Signature Based Rules

*Inclusive always on upper bound

Rule 1:

Destination IP from 10.1.4.12 to 10.11.27.189

Malspam

Rule 2:

Destination IP from 10.11.27.189 to 10.65.162.98

JexBoss Exploit

Rule 3:

Destination IP greater than 10.65.162.98
Source IP from 10.0.8.99 to 10.11.27.189

Malspam

Rule 4:

Destination IP greater than 10.65.162.98
Source IP from 10.11.27.189 to 10.65.162.98

JexBossExploit

Rule 5:

Destination IP greater than 10.65.162.98
Source IP from 10.65.162.98 to 123.232.95.208
Destination Port less than 7704
Source Port less than 5050

W32/SdbotInfected

Rule 6:

Destination IP greater than 10.65.162.98
Source IP greater than 178.144.255.150
Destination Port less than 7704
Source Port less than 5050

W32/SdbotInfected

Rule 7:

Destination IP greater than 10.65.162.98
Source IP greater than 10.65.162.98
Destination port less than 54900
Source Port from 54900 to 55479

NeutrinoExploit

Rule 8:

Destination IP from 10.65.162.98 to 147.31.121.65
Source IP greater than 10.65.162.98
Destination port less than 54900
Source Port greater than 58971

PacketInjection

Rule 9:

Destination IP greater than 10.65.162.98
Source IP greater than 10.65.162.98
Destination Port from 54900 to 55479

NeutrinoExploit

Rule 10:

Destination IP greater than 10.65.162.98
Source IP from 10.65.162.98 to 147.31.121.65
Destination port greater than 58970

PacketInjection

Anomaly-Based Rules

*Inclusive always on upper bound

Rule 1:

Destination Port less than 1134
Source Port less than 80
Destination IP less than 194.171.20.235
Source IP less than 192.168.8.199

Abnormal

Rule 2:

Source IP from 10.0.8.99 to 67.64.162.135

Source Port less than 53
Destination Port from 49206 to 54900
Destination IP less than 194.171.20.235

Abnormal

Rule 3:

Source IP from 67.64.162.135 to 192.168.8.199
Destination Port from 49206 to 54900
Source Port less than 80
Destination IP less than 194.171.20.235

Abnormal

Rule 4:

Source Port from 80 to 1134 81:1134
Destination Port less than 80
Destination IP less than 194.171.20.235
Source IP less than 192.168.8.199

Abnormal

Rule 5:

Source IP from 10.0.8.99 to 192.168.8.199
Destination Port less than 53
Destination IP less than 67.64.162.135
Source Port from 49206 to 54900

Abnormal

Rule 6:

Destination IP from 67.64.162.135 to 194.171.20.235
Source Port from 49206 to 54900
Destination Port less than 80
Source IP less than 192.168.8.199

Abnormal

Rule 7:

Destination IP from 190.213.190.227 to 194.171.20.235
Destination Port from 445 to 2553
Source Port from 80 to 54900
Source IP less than 192.168.8.199

Abnormal

Rule 8:

Source IP from 178.144.255.150 to 192.168.8.199
Destination Port from 2553 to 5050
Source Port from 80 to 54900
Destination IP less than 194.171.20.235

Abnormal

Rule 9:

Source Port less than 1134
Destination IP greater than 194.171.20.235
Source IP less than 192.168.8.199
Destination Port less than 54900

Abnormal

Rule 10:

Source IP less than 89.34.83.17
Source Port from 32682 to 54900
Destination IP greater than 194.171.20.235
Destination Port less than 54900

Abnormal

Rule 11:

Source Port from 54900 to 55479
Source IP less than 192.168.8.199
Destination Port less than 54900

Abnormal

Rule 12:

Source Port from 58971 to 59362
Source IP less than 192.168.8.199
Destination port less than 54900

Abnormal

Rule 13:

Destination Port less than 1134

Source IP from 192.168.8.199 to 203.140.17.26

Abnormal

Rule 14:

Destination Port from 29464 to 54900
Source IP from 192.168.8.199 to 203.140.17.26

Abnormal

Rule 15:

Destination IP less than 89.34.82.17
Source IP greater than 212.8.166.151
Destination Port less than 54900

Abnormal

Rule 16:

Destination IP greater than 178.144.255.150
Source IP greater than 203.140.17.26
Destination port less than 54900

Abnormal

Rule 17:

Destination Port from 54900 to 55479

Abnormal

Rule 18:

Destination Port from 58971 to 59362
Destination IP less than 192.168.8.199

Abnormal

Rule 19:

Destination IP greater than 192.168.8.199
Destination Port greater than 55479

Abnormal