# Progetto S9/L5

**Introduzione**: l'obiettivo di questo esercizio è analizzare una cattura di rete fornito come parte di un'esercitazione pratica di Threat Intelligence e indicatori di compromissioni (IOC). Attraverso un'analisi metodica del traffico di rete, il nostro scopo è identificare e interpretare gli eventi sospetti, formulare ipotesi sui potenziali vettori di attacco utilizzati e, infine, proporre un piano di mitigazione e prevenzione per affrontare le minacce individuate.

## Analisi e identificazione degli IOC

	Time	Source	Destination		Length Info
		192.168.200.150	192.168.200.255		286 Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential
		192.168.200.100	192.168.200.150	TCP	74 53060 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
		192.168.200.100	192.168.200.150	TCP	74 33876 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
	4 23.764777323	192.168.200.150	192.168.200.100	TCP	74 80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64
		192.168.200.150	192.168.200.100	TCP	60 443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
		192.168.200.100	192.168.200.150	TCP	66 53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
		192.168.200.100	192.168.200.150	TCP	66 53060 → 80 [RST, ACK] Seg=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
	8 28.761629461	PCSSystemtec_fd:87:	. PCSSystemtec_39:7d:	ARP	60 Who has 192.168.200.100? Tell 192.168.200.150
	9 28.761644619	PCSSystemtec_39:7d:	. PCSSystemtec_fd:87:	ARP	42 192.168.200.100 is at 08:00:27:39:7d:fe
	10 28.774852257	PCSSvstemtec 39:7d:	PCSSvstemtec fd:87:	ARP	42 Who has 192.168.200.150? Tell 192.168.200.100
	11 28.775230099	PCSSvstemtec fd:87:	. PCSSvstemtec 39:7d:	ARP	60 192.168.200.150 is at 08:00:27:fd:87:1e
i	12 36.774143445	192.168.200.100	192.168.200.150	TCP	74 41304 - 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PERM TSval=810535437 TSecr=0 WS=128
		192,168,200,100	192,168,200,150	TCP	74 56120 - 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PERM TSVal=810535437 TSecr=0 WS=128
		192.168.200.100	192.168.200.150	TCP	74 33878 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PERM TSval=810535437 TSecr=0 WS=128
		192.168.200.100	192.168.200.150	TCP	74 58636 - 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PERM TSVal=810535438 TSecr=0 WS=128
		192,168,200,100	192,168,200,150	TCP	74 52358 - 135 [SYN] Seg=0 Win=64240 Len=0 MSS=1460 SACK PERM TSVal=810535438 TSecr=0 WS=128
		192.168.200.100	192.168.200.150	TCP	74 46138 - 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PERM TSVal=810535438 TSecr=0 WS=128
		192,168,200,100	192,168,200,150	TCP	74 41182 - 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PERM TSval=810535438 TSecr=0 WS=128
		192.168.200.150	192.168.200.100	TCP	74 23 - 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK PERM TSval=4294952466 TSecr=810535437 WS=64
		192,168,200,150	192.168.200.100	TCP	74 111 - 56120 TSYN, ACK1 Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK PERM TSVal=4294952466 TSecr=810535437 WS=64
		192.168.200.150	192.168.200.100	TCP	60 443 - 33878 [RST. ACK] Seg=1 Ack=1 Win=0 Len=0
		192.168.200.150	192.168.200.100	TCP	60 554 - 58636 [RST. ACK] Seg=1 Ack=1 Win=0 Len=0
		192.168.200.150	192.168.200.100	TCP	60 135 - 52358 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
		192.168.200.100	192.168.200.150	TCP	66 41304 - 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
		192.168.200.100	192.168.200.150	TCP	66 56120 - 111 [ACK] Sea=1 Ack=1 Win=64256 Len=0 TSyal=810535438 TSecr=4294952466
		192.168.200.150	192.168.200.100	TCP	60 993 - 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
		192.168.200.150	192.168.200.100	TCP	74 21 - 41182 [SYN, ACK] Seg=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK PERM TSval=4294952466 TSecr=810535438 WS=64
		192.168.200.100	192.168.200.150	TCP	66 41182 - 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsyal=819535438 TSecr=4294952466
		192.168.200.100	192.168.200.150	TCP	74 59174 - 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PERM TSVal=810535438 TSecr=0 WS=128
		192,168,200,100	192.168.200.150	TCP	74 55656 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PERM TSVal=810535439 TSecr=0 WS=128
		192.168.200.100	192.168.200.150	TCP	74 53062 - 80 [SVN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PERM TSval=810535439 TSecr=0 WS=128
		192.168.200.150	192.168.200.100	TCP	74 53002 = 00 [SIN] Seque willimotate Celling Mas-1400 SACK_PERM 13VAL**01035439 13eCt =0 W3=120
		192.168.200.100	192.168.200.150	TCP	00 113 - 3914 [R31, ACK] Seq=1 ACK=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
		192.168.200.100	192.168.200.150	TCP	00 41304 - 23 [RS], ALK] 304-1 ALK-1 WIN-04230 L0N-0 10030435 15001-429492400 66 55120 - 111 [RS], ALK] 304-1 MIN-04250 L0N-0 TSVal-818535439 TSecr-4294952466
		192,168,200,150	192,168,200,100	TCP	00 30120 - 111 [KS1, ACK] SEQ=1 ACK-1 WIN-04230 LENE-0 ISVAL-010533439 ISECT-4234952400 74 22 - 55656 [SYN. ACK] SEQ=0 ACK-1 WIN-5792 LENE-0 ISSNALAGO SACK PERM TSVAL-4294952406 TSECT-810535439 WS-64
		192.168.200.150	192.168.200.100	TCP	/4 22 - 30000 [5TM, ACK] Seq=0 ACK=1 W1H=0/92 LeH=0 MSD=1400 SACK_PERM ISVAL-4294952400 ISECT=810030439 W3D=04 74 80 - 53062 [STM, ACK] Seq=0 ACK=1 W1H=5792 LeH=0 MSD=1400 SACK_PERM ISVAL-4294952406 ISECT=8100350439 W3D=04
		192.168.200.100	192.168.200.150	TCP	74 00 - 53002 [518, ACK] Seq-0 ACK-1 WIN-5792 Len-0 853-1400 SACK_PCKM 15801-4294952400 15801-010535439 WS-04 66 55656 - 22 [ACK] Seq-1 ACK-1 WIN-64256 Len-0 TSVal-81053531 75801-4294952460
		192.168.200.100	192.168.200.150	TCP	00 50000 - 22 [AUK] Set[-1 AUK-1 MIN-04250 Left-0 1594L-010530439 15etCr-4294952400 66 53062 - 80 [ACK] Set[-1 AUK-1 MIN-04250 Left-0 TS94L-010530439 TSetCr-4294952406
		192.168.200.100	192.168.200.150	TCP	00 53002 - 80 [AUK] S0d=1 ACK=1 MIN=04250 L0N=0 ISVAL=810539439 ISOCT=4294952400 66 41182 - 21 [RST, ACK] S0d=1 ACK=1 MIN=04256 L0N=0 ISVAL=810539439 ISOCT=4294952466
		192.168.200.100	192.168.200.150	TCP	00 41102 - 21 [KS], ACK] SEQ-1 ACK-1 W1-04250 LeH-0 15V41-01035939 15021-4294952400 66 55656 - 22 [RST, ACK] SEQ-1 ACK-1 W1-64256 LeH-0 TSV41-810535439 TSCC-4294952466
		192.168.200.100	192.168.200.150	TCP	00 00000 - 22 [NS], ALK] SEQ=1 ACK=1 Win-04/20 LENE SVAL=8818030439 ISEC=429492400 66 53062 - 80 [RST, ACK] SEQ=1 ACK=1 Win-04/256 Lene 0 ISVal=880535439 ISEC=4294952466
	+1 30.770003633	152.100.200.100	192.100.200.150	TOP-	00 33002 - 00 [R31, AGK] 3EQ=1 AGK=1 HIH=04230 ERH=0 139R(=010333439 15ECH=4294932400
		192.168.200.100	192.168.200.150	TCP	74 50684 - 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
		192.168.200.100	192.168.200.150	TCP	74 54220 - 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PERM TSval=810535439 TSecr=0 WS=128

