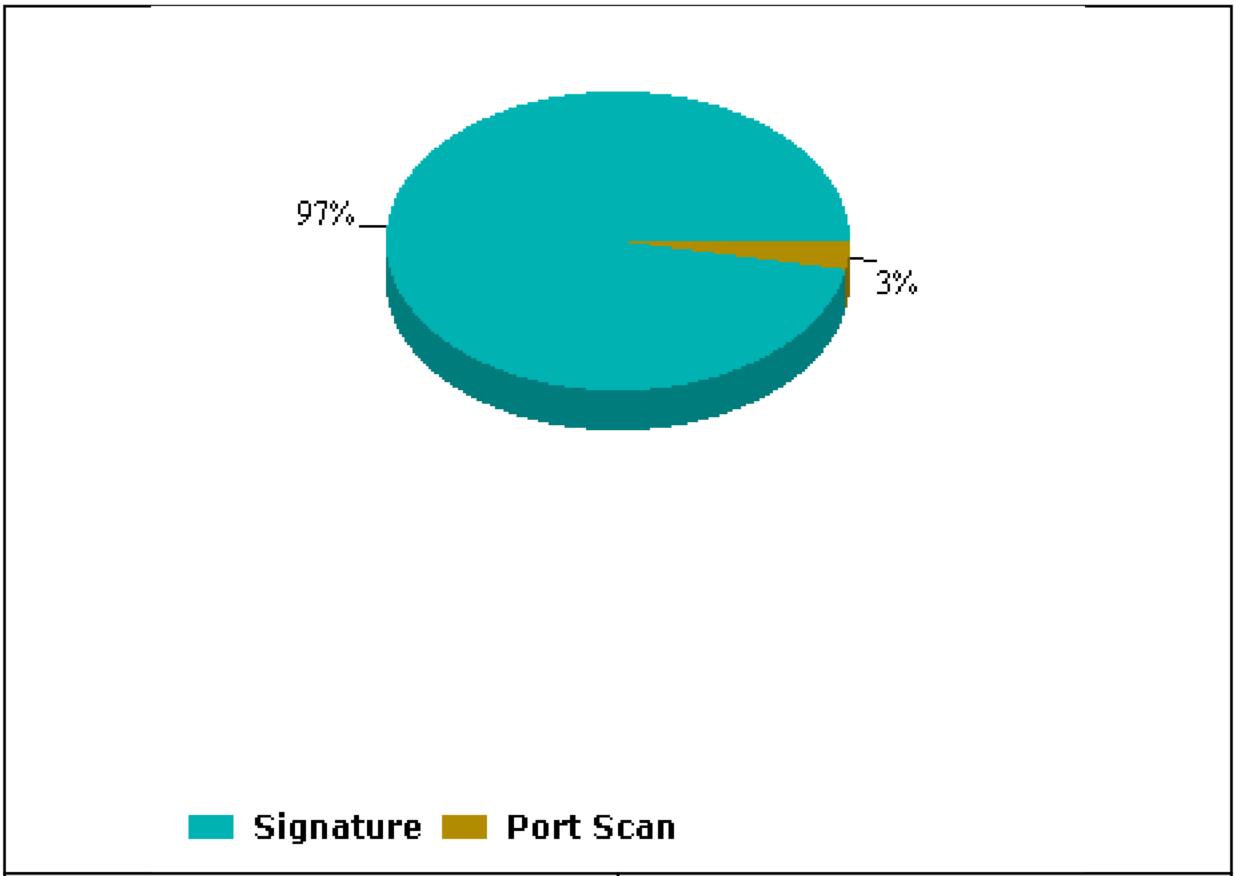
IntruShield™ IDS Report

# EXECUTIVE SUMMARY REPORT

| | |
|---|---|
| Admin Domain: | /eWEEK OpenHack 4 all |
| Sensor: | I2600 |
| Alert Severity: | Low, Medium, High |
| Alert State: | All Alerts |
| Start Date: | Sun Oct 27 00:00:00 PDT 2002 |
| End Date: | Sun Oct 27 23:59:59 PST 2002 |

