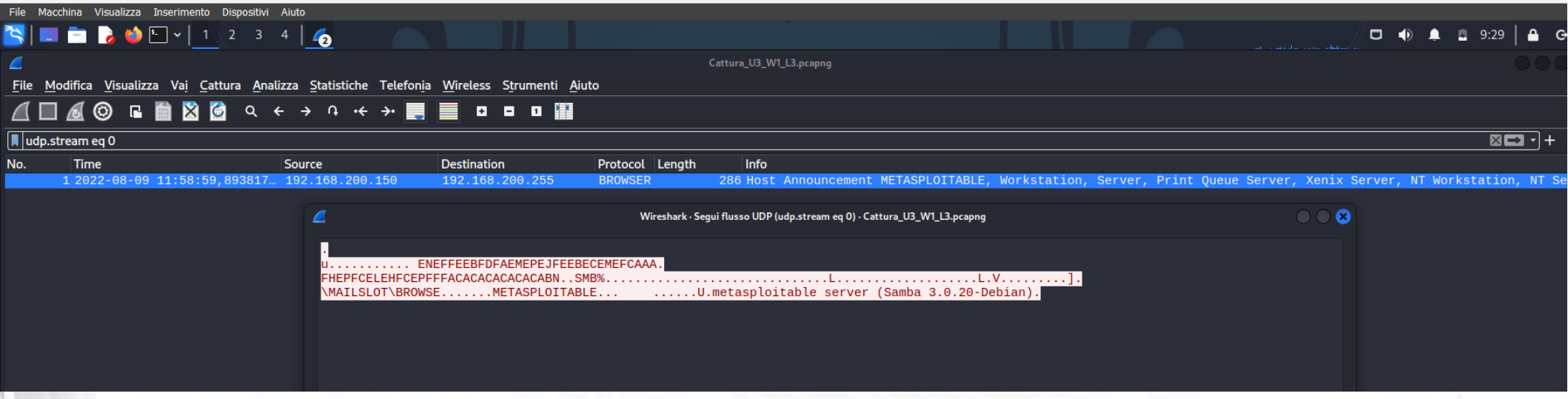
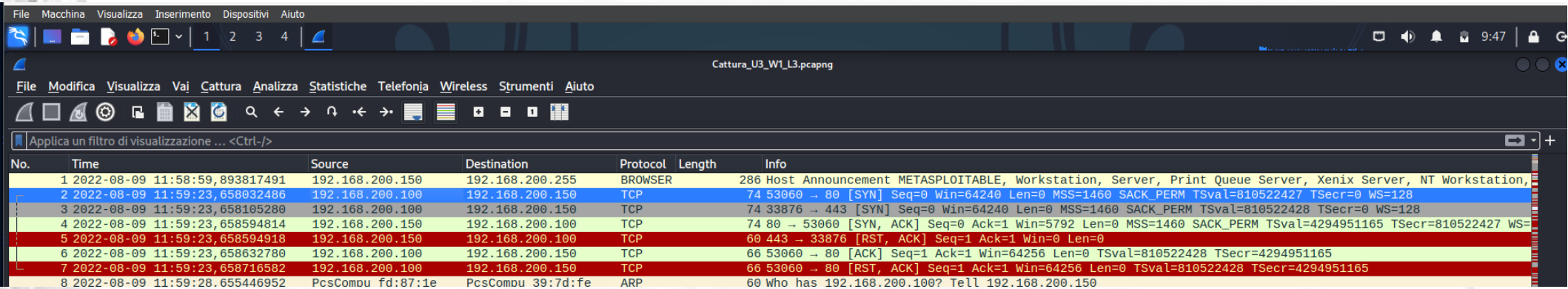
ESERCIZIO M6 D6

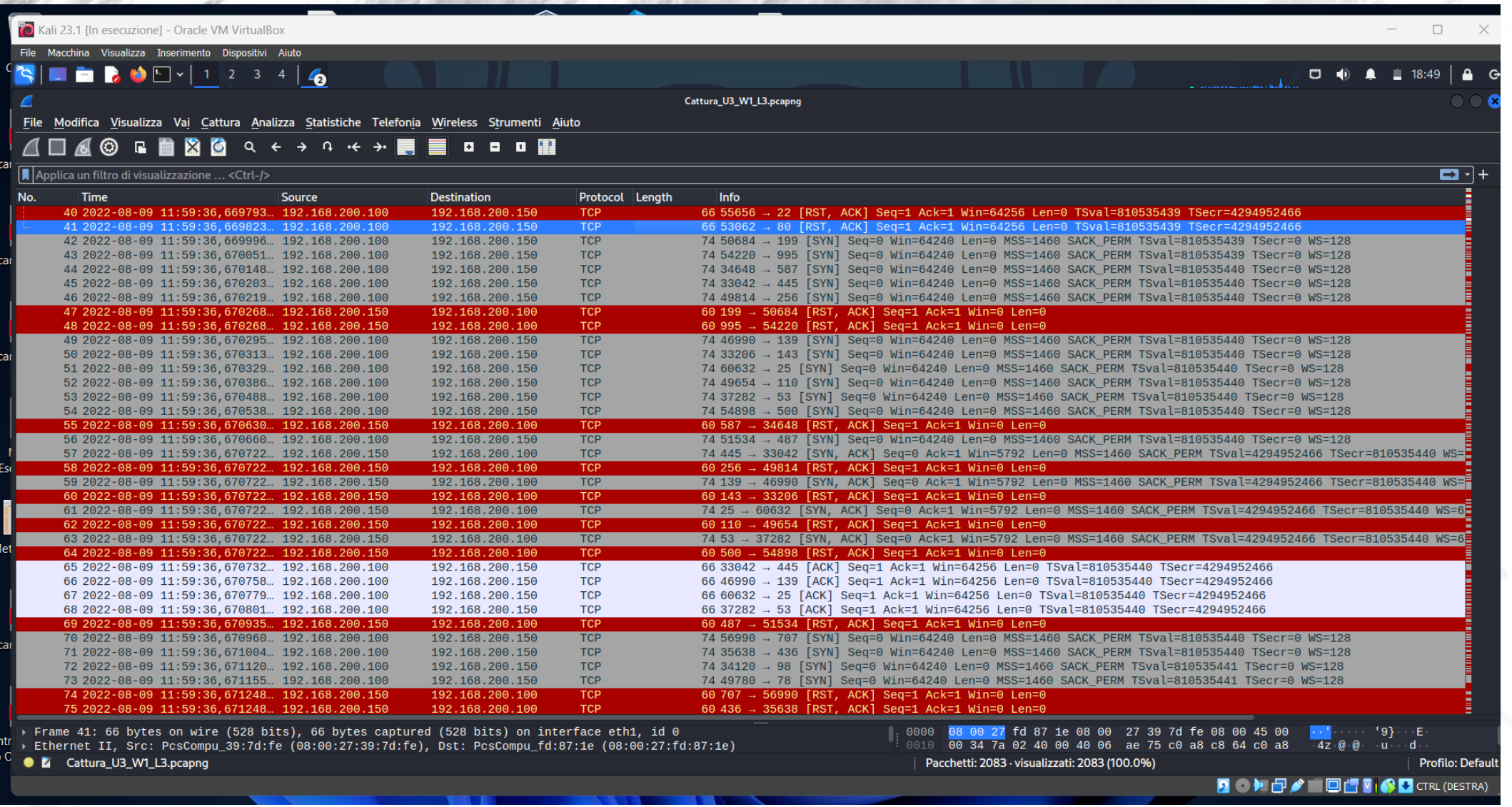
THREAT INTELLIGENCE & IOC



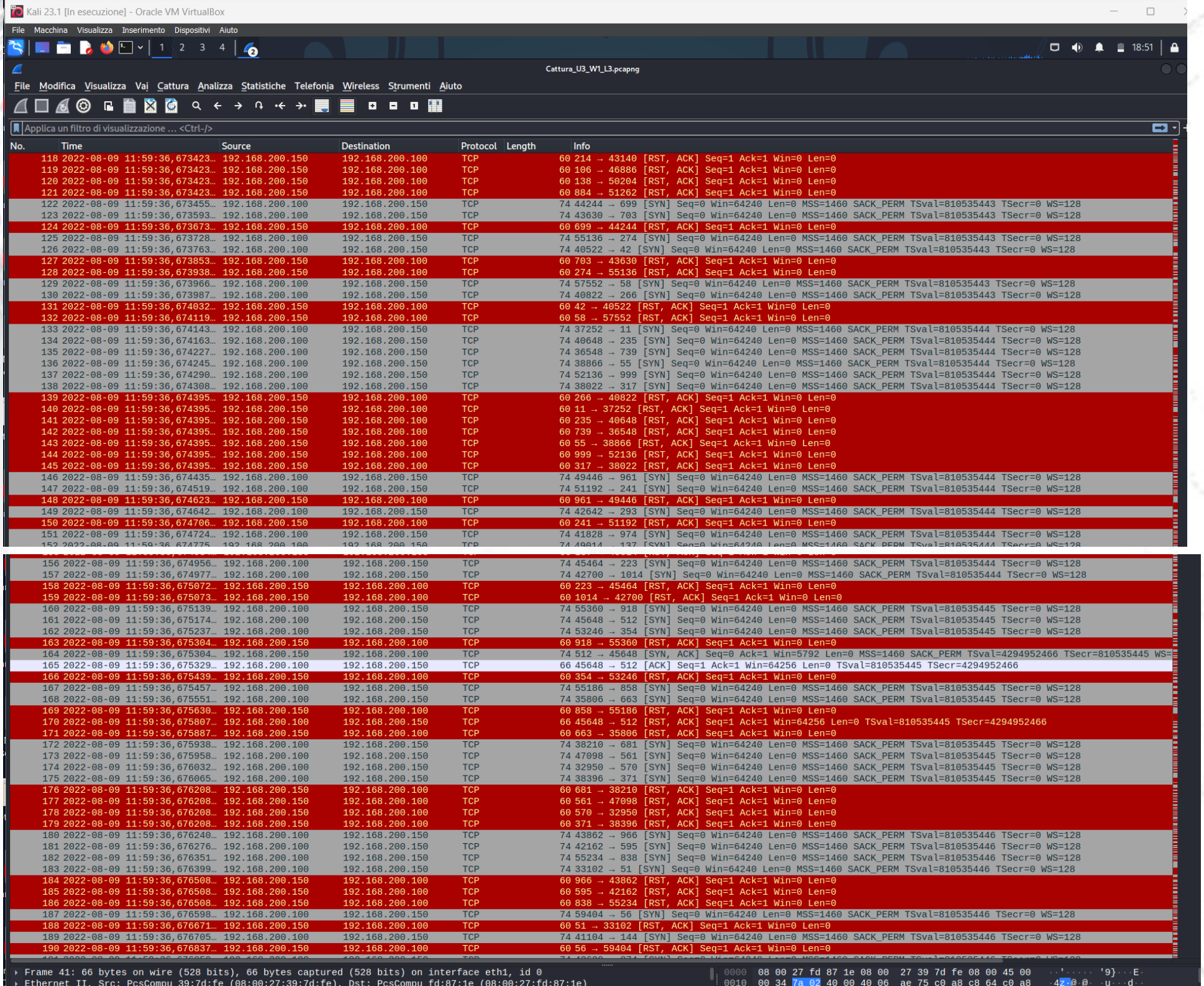
PER PRIMA COSA POSSIAMO NOTARE IL FILE PCAP INIZIA CON UNA PRIMA RIGA CHE IDENTIFICA L'HOST CON IP FINALE .150 CHE ESEGUE UN BROADCAST. ANALIZZANDO IL PACCHETTO POSSIAMO DECIFRARE SIA IL SERVIZIO CHE LA MACCHINA OVVERO UN SERVER SAMBA SMB CHE GIRA SU “METASPLOITABLE”



SUBITO DOPO LA PRIMA RICHIESTA BROADCAST SI Può NOTARE CHE CHE AVVIENE UNA COSSIONE SULLA PORTA 80 CON LA MACCHINA CON IP FINALE . 100 (COMPLETAMENTO 3WAYHANDSHAKE)



CONTIMNUANDO CON L'ANALISI SI POSSONO NOTARE DIVERSE RICHIESTE SYN TRA GLI HOST SU SVARIATE PORTE E TUTTO CIO' FAREBBE PENSARE AD UNA SCANSIONE TCP CONNECT SCAN FATTA PROBABILMENTE CON NMAP


Kali 23.1 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Cattura_U3_W1_L3.pcapng
File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto
Applica un filtro di visualizzazione … <Ctrl-/>
No. Time Source Destination Protocol Length Info
118 2022-08-09 11:59:36,673423… 192.168.200.150 192.168.200.100 TCP 60 214 → 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
119 2022-08-09 11:59:36,673423… 192.168.200.150 192.168.200.100 TCP 60 106 → 46886 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
120 2022-08-09 11:59:36,673423… 192.168.200.150 192.168.200.100 TCP 60 138 → 50204 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
121 2022-08-09 11:59:36,673423… 192.168.200.150 192.168.200.100 TCP 60 884 → 51262 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
122 2022-08-09 11:59:36,673455… 192.168.200.100 192.168.200.150 TCP 74 44244 → 699 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
123 2022-08-09 11:59:36,673593… 192.168.200.100 192.168.200.150 TCP 74 43630 → 703 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
124 2022-08-09 11:59:36,673673… 192.168.200.150 192.168.200.100 TCP 60 699 → 44244 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
125 2022-08-09 11:59:36,673728… 192.168.200.100 192.168.200.150 TCP 74 55136 → 274 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
126 2022-08-09 11:59:36,673763… 192.168.200.100 192.168.200.150 TCP 74 40522 → 42 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