42 36.776179338 192.168.200.100	192.168.200.150 TCP	74 50684 - 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
43 36.776233880 192.168.200.100	192.168.200.150 TCP	74 54220 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
44 36.776330610 192.168.200.100	192.168.200.150 TCP	74 34648 - 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
45 36.776385694 192.168.200.100	192.168.200.150 TCP	74 33042 - 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
46 36.776402500 192.168.200.100	192.168.200.150 TCP	74 49814 - 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
47 36.776451284 192.168.200.150	192.168.200.100 TCP	60 199 → 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48 36.776451357 192.168.200.150	192.168.200.100 TCP	60 995 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49 36.776478201 192.168.200.100	192.168.200.150 TCP	74 46990 - 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
50 36.776496366 192.168.200.100	192.168.200.150 TCP	74 33206 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
51 36.776512221 192.168.200.100	192.168.200.150 TCP	74 60632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
52 36.776568606 192.168.200.100	192.168.200.150 TCP	74 49654 - 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
53 36.776671271 192.168.200.100	192.168.200.150 TCP	74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
54 36.776720715 192.168.200.100	192.168.200.150 TCP	74 54898 → 500 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
55 36.776813123 192.168.200.150	192.168.200.100 TCP	60 587 - 34648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
56 36.776843423 192.168.200.100	192.168.200.150 TCP	74 51534 - 487 SYN Seg=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
57 36.776904828 192.168.200.150	192.168.200.100 TCP	74 445 → 33042 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK PERM TSval=4294952466 TSecr=810535440 WS=64
58 36.776904922 192.168.200.150	192.168.200.100 TCP	60 256 - 49814 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
59 36.776904961 192.168.200.150	192.168.200.100 TCP	74 139 → 46990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK PERM TSval=4294952466 TSecr=810535440 WS=64
60 36.776905004 192.168.200.150	192.168.200.100 TCP	60 143 - 33206 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
61 36.776905043 192.168.200.150	192.168.200.100 TCP	74 25 → 60632 [SYN, ACK] Seg=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSVal=4294952466 TSecr=810535440 WS=64
62 36.776905082 192.168.200.150	192.168.200.100 TCP	60 110 → 49654 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
63 36.776905123 192.168.200.150	192.168.200.100 TCP	74 53 - 37282 [SYN, ACK] Seg=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSVal=4294952466 TSecr=810535440 WS=64
64 36.776905162 192.168.200.150	192.168.200.100 TCP	60 500 → 54898 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
65 36.776914772 192.168.200.100	192.168.200.150 TCP	66 33042 → 445 [ACK] Seg=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
66 36.776941020 192.168.200.100	192.168.200.150 TCP	66 46990 → 139 ACK Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
67 36.776962320 192.168.200.100	192.168.200.150 TCP	66 60632 → 25 [ACK] Seg=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
68 36,776983878 192,168,200,100	192.168.200.150 TCP	66 37282 - 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
69 36.777118481 192.168.200.150	192.168.200.100 TCP	60 487 → 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
70 36.777143014 192.168.200.100	192.168.200.150 TCP	74 56990 - 707 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
71 36.777186821 192.168.200.100	192.168.200.150 TCP	74 35638 → 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
72 36.777302991 192.168.200.100	192.168.200.150 TCP	74 34120 → 98 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PERM TSval=810535441 TSecr=0 WS=128
73 36.777337934 192.168.200.100	192.168.200.150 TCP	74 49780 - 78 SYN Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
74 36.777430632 192.168.200.150	192.168.200.100 TCP	60 707 → 56990 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
75 36.777430741 192.168.200.150	192.168.200.100 TCP	60 436 → 35638 RST, ACK Seq=1 Ack=1 Win=0 Len=0
76 36.777473018 192.168.200.100	192.168.200.150 TCP	74 36138 → 580 [SYN] Seg=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
77 36.777522494 192.168.200.100	192.168.200.150 TCP	74 52428 → 962 SYN Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
78 36.777623082 192.168.200.150	192.168.200.100 TCP	60 98 - 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79 36.777623149 192.168.200.150	192.168.200.100 TCP	60 78 - 49780 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
80 36.777645027 192.168.200.100	192.168.200.150 TCP	74 41874 - 764 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128

