S9-L3

Durante la lezione teorica, abbiamo visto la Threat Intelligence e gli indicatori di compromissione. Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto. Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark.

Analizzate la cattura attentamente e rispondete ai seguenti quesiti: Identificare eventuali IOC, ovvero evidenze di attacchi in corso.

In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati. Consigliate un'azione per ridurre gli impatti dell'attacco.

1	File	Edit	Viou	Go Car	nturo	Apply	. S	taticti	ice Te	Janhar	ov Wire	oloce '	Tools b	lolo				(Cattura_U	3_W1_L3.	pcapng			
Time																								
Time						9	~		<u> </u>	• •	, L													
19 36.774685555 192.168.200.150 192.168.200.100 TCP 74 2341304 [SYN, ACK] Seq=0 Ack=1 Win=5792 LE 21 36.774685656 192.168.200.150 192.168.200.100 TCP 60 449 .33878 [RST, ACK] Seq=1 Ack=1 Win=5792 LE 23 6.774685737 192.168.200.150 192.168.200.100 TCP 60 449 .33878 [RST, ACK] Seq=1 Ack=1 Win=6 Len-22 36.774685737 192.168.200.150 192.168.200.100 TCP 60 13552358 [RST, ACK] Seq=1 Ack=1 Win=6 Len-23 36.774685737 192.168.200.150 192.168.200.150 TCP 66 4130423 [ACK] Seq=1 Ack=1 Win=6 Len-24 36.77471047 192.168.200.100 192.168.200.150 TCP 66 4130423 [ACK] Seq=1 Ack=1 Win=64256 Len-20 43 6.775141247 192.168.200.100 192.168.200.150 TCP 66 5120111 [ACK] Seq=1 Ack=1 Win=64256 Len-20 43 6.775141247 192.168.200.150 192.168.200.150 TCP 66 4130423 [ACK] Seq=1 Ack=1 Win=64256 Len-20 43 6.775141243 192.168.200.150 192.168.200.100 TCP 60 93346138 [RST, ACK] Seq=1 Ack=1 Win=64256 Len-20 43 6.775141243 192.168.200.150 192.168.200.100 TCP 74 2141182 [SYN, ACK] Seq=1 Ack=1 Win=64256 Len-20 23 6.775144243 192.168.200.150 192.168.200.150 TCP 74 5174113 [SYN] Seq=0 Ack=1 Win=54256 Len-20 43 6.77537800 192.168.200.150 TCP 74 5565622 [SYN] Seq=0 Ack=1 Win=64256 Len-20 43 6.775503806 192.168.200.150 192.168.200.150 TCP 74 5565622 [SYN] Seq=0 Min=64240 Len-20 MSS=14 31 36.775503806 192.168.200.150 192.168.200.150 TCP 74 5565622 [SYN] Seq=0 Win=64240 Len-20 MSS=14 32 36.775503806 192.168.200.150 192.168.200.150 TCP 74 5565622 [SYN] Seq=0 Win=64240 Len-20 MSS=14 34 36.775503806 192.168.200.150 192.168.200.150 TCP 74 5565622 [SYN] Seq=0 Win=64240 Len-20 MSS=14 34 36.775503806 192.168.200.150 192.168.200.150 TCP 74 5565622 [SYN] Seq=0 Ack=1 Win=54256 Len-20 33 36.775503806 192.168.200.150 192.168.200.150 TCP 74 50.566622 [ACK] Seq=1 Ack=1 Win=64256 Len-20 33 36.775503836 192.168.200.150 192.168.200.150 TCP 74 50.566622 [ACK] Seq=1 Ack=1 Win=64256 Len-20 33 36.775503836 192.168.200.150 192.168.200.150 TCP 74 50.56622 [ACK] Seq=1 Ack=1 Win=64256 Len-20 33 36.775503836 192.168.	■ Ar	oply a di	isplay 1	filter <(Ctrl-/>																			
20 36.7748855652 192.168.200.150 192.168.200.100 TCP 64 43. 33878 [RST, ACK] Seq=8 Ack=1 Win=5792.1 E 23 36.774885577 192.168.200.150 192.168.200.100 TCP 60 554 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len= 23 36.774885776 192.168.200.150 192.168.200.100 TCP 60 135 52356 [RST, ACK] Seq=1 Ack=1 Win=0 Len= 24 36.7747080454 192.168.200.100 192.168.200.150 TCP 60 43304 23 [ACK] Seq=1 Ack=1 Win=6 Len= 25 36.77471072 192.168.200.100 192.168.200.150 TCP 66 56120 111 [AcK] Seq=1 Ack=1 Win=64256 Len=0 25 36.775141104 192.163.200.150 192.168.200.150 TCP 66 56120 111 [AcK] Seq=1 Ack=1 Win=64256 Len=0 27 36.77514104 192.163.200.150 192.168.200.150 TCP 66 56120 111 [AcK] Seq=1 Ack=1 Win=64256 Len=0 27 36.77514704 192.163.200.150 192.168.200.150 TCP 66 56120 111 [AcK] Seq=1 Ack=1 Win=64256 Len=0 27 36.775147049 192.168.200.100 TCP 192.168.200.150 TCP 66 51120 113 [SYN] Seq=0 Ack=1 Win=64256 Len=0 29 36.77537800 192.168.200.100 192.168.200.150 TCP 74 59174 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1 30 36.775386094 192.168.200.100 192.168.200.150 TCP 74 59174 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1 31 36.775524204 192.163.200.100 192.168.200.150 TCP 74 53962 36 [SYN] Seq=0 Win=64240 Len=0 MSS=1 33 36.775519454 192.163.200.100 192.168.200.150 TCP 74 53962 36 [SYN] Seq=0 Win=64240 Len=0 MSS=1 33 36.775519454 192.163.200.100 192.168.200.150 TCP 74 53962 36 [SYN] Seq=0 Win=64240 Len=0 MSS=1 33 36.775519454 192.163.200.100 192.168.200.150 TCP 66 5120 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 33 36.775519454 192.163.200.100 192.168.200.150 TCP 66 5120 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 33 36.775519354 192.163.200.100 192.168.200.150 TCP 66 5120 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 33 36.775893786 192.168.200.100 192.168.200.150 TCP 66 5120 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 33 36.775893786 192.168.200.100 192.168.200.150 TCP 66 53862 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 39 36.775913232 192.163.200.100 192.168.200.150 TCP 66 53862 80 [RST, ACK] Seq=1 Ack=1 Win=64	No.	1	Time		Sou	rce				Destir	ation		P	rotocol	Length	Info								