127 2022-08-09 11:59:36,673853… 192.168.200.150 192.168.200.100 TCP 60 703 → 43630 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
128 2022-08-09 11:59:36,673938… 192.168.200.150 192.168.200.100 TCP 60 274 → 55136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
129 2022-08-09 11:59:36,673966… 192.168.200.100 192.168.200.150 TCP 74 57552 → 58 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
130 2022-08-09 11:59:36,673987… 192.168.200.100 192.168.200.150 TCP 74 40822 → 266 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
131 2022-08-09 11:59:36,674032… 192.168.200.150 192.168.200.100 TCP 60 42 → 40522 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
132 2022-08-09 11:59:36,674119… 192.168.200.150 192.168.200.100 TCP 60 58 → 57552 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
133 2022-08-09 11:59:36,674143… 192.168.200.100 192.168.200.150 TCP 74 37252 → 11 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
134 2022-08-09 11:59:36,674163… 192.168.200.100 192.168.200.150 TCP 74 40648 → 235 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
135 2022-08-09 11:59:36,674227… 192.168.200.100 192.168.200.150 TCP 74 36548 → 739 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
136 2022-08-09 11:59:36,674245… 192.168.200.100 192.168.200.150 TCP 74 38866 → 55 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
137 2022-08-09 11:59:36,674290… 192.168.200.100 192.168.200.150 TCP 74 52136 → 999 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
138 2022-08-09 11:59:36,674308… 192.168.200.100 192.168.200.150 TCP 74 38022 → 317 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
139 2022-08-09 11:59:36,674395… 192.168.200.150 192.168.200.100 TCP 60 266 → 40822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
140 2022-08-09 11:59:36,674395… 192.168.200.150 192.168.200.100 TCP 60 11 → 37252 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
141 2022-08-09 11:59:36,674395… 192.168.200.150 192.168.200.100 TCP 60 235 → 40648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
142 2022-08-09 11:59:36,674395… 192.168.200.150 192.168.200.100 TCP 60 739 → 36548 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
143 2022-08-09 11:59:36,674395… 192.168.200.150 192.168.200.100 TCP 60 55 → 38866 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
144 2022-08-09 11:59:36,674395… 192.168.200.150 192.168.200.100 TCP 60 999 → 52136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
