIS Extended Unicode Directory Travesal Attack	Signature	High	765	10-25-2002 18:45:37
HTTP: Abnomal %00 in Parameter	Signature	Low	599	10-25-2002 8:36:40
Scan: SYN FIN Based Probes	Signature	Low	423	10-25-2002 19:31:24
SNMP: Read Other Default Community String	Signature	Low	285	10-25-2002 15:10:32
HTTP: Netscape Enterprise Server Index Disclosure	Signature	Low	248	10-24-2002 6:22:49
HTTP: IIS 4.0 idc path disclosure	Signature	Low	142	10-25-2002 13:0:59
HTTP: Cross Site Script Attack	Signature	High	136	10-25-2002 18:46:2
ICMP: Netmask Request	Signature	Low	113	10-25-2002 14:15:32
ICMP: Timestamp Probe	Signature	Low	111	10-25-2002 15:2:21
HTTP: Read Password File Attempt	Signature	Medium	106	10-25-2002 18:45:16
IPHdr-SrcDstInvalidAddress	Signature	Low	93	10-25-2002 5:24:23
HTTP: Test Cgi DirectoryListing	Signature	Medium	86	10-25-2002 18:54:25
HTTP: CISCO HTTP Admin Authentication	Signature	Medium	84	10-24-2002 16:49:48
HTTP: Phf Execute Arbitary Command	Signature	High	81	10-25-2002 18:54:24
TCP-Illegal-FIN-Probe	Signature	Low	81	10-25-2002 19:57:54
HTTP: MISCROXEN Directorylist	Signature	Medium	67	10-25-2002 18:41:23

Top '20' Source IP Details

Source IP	Count
66.177.1.152	6539
206.196.68.166	5443
63.91.6.250	494
65.112.51.216	475
63.205.172.99	146
217.34.240.140	136
62.163.201.39	62
212.29.223.194	52
68.83.20.165	51
12.220.39.90	50
205.238.192.68	46
213.220.44.22	45
65.42.8.251	44
24.112.143.4	41
213.6.238.100	31
68.80.89.224	30
212.113.167.138	26
12.162.95.244	26
164.73.80.244	24
24.199.189.218	24

Top '20' Destination IP Details

Destination IP	Count
209.20.153.101	12890
209.20.153.105	906
209.20.153.110	133
209.20.153.100	23
209.20.153.102	21
209.20.153.104	19
209.20.153.106	19
209.20.153.109	19
209.20.153.107	18
209.20.153.108	18
209.20.153.98	12
209.20.153.99	11
64.4.12.138	2
63.111.13.100	2
*	1

Top '20' Source/Destination IP Pair Details

Source IP	Destination IP	Count
66.177.1.152	209.20.153.101	6539
206.196.68.166	209.20.153.101	5443
65.112.51.216	209.20.153.101	475
63.91.6.250	209.20.153.105	475
63.205.172.99	209.20.153.105	146
217.34.240.140	209.20.153.110	82
62.163.201.39	209.20.153.101	62
217.34.240.140	209.20.153.105	54
212.29.223.194	209.20.153.101	52
68.83.20.165	209.20.153.105	51
205.238.192.68	209.20.153.101	46
213.220.44.22	209.20.153.101	45
24.112.143.4	209.20.153.101	32
213.6.238.100	209.20.153.105	31
68.80.89.224	209.20.153.101	30
220.76.138.127	209.20.153.101	20
216.72.183.101	209.20.153.105	20
203.94.146.139	209.20.153.105	19
63.91.6.250	209.20.153.110	19
220.76.132.143	209.20.153.101	15

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.