81 36,777680898 192,168,200,100	192,168,200,150 TCP	74 51506 - 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
82 36,777758636 192,168,200,150	192.168.200.100 TCP	60 580 → 36138 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
83 36.777758696 192.168.200.150	192.168.200.100 TCP	60 962 - 52428 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
84 36,777871245 192,168,200,150	192.168.200.100 TCP	60 764 - 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85 36.777871293 192.168.200.150	192.168.200.100 TCP	60 435 - 51506 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
86 36,777893298 192,168,200,100	192.168.200.150 TCP	66 33042 - 445 [RST, ACK] Seg=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
87 36.777912717 192.168.200.100	192.168.200.150 TCP	66 46990 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
88 36.777986759 192.168.200.100	192.168.200.150 TCP	66 60632 → 25 [RST, ACK] Seg=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
89 36.778031265 192.168.200.100	192.168.200.150 TCP	66 37282 → 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
90 36.778179978 192.168.200.100	192.168.200.150 TCP	74 51450 → 148 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
91 36.778200161 192.168.200.100	192.168.200.150 TCP	74 48448 - 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
92 36.778307830 192.168.200.100	192.168.200.150 TCP	74 54566 → 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
93 36.778385846 192.168.200.150	192.168.200.100 TCP	60 148 → 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
94 36.778385948 192.168.200.150	192.168.200.100 TCP	60 806 → 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
95 36.778449494 192.168.200.150	192.168.200.100 TCP	60 221 → 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
96 36.778482791 192.168.200.100	192.168.200.150 TCP	74 42420 1007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
97 36.778591226 192.168.200.100	192.168.200.150 TCP	74 34646 - 206 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
98 36.778614095 192.168.200.100	192.168.200.150 TCP	74 54202 - 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535442 TSecr=0 WS=128
99 36.778663064 192.168.200.150	192.168.200.100 TCP	60 1007 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
100 36.778721080 192.168.200.150	192.168.200.100 TCP	60 206 - 34646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
101 36.778759636 192.168.200.100 102 36.778781327 192.168.200.100	192.168.200.150 TCP 192.168.200.150 TCP	74 40318 - 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535442 TSecr=0 WS=128
102 36.778781327 192.168.200.100	192.168.200.150 TCP	74 51276 - 677 [SYN] Seg=0 Win=64240 Len=0 MSS=1400 SACK_PERM TSVal=810535442 TSecr=0 WS=128 60 131 - 54202 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
104 36,778864493 192,168,200,100	192.168.200.100 TCP	00 101 - 34202 [KS], ALK] SE(-1 ACK-1 WIN-0 LEN-0 74 3956 - 856 (SYN) Seg-0 Win-64240 Len=0 MSS=1460 SACK PERM TSVal=810535442 TSecr=0 WS=128
105 36.778939327 192.168.200.100	192.168.200.190 TCP	74 35300 - 350 [SN] Seg-9 MI-04280 EU-0 MSS-1400 SNCN_PERM TSVAL-510535442 TSECT-0 WS-125
106 36.778939427 192.168.200.150	192.168.200.100 TCP	00 352 - 1 9310 [RST, ACK] 3641-1 ACK-1 Win-0 Len-0 60 677 - 51276 [RST, ACK] 8647-1 ACK-1 Win-0 Len-0
107 36.778983153 192.168.200.100	192.168.200.150 TCP	74 47238 - 84 [STW] Seg=0 Win=64240 Len=0 MSS=1460 SACK PERM TSval=810535442 TSecr=0 WS=128
108 36.779029210 192.168.200.150	192.168.200.100 TCP	74 47256 - 04 [SM] Seque Milliosade Cellio Mostato Short Fixth Tstat of 0555442 Tsect - 6 WS-120
109 36.779055243 192.168.200.100	192.168.200.150 TCP	74 56542 - 807 [SYN] Seg=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535442 TSecr=0 WS=128
110 36,779122299 192,168,200,150	192.168.200.100 TCP	60 84 - 47238 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
111 36,779145004 192,168,200,100	192,168,200,150 TCP	74 40138 - 948 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
112 36.779252884 192.168.200.150	192.168.200.100 TCP	60 807 - 56542 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
113 36.779273781 192.168.200.100	192.168.200.150 TCP	74 43140 - 214 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
114 36.779309462 192.168.200.100	192.168.200.150 TCP	74 46886 → 106 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
115 36.779354564 192.168.200.150	192.168.200.100 TCP	60 948 - 40138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
116 36.779378630 192.168.200.100	192.168.200.150 TCP	74 50204 - 138 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
117 36.779397023 192.168.200.100	192.168.200.150 TCP	74 51262 - 884 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
118 36.779605648 192.168.200.150	192.168.200.100 TCP	60 214 - 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
119 36.779605750 192.168.200.150	192.168.200.100 TCP	60 106 46886 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

