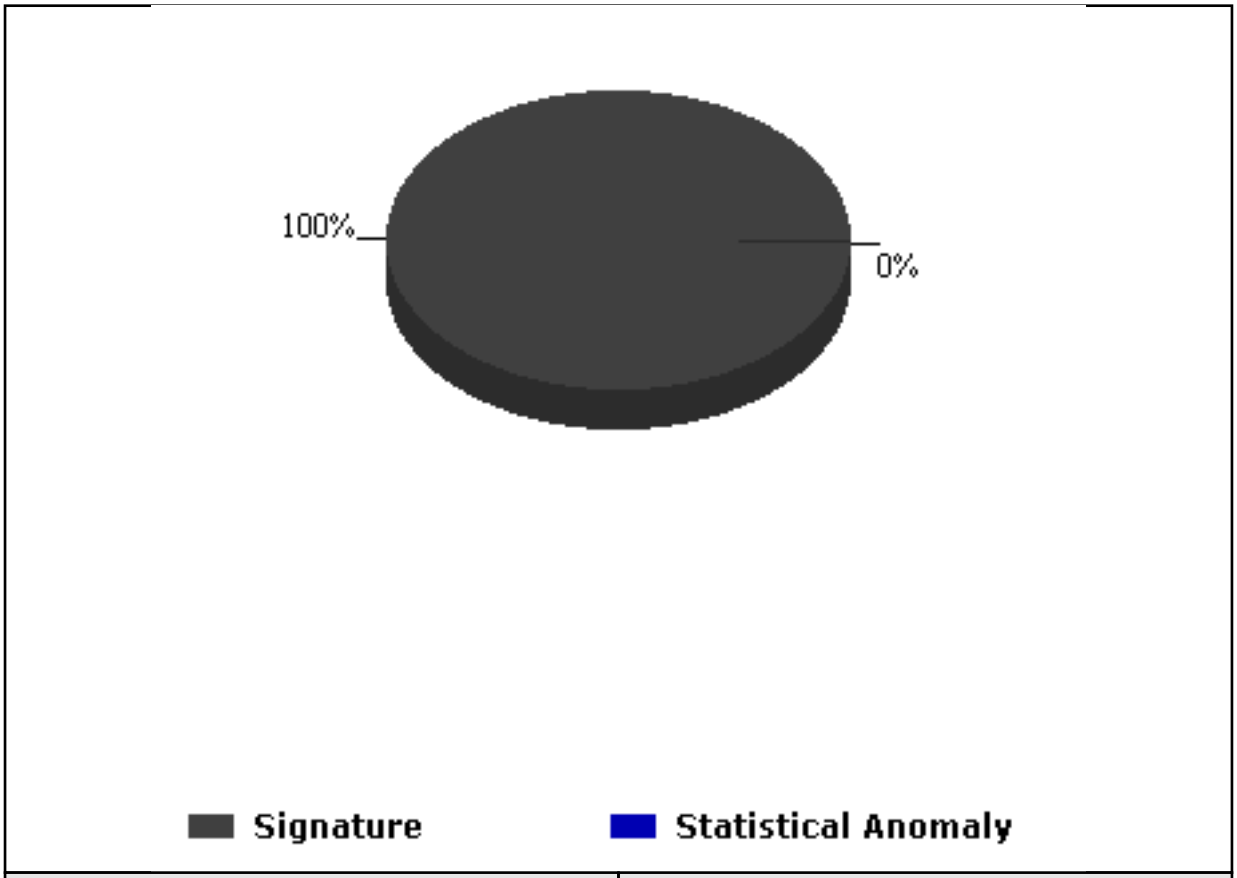
IntruShield™ IDS Report

EXECUTIVE SUMMARY REPORT

Admin Domain:	/eWEEK OpenHack 4 all
Sensor:	I2600
Alert Severity:	Low, Medium, High
Alert State:	All Alerts
Start Date:	Tue Oct 22 08:00:00 PDT 2002
End Date:	Tue Oct 22 23:59:59 PDT 2002

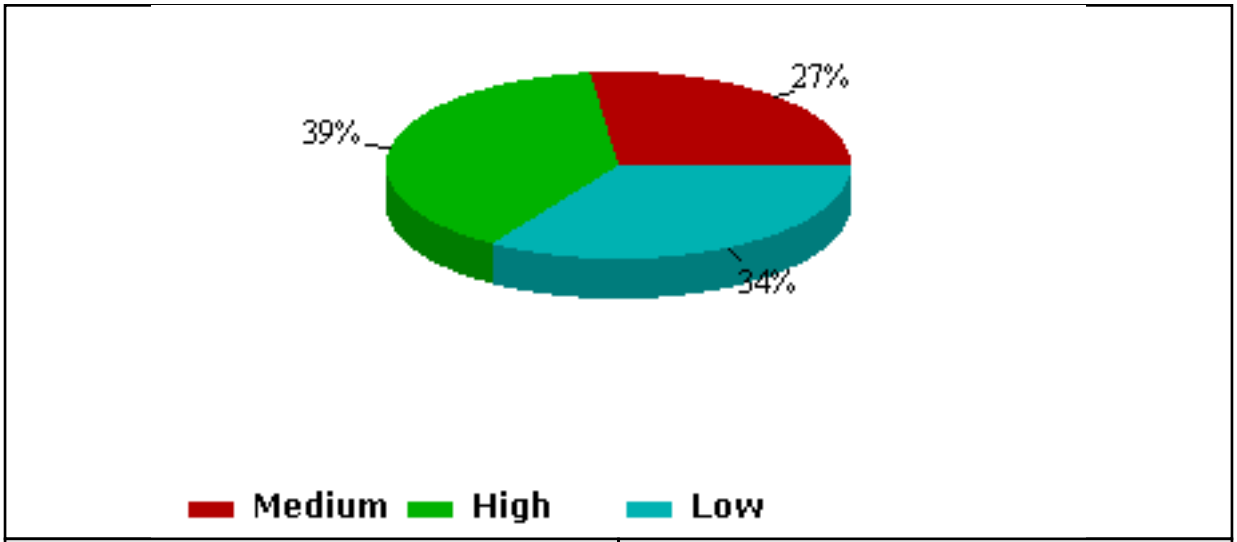
Total alerts detected by the sensor: 2863