23 6,774685776 192.168.290.150 192.168.290.100 TCP 60 544. 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len-23 36.774685776 192.168.290.150 192.168.200.100 TCP 60 554. 356366 [RST, ACK] Seq=1 Ack=1 Win=0 Len-23 36.774685776 192.168.200.150 192.168.200.100 TCP 60 135. 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len-24 36.77471072 192.168.200.100 192.168.200.150 TCP 66 41304 - 23 [ACK] Seq=1 Ack=1 Win=64256 Len-6 25 36.77471072 192.168.200.100 192.168.200.150 TCP 66 5120 - 111 [ACK] Seq=1 Ack=1 Win=64256 Len-6 27 36.77511473 192.168.200.150 192.168.200.150 TCP 60 993 - 46138 [RST, ACK] Seq=1 Ack=1 Win=64256 Len-6 27 36.7751474048 192.168.200.150 192.168.200.150 TCP 74 21 - 41182 [SYM, ACK] Seq=1 Ack=1 Win=64256 Len-6 29 36.77537800 192.168.200.100 192.168.200.150 TCP 74 5174 - 4118 [SYM, ACK] Seq=1 Ack=1 Win=64256 Len-6 29 36.77537800 192.168.200.100 192.168.200.150 TCP 74 5174 - 4118 [SYM, ACK] Seq=1 Ack=1 Win=64256 Len-6 29 36.77537800 192.168.200.100 192.168.200.150 TCP 74 5174 - 4118 [SYM] Seq=0 Win=64240 Len-0 WSS=14 31 36.775582604 192.168.200.100 192.168.200.150 TCP 74 5174 - 4118 [SYM] Seq=0 Win=64240 Len-0 WSS=14 32 36.775580604 192.168.200.100 192.168.200.150 TCP 74 53062 - 80 [SYM] Seq=0 Win=64240 Len-0 WSS=14 32 36.775580604 192.168.200.150 TCP 74 53062 - 80 [SYM] Seq=0 Win=64240 Len-0 WSS=14 32 36.775580504 192.168.200.150 TCP 74 53062 - 80 [SYM] Seq=0 Win=64240 Len-0 WSS=14 32 36.775652497 192.168.200.150 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len-6 33 36.7756796938 192.168.200.150 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len-0 33 36.775679638 192.168.200.150 192.168.200.150 TCP 66 53062 - 80 [SYM] Seq=0 Ack=1 Win=64256 Len-0 33 36.775693898 192.168.200.150 192.168.200.150 TCP 66 53062 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len-0 33 36.775693898 192.168.200.150 192.168.200.150 TCP 66 53062 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len-0 33 36.775693898 192.168.200.150 192.168.200.150 TCP 66 53062 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len-0 33 36.77569366 192.168.200.100 192.		19 3	36.77	4685505	192	2.168.2	200.	150		192.:	168.200	9.100	Т	CP										
22 36.774685737 192.168.200.150 192.168.200.100 TCP 60 554 - 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len= 24 36.774760464 192.168.200.150 192.168.200.150 TCP 66 41304 - 23 [ACK] Seq=1 Ack=1 Win=0 Len= 25 36.77471072 192.168.200.100 192.168.200.150 TCP 66 56120 - 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 25 36.775141104 192.168.200.150 192.168.200.150 TCP 66 56120 - 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 27 36.7514127 192.168.200.150 192.168.200.100 TCP 66 56120 - 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 27 36.75141273 192.168.200.150 192.168.200.150 TCP 74 21 - 41182 [SYN, ACK] Seq=1 Ack=1 Win=54256 Len=0 28 36.77514048 192.168.200.100 192.168.200.150 TCP 66 41182 - 21 [ACK] Seq=0 Ack=1 Win=5792 LE 28 36.775337800 192.168.200.100 192.168.200.150 TCP 74 59174 - 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1 30 36.775386694 192.168.200.100 192.168.200.150 TCP 74 55656 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1 31 36.775524204 192.168.200.100 192.168.200.150 TCP 74 55656 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1 33 36.775589806 192.168.200.100 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=0 Len= 33 36.775619454 192.168.200.100 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=0 Len= 33 36.77569938 192.168.200.100 192.168.200.150 TCP 66 5120 - 111 [RST, ACK] Seq=1 Ack=1 Win=0 Len= 33 36.77569938 192.168.200.100 192.168.200.150 TCP 66 5120 - 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=3 43 36.775813232 192.168.200.100 192.168.200.150 TCP 66 55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 192.168.200.150 TCP 66 53062 MS [ACK] Seq=1 Ack=1 Win=64256 Len=0 192.168.200.150 TCP 66 53062 MS [ACK] Seq=1 Ack=1 Win=64256 Len=0 192.168.200.150 TCP 66 53062 MS [ACK] Seq=1 Ack=1 Win=64256 Len=0 192.168.200.150 TCP 66 53062 MS [ACK] Seq=1 Ack=1 Win=64256 Len=0 192.168.200.150 TCP 66 53062 MS [ACK] Seq=1 Ack=1 Win=64256 Len=0 192.168.200.150 TCP 66 53062 MS [ACK] Seq=1 Ack=1 Win=64256 Len=0 192.168.200.150 TCP 74 50664 MS [ACK] Seq=1 Ack=1 Win=64256 Len=0 192.168.200.150 TCP 74 50664 MS [ACK] Seq=1 Ack=1 Win=64256 Len=0 192.168.200.1																								
23 36.7746985776 192.168.200.150 192.168.200.100 TCP 66 133 - 52358 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 25 36.7747014072 192.168.200.100 192.168.200.150 TCP 66 41304 - 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 25 36.775141073 192.168.200.150 192.168.200.150 TCP 66 56120 - 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 27 36.775141073 192.168.200.150 192.168.200.100 TCP 69 993 - 46138 [RST, ACK] Seq=0 Ack=1 Win=64256 Len=0 27 36.775141073 192.168.200.150 192.168.200.150 TCP 66 993 - 46138 [RST, ACK] Seq=0 Ack=1 Win=64256 Len=0 28 36.775174048 192.168.200.100 192.168.200.150 TCP 66 41182 - 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 29 36.7753174048 192.168.200.100 192.168.200.150 TCP 74 59174 - 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1 30 36.775386694 192.168.200.100 192.168.200.150 TCP 74 55656 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1 42 36.775589366 192.168.200.100 192.168.200.150 TCP 74 53656 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1 43 36.775569369 192.168.200.150 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 33 36.775569369 192.168.200.150 192.168.200.150 TCP 66 56120 - 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 33 36.77569386 192.168.200.150 192.168.200.150 TCP 66 56120 - 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 33 36.775693698 192.168.200.150 192.168.200.150 TCP 66 56120 - 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 33 36.775803786 192.168.200.150 192.168.200.150 TCP 74 22 - 55565 [SYN, ACK] Seq=1 Ack=1 Win=64256 Len=0 33 36.775803786 192.168.200.150 192.168.200.150 TCP 66 55056 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 33 36.775803786 192.168.200.100 192.168.200.150 TCP 66 55056 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 33 36.775803786 192.168.200.100 192.168.200.150 TCP 66 55056 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 33 36.775803786 192.168.200.100 192.168.200.150 TCP 66 55056 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 33 36.775803786 192.168.200.100 192.168.200.150 TCP 66 55056 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 33 36.775803880 192.168.200.100 192.168.200.150 TCP 66 55056 - 22 [RST, ACK] Seq=1 Ack=1 Win=642																								
24 36.774700464 192.168.200.100 192.168.200.150 TCP 66 41304 - 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 25 36.775141107 192.168.200.150 192.168.200.150 TCP 66 56120 - 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 27 36.775141104 192.168.200.150 192.168.200.100 TCP 60 993 - 46138 [RST, ACK] Seq=1 Ack=1 Win=61256 Len=0 27 36.775141273 192.168.200.150 192.168.200.100 TCP 74 21 - 41182 [SVN, ACK] Seq=0 Ack=1 Win=5792 LE 28 36.775147408 192.168.200.100 192.168.200.150 TCP 66 41182 - 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 29 36.775387800 192.168.200.100 192.168.200.150 TCP 74 59174 - 113 [SVN] Seq=0 Win=64240 Len=0 MSS=1 40.775387800 192.168.200.100 192.168.200.150 TCP 74 55656 - 22 [SVN] Seq=0 Win=64240 Len=0 MSS=1 40.775389800 192.168.200.150 192.168.200.150 TCP 74 53062 - 80 [SVN] Seq=0 Win=64240 Len=0 MSS=1 40.775389800 192.168.200.150 192.168.200.100 TCP 60 113 - 59174 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 33 36.77559404 192.168.200.100 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 33 36.77559403 192.168.200.150 192.168.200.150 TCP 66 5120 - 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 33 36.77559403 192.168.200.150 192.168.200.150 TCP 66 55656 [SVN, ACK] Seq=1 Ack=1 Win=64256 Len=0 36 36.77559938 192.168.200.150 192.168.200.150 TCP 66 55656 [SVN, ACK] Seq=1 Ack=1 Win=64256 Len=0 33 36.775803780 192.168.200.150 192.168.200.150 TCP 66 55656 . 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 33 36.775803780 192.168.200.100 192.168.200.150 TCP 66 55656 . 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 39 36.775803780 192.168.200.100 192.168.200.150 TCP 66 55656 . 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 39 36.775803780 192.168.200.100 192.168.200.150 TCP 66 55656 . 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 40 36.775875876 192.168.200.100 192.168.200.150 TCP 66 55656 . 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 40 36.775875876 192.168.200.100 192.168.200.150 TCP 66 55656 . 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 40 36.775875876 192.168.200.100 192.168.200.150 TCP 66 55656 . 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 40 36.77587587																								
25 36.77411072 192.168.200.150 192.168.200.150 TCP 60 993 - 46138 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=6 27 36.775141104 192.168.200.150 192.168.200.100 TCP 74 21 - 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Le 28 36.775174048 192.168.200.100 192.168.200.150 TCP 66 41182 - 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 29 36.77538406 192.168.200.100 192.168.200.150 TCP 66 41182 - 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 30 36.775386694 192.168.200.100 192.168.200.150 TCP 74 55156 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=14 31 36.775524204 192.168.200.100 192.168.200.150 TCP 74 55062 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=14 32 36.775589450 192.168.200.100 192.168.200.150 TCP 74 55062 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=14 32 36.775569454 192.168.200.100 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 33 36.77569454 192.168.200.100 192.168.200.150 TCP 66 56120 - 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 33 36.77569988 192.168.200.150 192.168.200.150 TCP 66 56120 - 111 [RST, ACK] Seq=0 Ack=1 Win=6792 Le 37 36.775893780 192.168.200.150 192.168.200.150 TCP 66 55120 - 111 [RST, ACK] Seq=0 Ack=1 Win=5792 Le 37 36.775893780 192.168.200.150 192.168.200.150 TCP 66 55062 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 38 36.775893780 192.168.200.150 192.168.200.150 TCP 66 55062 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 38 36.775893780 192.168.200.100 192.168.200.150 TCP 66 55062 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 38 36.775893780 192.168.200.100 192.168.200.150 TCP 66 55062 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 38 36.775893780 192.168.200.100 192.168.200.150 TCP 66 55062 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 38 36.775893780 192.168.200.100 192.168.200.150 TCP 66 55062 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 38 36.77589380 192.168.200.100 192.168.200.150 TCP 66 55062 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 38 36.77589380 192.168.200.100 192.168.200.150 TCP 66 55062 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 38 36.77649380 192.168.200.100 192.168.200.150 TCP 74 54200 - 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36.77667821281 192.168.2																								
