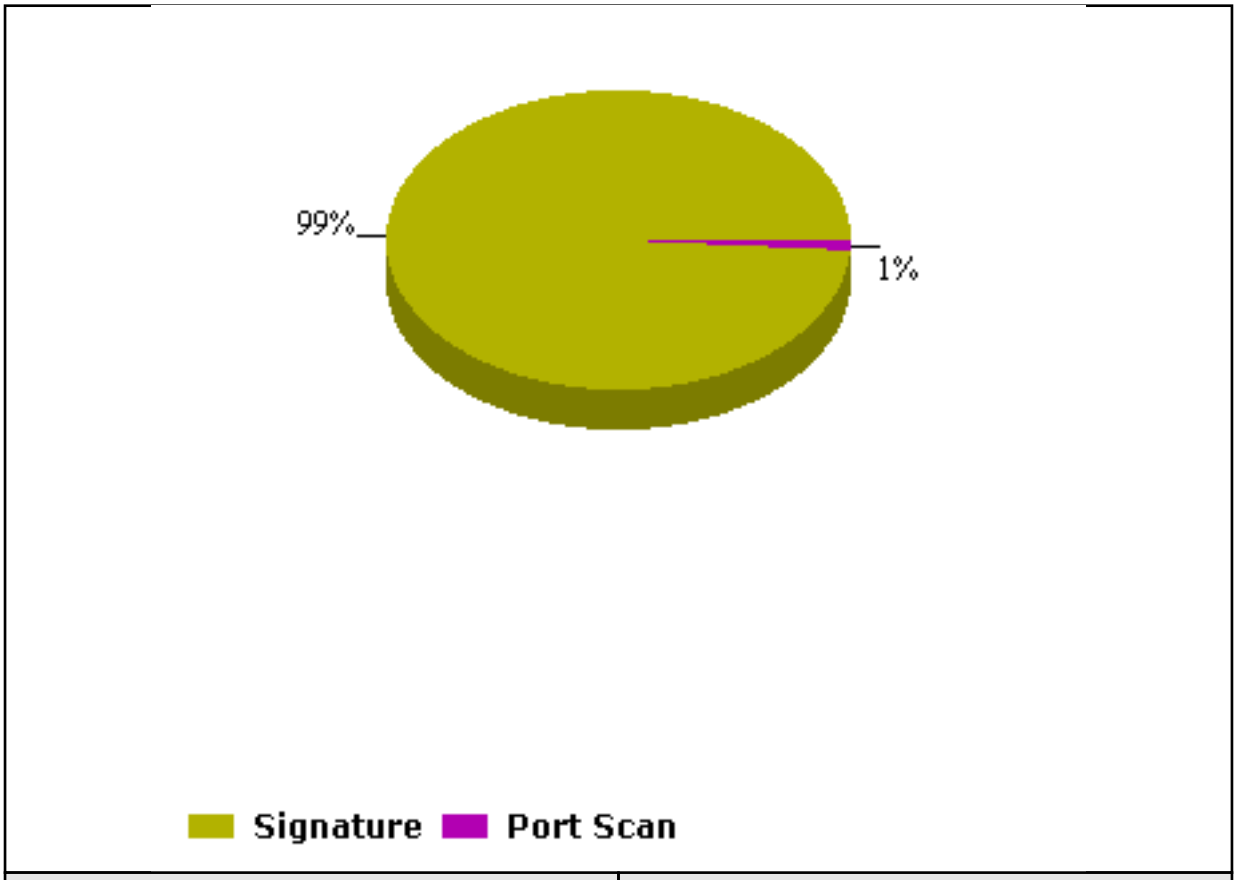
IntruShield™ IDS Report

EXECUTIVE SUMMARY REPORT

Admin Domain:	/eWEEK OpenHack 4 all
Sensor:	I2600
Alert Severity:	Low, Medium, High
Alert State:	All Alerts
Start Date:	Thu Oct 31 00:00:00 PST 2002
End Date:	Thu Oct 31 23:59:59 PST 2002

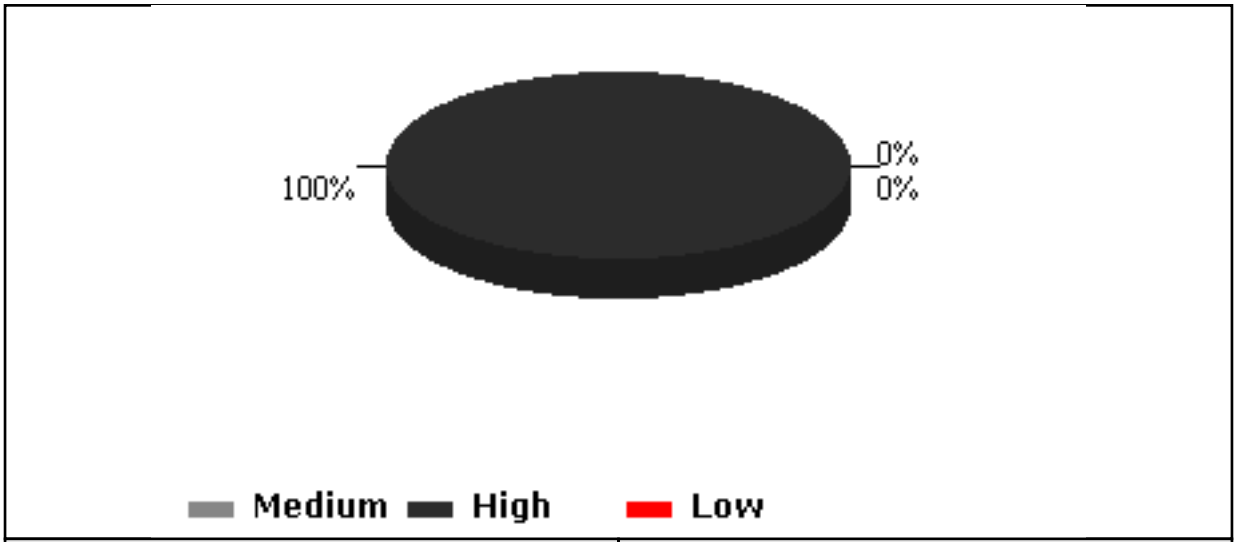
Total alerts detected by the sensor: 1211

