Snorby

Daily Security Report

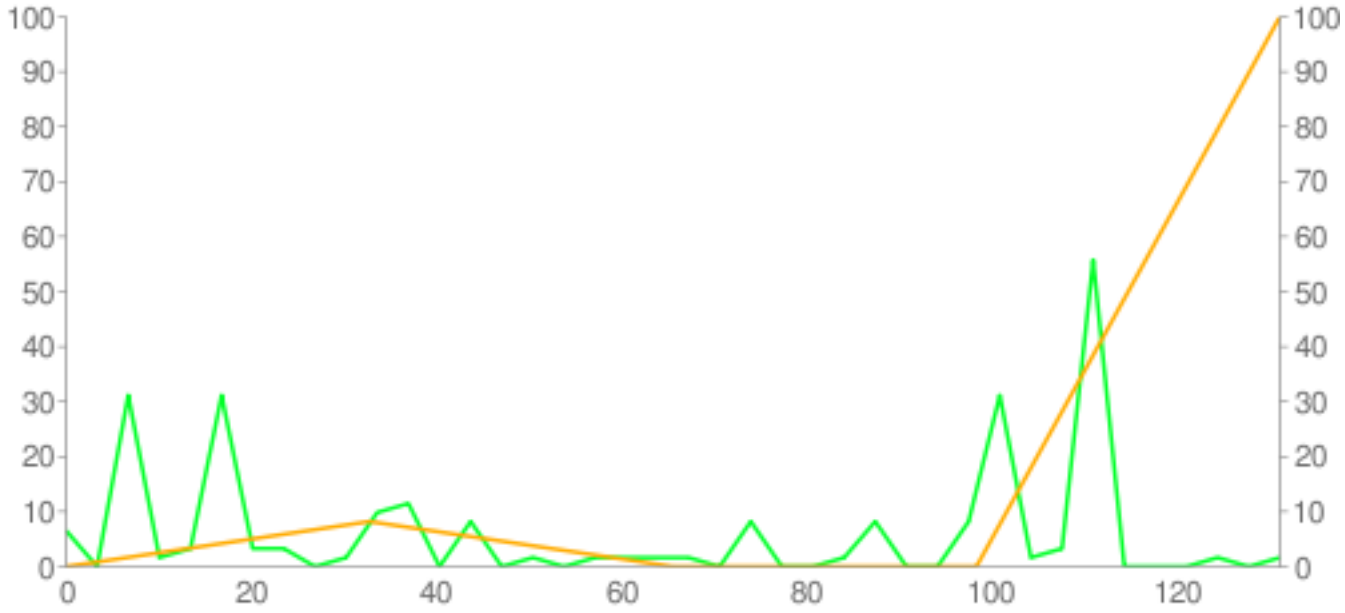
This report was generated: Monday, July 06, 2009

