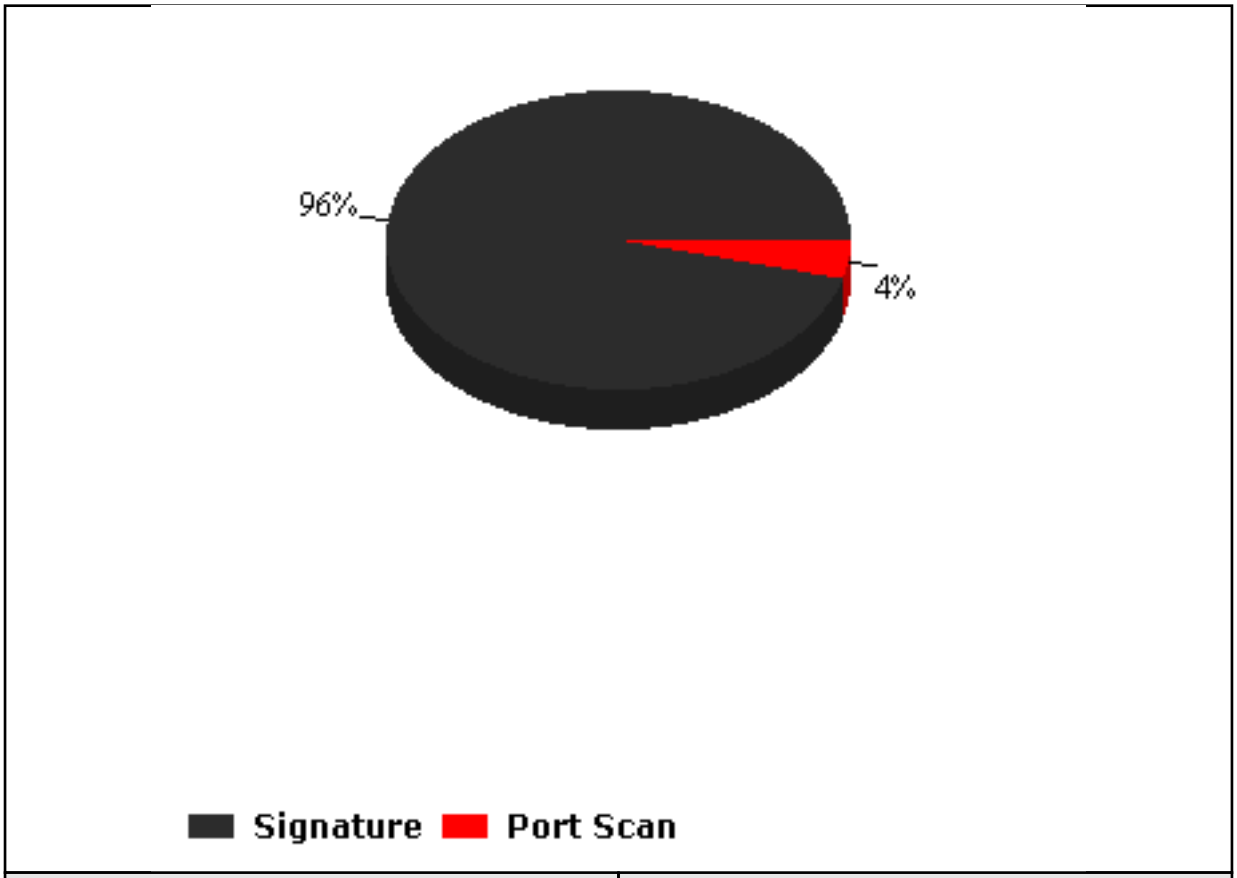
IntruShield™ IDS Report

EXECUTIVE SUMMARY REPORT

Admin Domain:	/eWEEK OpenHack 4 all
Sensor:	I2600
Alert Severity:	Low, Medium, High
Alert State:	All Alerts
Start Date:	Wed Nov 06 00:00:00 PST 2002
End Date:	Wed Nov 06 23:59:59 PST 2002