Total Alerts Per Alert Type



Alert Type	Alerts Detected
Signature	1197
Port Scan	14

Total Alerts Per Severity



Attack Severity	Alerts Detected
Medium	0
High	1211
Low	0

Top '20' Alert Details

Alert Name	Alert Type	Severity	Count	Last Detected
SNMP: Read Other Default Community String	Signature	Low	540	11-4-2002 11:36:7
HTTP: CGI EscapeCharacter DirectoryTraversal	Signature	High	112	11-6-2002 20:14:31
SNMP: Cisco IOS Undocumented Community String	Signature	Medium	60	11-4-2002 11:36:7
HTTP: IIS Command Execution	Signature	High	46	11-6-2002 19:22:44
HTTP: IIS CMD.EXE Execution	Signature	High	45	11-6-2002 20:13:16
HTTP: Abnomal %00 in Parameter	Signature	Low	40	11-5-2002 21:18:12
SNMP: Read Public Community String	Signature		32	11-6-2002 11:39:27
RPC: Portmap Dump Request	Signature	Medium	30	11-2-2002 16:6:50
IPHdr-SrcDstInvalidAddress	Signature	Low	22	11-7-2002 3:16:36
HTTP: IIS 4.0 idc path disclosure	Signature	Low	19	11-6-2002 20:14:52
HTTP: Faxsurvey Execute Command	Signature	High	13	11-6-2002 20:12:57
TCP SYN port scan	Port Scan	Medium	13	11-6-2002 21:13:20
DNS: Invalid Field Value	Signature	Low	13	11-5-2002 16:45:17
HTTP: Nimda Worm - IIS Extended Unicode Directory Travesal Attack	Signature	High	13	11-6-2002 19:22:35
HTTP: Interpreter AccessAttempt	Signature	Medium	11	11-5-2002 21:20:32
unicode-utf8-too-long-encoding	Signature	High	10	11-6-2002 19:22:35
ORACLE: 9iAS PL/SQL OWA UTIL Unauthorized Stored Procedure Access Vulnerability	Signature	Medium	9	10-31-2002 3:15:11
ORACLE: 9iAS Unautheticated User Access To Sensitive Services Vulnerability	Signature	Medium	8	10-31-2002 3:15:17
HTTP: IIS multiple sample ASP script View File Attempt	Signature	Medium	8	11-6-2002 20:13:21
HTTP: Allaire JRun WEB-INF Disclosure	Signature	High	6	11-5-2002 21:5:59

Top '20' Source IP Details

Source IP	Count
200.181.177.193	670
212.186.111.58	404
161.109.100.250	41
161.109.100.20	24
220.82.1.136	13
66.2.65.8	12
63.151.3.233	11
168.156.250.33	8
65.211.58.5	6
220.76.134.183	5
220.75.249.42	4
165.230.240.114	3
212.170.197.26	2
66.92.239.164	2
65.209.235.11	2
204.155.166.29	2
198.151.130.145	1
192.234.12.115	1

Top '20' Destination IP Details

Destination IP	Count
209.20.153.101	522
209.20.153.105	350
209.20.153.110	335
209.20.153.100	3
209.20.153.99	1

Top '20' Source/Destination IP Pair Details

Source IP	Destination IP	Count
212.186.111.58	209.20.153.101	404
200.181.177.193	209.20.153.110	335
200.181.177.193	209.20.153.105	335
161.109.100.250	209.20.153.101	38
161.109.100.20	209.20.153.101	24
220.82.1.136	209.20.153.101	13
66.2.65.8	209.20.153.101	12
63.151.3.233	209.20.153.105	11
168.156.250.33	209.20.153.101	8
65.211.58.5	209.20.153.101	6
220.76.134.183	209.20.153.101	5
220.75.249.42	209.20.153.101	4
161.109.100.250	209.20.153.100	3
165.230.240.114	209.20.153.101	3
65.209.235.11	209.20.153.101	2
66.92.239.164	209.20.153.101	2
212.170.197.26	209.20.153.105	2
204.155.166.29	209.20.153.105	1
198.151.130.145	209.20.153.99	1
192.234.12.115	209.20.153.105	1