26 36.775141104 192.168.200.150 192.168.200.100 TCP 60 993 - 40138 [RST, ACK] Seq=1 Ack=1 Win=0 Lene 73 6.775174048 192.168.200.150 192.168.200.150 TCP 66 41182 - 21 [AcK] Seq=1 Ack=1 Win=04256 Lene 92 36.77537800 192.168.200.100 192.168.200.150 TCP 66 41182 - 21 [AcK] Seq=1 Ack=1 Win=64256 Lene 93 63.77537800 192.168.200.100 192.168.200.150 TCP 74 59174 - 113 [SYN] Seq=0 Win=64240 Lene 9 MSS=14 31 36.775524204 192.168.200.100 192.168.200.150 TCP 74 59556 - 22 [SYN] Seq=0 Win=64240 Lene 9 MSS=14 31 36.775524204 192.168.200.150 192.168.200.150 TCP 74 53062 - 80 [SYN] Seq=0 Win=64240 Lene 9 MSS=14 32 36.7755189806 192.168.200.150 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=0 Lene 33 36.775519454 192.168.200.100 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Lene 9 MSS=14 32 36.775508986 192.168.200.100 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Lene 9 MSS=14 32 36.775508497 192.168.200.150 192.168.200.150 TCP 66 5120 - 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Lene 9 MSS=14 36.7755083786 192.168.200.150 192.168.200.150 TCP 66 55656 - 22 [AcK] Seq=1 Ack=1 Win=64256 Lene 9 MSS=14 36.7755083786 192.168.200.150 192.168.200.150 TCP 66 55656 - 22 [AcK] Seq=1 Ack=1 Win=64256 Lene 9 MSS=14 36.7755083786 192.168.200.150 192.168.200.150 TCP 66 55656 - 22 [AcK] Seq=1 Ack=1 Win=64256 Lene 9 MSS=14 40 MS																			-					
27 36.775141273 192.168.200.150 192.168.200.150 TCP 74 21 — 41182 [SYN, ACK] Seq=0 Ack=1 Win=6792 LE 28 36.775174048 192.168.200.100 192.168.200.150 TCP 74 59174 — 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1 30 36.775386694 192.168.200.100 192.168.200.150 TCP 74 59174 — 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1 31 36.775524204 192.168.200.100 192.168.200.150 TCP 74 53062 — 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1 32 36.775589806 192.168.200.150 192.168.200.150 TCP 74 53062 — 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1 34 36.775589806 192.168.200.100 192.168.200.150 TCP 66 113 — 59174 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 33 36.7755919454 192.168.200.100 192.168.200.150 TCP 66 56120 — 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 36 36.7755796038 192.168.200.150 192.168.200.100 TCP 74 22 — 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Le 37 36.7755803766 192.168.200.150 192.168.200.150 TCP 74 80 — 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Le 37 36.7755803766 192.168.200.150 192.168.200.150 TCP 66 55656 — 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 39 36.775803786 192.168.200.100 192.168.200.150 TCP 66 55656 — 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 39 36.775803786 192.168.200.100 192.168.200.150 TCP 66 55656 — 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 39 36.775803786 192.168.200.100 192.168.200.150 TCP 66 55656 — 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 39 36.775803786 192.168.200.100 192.168.200.150 TCP 66 55656 — 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 39 36.775803880 192.168.200.100 192.168.200.150 TCP 66 55656 — 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 30 36.7756793880 192.168.200.100 192.168.200.150 TCP 66 53662 — 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 30 36.776578050 192.168.200.150 TCP 66 53662 — 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 30 36.776578050 192.168.200.150 TCP 74 50684 — 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1 42 36.77667806 192.168.200.100 192.168.200.150 TCP 74 50684 — 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1 42 36.77667806 192.168.200.100 192.168.200.150 TCP 74 50684 — 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1 42 36.776678060 192.168.2																								
28 36.775174048 192.168.200.100 192.168.200.150 TCP 66 41182 - 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 29 36.775337800 192.168.200.100 192.168.200.150 TCP 74 55656 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=14 31 36.775524204 192.168.200.100 192.168.200.150 TCP 74 55656 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=14 32 36.775589806 192.168.200.150 192.168.200.150 TCP 74 53062 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=14 36.775589806 192.168.200.100 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 33 36.775594204 192.168.200.100 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 48 36.77559638 192.168.200.150 192.168.200.150 TCP 66 56120 - 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 48 36.775797904 192.168.200.150 192.168.200.100 TCP 74 80 - 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 38 36.775803786 192.168.200.100 192.168.200.150 TCP 66 55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 38 36.775813232 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 39 36.7758061964 