120 36, 779605798 192, 168, 200, 150	192.168.200.100 TCP	68.138 . 58284 [PST. ACK] Sec=1 Ack=1 Win=8 Len=8	
121 36.779605843 192.168.200.150 122 36.779637573 192.168.200.100	192.168.200.100 TCP 192.168.200.150 TCP	68 884 - 51262 [RST, ACK] Seg-1 Ack-1 Win-0 Len-0 74 44244 - 699 [SYN] Seg-0 Win-64240 Len-0 MSS=1460 SACK_PERM TSVal=810535443 TSecr=0 WS=128	
123 36.779776288 192.168.200.100 124 36.779856941 192.168.200.150 125 36.779911109 192.168.200.100	192.168.200.150 TCP 192.168.200.100 TCP 192.168.200.150 TCP	74 43630 . 783 [SYN] Seg-0 Min-64240 Len-0 MSS-1460 SACK_PERM TSVal-810535443 TSecr=0 WS-128 60 699 . 44244 [RST, ACK] Seg-1 Ack-1 Win-0 Len-0 74 55136 . 274 [SYN] Seg-0 Min-64240 Len-0 MSS-1460 SACK_PERM TSVal-810535443 TSecr=0 WS-128	
126 36.779946174 192.168.200.100 127 36.780035851 192.168.200.150	192.168.200.150 TCP 192.168.200.100 TCP	74 48522 _ 42 [SVH] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128 60 783 _ 436800 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 274 _ 55130 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
128 36.780121127 192.168.200.150 129 36.780149473 192.168.200.100 130 36.780170333 192.168.200.100	192.168.200.100 TCP 192.168.200.150 TCP 192.168.200.150 TCP	60 274 - 55136 [RST, ACK] Seq=1 Ack=1 Min=0 Len=0 74 57552 - 58 [SYN] Seq=0 Win=54240 Len=0 MSS=1460 SACK_PERM TSVal=810535443 TSecr=0 WS=128 74 40822 - 266 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535443 TSecr=0 WS=128	
131 36.780215176 192.168.200.150 132 36.780301750 192.168.200.150	192.168.200.100 TCP 192.168.200.100 TCP	60 42 - 40522 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 58 - 57552 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
133 36.780325837 192.168.200.100 134 36.780346429 192.168.200.100 135 36.780409818 192.168.200.100	192.168.200.150 TCP 192.168.200.150 TCP 192.168.200.150 TCP	74 37252 - 11 [SYN] Seg=0 Min-64240 Len=0 MS=1460 SACK, PERN TSVal=810535444 TSecr=0 WS=128 74 40648 - 235 [SYN] Seg=0 Win=64240 Len=0 MSS=1460 SACK, PERN TSVal=810535444 TSecr=0 WS=128 74 36548 - 739 [SYN] Seg=0 Win=64240 Len=0 MSS=1460 SACK, PERN TSVal=810535444 TSecr=0 WS=128	
136 36.780427899 192.168.200.100 137 36.780472830 192.168.200.100	192.168.200.150 TCP 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 74 52136 - 999 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PERM TSVal=810535444 TSecr=0 WS=128	
138 36.780490897 192.168.200.100 139 36.780577880 192.168.200.150 140 36.780577981 192.168.200.150	192.168.200.150 TCP 192.168.200.100 TCP 192.168.200.100 TCP	74 38022 - 317 [SYM] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535444 TSecr=0 WS=128 60 266 - 40822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 80.11 - 37252 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 80.11 - 37252 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
141 36.780578026 192.168.200.150 142 36.780578074 192.168.200.150	192.168.200.100 TCP 192.168.200.100 TCP	74 38022 - 317 [SN] SN]= WINT-8220 CHIEV MSS-1400 SACK_PERM ISVAL-81033444 ISOT-8 WS-128 00 11 - 37252 [RST, ACK] SNET ACK-1 WINT-8 LENE 00 125 - 40040 [RST, ACK] SNET ACK-1 WINT-8 LENE 01 255 - 40040 [RST, ACK] SNET ACK-1 WINT-8 LENE 00 55 - 38050 [RST, ACK] SNET ACK-1 WINT-8 LENE 00 55 - 38050 [RST, ACK] SNET ACK-1 WINT-8 LENE 00 99 - 500 [RST, ACK] SNET ACK-1 WINT-8 LENE 00 99 - 500 [RST, ACK] SNET ACK-1 WINT-8 LENE 00 99 - 500 [RST, ACK] SNET ACK-1 WINT-8 LENE 00 99 - 500 [RST, ACK] SNET ACK-1 WINT-8 LENE	
143 36.780578119 192.168.200.150 144 36.780578158 192.168.200.150 145 36.780578198 192.168.200.150	192.168.200.100 TCP 192.168.200.100 TCP 192.168.200.100 TCP	60 55 - 38866 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 999 - 52136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 917	
146 36.780617671 192.168.200.100 147 36.780701625 192.168.200.100	192.168.200.150 TCP 192.168.200.150 TCP	74 51192 - 241 [SYN] Seg-0 Win-64240 Len=0 MSS-1460 SACK PERM TSval=810535444 TSecr=0 WS-128	