Daily Report Summary

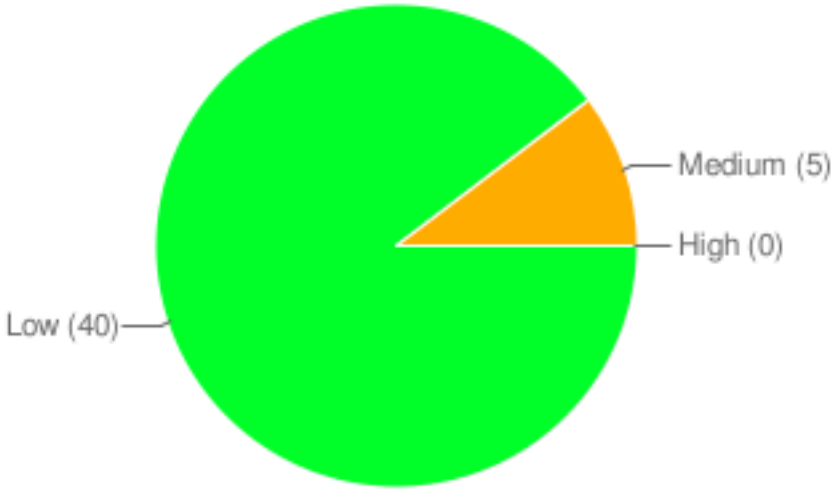
Event Severity Summary

Low Severity	Medium Severity	High Severity	Total Event Count
40	5	0	507

Event Severity vs Sessions



Event Severity



Medium Severity

Event Name	Sensor ID	Source Address	Destination Address	Session Count
DNS SPOOF query response with TTL of 1 min. and no authority	1	10.1.1.210	10.4.1.10	1
ICMP L3retriever Ping	1	10.1.1.47	10.4.1.10	11
WEB-CGI wrap access	1	10.4.1.10	157.166.224.31	1
WEB-CGI wrap access	2	10.4.1.11	157.166.224.31	1
DNS SPOOF query response with TTL of 1 min. and no authority	1	10.1.1.20	10.4.1.10	131

Low Severity

Event Name	Sensor ID	Source Address	Destination Address	Session Count
(portscan) Open Port	1	10.4.1.10	10.1.1.130	9
(portscan) Open Port	1	10.4.1.10	213.225.74.236	1
(portscan) Open Port	1	10.4.1.10	93.186.193.46	41
(portscan) Open Port	1	10.4.1.10	205.188.9.91	4
(portscan) Open Port	1	10.4.1.10	72.14.247.111	5
ICMP Destination Unreachable Port Unreachable	1	10.4.1.254	10.4.1.10	41
(portscan) Open Port	1	10.4.1.10	72.14.247.109	5
(portscan) Open Port	1	10.0.1.9	75.127.77.214	5
(portscan) TCP Portsweep	1	10.4.1.10	173.45.230.150	1
(portscan) Open Port	1	10.4.1.10	74.125.95.121	3
ICMP Destination Unreachable Port Unreachable	2	10.4.1.254	10.4.1.11	15
(portscan) Open Port	1	10.4.1.10	174.36.30.10	17
(portscan) UDP Portsweep	1	10.4.1.10	10.4.1.254	1
(portscan) Open Port	1	10.4.1.10	168.143.162.100	12
(portscan) TCP Portsweep	1	10.4.1.10	168.143.162.100	1
(portscan) Open Port	1	10.4.1.10	128.121.146.100	4
(portscan) Open Port	1	10.0.1.9	209.85.201.125	1
(portscan) Open Port	1	10.4.1.10	74.125.95.113	4
(portscan) Open Port	1	10.4.1.10	168.143.162.68	4
(portscan) Open Port	1	10.4.1.10	174.36.30.66	3

Copyright (c) Snorby.org

Event Name	Sensor ID	Source Address	Destination Address	Session Count
(portscan) TCP Portscan	1	10.1.1.47	10.4.1.10	3
(portscan) Open Port	1	10.4.1.10	199.212.0.43	1
(portscan) Open Port	1	10.4.1.10	74.125.95.102	12
(portscan) Open Port	1	10.0.1.9	205.188.251.44	1
(portscan) TCP Portsweep	1	10.0.1.9	72.128.11.55	1
(portscan) Open Port	1	10.4.1.10	74.125.95.17	3
ICMP PING	1	10.1.1.47	10.4.1.10	11
(portscan) Open Port	1	10.4.1.10	74.125.95.100	2
(portscan) TCP Portsweep	1	10.4.1.10	65.74.177.129	1
ICMP Echo Reply	1	10.4.1.10	10.1.1.47	11
ICMP Destination Unreachable Port Unreachable	1	10.4.1.10	10.1.1.47	42
(portscan) Open Port	1	10.4.1.10	65.74.177.129	3
(portscan) Open Port	1	10.4.1.10	130.237.188.200	6
ICMP Destination Unreachable Communication Administratively Prohibited	1	72.128.11.55	10.4.1.10	75
ICMP Destination Unreachable Port Unreachable	1	10.0.1.1	10.0.1.9	1
ICMP Destination Unreachable Port Unreachable	1	10.0.1.9	10.0.1.1	2
(portscan) Open Port	1	10.0.1.9	205.188.9.91	1
(portscan) Open Port	1	10.0.1.9	168.143.162.100	4
(portscan) Open Port	1	10.4.1.10	76.74.9.18	2
(portscan) Open Port	1	10.4.1.10	64.233.169.125	3

Copyright (c) Snorby.org