145 2022-08-09 11:59:36,674395… 192.168.200.150 192.168.200.100 TCP 60 317 → 38022 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
146 2022-08-09 11:59:36,674435… 192.168.200.100 192.168.200.150 TCP 74 49446 → 961 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
147 2022-08-09 11:59:36,674519… 192.168.200.100 192.168.200.150 TCP 74 51192 → 241 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
148 2022-08-09 11:59:36,674623… 192.168.200.150 192.168.200.100 TCP 60 961 → 49446 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
149 2022-08-09 11:59:36,674642… 192.168.200.100 192.168.200.150 TCP 74 42642 → 293 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
150 2022-08-09 11:59:36,674706… 192.168.200.150 192.168.200.100 TCP 60 241 → 51192 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
151 2022-08-09 11:59:36,674724… 192.168.200.100 192.168.200.150 TCP 74 41828 → 974 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
156 2022-08-09 11:59:36,674956… 192.168.200.100 192.168.200.150 TCP 74 45464 → 223 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
157 2022-08-09 11:59:36,674977… 192.168.200.100 192.168.200.150 TCP 74 42700 → 1014 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
158 2022-08-09 11:59:36,675072… 192.168.200.150 192.168.200.100 TCP 60 223 → 45464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
159 2022-08-09 11:59:36,675073… 192.168.200.150 192.168.200.100 TCP 60 1014 → 42700 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
160 2022-08-09 11:59:36,675139… 192.168.200.100 192.168.200.150 TCP 74 55360 → 918 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
161 2022-08-09 11:59:36,675174… 192.168.200.100 192.168.200.150 TCP 74 45648 → 512 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
162 2022-08-09 11:59:36,675237… 192.168.200.100 192.168.200.150 TCP 74 53246 → 354 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
163 2022-08-09 11:59:36,675304… 192.168.200.150 192.168.200.100 TCP 60 918 → 55360 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
164 2022-08-09 11:59:36,675304… 192.168.200.150 192.168.200.100 TCP 74 512 → 45648 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535445 WS=
165 2022-08-09 11:59:36,675329… 192.168.200.100 192.168.200.150 TCP 66 45648 → 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466
