

Port Scan Detector Output File

Simon Targa

Mirko Bez

January 11, 2016

Contents

1	List of potential attackers	2
2	TCP Details	2
2.1	Type of TCP SCAN DETECTED	2
3	UDP Details	2
4	Summary	2
5	TCP PORT FREQUENCY	3
6	UDP PORT FREQUENCY	4

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	192.168.43.1	11.01.16 13:55:27	11.01.16 13:56:12	0	2844	0	0	0

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	192.168.43.1	0	0	0	0	0	0	0	0	0

2.1 Type of TCP SCAN DETECTED

IP-Address	SYN	XMAS	ACK	MAIMON	NULL	FIN	UK	TCP
192.168.43.1	0	0	0	0	0	0	0	0

3 UDP Details

ID	IP-Address	SCAN DETECTED	TOTAL SCORE
1	192.168.43.1	17	2844

4 Summary

List containing the result and some meta data

Filter Expression	dst host 192.168.43.65
Device used	wlan0
Number of TCP scan detected	0
Number of different scanners	0
Number of different sources (i.e. # potential attackers)	1
Number of received packets	2848
Scan begin	Mon Jan 11 13:55:24 2016
Scan end	Mon Jan 11 13:56:15 2016
Total Elapsed time	51 seconds

5 TCP PORT FREQUENCY

List of the tcp port visited from the single host and the times

ID	IP	TOT TCP	PORT	TIMES
1	192.168.43.1	0		

6 UDP PORT FREQUENCY

List of the tcp port visited from the single host and the times

ID	IP	TOT UDP	PORT	TIMES	ID	IP	TOT TCP	PORT	TIMES
1	192.168.43.1	2844	34860	4				59087	1
			59879	1				34019	1
			55690	1				39420	1
			54523	1				46308	1
			46095	4				53158	4
			46922	1				54127	4
			45922	4				33891	1
			41142	1				59269	1
			49912	2				43482	1
			38586	4				54970	1
			48773	1				56502	4
			36375	1				33570	4
			48572	4				48228	1
			45191	8				48633	1
			52110	4				53366	1
			40492	4				53046	1
			55678	1				50872	4
			40292	1				54655	4
			36662	1				56091	1
			47157	1				48001	1
			60882	4				54359	1
			42698	4				52078	1
			36241	1				34039	4
			46082	1				40579	4
			57480	1				47615	1
			48736	1				48373	1
			41961	4				60185	1
			54656	4				42094	1
			57940	5				39175	4
			43224	1				57500	4
			46505	1				56955	1
			38889	1				44750	1
			35442	4				59303	1
			40297	4				41591	1
			44742	1				47926	4
			38972	1				43556	4
			40562	1				46404	1
			48246	1				51778	1
			60234	4				38073	1
			35291	4				50697	4

ID	IP	TOT TCP	PORT	TIMES
			40690	4
			59715	1
			59547	1
			43911	1
			56297	2
			39972	4
			38300	4
			54546	1
			34066	1
			50883	1
			41805	1
			50404	4
			50236	4
			56646	1
			60616	1
			54840	1
			49624	1
			46821	4
			37993	4
			39667	1
			42517	1
			56360	1
			48391	1
			43664	4
			46326	4
			59450	4
			51762	1
			36172	1
			36548	4
			49316	1
			52465	1
			51543	1
			46264	4
			52389	1
			52333	1
			37942	4
			51879	1
			58554	4
			46731	4
			48817	4

ID	IP	TOT TCP	PORT	TIMES
			43303	4
			32774	1
			41057	1
			36474	4
			56999	1
			45282	4
			53939	1
			42494	1
			44538	4
			46454	1
			48881	1
			51953	4
			37394	1
			52639	1
			50834	4
			38026	1
			41521	4
			57533	1
			36995	2
			53374	4
			50809	4
			48223	1
			57342	1
			58530	1
			54235	1
			52514	4
			52341	4
			53025	1
			49560	1
			58401	1
			55083	1
			55763	4
			53942	4
			40230	1
			37372	1
			36287	1
			60719	1
			44023	4
			53525	4
			40644	1