148 36.780805705 192.168.200.150 149 36.780824718 192.168.200.100 150 36.780889399 192.168.200.150	192.168.200.100 TCP 192.168.200.150 TCP 192.168.200.100 TCP	60 901 _ 49446 [RST, ACK] Seperi Acksi Mineo Len=0 74 42642 _ 293 [SYI] Sep=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535444 TSecr=0 WS=128 60 241 _ 51192 [RST, ACK] Sep=1 Ack=1 Win=0 Len=0	
151 36.786906540 192.168.200.100 152 36.786958307 192.168.200.100	192.168.200.150 TCP 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 74 49014 - 137 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535444 TSecr=0 WS=128	
153 36.781007559 192.168.200.150 154 36.781116869 192.168.200.150 155 36.781116971 192.168.200.150	192.168.200.100 TCP 192.168.200.100 TCP 192.168.200.100 TCP	60 293 - 42642 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 974 - 41828 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 197 - 49914 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
156 36.781138769 192.168.200.100 157 36.781159927 192.168.200.100	192.168.200.150 TCP 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 74 42700 - 1014 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128	
158 36.781255484 192.168.200.150	192.168.200.100 TCP	60 223 - 45464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
159 36.781255593 192.168.200.150	192.168.200.100 TCP	60 1014 - 42700 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
160 36.781321950 192.168.200.100 161 36.781356928 192.168.200.100	192.168.200.150 TCP 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 74 45648 - 512 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PERM TSval=810535445 TSecr=0 WS=128	
162 36.781420319 192.168.200.100 163 36.781487105 192.168.200.150 164 36.781487210 192.168.200.150	192.168.200.150 TCP 192.168.200.100 TCP 192.168.200.100 TCP	74 53246 _ 354 [SYM] Seg=9 WinF64249 Len=9 MSS=1460 SACK_PERM TSVal=818535445 TSecr=0 WS=128 60 918 _ 55860 [RST, ACK] Seg=1 ACK=1 Win=0 Len=0 74 512 _ 45640 [SYN, ACK] Seg=0 ACK=1 Win=5792 Len=0 WSS=1460 SACK_PERM TSVal=4294952466 TSecr=810535445 WS=64	
165 36.781512468 192.168.200.100 166 36.781621871 192.168.200.150 167 36.781640161 192.168.200.100	192.168.200.150 TCP 192.168.200.100 TCP	66 45648 - 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466 60 354 - 53246 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
168 36.781734418 192.168.200.100	192.168.200.150 TCP 192.168.200.150 TCP 192.168.200.100 TCP	74 55186 858 [SYN] Seq=0 Win=04240 Len=0 MSS=1408 SACK_PERM TSVal=810535445 TSecr=0 WS=128 74 35806 663 [SYN] Seq=0 Win=64240 Len=0 MSS=1406 SACK_PERM TSVal=810535445 TSecr=0 WS=128 68 858 55186 [RST. ACK] Seq=1 Ack=1 Win=0 Len=0	
169 36.781812691 192.168.200.150 170 36.781989537 192.168.200.100 171 36.782069902 192.168.200.150	192.168.200.100 TCP 192.168.200.150 TCP 192.168.200.100 TCP	60 858 . 55186 [87], ACK) Seq:1 Ack:1 Min-8 Len=8 60 45648 . 512 [87], ACK) Seq:1 Ack:1 Min-82 Len=0 60 45648 . 512 [87], ACK] Seq:1 Ack:1 Min-82 Len=0 60 663 . 35860 [87], ACK] Seq:1 Ack:1 Min-8 Len=0 74 38218 . 581 [37]] Seq:0 Min-82428 Len=0 MSS-1460 SACK_PERM TSVal=816535445 TSecr=0 MS=128	
172 36.782120740 192.168.200.100 173 36.782140866 192.168.200.100 174 36.782215091 192.168.200.100	192.168.200.150 TCP 192.168.200.150 TCP 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 74 32950 - 570 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535445 TSecr=0 WS=128	
175 36.782248180 192.168.200.100 176 36.782390780 192.168.200.150 177 36.782390884 192.168.200.150	192.168.200.150 TCP 192.168.200.100 TCP 192.168.200.100 TCP	74 38396 _ 371 [SYM] Seg=0 WinF64240 Len=0 MSS=1480 SACK_PERM TSVal=818585445 TSecr=0 WS=128 60 681 _ 38210 [RST, ACK] Seg=1 ACk=1 Win=0 Len=0 60 561 _ 47898 [RST, ACK] Seg=1 ACk=1 Win=0 Len=0	
177 36.782390884 192.168.200.150 178 36.782390930 192.168.200.150 179 36.782390978 192.168.200.150	192.168.200.100 TCP 192.168.200.100 TCP	00 501 4/098 [RS1, ACK] SEQ1-1 ACK=1 WIN-0 LEN-0 60 570 32950 [RS1, ACK] SEQ1-1 ACK=1 WIN-0 LEN-0 60 371 38396 [RS1, ACK] SEQ1-1 ACK=1 WIN-0 LEN-0	
