Port Scan Detector Output File

Simon Targa Mirko Bez

January 11, 2016

Contents

1 List of potential attackers

ICMP, UDP, IP, UK (Unknown), TCP indicate the number of the packets of that type received.

ID	IP Address	First Packet	Last Packet	ICMP	UDP	IP	UK	TCP
1	127.0.0.1	11.01.16 15:58:27	11.01.16 15:58:34	0	0	0	0	10240

2 TCP Details

SYN, FIN, XMAS, NULL, ACK, UK (Unkown) indicate the number of the tcp packets of that type received.

ID	IP	TCP	SCAN DETECTED	SYN	FIN	XMAS	NULL	ACK	MAIMON	UK
1	127.0.0.1	10240	9	0	3072	0	0	0	2048	5120

2.1 Type of TCP SCAN DETECTED

IP-Address	SYN	XMAS	ACK	MAIMON	NULL	FIN	UK	TCP
127.0.0.1	0	0	0	4	0	5	9	9

3 UDP Details

ID	IP-Address	SCAN DETECTED	TOTAL SCORE
1	127.0.0.1	0	0

4 Summary

List containing the result and some meta data

Filter Expression	dst host 127.0.0.1
Device used	lo
Number of TCP scan detected	9
Number of different scanners	1
Number of different sources (i.e. # potential attackers)	1
Number of received packets	10241
Scan begin	Mon Jan 11 15:58:23 2016
Scan end	Mon Jan 11 15:58:35 2016
Total Elapsed time	12 seconds