ID	IP	TOT TCP	PORT	TIMES
			43825	1
			60200	1
			39853	1
			60827	4
			40066	4
			47150	1
			37005	5
			43808	1
			37986	1
			38281	4
			44326	4
			60809	1
			53582	1
			52991	1
			57817	1
			42693	4
			54475	4
			46120	1
			52425	1
			38430	1
			53675	1
			37489	4
			47307	4
			54088	1
			44087	1
			38321	1
			57999	1
			34516	4
			39673	4
			36134	1
			37459	1
			49530	1
			56303	1
			44600	4
			41994	4
			41569	1
			32833	1
			37900	1
			42669	1
			47427	4

ID	IP	TOT TCP	PORT	TIMES
			36355	4
			49220	1
			60082	1
			40939	1
			34807	1
			39248	4
			41384	4
			39471	1
			58103	1
			42461	1
			45909	1
			46029	4
			42301	4
			48231	1
			44968	1
			35047	1
			54558	1
			57199	4
			44382	4
			36501	4
			46259	1
			59043	1
			43520	4
			34370	1
			51799	1
			55107	4
			50525	1
			40490	1
			51057	4
			41180	1
			49866	1
			34108	5
			39195	4
			38362	4
			59286	1
			55809	1
			57405	1
			54476	1
			47697	4
			44296	4

ID	IP	TOT TCP	PORT	TIMES
			35131	1
			37598	1
			41761	1
			40857	1
			46784	4
			54360	4
			42304	1
			48304	1
			51540	2
			56593	1
			33192	4
			35759	4
			48799	1
			35744	2
			58819	1
			43083	1
			36411	4
			56663	4
			53312	2
			35070	1
			51366	1
			56034	1
			43201	4
			36176	4
			34661	1
			57660	1
			52891	1
			34315	1
			45036	4
			47262	4
			48360	1
			35505	1
			37614	1
			35497	1
			57783	4
			48648	4
			42082	1
			34481	1
			33101	1
			47378	1

ID	IP	TOT TCP	PORT	TIMES
			40313	4
			36075	4
			35437	1
			38490	1
			51279	1
			46014	1
			45459	4
			54162	4
			37517	1
			46190	1
			55889	1
			47143	1
			57616	4
			60583	4
			53294	1
			60452	1
			44807	1
			46205	1
			54702	4
			52677	4
			35122	1
			51686	1
			53004	1
			47529	1
			50262	4
			36027	4
			59460	1
			47891	1
			50206	1
			45721	1
			36956	4
			35270	4
			35634	1
			35258	1
			48294	1
			51129	1
			36605	4
			51017	4
			44529	8
			42212	4

ID	IP	TOT TCP	PORT	TIMES
			49946	1
			40114	1
			43675	1
			41461	1
			45055	1
			58866	1
			37893	1
			58461	4
			55629	4
			59011	4
			55364	4
			35432	1
			57025	1
			55014	1
			58150	1
			49155	4
			60674	4
			35480	1
			42048	1
			44206	1
			58083	1
			54215	4
			41236	4
			33222	4
			49763	1
			50895	1
			35687	4
			36386	1
			56591	1
			58391	1
			51896	4
			53866	1
			35322	1
			53517	4
			56134	1
			42653	1
			44064	4
			41535	1
			36881	1
			41795	1

ID	IP	TOT TCP	PORT	TIMES
			46837	4
			55413	2
			40486	1
			60189	4
			57536	1
			60209	1
			42481	4
			53667	1
			48127	1
			57100	4
			46138	1
			46179	1
			39918	4
			51961	1
			50859	4
			59350	1
			58172	1
			45764	1
			35227	4
			39473	1
			43195	1
			44654	5
			51875	4
			55499	4
			56345	1
			60269	1
			56926	1
			35600	1
			49578	4
			56868	4
			34143	1
			37610	1
			54090	1
			38702	1
			47611	4
			56526	4
			58233	1
			58147	1
			34831	1
			51567	1

