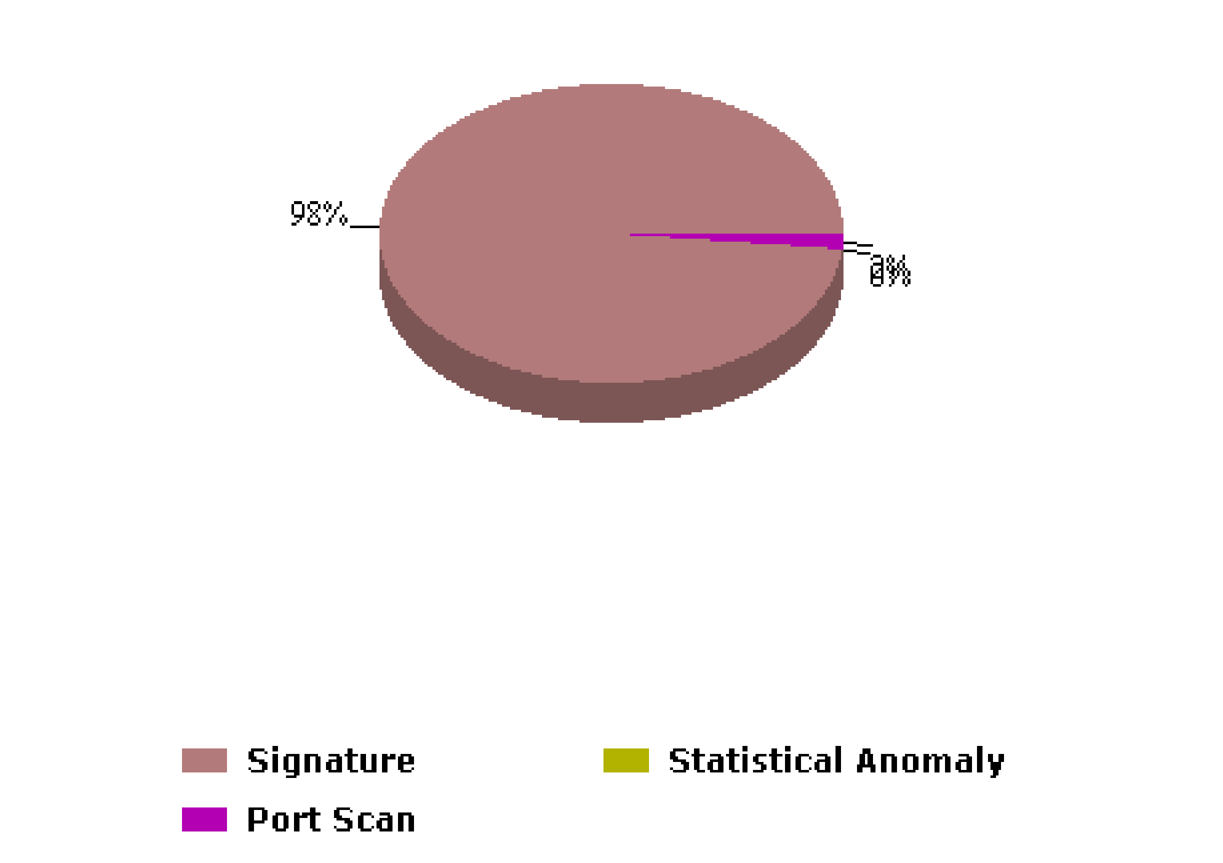
IntruShield™ IDS Report

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:	Fri Nov 08 23:59:59 PST 2002

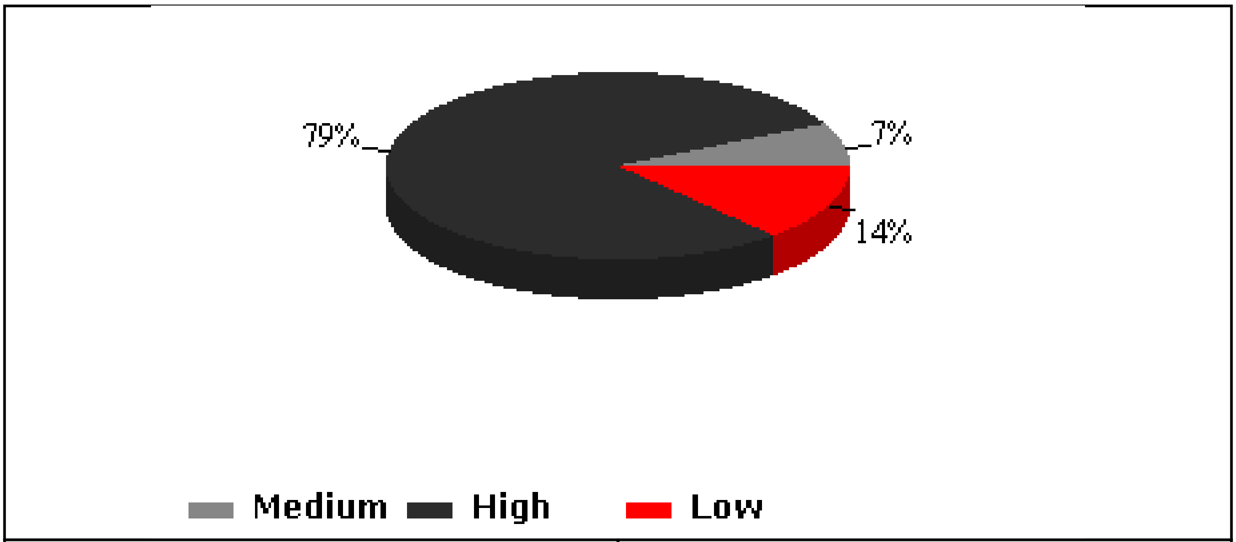
Total alerts detected by the sensor: 52879

