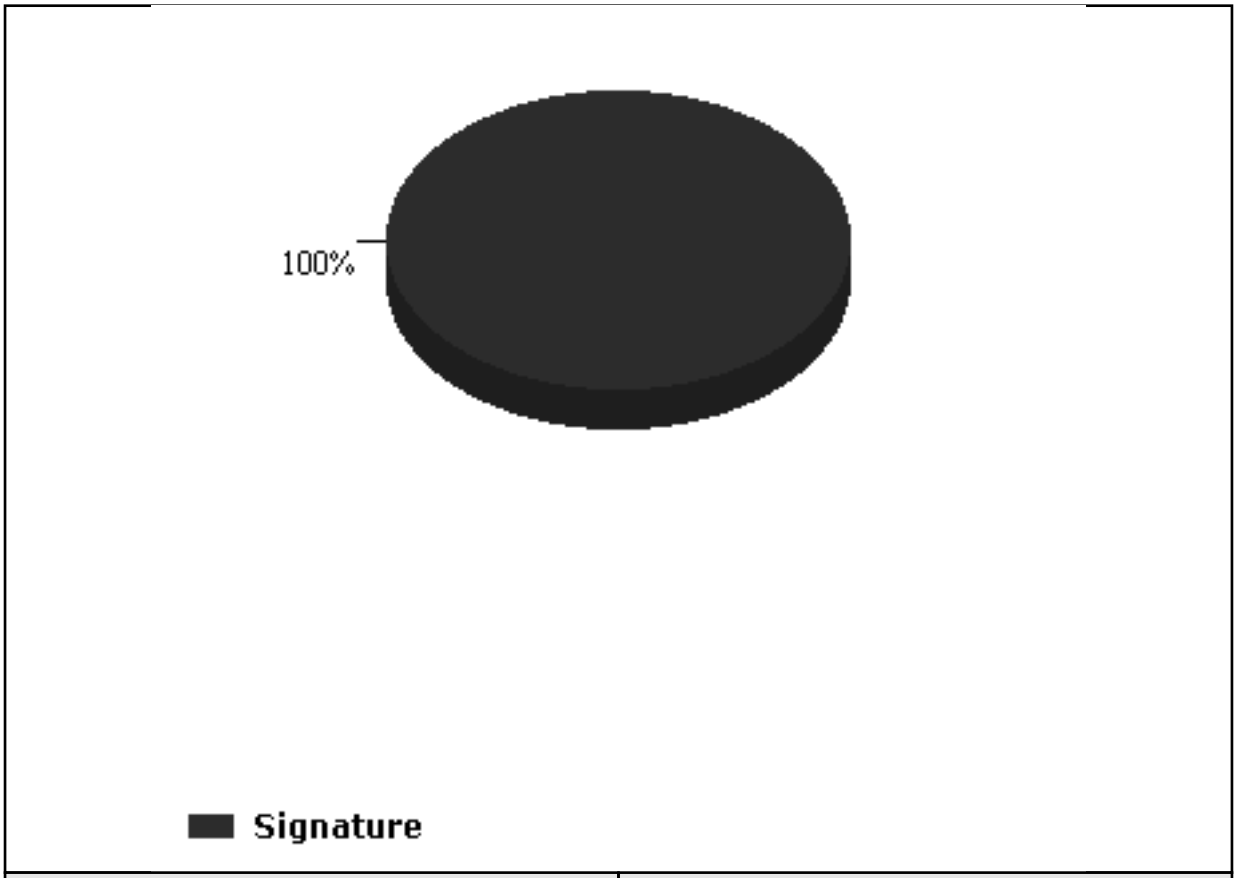
IntruShield™ IDS Report

EXECUTIVE SUMMARY REPORT

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

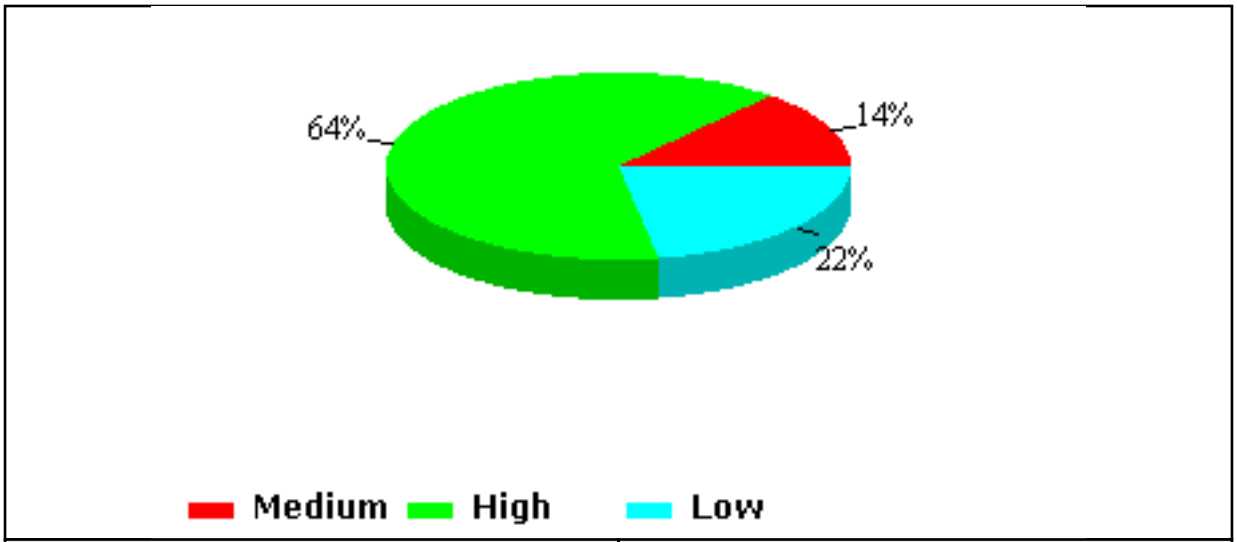
Total alerts detected by the sensor: 9613