166 2022-08-09 11:59:36,675439… 192.168.200.150 192.168.200.100 TCP 60 354 → 53246 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
167 2022-08-09 11:59:36,675457… 192.168.200.100 192.168.200.150 TCP 74 55186 → 858 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
168 2022-08-09 11:59:36,675551… 192.168.200.100 192.168.200.150 TCP 74 35806 → 663 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
169 2022-08-09 11:59:36,675630… 192.168.200.150 192.168.200.100 TCP 60 858 → 55186 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
170 2022-08-09 11:59:36,675807… 192.168.200.100 192.168.200.150 TCP 66 45648 → 512 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466
171 2022-08-09 11:59:36,675887… 192.168.200.150 192.168.200.100 TCP 60 663 → 35806 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
172 2022-08-09 11:59:36,675938… 192.168.200.100 192.168.200.150 TCP 74 38210 → 681 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
173 2022-08-09 11:59:36,675958… 192.168.200.100 192.168.200.150 TCP 74 47098 → 561 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
174 2022-08-09 11:59:36,676032… 192.168.200.100 192.168.200.150 TCP 74 32950 → 570 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
175 2022-08-09 11:59:36,676065… 192.168.200.100 192.168.200.150 TCP 74 38396 → 371 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
176 2022-08-09 11:59:36,676208… 192.168.200.150 192.168.200.100 TCP 60 681 → 38210 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
177 2022-08-09 11:59:36,676208… 192.168.200.150 192.168.200.100 TCP 60 561 → 47098 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
178 2022-08-09 11:59:36,676208… 192.168.200.150 192.168.200.100 TCP 60 570 → 32950 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
179 2022-08-09 11:59:36,676208… 192.168.200.150 192.168.200.100 TCP 60 371 → 38396 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
180 2022-08-09 11:59:36,676240… 192.168.200.100 192.168.200.150 TCP 74 43862 → 966 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
181 2022-08-09 11:59:36,676276… 192.168.200.100 192.168.200.150 TCP 74 42162 → 595 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
182 2022-08-09 11:59:36,676351… 192.168.200.100 192.168.200.150 TCP 74 55234 → 838 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
183 2022-08-09 11:59:36,676399… 192.168.200.100 192.168.200.150 TCP 74 33102 → 51 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