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 39 36.7759875876 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 42 36.776075938 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 42 36.776035894 192.168.200.100 192.168.200.150 TCP 74 50684 - 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1 43 36.776385094 192.168.200.100 192.168.200.150 TCP 74 50684 - 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1 45 36.776451284 192.168.200.100 192.168.200.150 TCP 74 40684 - 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1 45 36.776451284 192.168.200.100 192.168.200.150 TCP 74 40684 - 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1 45 36.776451284 192.168.200.100 192.168.200.150 TCP 74 40684 - 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1 45 36.776451284 192.168.200.150 192.168.200.150 TCP 74 40684 - 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1 45 36.776451284 192.168.200.100 192.168.200.150 TCP 74 43042 - 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36.77																								
29 36.775337800 192.168.200.100 192.168.200.150 TCP 74 55056 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=14 30 36.775580806 192.168.200.100 192.168.200.150 TCP 74 55065 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=14 32 36.775589806 192.168.200.150 192.168.200.150 TCP 74 55062 - 30 [SYN] Seq=0 Win=64240 Len=0 MSS=14 32 36.775589806 192.168.200.150 192.168.200.150 TCP 66 113 - 59174 [RST, ACK] Seq=1 Ack=1 Win=64256 L 34 36.77559247 192.168.200.100 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=64256 L 36 36.775796938 192.168.200.150 192.168.200.150 TCP 66 55062 - 111 [RST, ACK] Seq=1 Ack=1 Win=54256 L 36 36.775796938 192.168.200.150 192.168.200.150 TCP 74 80 - 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Le 37 36.775803786 192.168.200.150 192.168.200.150 TCP 66 55656 Syn, ACK] Seq=0 Ack=1 Win=5792 Le 37 36.775803786 192.168.200.160 192.168.200.150 TCP 66 53062 [SYN, ACK] Seq=1 Ack=1 Win=64256 Len=0 38 36.7755813232 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [AcK] Seq=1 Ack=1 Win=64256 Len=0 39 36.775801349 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 40 36.775975876 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 40 36.775975876 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 42 36.77617933 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 42 36.77617933 192.168.200.100 192.168.200.150 TCP 74 50684 - 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1 42 36.776330610 192.168.200.100 192.168.200.150 TCP 74 50684 - 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1 43 36.77631284 192.168.200.100 192.168.200.150 TCP 74 34648 - 557 [SYN] Seq=0 Win=64240 Len=0 MSS=1 45 36.776451284 192.168.200.150 TCP 74 34648 - 557 [SYN] Seq=0 Win=64240 Len=0 MSS=1 48 36.776451284 192.168.200.150 192.168.200.150 TCP 74 34648 - 557 [SYN] Seq=0 Win=64240 Len=0 MSS=1 48 36.776451284 192.168.200.150 192.168.200.150 TCP 74 49864 - 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 48 36.776451281 192.168.200.150 192.168.200.1																								
30 36.775386694 192.168.200.100 192.168.200.150 TCP 74 55656 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=14 31 36.775524204 192.168.200.150 192.168.200.150 TCP 74 55062 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=14 32 36.775514945 192.168.200.100 192.168.200.150 TCP 66 113 - 59174 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=3 36.775619454 192.168.200.100 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=3 36.775652497 192.168.200.150 192.168.200.150 TCP 66 56120 - 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=3 36.7757970938 192.168.200.150 192.168.200.100 TCP 74 22 - 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Lens 3 36.775803786 192.168.200.150 192.168.200.100 TCP 74 80 - 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Lens 3 36.775803786 192.168.200.100 192.168.200.150 TCP 66 55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 38 36.77581323 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [AcK] Seq=1 Ack=1 Win=64256 Len=0 38 36.77581323 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [AcK] Seq=1 Ack=1 Win=64256 Len=0 39 36.775861964 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [AcK] Seq=1 Ack=1 Win=64256 Len=0 39 36.775805583 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [AcK] Seq=1 Ack=1 Win=64256 Len=0 30 36.77580583 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [AcK] Seq=1 Ack=1 Win=64256 Len=0 30 36.77580583 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 30 36.77580583 192.168.200.100 192.168.200.150 TCP 74 50684 - 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1 43 36.776385694 192.168.200.100 192.168.200.150 TCP 74 50684 - 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1 45 36.776385694 192.168.200.100 192.168.200.150 TCP 74 30464 - 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36.776385694 192.168.200.100 192.168.200.150 TCP 74 34648 - 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36.776345200 192.168.200.100 192.168.200.150 TCP 74 36468 - 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36.776345200 192.168.200.150 192.168.200.150 TCP 74 40690 - 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36.776545200 192.168.2	_								_															