Total Alerts Per Alert Type



Alert Type	Alerts Detected
Signature	2854
Statistical Anomaly	9

Total Alerts Per Severity



Attack Severity	Alerts Detected
Medium	771
High	1111
Low	981

Top '20' Alert Details

Alert Name	Alert Type	Severity	Count	Last Detected
HTTP: CGI EscapeCharacter DirectoryTraversal	Signature	High	600	10-25-2002 18:46:39
HTTP: Abnomal %00 in Parameter	Signature	Low	247	10-25-2002 8:36:40
HTTP: Cross Site Script Attack	Signature	High	196	10-25-2002 18:46:2
Scan: NULL Probe	Signature	Low	116	10-25-2002 19:31:24
SNMP: Read Other Default Community String	Signature	Low	93	10-25-2002 15:10:32
HTTP: Read Password File Attempt	Signature	Medium	91	10-25-2002 18:45:16
HTTP: IIS 4.0 idc path disclosure	Signature	Low	76	10-25-2002 13:0:59
HTTP: Netscape Enterprise Server Index Disclosure	Signature	Low	73	10-24-2002 6:22:49
ICMP: Netmask Request	Signature	Low	67	10-25-2002 14:15:32
ICMP: Timestamp Probe	Signature	Low	66	10-25-2002 15:2:21
HTTP: MISCROXEN Directorylist	Signature	Medium	64	10-25-2002 18:41:23
HTTP: URI Too Long	Signature	Medium	56	10-25-2002 13:0:57
NMAP XMAS Probe	Signature	Medium	51	10-25-2002 19:55:17
TCPHdr-Flags-URGNoACK	Signature	Low	45	10-25-2002 19:31:24
TCP-Illegal-FIN-Probe	Signature	Low	45	10-25-2002 19:57:54
Scan: SYN FIN Based Probes	Signature	Low	45	10-25-2002 19:31:24
NMAP XMAS with SYN Probe	Signature	Medium	37	10-25-2002 19:31:24
HTTP: Phf Execute Arbitary Command	Signature	High	36	10-25-2002 18:54:24
HTTP: Nimda Worm - IIS Extended Unicode Directory Travesal Attack	Signature	High	34	10-25-2002 18:45:37
HTTP: Test Cgi DirectoryListing	Signature	Medium	34	10-25-2002 18:54:25

Top '20' Source IP Details

Source IP	Count
203.121.0.9	1239
210.19.85.134	276
24.125.75.81	232
65.112.51.216	218
24.199.220.66	108
68.154.57.162	103
66.177.1.152	69
192.168.2.4	63
217.39.226.162	60
212.120.124.107	50
203.109.175.99	41
168.103.176.96	40
212.29.223.194	38
213.157.185.218	36
212.127.136.251	33
65.165.110.2	32
130.89.166.246	24
172.138.26.157	22
12.166.224.9	18
198.190.230.66	16

Top '20' Destination IP Details

Destination IP	Count
209.20.153.101	2557
209.20.153.110	128
209.20.153.105	109
209.20.153.102	18
209.20.153.100	9
*	9
64.4.12.138	5
10.0.10.10	4
199.183.74.19	3
209.20.153.98	3
209.20.153.99	3
209.20.153.104	3
209.20.153.106	3
209.20.153.107	3
209.20.153.108	3
209.20.153.109	3

Top '20' Source/Destination IP Pair Details

Source IP	Destination IP	Count
203.121.0.9	209.20.153.101	1239
210.19.85.134	209.20.153.101	276
24.125.75.81	209.20.153.101	232
65.112.51.216	209.20.153.101	218
24.199.220.66	209.20.153.101	108
68.154.57.162	209.20.153.101	103
192.168.2.4	209.20.153.101	63
217.39.226.162	209.20.153.110	60
203.109.175.99	209.20.153.101	41
168.103.176.96	209.20.153.105	40
212.29.223.194	209.20.153.101	38
213.157.185.218	209.20.153.101	36
212.127.136.251	209.20.153.101	33
212.120.124.107	209.20.153.101	30
130.89.166.246	209.20.153.101	24
65.165.110.2	209.20.153.110	24
66.177.1.152	209.20.153.101	23
212.120.124.107	209.20.153.110	20
198.190.230.66	209.20.153.105	16
172.138.26.157	209.20.153.105	14

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.