

Ethernet 6

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(ip.src == 192.168.4.124) && (ip.dst == 128.46.4.92)

No.	Time	Source	Destination	Protocol	Length	Info
58	2.107756	128.46.4.92	192.168.4.124	ICMP	94	Destination unreachable (Host administratively prohibited)
60	2.171742	192.168.4.124	128.46.4.92	TCP	66	61940 → 6 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
61	2.207849	128.46.4.92	192.168.4.124	ICMP	94	Destination unreachable (Host administratively prohibited)
62	2.272042	192.168.4.124	128.46.4.92	TCP	66	61941 → 7 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
63	2.373018	192.168.4.124	128.46.4.92	TCP	66	61942 → 8 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
67	2.474229	192.168.4.124	128.46.4.92	TCP	66	61943 → 9 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
68	2.575297	192.168.4.124	128.46.4.92	TCP	66	61944 → 10 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
75	2.676523	192.168.4.124	128.46.4.92	TCP	66	61945 → 11 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
76	2.712279	128.46.4.92	192.168.4.124	ICMP	94	Destination unreachable (Host administratively prohibited)
77	2.777414	192.168.4.124	128.46.4.92	TCP	66	61946 → 12 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
80	2.878074	192.168.4.124	128.46.4.92	TCP	66	61947 → 13 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
82	2.979205	192.168.4.124	128.46.4.92	TCP	66	61948 → 14 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
85	3.080665	192.168.4.124	128.46.4.92	TCP	66	61949 → 15 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
98	3.181296	192.168.4.124	128.46.4.92	TCP	66	61951 → 16 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
117	3.282373	192.168.4.124	128.46.4.92	TCP	66	61952 → 17 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
119	3.383565	192.168.4.124	128.46.4.92	TCP	66	61953 → 18 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
130	3.484605	192.168.4.124	128.46.4.92	TCP	66	61954 → 19 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
140	3.585853	192.168.4.124	128.46.4.92	TCP	66	61955 → 20 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
141	3.686786	192.168.4.124	128.46.4.92	TCP	66	61956 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
142	3.722767	128.46.4.92	192.168.4.124	ICMP	94	Destination unreachable (Host administratively prohibited)
146	3.788057	192.168.4.124	128.46.4.92	TCP	66	61957 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
148	3.820805	192.168.4.124	128.46.4.92	TCP	54	61957 → 22 [ACK] Seq=1 Ack=1 Win=262656 Len=0
149	3.821661	192.168.4.124	128.46.4.92	TCP	54	61957 → 22 [FIN, ACK] Seq=1 Ack=1 Win=262656 Len=0
150	3.821850	192.168.4.124	128.46.4.92	TCP	66	61958 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
154	3.873992	192.168.4.124	128.46.4.92	TCP	54	61957 → 22 [RST, ACK] Seq=2 Ack=22 Win=0 Len=0
155	3.922175	192.168.4.124	128.46.4.92	TCP	66	61959 → 24 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
159	4.023671	192.168.4.124	128.46.4.92	TCP	66	61960 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
161	4.124731	192.168.4.124	128.46.4.92	TCP	66	61961 → 26 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
162	4.225421	192.168.4.124	128.46.4.92	TCP	66	61962 → 27 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
163	4.325744	192.168.4.124	128.46.4.92	TCP	66	61963 → 28 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
164	4.426953	192.168.4.124	128.46.4.92	TCP	66	61964 → 29 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
165	4.528086	192.168.4.124	128.46.4.92	TCP	66	61965 → 30 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
166	4.629278	192.168.4.124	128.46.4.92	TCP	66	61966 → 31 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
167	4.730703	192.168.4.124	128.46.4.92	TCP	66	61967 → 32 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
168	4.758943	128.46.4.92	192.168.4.124	ICMP	94	Destination unreachable (Host administratively prohibited)
169	4.832142	192.168.4.124	128.46.4.92	TCP	66	61968 → 33 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
170	4.932690	192.168.4.124	128.46.4.92	TCP	66	61969 → 34 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
172	5.033221	192.168.4.124	128.46.4.92	TCP	66	61970 → 35 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
173	5.134448	192.168.4.124	128.46.4.92	TCP	66	61971 → 36 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
174	5.235125	192.168.4.124	128.46.4.92	TCP	66	61972 → 37 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
175	5.336317	192.168.4.124	128.46.4.92	TCP	66	61973 → 38 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
178	5.437396	192.168.4.124	128.46.4.92	TCP	66	61974 → 39 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
180	5.538864	192.168.4.124	128.46.4.92	TCP	66	61975 → 40 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

This picture shows the Wireshark output of the port scanning process. I had my range set to scan ports 0-200 with the port I was looking to attack as port 22. This screenshot shows not only the scanning process but also the fact that port 22 is in fact open.