184 2022-08-09 11:59:36,676508… 192.168.200.150 192.168.200.100 TCP 60 966 → 43862 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
185 2022-08-09 11:59:36,676508… 192.168.200.150 192.168.200.100 TCP 60 595 → 42162 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
186 2022-08-09 11:59:36,676508… 192.168.200.150 192.168.200.100 TCP 60 838 → 55234 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
187 2022-08-09 11:59:36,676598… 192.168.200.100 192.168.200.150 TCP 74 59404 → 56 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
188 2022-08-09 11:59:36,676671… 192.168.200.150 192.168.200.100 TCP 60 51 → 33102 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
189 2022-08-09 11:59:36,676705… 192.168.200.100 192.168.200.150 TCP 74 41104 → 144 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
190 2022-08-09 11:59:36,676837… 192.168.200.150 192.168.200.100 TCP 60 56 → 59404 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 41: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth1, id 0
Ethernet II, Src: PcsCompu_39:7d:fe (08:00:27:39:7d:fe), Dst: PcsCompu_fd:87:1e (08:00:27:fd:87:1e)
0000 08 00 27 fd 87 1e 08 00 27 39 7d fe 08 00 45 00
0010 00 34 7a 02 40 00 40 06 ae 75 c0 a8 c8 64 c0 a8

CONTINUANDO CON L'ANALISI DEI PACCHETTI TRA .150 E .100 DATA L'ELEVATO NUMERO DI RICHIESTE IN BREVISSIMO TEMPO E SOPRATTUTTO L'ORDINE CASUALE DELLE RICHIESTE POTREMMO ESSERE ABBASTANZA SICURI CHE LAPRIMA IMPRESSIONE, OVVERO QUELLA DI UNA SCANSIONE NMAP SIA CORRETTA E CON TIPOLOGIA DI SCANSIONE -sT (tcp cnnect port scan)

No.	Time	Source	Destination	Protocol	Length	Info
190	2022-08-09 11:59:36,676837…	192.168.200.150	192.168.200.100	TCP	60	56 → 59404 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
191	2022-08-09 11:59:36,676859…	192.168.200.100	192.168.200.150	TCP	74	42620 → 874 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
192	2022-08-09 11:59:36,676901…	192.168.200.100	192.168.200.150	TCP	74	58110 → 920 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
193	2022-08-09 11:59:36,677147…	192.168.200.150	192.168.200.100	TCP	60	144 → 41104 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
194	2022-08-09 11:59:36,677147…	192.168.200.150	192.168.200.100	TCP	60	874 → 42620 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