ID	IP	TOT TCP	PORT	TIMES
			45465	4
			54312	4
			48097	1
			42111	1
			37419	1
			40904	1
			57401	5
			54157	4
			35500	1
			55564	1
			48073	1
			52847	1
			42267	4
			51293	4
			59913	1
			36318	1
			39370	1
			57888	1
			37200	4
			43650	4
			37454	1
			40498	1
			32890	1
			34285	1
			44201	4
			59197	4
			52123	1
			44283	1
			37004	1
			46938	1
			57135	4
			36440	4
			59402	1
			55577	1
			39366	1
			50683	1
			55423	4
			41853	4
			52650	1
			56624	1

ID	IP	TOT TCP	PORT	TIMES
			39466	1
			39163	1
			50175	4
			37507	4
			41546	1
			55685	1
			42586	1
			58182	1
			39399	4
			59497	4
			41576	1
			57081	1
			39888	1
			54806	1
			48049	4
			52909	4
			39831	1
			43454	1
			48624	1
			38314	4
			41607	4
			35477	1
			36536	1
			39447	1
			44141	1
			40097	4
			46886	4
			59190	1
			41756	4
			38836	1
			37770	1
			60613	4
			53531	1
			59111	1
			50152	4
			44813	1
			52368	1
			39636	4
			54634	1
			53076	1

ID	IP	TOT TCP	PORT	TIMES
			40755	1
			56058	1
			42676	1
			32922	1
			44719	1
			58524	1
			46856	1
			43740	4
			57987	4
			41724	4
			54835	1
			37715	1
			41436	1
			35631	4
			46977	1
			56844	4
			46592	1
			41029	1
			38400	4
			54461	1
			51844	1
			45362	4
			48896	4
			34345	4
			47910	4
			40135	1
			60404	1
			35185	1
			43186	1
			42497	4
			49592	4
			59873	2
			43867	1
			56273	1
			46413	1
			38341	4
			41069	4
			48250	1
			42372	1
			43875	1

ID	IP	TOT TCP	PORT	TIMES
			48744	1
			42717	4
			52397	4
			37796	1
			44710	1
			35928	1
			45827	4
			44420	4
			35162	1
			34746	1
			59561	1
			44686	1
			56042	4
			41421	4
			32990	1
			40818	1
			47503	5
			55358	4
			46693	4
			43257	1
			37879	1
			57233	1
			33063	1
			57013	4
			58255	4
			35331	1
			44842	1
			35583	1
			57825	1
			36496	4
			46365	4
			59237	1
			36540	1
			43322	1
			47806	1
			56278	4
			52288	4
			50211	1
			47572	1
			51538	1

ID	IP	TOT TCP	PORT	TIMES
			44792	1
			34324	4
			51372	4
			56651	1
			60332	1
			36111	1
			59431	1
			50170	4
			54742	4
			45551	1
			58970	1
			45812	1
			48715	1
			35859	4
			57700	4
			41209	5
			59811	1
			41103	1
			60588	1
			54803	4
			48783	4
			60161	1
			33486	1
			51735	1
			53586	1
			33562	4
			33054	4
			50423	1
			59539	1
			33779	1
			51353	1
			39303	4
			36980	4
			33136	1
			47595	1
			42432	1
			44056	1
			40480	4
			33077	4
			56288	1

ID	IP	TOT TCP	PORT	TIMES
			46043	1
			38303	1
			41815	1
			44188	4
			52381	4
			54788	1
			35630	1
			34816	1
			58986	1
			37386	4
			51561	4
			45597	1
			38819	1
			46337	1
			58656	1
			38985	4
			37609	4
			54513	4
			39437	1
			41484	1
			33156	1
			52495	4
			45184	1
			57042	4
			52942	1
			35309	1
			33244	4
			51643	1
			49874	1
			32834	4
			46653	4
			54499	4
			47269	4
			58091	1
			47961	1
			42539	1
			51995	1
			34718	4
			58416	4
			57818	1