*Ethernet 6

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(ip.src == 192.168.4.124) && (ip.dst == 128.46.4.92)

No.	Time	Source	Destination	Protocol	Length	Info
579	19.730432	192.168.4.124	128.46.4.92	TCP	66	62116 → 181 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
580	19.758141	128.46.4.92	192.168.4.124	ICMP	94	Destination unreachable (Host administratively prohibited)
581	19.831058	192.168.4.124	128.46.4.92	TCP	66	62117 → 182 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
585	19.932136	192.168.4.124	128.46.4.92	TCP	66	62118 → 183 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
589	20.033259	192.168.4.124	128.46.4.92	TCP	66	62119 → 184 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
590	20.134974	192.168.4.124	128.46.4.92	TCP	66	62120 → 185 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
591	20.236008	192.168.4.124	128.46.4.92	TCP	66	62121 → 186 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
592	20.337278	192.168.4.124	128.46.4.92	TCP	66	62122 → 187 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
594	20.359328	192.168.4.124	128.46.4.92	SSH	98	Client: Encrypted packet (len=44)
595	20.359711	192.168.4.124	128.46.4.92	SSH	98	Client: Encrypted packet (len=44)
597	20.437959	192.168.4.124	128.46.4.92	TCP	66	62123 → 188 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
601	20.456907	192.168.4.124	128.46.4.92	TCP	54	60586 → 22 [ACK] Seq=89 Ack=4713 Win=1026 Len=0
602	20.458322	192.168.4.124	128.46.4.92	SSH	98	Client: Encrypted packet (len=44)
603	20.458776	192.168.4.124	128.46.4.92	SSH	98	Client: Encrypted packet (len=44)
608	20.487317	192.168.4.124	128.46.4.92	SSH	98	Client: Encrypted packet (len=44)
609	20.487599	192.168.4.124	128.46.4.92	SSH	98	Client: Encrypted packet (len=44)
612	20.538533	192.168.4.124	128.46.4.92	TCP	66	62124 → 189 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
615	20.639260	192.168.4.124	128.46.4.92	TCP	66	62125 → 190 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
616	20.739488	192.168.4.124	128.46.4.92	TCP	66	62126 → 191 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
617	20.768388	128.46.4.92	192.168.4.124	ICMP	94	Destination unreachable (Host administratively prohibited)
618	20.841026	192.168.4.124	128.46.4.92	TCP	66	62127 → 192 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
620	20.942468	192.168.4.124	128.46.4.92	TCP	66	62128 → 193 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
628	21.044017	192.168.4.124	128.46.4.92	TCP	66	62129 → 194 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
629	21.144714	192.168.4.124	128.46.4.92	TCP	66	62130 → 195 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
631	21.245919	192.168.4.124	128.46.4.92	TCP	66	62131 → 196 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
633	21.347280	192.168.4.124	128.46.4.92	TCP	66	62132 → 197 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
636	21.448141	192.168.4.124	128.46.4.92	TCP	66	62133 → 198 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
638	21.549661	192.168.4.124	128.46.4.92	TCP	66	62134 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
643	21.650919	192.168.4.124	128.46.4.92	TCP	66	62135 → 200 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
648	21.752944	192.168.4.124	128.46.4.92	TCP	66	62136 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
650	21.783398	192.168.4.124	128.46.4.92	TCP	54	62136 → 22 [ACK] Seq=1 Ack=1 Win=262656 Len=0
651	21.786688	192.168.4.124	128.46.4.92	TCP	54	26355 → 22 [SYN] Seq=0 Win=8192 Len=0
652	21.788415	192.168.4.124	128.46.4.92	TCP	54	26989 → 22 [SYN] Seq=0 Win=8192 Len=0
653	21.791551	192.168.4.124	128.46.4.92	TCP	54	16668 → 22 [SYN] Seq=0 Win=8192 Len=0
654	21.794649	192.168.4.124	128.46.4.92	TCP	54	18639 → 22 [SYN] Seq=0 Win=8192 Len=0
655	21.796619	192.168.4.124	128.46.4.92	TCP	54	35984 → 22 [SYN] Seq=0 Win=8192 Len=0
656	21.798124	192.168.4.124	128.46.4.92	TCP	54	51969 → 22 [SYN] Seq=0 Win=8192 Len=0
657	21.799470	192.168.4.124	128.46.4.92	TCP	54	599 → 22 [SYN] Seq=0 Win=8192 Len=0
658	21.802009	192.168.4.124	128.46.4.92	TCP	54	48050 → 22 [SYN] Seq=0 Win=8192 Len=0
659	21.803595	192.168.4.124	128.46.4.92	TCP	54	44875 → 22 [SYN] Seq=0 Win=8192 Len=0
660	21.805025	192.168.4.124	128.46.4.92	TCP	54	6379 → 22 [SYN] Seq=0 Win=8192 Len=0
661	21.805561	192.168.4.124	128.46.4.92	TCP	54	62136 → 22 [FIN, ACK] Seq=1 Ack=1 Win=262656 Len=0
669	21.833090	192.168.4.124	128.46.4.92	TCP	54	62136 → 22 [RST, ACK] Seq=2 Ack=22 Win=0 Len=0

This screenshot shows the actual attack on port 22 (towards the bottom, No. 648 and on), where it sends multiple packets to port 22. The source IP was set as my PC's IP and the destination IP was set as my ThinLinc ECE IP.