195	2022-08-09 11:59:36,677147…	192.168.200.150	192.168.200.100	TCP	60	920 → 58110 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
196	2022-08-09 11:59:36,677209…	192.168.200.100	192.168.200.150	TCP	74	42696 → 964 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535447 TSecr=0 WS=128
197	2022-08-09 11:59:36,677244…	192.168.200.100	192.168.200.150	TCP	74	57372 → 333 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535447 TSecr=0 WS=128
198	2022-08-09 11:59:36,677375…	192.168.200.150	192.168.200.100	TCP	60	964 → 42696 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
199	2022-08-09 11:59:36,677375…	192.168.200.150	192.168.200.100	TCP	60	333 → 57372 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
200	2022-08-09 11:59:36,679215…	192.168.200.100	192.168.200.150	TCP	74	52872 → 203 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
201	2022-08-09 11:59:36,679260…	192.168.200.100	192.168.200.150	TCP	74	37880 → 880 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
202	2022-08-09 11:59:36,679368…	192.168.200.100	192.168.200.150	TCP	74	50932 → 939 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
203	2022-08-09 11:59:36,679442…	192.168.200.100	192.168.200.150	TCP	74	47472 → 743 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
204	2022-08-09 11:59:36,679492…	192.168.200.150	192.168.200.100	TCP	60	203 → 52872 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
205	2022-08-09 11:59:36,679492…	192.168.200.150	192.168.200.100	TCP	60	880 → 37880 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
206	2022-08-09 11:59:36,679538…	192.168.200.100	192.168.200.150	TCP	74	41984 → 831 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
207	2022-08-09 11:59:36,679556…	192.168.200.100	192.168.200.150	TCP	74	57854 → 122 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
208	2022-08-09 11:59:36,679642…	192.168.200.150	192.168.200.100	TCP	60	939 → 50932 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
209	2022-08-09 11:59:36,679642…	192.168.200.150	192.168.200.100	TCP	60	743 → 47472 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
210	2022-08-09 11:59:36,679698…	192.168.200.100	192.168.200.150	TCP	74	57402 → 237 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
211	2022-08-09 11:59:36,679760…	192.168.200.100	192.168.200.150	TCP	74	33718 → 359 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