180 36.782422713 192.168.200.100 181 36.782459407 192.168.200.100 182 36.782534412 192.168.200.100	192.168.200.150 TCP 192.168.200.150 TCP 192.168.200.150 TCP	74 43862 - 966 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=516535446 TSecr=0 WS=128 74 42162 - 595 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=516535446 TSecr=0 WS=128 74 55234 - 838 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=516535446 TSecr=0 WS=128	
183 36.782582077 192.168.200.100	192.168.200.150 TCP	74 33102 - 51 [SYN] Seg=0 Win=64240 Len=0 MSS=1460 SACK PERM TSval=810535446 TSecr=0 WS=128	
185 36.782690655 192.168.200.150 186 36.782690713 192.168.200.150	192.168.200.100 TCP 192.168.200.100 TCP	60 966 _ 43862 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 595 _ 42162 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 838 _ 55234 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
187 36.782780538 192.168.200.100 188 36.782854473 192.168.200.150 189 36.782887993 192.168.200.100	192.168.200.150 TCP 192.168.200.100 TCP 192.168.200.150 TCP	74 58404 - 56 [SYN] seg-0 Wilm-62400 Len-0 MSS-1400 SACK_PERM TSVal=510535440 TSecr=0 WS=128 60 51 - 33102 [R5] AGK Seg-1 ACK±1 Win=0 Len-0 74 41104 - 144 [SYN] Seg-0 Win-62400 Len-0 MSS-1400 SACK_PERM TSVal=610535446 TSecr=0 WS=128 60 56 - 59404 [R5] AGK Seg-1 ACK±1 Win=0 Len-0	
190 36.783020182 192.168.200.150 191 36.783042408 192.168.200.100 192 36.783084243 192.168.200.100	192.168.200.100 TCP 192.168.200.150 TCP 192.168.200.150 TCP	60 56 _ 59404 [8ST, ACK] Segr <u>1 Ack=1 Win-8 Len-9</u> 74 42620 _ 874 [SYN] Seg-0 Win-64240 Len-9 MSS-1460 SACK_PERM TSVal-810535446 TSecr=0 WS-128 74 58110 _ 920 [SYN] Seg-0 Win-64240 Len-0 MSS-1460 SACK_PERM TSVal-810535446 TSecr=0 WS-128	
193 36.783329650 192.168.200.150 194 36 783329795 192 168 200 150	192.168.200.100 TCP 192.168.200.100 TCP	74 0010 - 320 [OII] SELPO MINIOZZO CELPO MOSCIZIO SICKI-PENN ISVAT-DIOSSANO ISECT-D MOSTIZO 60 144 - 47620 [RST, ACK] Sect-Ack:1 Win-9 Len-9 60 874 - 42620 [RST, ACK] Sect-Ack:1 Win-9 Len-9 60 920 - 58110 [RST, ACK] Sect-Ack:1 Win-9 Len-9	
195 36.783329836 192.168.200.150 196 36.783391839 192.168.200.100 197 36.783426736 192.168.200.100	192.168.200.100 TCP 192.168.200.150 TCP 192.168.200.150 TCP	66 920 - 58110 [RST, ACK] Seg-1 Ack=1 Win=0 Len=0 74 42696 - 964 [SYN] Seg=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535447 TSecr=0 WS=128 74 57372 - 333 [SYN] Seg=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535447 TSecr=0 WS=128	
197 30.793420730 192.106.200.100	192.100.200.130	14 31317 = 333   314  366-6 MIH-04546 FGH-6 USS-T406 SMYL-EGU 1989F-010393441 19601-6 MS-150	
198 36.783557923 192.168.200.150 199 36.783557992 192.168.200.150	192.168.200.100 TCP 192.168.200.100 TCP	60 964 42696 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 333 57372 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
200 36.785397588 192.168.200.100 201 36.785443154 192.168.200.100	192.168.200.150 TCP 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 74 37880 - 880 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128	
202 36.785551331 192.168.200.100 203 36.785624918 192.168.200.100 204 36 785675017 192 168 200 150	192.168.200.150 TCP 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 74 47472 - 743 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535449 TSecr=0 WS=128 62 930 - 52872 [SST AKK] Seq=1 Akki Seq=1 Akki Win=3 Len=0	
204 36.785675017 192.168.200.150 205 36.785675093 192.168.200.150 206 36.785721042 192.168.200.100	192.168.200.100 TCP 192.168.200.100 TCP 192.168.200.150 TCP	69 203 - 52872 [BST, ACK] Seq=1 Ack=1 Win=9 Len=0 60 880 - 37880 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 74 41984 - 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535449 TSecr=0 WS=128	