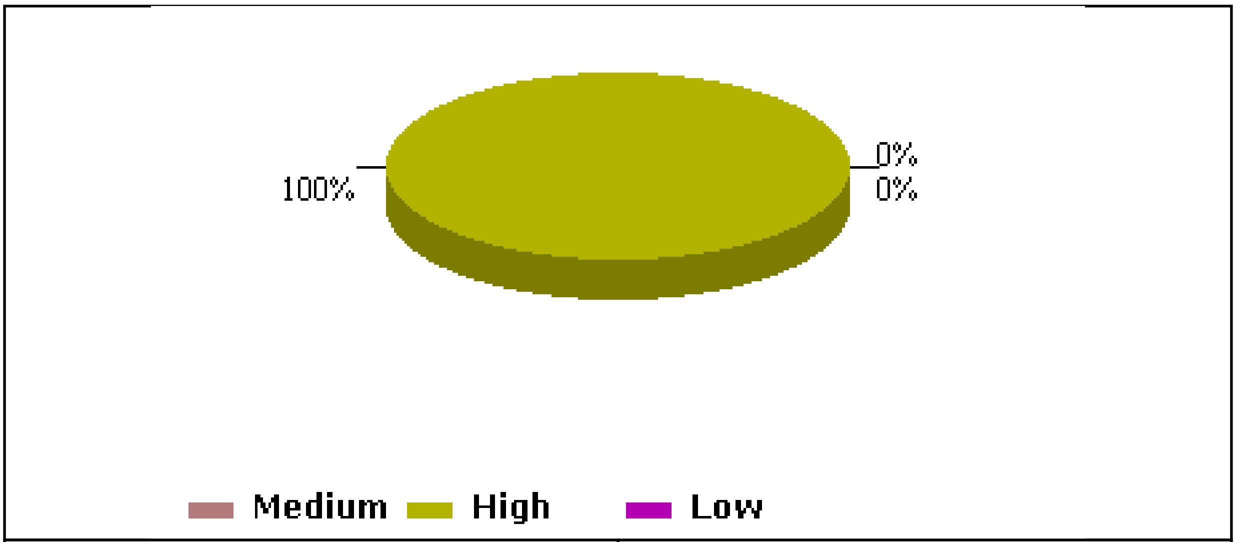
**Total alerts detected by the sensor:** 2103

## Total Alerts Per Alert Type



| Alert Type | Alerts Detected |
|---|---|
| Signature | 2039 |
| Port Scan | 64 |

## Total Alerts Per Severity



| Attack Severity | Alerts Detected |
|---|---|
| Medium | 0 |
| High | 2103 |
| Low | 0 |