ID	IP	TOT TCP	PORT	TIMES
			52779	1
			49966	1
			33510	1
			32954	4
			39084	4
			34707	1
			51145	1
			49328	1
			53818	5
			36557	4
			38397	4
			58583	1
			39121	1
			56944	1
			35864	1
			58397	4
			56701	8
			32937	1
			50600	1
			33335	1
			49034	1
			42367	4
			42943	4
			51173	1
			49280	1
			54200	1
			50841	1
			46930	4
			53060	4
			56617	1
			46466	1
			45433	1
			55105	1
			41678	4
			59823	4
			57669	1
			56305	1
			40792	1
			49229	1
			37725	4

ID	IP	TOT TCP	PORT	TIMES
			45654	4
			47169	1
			60366	1
			45379	1
			42922	1
			33821	4
			58310	4
			35750	1
			44475	1
			53570	1
			49604	1
			43254	4
			56173	4
			42928	1
			37833	1
			53715	1
			38313	1
			51378	4
			43206	4
			36765	1
			59320	1
			55448	1
			49461	1
			39393	4
			51277	4
			35931	1
			33437	1
			32978	1
			59066	1
			34934	4
			42252	4
			36625	1
			47868	1
			57714	1
			38719	1
			46147	4
			34444	4
			59889	1
			40117	1
			57369	1

ID	IP	TOT TCP	PORT	TIMES
			36464	1
			44161	4
			35095	1
			43958	1
			58821	1
			43976	1
			52941	4
			56565	4
			58803	1
			41720	1
			50956	1
			53375	1
			55517	4
			51606	4
			54590	1
			45550	1
			38056	1
			34428	2
			50305	4
			49631	4
			36384	1
			60502	1
			52366	1
			41109	1
			60310	4
			58759	1
			55858	1
			49803	1
			57375	1
			46319	4
			34176	4
			34308	1
			41042	4
			36120	1
			44451	1
			39633	1
			48170	1
			40996	4
			33642	1
			37909	4

ID	IP	TOT TCP	PORT	TIMES
			36156	1
			59384	1
			51716	4
			37710	4
			47502	4
			51880	4
			45067	5
			51226	1
			40365	1
			60992	1
			34074	4
			60878	4
			37555	1
			39148	1
			58015	1
			46295	1
			53137	4
			38910	4
			47667	1
			43830	1
			51438	1
			54105	1
			41010	4
			58910	4
			42425	1
			59617	1
			59325	1
			43543	1
			43595	4
			40379	4
			55426	1
			37311	1
			44574	1
			58191	1
			50369	4
			36034	4
			38192	1
			38908	1
			39156	1
			34802	1

ID	IP	TOT TCP	PORT	TIMES
			51350	4
			38446	4
			56400	1
			45974	1
			45593	1
			41446	1
			60261	4
			48358	1
			50342	1
			60630	1
			44886	1
			43971	4
			43704	4
			43104	1
			48215	1
			51388	1
			33508	1
			55795	4
			35150	4
			46517	1
			33191	1
			34037	1
			46350	1
			54123	4
			50020	4
			46873	1
			51698	1
			48962	1
			37722	1
			41411	4
			53351	4
			43855	1
			59766	1
			48938	5
			49772	1
			34662	4
			37332	4
			40980	1
			39504	1
			45353	1

ID	IP	TOT TCP	PORT	TIMES
			58101	1
			37866	4
			53691	4
			54478	1
			35896	1
			46830	1
			49596	1
			38484	4
			38604	4
			45937	1
			45809	1
			38223	1
			41827	1
			44836	4
			52732	4
			57240	1
			43877	1
			42899	1
			36642	1
			33632	4
			55260	4
			37638	1
			36044	1
			37170	1
			51354	1
			59838	4
			50449	4
			49415	1
			33370	1
			33667	1
			49073	1
			46902	4
			40761	4
			52327	1
			52222	1
			40787	1
			58620	1
			52618	4
			39206	4
			41692	1