Total Alerts Per Alert Type



Alert Type	Alerts Detected
Signature	52033
Statistical Anomaly	23
Port Scan	823

Total Alerts Per Severity



Attack Severity	Alerts Detected
Medium	3906
High	41818
Low	7155

Top '20' Alert Details

Alert Name	Alert Type	Severity	Count	Last Detected
HTTP: CGI EscapeCharacter DirectoryTraversal	Signature	High	9346	11-6-2002 20:14:31
HTTP: IIS CMD.EXE Execution	Signature	High	7305	11-8-2002 14:43:14
HTTP: IIS Command Execution	Signature	High	7246	11-8-2002 14:43:14
SNMP: Read Other Default Community String	Signature	Low	4544	11-8-2002 8:23:3
unicode-utf8-too-long-encoding	Signature	High	3727	11-6-2002 19:22:35
HTTP: Nimda Worm - IIS Extended Unicode Directory Travesal Attack	Signature	High	2819	11-6-2002 19:22:35
HTTP: Abnomal %00 in Parameter	Signature	Low	1452	11-5-2002 21:18:12
Scan: NULL Probe	Signature	Low	974	11-6-2002 13:9:48
TCPHdr-Ports-EqualZero	Signature	Low	843	10-30-2002 19:58:52
TCP SYN port scan	Port Scan	Medium	763	11-9-2002 0:2:47
HTTP: IIS 4.0 idc path disclosure	Signature	Low	762	11-8-2002 19:19:14
HTTP: Cross Site Script Attack	Signature	High	635	11-5-2002 21:14:8
Scan: SYN FIN Based Probes	Signature	Low	598	11-6-2002 13:9:48
HTTP: Netscape Enterprise Server Index Disclosure	Signature	Low	570	10-24-2002 6:22:49
IPHdr-SrcDstInvalidAddress	Signature	Low	416	11-8-2002 11:47:54
SNMP: Cisco IOS Undocumented Community String	Signature	Medium	382	11-8-2002 8:17:41
ICMP: Netmask Request	Signature	Low	373	11-8-2002 23:38:11
ICMP: Timestamp Probe	Signature	Low	372	11-8-2002 23:38:11
HTTP: Read Password File Attempt	Signature	Medium	360	11-8-2002 18:40:33
NMAP XMAS Probe	Signature	Medium	336	11-6-2002 13:9:48

Top '20' Source IP Details

Source IP	Count
195.10.112.44	6638
66.177.1.152	6608
206.196.68.166	5443
161.109.100.250	4574
24.91.27.101	4072
67.96.113.140	2304
200.181.177.193	2010
151.24.188.80	1489
172.133.91.60	1311
203.121.0.9	1239
200.181.177.214	1207
65.112.51.216	1170
218.8.83.130	1160
68.46.68.173	1127
134.6.51.60	649
63.91.6.250	494
212.186.111.58	404
24.125.75.81	402
213.97.20.166	395
63.206.195.138	344

Top '20' Destination IP Details

Destination IP	Count
209.20.153.101	43272
209.20.153.105	5880
209.20.153.110	2603
209.20.153.100	258
209.20.153.102	142
209.20.153.104	118
209.20.153.108	116
209.20.153.106	96
209.20.153.109	85
209.20.153.99	77
0.0.0.0	74
209.20.153.107	56
209.20.153.98	48
*	23
64.4.12.138	11
209.20.130.35	6
10.0.10.10	6
199.183.74.19	3
10.0.5.10	2
63.111.13.100	2

Top '20' Source/Destination IP Pair Details

Source IP	Destination IP	Count
195.10.112.44	209.20.153.101	6638
66.177.1.152	209.20.153.101	6562
206.196.68.166	209.20.153.101	5443
161.109.100.250	209.20.153.101	4570
24.91.27.101	209.20.153.101	4072
67.96.113.140	209.20.153.101	2304
151.24.188.80	209.20.153.105	1489
172.133.91.60	209.20.153.101	1310
203.121.0.9	209.20.153.101	1239
65.112.51.216	209.20.153.101	1170
218.8.83.130	209.20.153.101	1160
68.46.68.173	209.20.153.101	1127
200.181.177.193	209.20.153.105	1005
200.181.177.193	209.20.153.110	1005
200.181.177.214	209.20.153.105	608
200.181.177.214	209.20.153.110	599
63.91.6.250	209.20.153.105	475
212.186.111.58	209.20.153.101	404
213.97.20.166	209.20.153.101	395
63.206.195.138	209.20.153.101	344

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.