# Top '20' Alert Details

| Alert Name | Alert Type | Severity | Count | Last Detected |
|---|---|---|---|---|
| HTTP: IIS CMD.EXE Execution | Signature | High | 401 | 10-31-2002 8:16:6 |
| HTTP: IIS Command Execution | Signature | High | 393 | 10-31-2002 8:16:6 |
| HTTP: CGI EscapeCharacter DirectoryTraversal | Signature | High | 369 | 10-31-2002 14:23:42 |
| unicode-utf8-too-long-encoding | Signature | High | 191 | 10-31-2002 8:16:6 |
| HTTP: Nimda Worm - IIS Extended Unicode Directory Travesal Attack | Signature | High | 135 | 10-31-2002 8:16:6 |
| TCP SYN port scan | Port Scan | Medium | 60 | 10-31-2002 14:24:24 |
| HTTP: IIS 4.0 idc path disclosure | Signature | Low | 54 | 10-31-2002 7:55:59 |
| HTTP: URI Too Long | Signature | Medium | 34 | 10-30-2002 6:23:18 |
| HTTP: Abnomal %00 in Parameter | Signature | Low | 33 | 10-31-2002 3:18:56 |
| HTTP: Netscape Directory Indexing Browse Directory | Signature | Medium | 18 | 10-30-2002 11:39:1 |
| TFTP: WriteFile Attempt | Signature | High | 16 | 10-27-2002 21:14:33 |
| DNS:  Invalid Field Value | Signature | Low | 15 | 10-31-2002 14:23:25 |
| HTTP: ExpressionCalculator InputValidation | Signature | Medium | 15 | 10-31-2002 3:9:1 |
| HTTP: Cobalt Raq Apache .htaccess Disclosure | Signature | Medium | 13 | 10-31-2002 7:56:11 |
| SNMP: Read Other Default Community String | Signature | Low | 13 | 10-30-2002 22:9:47 |
| HTTP: IISHACK - IIS ISM.DLL BufferOverflow | Signature | High | 12 | 10-30-2002 6:21:48 |
| Scan: Amanda Client Version Probe | Signature | Low | 12 | 10-30-2002 20:3:2 |
| SNMP: Read Public Community String | Signature | &nbsp; | 12 | 10-31-2002 9:35:10 |
| ICMP:  Timestamp Probe | Signature | Low | 10 | 10-31-2002 9:35:12 |
| HTTP: IIS multiple sample ASP script View File Attempt | Signature | Medium | 10 | 10-31-2002 3:17:48 |

## Top '20' Source IP Details

| Source IP | Count |
|---|---|
| 172.133.91.60 | 1311 |
| 66.75.181.155 | 301 |
| 202.156.83.133 | 222 |
| 24.27.30.3 | 40 |
| 80.13.76.147 | 34 |
| 66.68.87.36 | 33 |
| 68.128.12.228 | 24 |
| 202.156.2.154 | 20 |
| 24.247.13.96 | 19 |
| 172.168.61.175 | 18 |
| 24.161.241.126 | 17 |
| 24.243.183.82 | 16 |
| 66.188.135.37 | 13 |
| 193.252.205.189 | 10 |
| 12.251.6.163 | 3 |
| 80.202.212.211 | 3 |
| 217.134.31.90 | 3 |
| 68.47.192.14 | 3 |
| 216.56.44.13 | 2 |
| 210.90.201.253 | 2 |

## Top '20' Destination IP Details

| Destination IP | Count |
|---|---|
| 209.20.153.101 | 1967 |
| 209.20.153.105 | 133 |
| 209.20.153.100 | 3 |

# Top '20' Source/Destination IP Pair Details

| Source IP | Destination IP | Count |
|---|---|---|
| 172.133.91.60 | 209.20.153.101 | 1310 |
| 66.75.181.155 | 209.20.153.101 | 301 |
| 202.156.83.133 | 209.20.153.101 | 222 |
| 24.27.30.3 | 209.20.153.105 | 40 |
| 80.13.76.147 | 209.20.153.101 | 34 |
| 66.68.87.36 | 209.20.153.105 | 33 |
| 68.128.12.228 | 209.20.153.101 | 24 |
| 202.156.2.154 | 209.20.153.101 | 20 |
| 24.247.13.96 | 209.20.153.101 | 19 |
| 172.168.61.175 | 209.20.153.105 | 18 |
| 24.161.241.126 | 209.20.153.105 | 17 |
| 24.243.183.82 | 209.20.153.105 | 16 |
| 66.188.135.37 | 209.20.153.101 | 13 |
| 193.252.205.189 | 209.20.153.101 | 10 |
| 217.134.31.90 | 209.20.153.100 | 3 |
| 80.202.212.211 | 209.20.153.105 | 3 |
| 68.47.192.14 | 209.20.153.105 | 3 |
| 12.251.6.163 | 209.20.153.101 | 3 |
| 220.78.34.16 | 209.20.153.101 | 2 |
| 141.149.32.15 | 209.20.153.101 | 2 |