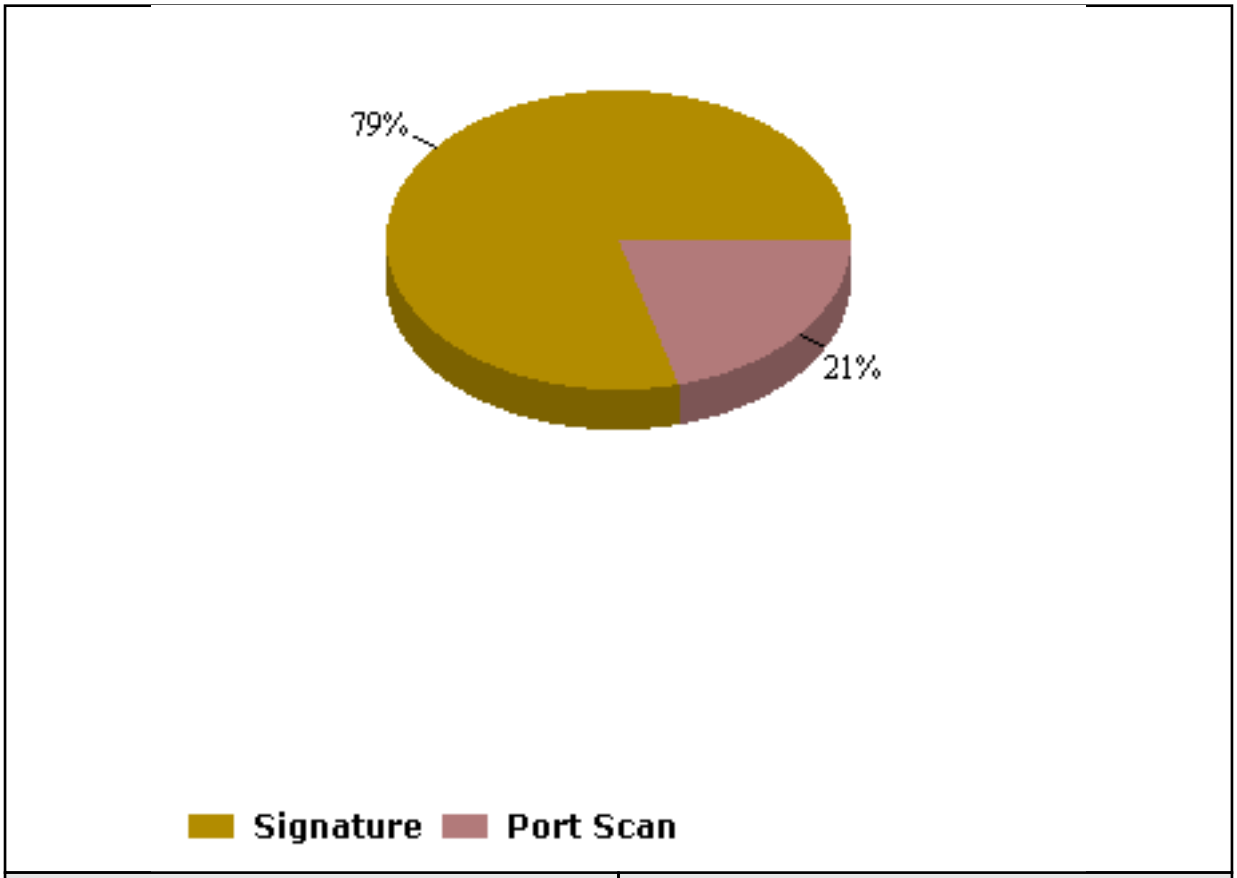
IntruShield™ IDS Report

EXECUTIVE SUMMARY REPORT

Admin Domain:	/eWEEK OpenHack 4 all
Sensor:	I2600
Alert Severity:	Low, Medium, High
Alert State:	All Alerts
Start Date:	Tue Oct 29 00:00:00 PST 2002
End Date:	Tue Oct 29 23:59:59 PST 2002

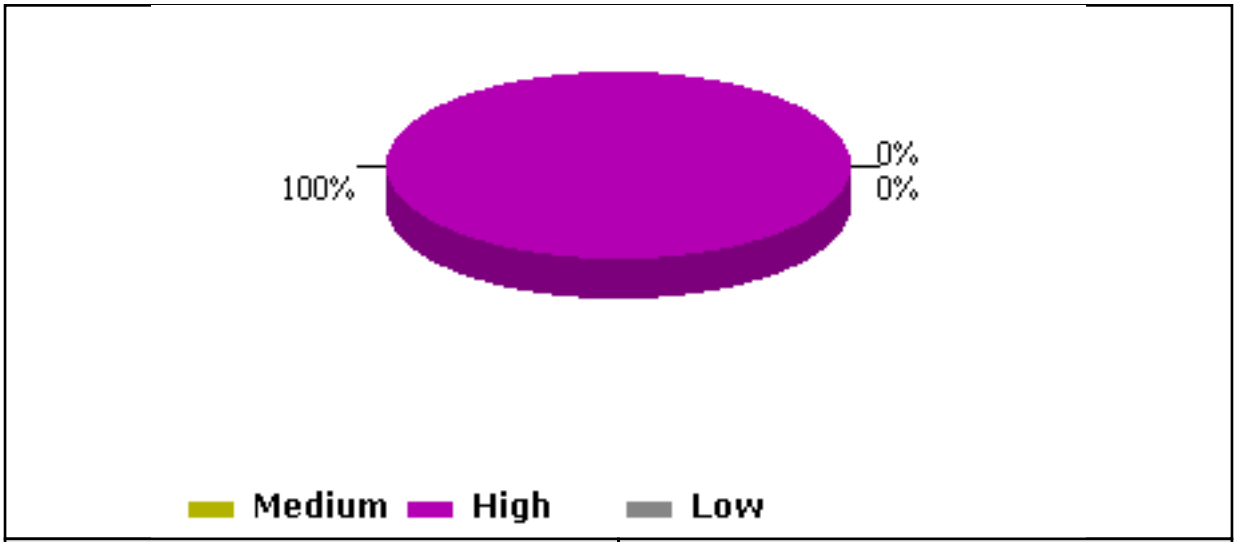
Total alerts detected by the sensor: 343