31 36.775524204 192.168.200.100 192.168.200.150 TCP 74 53062 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=14 32 36.775589806 192.168.200.100 192.168.200.100 TCP 60 113 - 59174 [RST, ACK] Seq=1 Ack=1 Win=64256 Len 36.775652497 192.168.200.100 192.168.200.150 TCP 66 41394 - 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len 36 36.775652497 192.168.200.100 192.168.200.100 TCP 66 56120 - 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len 36 36.775797094 192.168.200.150 192.168.200.100 TCP 74 22 - 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Le 37 36.775893786 192.168.200.150 192.168.200.150 TCP 66 55656 - 22 [AcK] Seq=1 Ack=1 Win=64256 Len=0 38 36.775893786 192.168.200.100 192.168.200.150 TCP 66 55656 - 22 [AcK] Seq=1 Ack=1 Win=64256 Len=0 38 36.775813232 192.168.200.100 192.168.200.150 TCP 66 53662 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 39 36.775861964 192.168.200.100 192.168.200.150 TCP 66 53656 - 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 39 36.775905853 192.168.200.100 192.168.200.150 TCP 66 53665 - 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 39 36.77630380 192.168.200.100 192.168.200.150 TCP 66 53665 - 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len 43 36.77630380 192.168.200.100 192.168.200.150 TCP 66 53665 - 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len 43 36.77633081 192.168.200.100 192.168.200.150 TCP 74 54684 - 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1 43 36.77633650 192.168.200.100 192.168.200.150 TCP 74 54684 - 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1 45 36.776385694 192.168.200.100 192.168.200.150 TCP 74 34648 - 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1 46 36.776432081 192.168.200.150 TCP 74 49814 - 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 46 36.776432081 192.168.200.150 TCP 74 49814 - 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36-776451284 TSP_168.200.150 TCP 74 49814 - 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36-776451284 TSP_168.200.150 TCP 74 49814 - 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36-776451284 TSP_168.200.150 TCP 74 49814 - 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36-776451281 TSP_168.200.150 TCP 74 49814 - 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36-77645																		_						
32 36.775589806 192.168.200.150 192.168.200.100 TCP 60 113 - 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=33 36.775619454 192.168.200.100 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=64256 LS 35 36.775796938 192.168.200.150 192.168.200.100 TCP 66 551620 - 111 [RST, ACK] Seq=1 Ack=1 Win=64256 LS 35 36.775797004 192.168.200.150 192.168.200.100 TCP 74 22 - 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 LS 37 36.775893786 192.168.200.150 192.168.200.100 TCP 74 80 - 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 LS 37 36.775893786 192.168.200.100 192.168.200.150 TCP 66 55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 38 36.775813232 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 39 36.775861964 192.168.200.100 192.168.200.150 TCP 66 55656 - 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 40 36.775975876 192.168.200.100 192.168.200.150 TCP 66 55656 - 22 [RST, ACK] Seq=1 Ack=1 Win=64256 LS 41 36.776095853 192.168.200.100 192.168.200.150 TCP 66 55656 - 22 [RST, ACK] Seq=1 Ack=1 Win=64256 LS 41 36.776095853 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 LS 42 36.776179338 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [RST, ACK] Seq=0 Win=64240 Len=0 WSS=1 43 36.77633380 192.168.200.100 192.168.200.150 TCP 74 50684 - 199 [SYN] Seq=0 Win=64240 Len=0 WSS=1 44 36.77633380 192.168.200.100 192.168.200.150 TCP 74 34648 - 587 [SYN] Seq=0 Win=64240 Len=0 WSS=1 45 36.776385694 192.168.200.100 192.168.200.150 TCP 74 34648 - 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36-776451284 199.168.200.100 192.168.200.150 TCP 74 49814 - 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36-776451284 199.168.200.150 TCP 74 49814 - 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36-776451284 199.168.200.150 TCP 74 49814 - 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36-776451284 199.168.200.150 TCP 74 49814 - 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36-776451284 199.168.200.150 TCP 74 49814 - 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36-776451281 192.168.200.150 TCP 74 49864 - 110 [SYN] Seq=0 Win=64240 Len=0 M																								