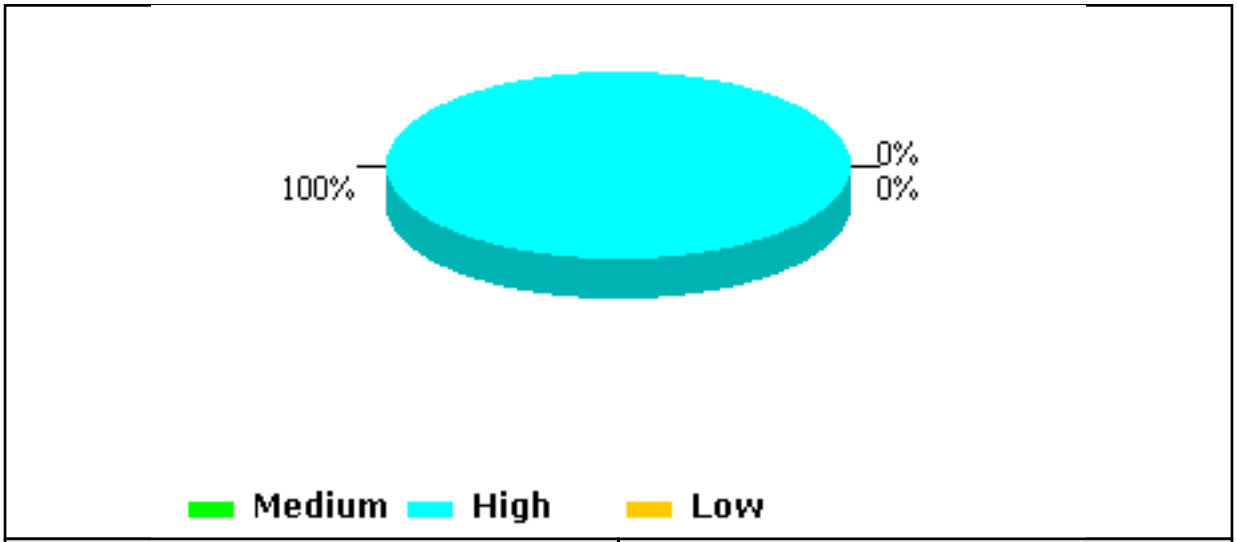
Total alerts detected by the sensor: 329

Total Alerts Per Alert Type



Alert Type	Alerts Detected
Signature	315
Port Scan	14

Total Alerts Per Severity



Attack Severity	Alerts Detected
Medium	0
High	329
Low	0

Top '20' Alert Details

Alert Name	Alert Type	Severity	Count	Last Detected
HTTP: CGI EscapeCharacter DirectoryTraversal	Signature	High	67	11-6-2002 20:14:31
HTTP: IIS Command Execution	Signature	High	29	11-6-2002 19:22:44
HTTP: IIS CMD.EXE Execution	Signature	High	26	11-6-2002 20:13:16
HTTP: Apache Win32 Directory Listing	Signature	Medium	17	11-6-2002 14:55:37
HTTP: Cobalt Raq Apache .htaccess Disclosure	Signature	Medium	15	11-6-2002 20:14:11
HTTP: IIS iisadmpwd Proxied Password Attack Attempt	Signature	Medium	13	11-6-2002 20:14:4
HTTP: IIS 4.0 idc path disclosure	Signature	Low	13	11-6-2002 20:14:52
TCP SYN port scan	Port Scan	Medium	9	11-6-2002 21:13:20
HTTP: Nimda Worm - IIS Extended Unicode Directory Travesal Attack	Signature	High	8	11-6-2002 19:22:35
HTTP: Phf Execute Arbitary Command	Signature	High	7	11-6-2002 20:12:53
HTTP: IIS multiple sample ASP script View File Attempt	Signature	Medium	7	11-6-2002 20:13:21
HTTP: IIS JET VBA Run Command Attempt	Signature	High	7	11-6-2002 20:14:15
TCPHdr-Flags-URGNoACK	Signature	Low	6	11-6-2002 13:9:48
TCP-Illegal-FIN-Probe	Signature	Low	6	11-6-2002 13:9:48
Scan: SYN FIN Based Probes	Signature	Low	6	11-6-2002 13:9:48
ORACLE: Application Server Printenv Information Disclosure	Signature	Low	6	11-6-2002 20:14:47
HTTP: Finger Leak User Info	Signature	Medium	5	11-6-2002 20:13:2
NMAP XMAS with SYN Probe	Signature	Medium	5	11-6-2002 13:9:48
NMAP XMAS Probe	Signature	Medium	5	11-6-2002 13:9:48
Scan: NULL Probe	Signature	Low	5	11-6-2002 13:9:48

Top '20' Source IP Details

Source IP	Count
24.208.179.93	113
68.46.68.173	79
209.246.65.152	42
216.112.42.62	34
209.101.84.213	23
213.73.198.69	15
213.23.10.202	6
148.100.223.223	4
148.100.215.128	3
163.118.155.101	2
61.56.85.61	2
208.41.236.144	2
216.251.169.203	1
207.76.125.69	1
64.29.214.250	1
195.29.64.85	1

Top '20' Destination IP Details

Destination IP	Count
209.20.153.101	324
209.20.153.100	4
209.20.153.105	1

Top '20' Source/Destination IP Pair Details

Source IP	Destination IP	Count
24.208.179.93	209.20.153.101	113
68.46.68.173	209.20.153.101	79
209.246.65.152	209.20.153.101	42
216.112.42.62	209.20.153.101	34
209.101.84.213	209.20.153.101	23
213.73.198.69	209.20.153.101	15
213.23.10.202	209.20.153.101	6
148.100.223.223	209.20.153.101	4
148.100.215.128	209.20.153.100	3
61.56.85.61	209.20.153.101	2
208.41.236.144	209.20.153.101	2
163.118.155.101	209.20.153.101	2
207.76.125.69	209.20.153.105	1
64.29.214.250	209.20.153.100	1
195.29.64.85	209.20.153.101	1
216.251.169.203	209.20.153.101	1