ID	IP	TOT TCP	PORT	TIMES
			58267	1
			42124	1
			49114	1
			59392	4
			52985	4
			35963	1
			35100	1
			59216	1
			42002	1
			42334	4
			32817	4
			49277	4
			54097	1
			37819	1
			38703	1
			41124	1
			34717	4
			50200	1
			34962	1
			35940	4
			57276	1
			36366	4
			58587	1
			55818	1
			49489	1
			46343	2
			58284	1
			49322	1
			49995	1
			48247	1
			42208	4
			49159	4
			53041	1
			55394	1
			55912	1
			45005	1
			60936	4
			39349	1
			42138	1
			55090	1

ID	IP	TOT TCP	PORT	TIMES
			59864	1
			57452	4
			52125	4
			48051	1
			38200	1
			44870	1
			46549	1
			46859	4
			59534	4
			53619	1
			37596	1
			46528	1
			35656	1
			42600	4
			48357	1
			35088	1
			53496	1
			41562	1
			58575	4
			43997	4
			43853	1
			38410	1
			56496	1
			33951	1
			56259	4
			59929	4
			48069	1
			41065	1
			41634	1
			52075	1
			39433	4
			32832	4
			39510	1
			40589	1
			54450	1
			45078	1
			46871	4
			33308	4
			48333	1
			47678	1

ID	IP	TOT TCP	PORT	TIMES
			52480	1
			55475	1
			35347	4
			48780	8
			40952	1
			43546	1
			56965	1
			39529	1
			34395	4
			35040	4
			34520	1
			32912	1
			59447	1
			52445	1
			35132	4
			53974	4
			54382	1
			46085	1
			42179	1
			49471	1
			54380	4
			36965	4
			43931	1
			55124	1
			38873	1
			50988	1
			39174	4
			34061	1
			51286	1
			37671	1
			40747	1
			48340	4
			40382	4
			43356	1
			46071	1
			35499	1
			47609	1
			40234	4
			56349	4
			39298	1

ID	IP	TOT TCP	PORT	TIMES
			58460	1
			45420	1
			42631	1
			50822	4
			49808	4
			59387	1
			44489	1
			49694	1
			55462	1
			52755	4
			59769	4
			52496	1
			48216	1
			34510	1
			41212	1
			41892	4
			56830	4
			46876	1
			36867	1
			38279	1
			34451	1
			51577	4
			57191	4
			58842	1
			36103	1
			36381	1
			56752	1
			47096	4
			56192	4
			43360	1
			52142	1
			36280	1
			35434	4
			58087	4
			39980	4
			52423	1
			51581	1
			55230	1
			53955	4
			57433	1

ID	IP	TOT TCP	PORT	TIMES
			55696	4
			54485	1
			59772	1
			54607	4
			59950	1
			48816	1
			52384	4
			43943	4
			54308	4
			37141	1
			46373	1
			34366	1
			37168	1
			56165	4
			52550	4
			44777	1
			42963	1
			47477	1
			34576	1
			44163	4
			54448	4
			41381	1
			50506	1
			58053	1
			58156	1
			42222	4
			37305	4
			56215	1
			33026	1
			36821	1
			48006	1
			40918	4
			58914	4
			35832	1
			49219	1
			49064	2
			56089	1
			39967	4
			38557	4
			56484	1

ID	IP	TOT TCP	PORT	TIMES
			35388	1
			41114	1
			55930	2
			50711	4
			35852	4
			56364	1
			34616	1
			48986	1
			34103	1
			47888	4
			35642	4
			48564	1
			38955	1
			60016	1
			43640	1
			50627	4
			38826	4
			37793	1
			58135	1
			41787	1
			39287	1
			39719	4
			41089	1
			38312	1
			36029	1
			38608	1
			45999	4
			52089	4
			52275	1
			59222	1
			40346	1
			50925	4
			47882	4
			36768	1
			39897	1
			42392	1
			37488	1
			51142	4
			41608	4
			57790	1