33 36.775619454 192.168.200.100 192.168.200.150 TCP 66 41304 - 23 [RST, ACK] Seq=1 Ack=1 Win=64256 L 34 36.775652497 192.168.200.150 192.168.200.150 TCP 66 56120 - 111 [RST, ACK] Seq=2 Ack=1 Win=54256 L 35 36.775797604 192.168.200.150 192.168.200.100 TCP 74 22 - 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Le 37 36.775803786 192.168.200.100 192.168.200.150 TCP 66 55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 38 36.775813232 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 39 36.77581361964 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 40 36.775975876 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 40 36.775975876 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 40 36.776005853 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 42 36.776179338 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 43 36.776330810 192.168.200.100 192.168.200.150 TCP 74 50684 - 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1 43 36.776330810 192.168.200.100 192.168.200.150 TCP 74 50684 - 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1 45 36.776380610 192.168.200.100 192.168.200.150 TCP 74 34648 - 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1 45 36.776380610 192.168.200.100 192.168.200.150 TCP 74 49814 - 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 46 36.7764951284 192.168.200.150 192.168.200.150 TCP 74 49814 - 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 46 36.77649510 192.168.200.150 192.168.200.150 TCP 74 46990 - 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36.776451284 192.168.200.150 192.168.200.150 TCP 74 46990 - 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776495066 192.168.200.150 192.168.200.150 TCP 74 46990 - 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776618201 192.168.200.100 192.168.200.150 TCP 74 46900 - 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.7766180606 192.168.200.100 192.168.200.150 TCP 74 469636 192.168.200.100 192.168.200.150 TCP 74 469636 1																								
34 36.775652497 192.168.200.100 192.168.200.150 TCP 66 56120 — 111 [RST, ACK] Seq=1 Ack=1 Win=64256 35 36.775796938 192.168.200.150 192.168.200.100 TCP 74 22 — 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Le 37 36.775797004 192.168.200.100 192.168.200.150 TCP 74 80 — 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Le 37 36.775803786 192.168.200.100 192.168.200.150 TCP 66 55656 — 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 38 36.775813232 192.168.200.100 192.168.200.150 TCP 66 55656 — 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 39 36.775861964 192.168.200.100 192.168.200.150 TCP 66 53062 — 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 4 36.775975876 192.168.200.100 192.168.200.150 TCP 66 55656 — 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 4 36.77607938 192.168.200.100 192.168.200.150 TCP 66 53062 — 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 4 36.776179338 192.168.200.100 192.168.200.150 TCP 66 53062 — 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 4 36.776179338 192.168.200.100 192.168.200.150 TCP 74 50684 — 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1 4 36.776330610 192.168.200.100 192.168.200.150 TCP 74 54220 — 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1 4 36.776330610 192.168.200.100 192.168.200.150 TCP 74 33042 — 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1 4 36.776492500 192.168.200.100 192.168.200.150 TCP 74 33042 — 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1 4 36.776492500 192.168.200.100 192.168.200.150 TCP 74 49814 — 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 4 36.776492500 192.168.200.150 TCP 74 49814 — 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 4 36.776492501 192.168.200.150 TCP 74 49814 — 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 4 36.77649261 192.168.200.150 192.168.200.150 TCP 74 49814 — 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 4 50.776496366 192.168.200.150 192.168.200.150 TCP 74 49814 — 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50.6776496366 192.168.200.150 192.168.200.150 TCP 74 46990 — 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50.6776540666 192.168.200.100 192.168.200.150 TCP 74 46990 — 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50.776563666 192.168.200.100 192.168.200.150 TCP 74 46990 — 139 [SYN																								
35 36.775796938 192.168.200.150 192.168.200.100 TCP 74 22 - 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Letter 36 36.775797004 192.168.200.150 192.168.200.100 TCP 74 80 - 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Letter 37 36.775803786 192.168.200.100 192.168.200.150 TCP 66 55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 38 36.775813232 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 39 36.775861964 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 40 36.775975876 192.168.200.100 192.168.200.150 TCP 66 55656 - 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 40 36.775975876 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 42 36.776179338 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 42 36.776179338 192.168.200.100 192.168.200.150 TCP 74 50684 - 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1 43 36.776339610 192.168.200.100 192.168.200.150 TCP 74 54220 - 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1 44 36.776396610 192.168.200.100 192.168.200.150 TCP 74 34048 - 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1 46 36.77649250 192.168.200.100 192.168.200.150 TCP 74 34042 - 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1 46 36.77649250 192.168.200.100 192.168.200.150 TCP 74 49814 - 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36-776451284 192.168.200.150 192.168.200.150 TCP 74 49814 - 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 49 36.77649366 192.168.200.150 192.168.200.150 TCP 74 46990 - 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776496366 192.168.200.150 192.168.200.150 TCP 74 46990 - 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776496366 192.168.200.100 192.168.200.150 TCP 74 46990 - 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776696666 192.168.200.100 192.168.200.150 TCP 74 46990 - 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776696666 192.168.200.100 192.168.200.150 TCP 74 46990 - 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776696666 192.168.200.100 192.168.200.150 TCP 74 46990 - 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776696																		_	_					