Total Alerts Per Alert Type



Alert Type	Alerts Detected
Signature	272
Port Scan	71

Total Alerts Per Severity



Attack Severity	Alerts Detected
Medium	0
High	343
Low	0

Top '20' Alert Details

Alert Name	Alert Type	Severity	Count	Last Detected
TCP SYN port scan	Port Scan	Medium	56	10-31-2002 14:24:24
SNMP: Read Other Default Community String	Signature	Low	56	10-30-2002 22:9:47
SNMP: Read Public Community String	Signature		44	10-31-2002 9:35:10
NMAP XMAS Probe	Signature	Medium	35	10-29-2002 17:3:41
IPHdr-SrcDstInvalidAddress	Signature	Low	33	10-31-2002 7:11:12
DNS: Invalid Field Value	Signature	Low	21	10-31-2002 14:23:25
HTTP: IIS Command Execution	Signature	High	16	10-31-2002 8:16:6
HTTP: IIS CMD.EXE Execution	Signature	High	14	10-31-2002 8:16:6
HTTP: CGI EscapeCharacter DirectoryTraversal	Signature	High	12	10-31-2002 14:23:42
TCP XMAS port scan	Port Scan	High	7	10-29-2002 10:4:25
UDP port scan	Port Scan	Medium	7	10-29-2002 20:46:0
DNS: BindVersionQuery	Signature	Medium	5	10-31-2002 7:57:13
HTTP: Nimda Worm - IIS Extended Unicode Directory Travesal Attack	Signature	High	5	10-31-2002 8:16:6
ICMP: Timestamp Probe	Signature	Low	4	10-31-2002 9:35:12
ICMP: Netmask Request	Signature	Low	4	10-31-2002 9:35:12
ORACLE: Application Server Default Page Server Information Leak	Signature	Low	3	10-31-2002 14:23:41
HTTP: Apache Win32 PHP.EXE Remote File Disclosure	Signature	High	3	10-31-2002 14:23:41
HTTP: MicrosoftFrontPage Shtml.exePathDisclosure	Signature	Medium	3	10-29-2002 9:30:26
TCP-Illegal-FIN-Probe	Signature	Low	2	10-31-2002 10:47:15
SNMP: Cisco IOS Undocumented Community String	Signature	Medium	2	10-30-2002 19:55:7

Top '20' Source IP Details

Source IP	Count
198.151.130.145	53
209.170.112.107	42
207.43.98.2	41
213.162.13.196	38
200.84.41.158	26
220.82.1.136	20
165.230.240.114	18
24.31.51.84	17
195.70.40.201	12
217.10.142.100	10
66.46.181.116	7
24.162.144.206	6
220.78.96.119	5
220.75.14.31	5
193.217.145.1	4
80.35.108.44	4
212.47.132.34	4
66.156.142.99	3
216.8.128.193	3
134.129.56.222	3

Top '20' Destination IP Details

Destination IP	Count
209.20.153.101	191
209.20.153.105	72
209.20.153.100	58
209.20.153.99	17
209.20.153.110	5

Top '20' Source/Destination IP Pair Details

Source IP	Destination IP	Count
209.170.112.107	209.20.153.101	42
207.43.98.2	209.20.153.105	41
213.162.13.196	209.20.153.100	38
198.151.130.145	209.20.153.101	28
200.84.41.158	209.20.153.101	26
220.82.1.136	209.20.153.101	20
165.230.240.114	209.20.153.101	18
24.31.51.84	209.20.153.101	17
198.151.130.145	209.20.153.99	17
195.70.40.201	209.20.153.101	12
217.10.142.100	209.20.153.100	10
198.151.130.145	209.20.153.105	8
66.46.181.116	209.20.153.100	7
24.162.144.206	209.20.153.101	6
220.78.96.119	209.20.153.101	5
220.75.14.31	209.20.153.101	5
193.217.145.1	209.20.153.105	4
80.35.108.44	209.20.153.105	4
66.156.142.99	209.20.153.105	3
220.75.249.42	209.20.153.101	3