212	2022-08-09 11:59:36,680027…	192.168.200.150	192.168.200.100	TCP	60	831 → 41984 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
213	2022-08-09 11:59:36,680027…	192.168.200.150	192.168.200.100	TCP	60	122 → 57854 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
214	2022-08-09 11:59:36,680027…	192.168.200.150	192.168.200.100	TCP	60	237 → 57402 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
215	2022-08-09 11:59:36,680027…	192.168.200.150	192.168.200.100	TCP	60	359 → 33718 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
216	2022-08-09 11:59:36,680071…	192.168.200.100	192.168.200.150	TCP	74	35164 → 586 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
217	2022-08-09 11:59:36,680109…	192.168.200.100	192.168.200.150	TCP	74	59734 → 129 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128
218	2022-08-09 11:59:36,680273…	192.168.200.150	192.168.200.100	TCP	60	586 → 35164 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
219	2022-08-09 11:59:36,680273…	192.168.200.150	192.168.200.100	TCP	60	129 → 59734 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
220	2022-08-09 11:59:36,680606…	192.168.200.100	192.168.200.150	TCP	74	45416 → 545 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128
221	2022-08-09 11:59:36,680632…	192.168.200.100	192.168.200.150	TCP	74	45154 → 400 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128
222	2022-08-09 11:59:36,680681…	192.168.200.100	192.168.200.150	TCP	74	38180 → 239 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128
223	2022-08-09 11:59:36,680717…	192.168.200.100	192.168.200.150	TCP	74	37952 → 520 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128
224	2022-08-09 11:59:36,680840…	192.168.200.150	192.168.200.100	TCP	60	545 → 45416 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
225	2022-08-09 11:59:36,680840…	192.168.200.150	192.168.200.100	TCP	60	400 → 45154 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
226	2022-08-09 11:59:36,680886…	192.168.200.100	192.168.200.150	TCP	74	43106 → 769 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128

Considerando l'analisi appena fatta, potrei consigliare come azione per ridurre il rischio:

- utilizzare un FIREWALL per andare a bloccare i ping sulle porte che non vogliamo che siano raggiungibili dall'esterno e che potrebbero essere sfruttate per sferrare degli attacchi potenzialmente anche molto pericolosi per i nostri sistemi.