ID	IP	TOT TCP	PORT	TIMES
			54966	1
			60896	1
			59275	1
			33288	4
			41490	4
			35478	1
			57925	1
			45798	1
			53435	1
			38709	4
			58764	4
			45266	1
			39009	1
			44194	1
			43039	1
			39227	4
			59155	4
			46475	1
			54996	1
			47235	1
			33281	1
			43637	4
			52086	4
			54924	1
			54207	1
			40435	1
			50133	1
			34986	4
			50381	4
			55376	1
			47789	1
			54542	5
			60724	1
			35168	4
			52083	4
			45269	1
			38930	1
			44846	1
			50018	1
			52422	4

ID	IP	TOT TCP	PORT	TIMES
			51821	4
			41014	1
			44770	1
			54211	1
			44873	4
			55352	4
			48395	1
			45155	1
			54013	1
			52635	1
			40608	4
			34053	4
			49259	1
			36373	1
			60590	1
			35838	1
			39981	4
			42443	4
			59994	1
			44784	1
			36590	1
			45776	1
			55349	4
			34132	4
			36235	4
			43941	1
			59060	1
			51650	1
			39951	4
			45207	1
			55894	1
			43779	4
			55002	1
			42998	1
			44927	4
			54266	1
			46552	4
			42802	4
			47945	5
			36883	4

ID	IP	TOT TCP	PORT	TIMES
			43213	1
			42053	1
			52021	1
			51359	1
			60626	4
			49091	4
			50341	4
			47089	1
			38000	1
			39440	1
			51728	4
			39956	1
			59690	1
			45192	4
			51245	1
			51285	4
			44617	1
			50307	1
			48582	4
			42359	4
			57381	1
			43451	1
			35113	1
			58197	4
			40807	4
			44022	4
			32965	4
			43947	1
			54955	1
			43325	1
			37050	1
			44535	4
			45836	4
			52542	1
			49892	1
			54596	1
			35867	1
			41881	4
			34405	4
			35013	1

ID	IP	TOT TCP	PORT	TIMES
			36212	1
			48639	1
			51402	1
			46077	4
			43316	1
			38273	1
			40082	1
			46616	1
			58542	4
			47691	1
			33786	1
			50048	1
			41333	4
			54885	1
			51008	1
			43530	1
			57776	1
			33670	4
			48465	4
			60341	1
			43307	1
			33996	1
			50971	4
			42523	4
			55162	1
			41359	1
			50335	1
			39355	1
			36234	4
			40998	4
			52068	1
			44429	1
			47556	1
			53429	4
			39096	4
			38629	1
			39172	1
			49370	1
			49107	4
			49746	4

ID	IP	TOT TCP	PORT	TIMES
			51024	1
			52475	1
			57021	1
			45081	1
			57280	4
			50009	4
			37329	1
			40125	1
			55114	1
			39706	1
			42022	4
			35407	4
			52956	1
			54753	1
			60400	1
			40525	1
			59483	4
			49918	4
			55313	1
			57585	1
			43863	1
			35779	1
			37249	4
			38456	4
			55049	1
			40401	1
			48878	1
			53681	1
			38114	4
			39666	4
			48645	1
			33600	1
			40751	1
			38949	1
			52463	4
			47574	4
			52756	1
			55587	1
			33041	1
			36067	1

ID	IP	TOT TCP	PORT	TIMES
			56070	4
			36894	4
			53796	1
			57967	1
			44978	1
			39977	1
			54574	4
			54798	4
			40508	1
			47127	1
			57378	1
			43991	1
			48561	4
			42420	4
			45804	1
			37455	1
			43762	1
			38088	1
			43501	4
			58521	4
			52284	1
			44973	1
			55138	1
			44555	1
			34161	4
			47568	4
			38095	1
			50067	1
			39604	1
			56557	1
			45653	4
			32962	4
			41711	1
			60343	1
			37557	1
			50995	1
			34603	4
			44039	4