207 36.785738953 192.168.200.100 208 36.785824656 192.168.200.150 209 36.785824723 192.168.200.150	192.168.200.150 TCP 192.168.200.100 TCP 192.168.200.100 TCP	74 57854 _ 122 [SYM] Seg=0 WinF64240 Len=0 MSS=1460 SACK_PERM TSVal=810535449 TSecr=0 WS=128 60 939 _ 50932 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0 60 743 _ 47472 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0	
210 36.785880968 192.168.200.100 211 36.785943368 192.168.200.100	192.168.200.150 TCP 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 74 33718 - 359 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=8105355449 TSecr=0 WS=128	
212 36.786209855 192.168.200.150 213 36.786209978 192.168.200.150 214 36.786210019 192.168.200.150	192.168.200.100 TCP 192.168.200.100 TCP 192.168.200.100 TCP	60 831 - 41984 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0 60 122 - 57854 [RST ACK] Seg=1 Ack=1 Win=0 Len=0	
215 36.786210059 192.168.200.150 216 36.786254145 192.168.200.100	192.168.200.100 TCP 192.168.200.150 TCP	60 359 - 33718 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 74 35164 - 586 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128	
217 36.786292426 192.168.200.100 218 36.786455822 192.168.200.150 219 36.786455938 192.168.200.150	192.168.200.150 TCP 192.168.200.100 TCP 192.168.200.100 TCP	74 59734 _ 129 [SYN] Seg=0 WinF64240 Len=0 MSS=1460 SACK_PERM TSVal=810535450 TSecr=0 WS=128 60 586 _ 35104 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0 60 129 _ 59734 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0	
220 36.786788804 192.168.200.100 221 36.786815129 192.168.200.100	192.168.200.150 TCP 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 74 45154 - 400 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128	
222 36.786864594 192.168.200.100 223 36.786899954 192.168.200.100 224 36 787023089 192 168 200 150	192.168.200.150 TCP 192.168.200.150 TCP	74 38180 - 239 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=818535450 TSecr=0 WS=128 74 37952 - 520 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=818535450 TSecr=0 WS=128 65 545 - 45446 [STA AKK] Seq=1 AKK] Seq=1 AKK] SACK_PERM TSval=818535450 TSecr=0 WS=128	
224 36.787023089 192.168.200.150 225 36.787023195 192.168.200.150 226 36.787069390 192.168.200.100	192.168.200.100 TCP 192.168.200.100 TCP 192.168.200.150 TCP	60 545 - 45416 [RST, ACK] Seq=1 Ack=1 Win=9 Len=0 60 400 - 45154 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 74 43106 - 769 [SYN] Seq=0 Win=64240 Len=0 MSS=1400 SACK_PERM TSVal=810535450 TSecr=0 WS=128	
227 36.787191686 192.168.200.150 228 36.787191781 192.168.200.150 229 36.787229817 192.168.200.100	192.168.200.100 TCP 192.168.200.100 TCP 192.168.200.150 TCP	60 239 - 38180 [RST, ACK] Seq=1 Ack=1 Min=0 Len=0 60 520 - 37952 [RST, ACK] Seq=1 Ack=1 Min=0 Len=0 74 42460 - 489 [SYN] Seq=0 Min=62460 Len=0 MSS=1460 SACK_PERM TSVal=810535450 TSecr=0 MS=128	
230 36.787306501 192.168.200.150 231 36.787346317 192.168.200.100	192.168.200.100 TCP 192.168.200.150 TCP	74 #2400 - 405 [cm] Selj-8 WIN-04240 CENE 985-1400 SACK_PERM TSV81-80535430 TSCH-9 85-126 0769 - 43106 [RST, AKI) Seq-1 AKEH WIN-0 LENE 74 49988 - 19 [STN] Seq-0 WIN-64240 LENEO WSS-1460 SACK_PERM TSV81-816353451 TSCH-8 WS-128 74 44644 - 446 [STN] Seq-0 WIN-64240 LENEO WSS-1460 SACK_PERM TSV81-816353451 TSCH-8 WS-128	
232 36.787470054 192.168.200.100 233 36.787572344 192.168.200.150 234 36.787572497 192.168.200.150	192.168.200.150 TCP 192.168.200.100 TCP 192.168.200.100 TCP	74 44644 _ 846 [SYN] Seg=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535451 TSecr=0 WS=128 60 489 _ 42460 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0 60 19 _ 49988 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0	
235 36.787596289 192.168.200.100 236 36.787752589 192.168.200.150	192.168.200.150 TCP 192.168.200.100 TCP	00 19 - 49900 [R3], RANJ SULTA RANE WILLO EDITO 74 51723 - 345 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal=810535451 TSecr=0 WS=128 60 846 - 44644 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	