Total Alerts Per Alert Type



Alert Type	Alerts Detected
Signature	9613

Total Alerts Per Severity



Attack Severity	Alerts Detected
Medium	1303
High	6161
Low	2149

Top '20' Alert Details

Alert Name	Alert Type	Severity	Count	Last Detected
HTTP: CGI EscapeCharacter DirectoryTraversal	Signature	High	1798	10-25-2002 18:46:39
HTTP: IIS CMD.EXE Execution	Signature	High	1394	10-25-2002 18:45:38
HTTP: IIS Command Execution	Signature	High	1287	10-25-2002 18:45:38
SNMP: Read Other Default Community String	Signature	Low	787	10-25-2002 15:10:32
unicode-utf8-too-long-encoding	Signature	High	665	10-25-2002 18:45:38
HTTP: Nimda Worm - IIS Extended Unicode Directory Travesal Attack	Signature	High	552	10-25-2002 18:45:37
HTTP: Abnomal %00 in Parameter	Signature	Low	307	10-25-2002 8:36:40
HTTP: Netscape Enterprise Server Index Disclosure	Signature	Low	249	10-24-2002 6:22:49
HTTP: CISCO HTTP Admin Authentication	Signature	Medium	167	10-24-2002 16:49:48
HTTP: Cross Site Script Attack	Signature	High	145	10-25-2002 18:46:2
HTTP: IIS 4.0 idc path disclosure	Signature	Low	122	10-25-2002 13:0:59
IPHdr-SrcDstInvalidAddress	Signature	Low	107	10-25-2002 5:24:23
HTTP: Read Password File Attempt	Signature	Medium	102	10-25-2002 18:45:16
TCPHdr-Ports-EqualZero	Signature	Low	94	10-23-2002 19:12:38
TCP-Illegal-FIN-Probe	Signature	Low	78	10-25-2002 19:57:54
TCPHdr-Flags-URGNoACK	Signature	Low	76	10-25-2002 19:31:24
HTTP: MISCROXEN Directorylist	Signature	Medium	67	10-25-2002 18:41:23
ICMP: Netmask Request	Signature	Low	65	10-25-2002 14:15:32
ICMP: Timestamp Probe	Signature	Low	64	10-25-2002 15:2:21
NMAP XMAS with SYN Probe	Signature	Medium	61	10-25-2002 19:31:24

Top '20' Source IP Details

Source IP	Count
195.10.112.44	6638
134.6.51.60	649
65.112.51.216	477
64.192.210.101	255
80.36.169.182	223
24.125.75.81	170
62.87.140.196	123
66.161.168.144	118
195.16.42.93	104
209.101.186.162	96
66.192.198.234	66
24.163.50.51	64
63.99.204.104	53
64.171.0.30	48
68.5.71.31	43
148.223.46.10	33
212.58.177.99	33
64.83.29.44	31
172.18.126.241	24
208.234.49.217	24

Top '20' Destination IP Details

Destination IP	Count
209.20.153.101	8337
209.20.153.105	554
209.20.153.110	364
209.20.153.100	64
209.20.153.102	61
209.20.153.104	59
209.20.153.109	59
209.20.153.108	58
209.20.153.106	44
209.20.153.99	4
209.20.153.107	4
209.20.153.98	4
64.4.12.138	1

Top '20' Source/Destination IP Pair Details

Source IP	Destination IP	Count
195.10.112.44	209.20.153.101	6638
65.112.51.216	209.20.153.101	477
64.192.210.101	209.20.153.101	255
80.36.169.182	209.20.153.101	223
24.125.75.81	209.20.153.110	170
134.6.51.60	209.20.153.101	166
66.161.168.144	209.20.153.105	118
62.87.140.196	209.20.153.105	105
195.16.42.93	209.20.153.101	104
134.6.51.60	209.20.153.105	97
209.101.186.162	209.20.153.101	96
134.6.51.60	209.20.153.110	94
66.192.198.234	209.20.153.110	66
24.163.50.51	209.20.153.101	64
134.6.51.60	209.20.153.104	55
134.6.51.60	209.20.153.109	55
134.6.51.60	209.20.153.108	54
134.6.51.60	209.20.153.102	53
63.99.204.104	209.20.153.105	53
68.5.71.31	209.20.153.105	43