L'esame approfondito delle righe di log fornite ha rilevato una serie di indicatori di compromissioni (IOC) che confermano un'attività di ricognizione mirata e metodica. L'analisi si è concentrata sul traffico scambiato tra due host.

## Determinazione dei ruoli: attaccante e bersaglio.

L'identificazione dei ruoli è necessaria per comprendere la natura dell'attacco. L'analisi del traffico, basata sulla direzione e sul comportamento dei pacchetti, permettono di distinguere l'attaccante e il bersaglio.

#### Attaccante: 192.168.200.100

L'host attaccante è il soggetto attivo della comunicazione.

- Inizia le scansioni: tutti i pacchetti SYN provengono dall'indirizzo 192.168.200.100. È questo host che sta inviando le richieste di connessione a diverse porte del bersaglio.
- Inizia la mappatura: i pacchetti ARP che chiedono "Chi ha 192.168.200.150?" provengono da questo host, indicando che sta cercando attivamente di mappare la rete.

## Bersaglio: 192.168.200.150

Il bersaglio è l'host che è il destinatario dell'attività malevola.

• Risposte alle richieste: l'host 192.168.200.150 è la destinazione di tutti i pacchetti SYN e risponde con SYN, ACK (se la porta è aperta) o RST, ACK (se la porta è chiusa).

## Analisi delle scansioni TCP

Le righe di log mostrano un'intensa attività di scansione delle porte TCP. L'aggressore ha inviato pacchetti SYN per richiedere una connessione su diverse porte, ricevendo risposte che indicano lo stato di ciascuna porta.

- Scansione e Analisi della Porta 80 (HTTP):
  - L'attaccante ha inviato un pacchetto SYN sulla porta 80, ricevendo una risposta SYN, ACK dal bersaglio. Questa risposta indica che il servizio HTTP è attivo. L'attaccante ha poi completato il three-way handshake con un ACK, confermando che la porta è aperta. Questo è un metodo di scansione aggressivo e meno furtivo, noto come full-connect scan, che lascia una traccia più evidente nei log.
- Scansione e Analisi della Porta 443 (HTTPS): A differenza della porta 80, l'attaccante ha inviato un pacchetto SYN sulla porta 443, ma ha ricevuto una risposta RST, ACK. Questa risposta indica che la porta è chiusa. L'attaccante non ha continuato la connessione, confermando che la scansione su questa porta è fallita. Questo comportamento è tipico di una SYN scan (half-open scan), che permette all'aggressore di sondare le porte senza stabilire una connessione completa.
- Scansione e Analisi delle Porte 23 (Telnet) e 111 (RPC): Le risposte SYN, ACK a queste richieste indicano che i servizi Telnet e RPC sono attivi sul bersaglio. La presenza del servizio Telnet (porta 23) è una scoperta critica, in quanto si tratta di un protocollo non sicuro che trasmette i dati, comprese le credenziali, in chiaro. Questo rappresenta un'enorme vulnerabilità che un attaccante cercherà sicuramente di sfruttare. La porta 111 (RPC), un servizio per chiamate di procedura remota, è anch'essa un potenziale punto di ingresso che richiede un'indagine più approfondita.

## Mappatura della rete con ARP

Le righe di log mostrano anche un'attività di mappatura della rete a livello ARP. L'aggressore invia una richiesta per scoprire l'indirizzo MAC del bersaglio, e il bersaglio risponde con il proprio indirizzo MAC. Questa attività, pur non essendo di per sé un attacco, è una fase preparatoria cruciale che permette all'attaccante di avere una visione completa della rete.

### Considerazioni

L'analisi cumulativa degli IOC dimostra che l'attacco non è ancora nella fase di exploit, ma si trova in una fase avanzata di ricognizione. L'aggressore ha identificato un bersaglio vulnerabile e sta metodicamente raccogliendo tutte le informazioni necessarie per lanciare un attacco mirato e ad alta probabilità di successo.

#### Misure di sicurezza

## Risposta all'attacco attuale

- **Isolamento dell'Aggressore**: La prima e più critica azione è bloccare immediatamente l'indirizzo IP dell'aggressore (192.168.200.100) a livello di firewall o router, negandogli ogni ulteriore comunicazione con la rete interna.
- **Isolamento del Bersaglio**: L'host bersaglio (192.168.200.150) deve essere immediatamente isolato dalla rete per prevenire una potenziale compromissione o l'uso come punto di pivot.

#### Prevenzione attacchi futuri

- **Implementazione di un IDS/IPS**: L'installazione di un Intrusion Detection/Prevention System (IDS/IPS) è essenziale. Questo sistema è in grado di rilevare automaticamente schemi di traffico anomali, come le scansioni delle porte, e bloccare la fonte malevola in tempo reale.
- **Riduzione della Superficie di Attacco**: Tutti i servizi non essenziali e le porte non utilizzate sull'host devono essere disattivati. In particolare, il servizio Telnet (porta 23) dovrebbe essere disabilitato e sostituito con un'alternativa più sicura come SSH (Secure Shell).
- **Verifica delle Patch**: Assicurarsi che tutti i sistemi e le applicazioni siano costantemente aggiornati con le ultime patch di sicurezza per prevenire lo sfruttamento di vulnerabilità note.
- **Subnetting**: Utilizzare VLAN per segmentare la rete e isolare i sistemi critici da altri host, in modo da contenere un eventuale attacco.

#### Conclusioni

L'esercitazione ha dimostrato l'importanza fondamentale della Threat Intelligence e della capacità di analizzare i dati di rete per identificare segnali di un'attività malevola. La cattura di rete ha fornito prove inequivocabili di una fase di ricognizione aggressiva. Agendo prontamente sulla base degli IOC individuati, è possibile prevenire un attacco di successo e rafforzare le difese per il futuro.