36 36.775797004 192.168.200.150 192.168.200.100 TCP 74 80 → 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Letter 37 36.775803786 192.168.200.100 192.168.200.150 TCP 66 55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 38 36.775813232 192.168.200.100 192.168.200.150 TCP 66 53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 39 36.775861964 192.168.200.100 192.168.200.150 TCP 66 53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 40 36.775975876 192.168.200.100 192.168.200.150 TCP 66 55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 40 36.775075853 192.168.200.100 192.168.200.150 TCP 66 53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 42 36.776179338 192.168.200.100 192.168.200.150 TCP 66 53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1 43 36.776233880 192.168.200.100 192.168.200.150 TCP 74 50684 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1 44 36.776330610 192.168.200.100 192.168.200.150 TCP 74 54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1 45 36.776385694 192.168.200.100 192.168.200.150 TCP 74 33042 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1 46 36.776491284 192.168.200.100 192.168.200.150 TCP 74 49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36.776451387 192.168.200.150 TCP 74 40910 → 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 49 36.776496366 192.168.200.150 192.168.200.150 TCP 74 46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 49 36.776451387 192.168.200.150 TCP 74 46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 51 36.776496366 192.168.200.100 192.168.200.150 TCP 74 46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 51 36.776512221 192.168.200.100 192.168.200.150 TCP 74 46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 52 36.776568606 192.168.200.100 192.168.200.150 TCP 74 46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 52 36.776568606 192.168.200.100 192.168.200.150 TCP 74 46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 52 36.776568606 192.168.200.100 192.168.200.150 TCP 74 46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 52 36.776568606 192.168.200.100 192.168.200.150 TCP 74 46954 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 52 36.776568606 192.168.200.100 192	_								_															
37 36.775803786 192.168.200.100 192.168.200.150 TCP 66 55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 38 36.775813232 192.168.200.100 192.168.200.150 TCP 66 53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 39 36.775876 192.168.200.100 192.168.200.150 TCP 66 55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 40 36.775975876 192.168.200.100 192.168.200.150 TCP 66 55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 42 36.776095853 192.168.200.100 192.168.200.150 TCP 66 55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 42 36.776179338 192.168.200.100 192.168.200.150 TCP 74 50684 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1 43 36.776338610 192.168.200.100 192.168.200.150 TCP 74 54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1 44 36.776338610 192.168.200.100 192.168.200.150 TCP 74 34648 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1 45 36.776385694 192.168.200.100 192.168.200.150 TCP 74 49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36.776451284 192.168.200.150 192.168.200.150 TCP 74 49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 48 36.776478201 192.168.200.150 192.168.200.150 TCP 74 49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776496366 192.168.200.100 192.168.200.150 TCP 74 46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776496366 192.168.200.100 192.168.200.150 TCP 74 46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776496366 192.168.200.100 192.168.200.150 TCP 74 46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776658606 192.168.200.100 192.168.200.150 TCP 74 46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776658606 192.168.200.100 192.168.200.150 TCP 74 49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776658606 192.168.200.100 192.168.200.150 TCP 74 49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776658606 192.168.200.100 192.168.200.150 TCP 74 49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776658606 192.168.200.100 192.168.200.150 TCP 74 49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776658606 192.168.200.100 192.168.200.150 TCP 74 49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776658606 19																								
38 36.775813232 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 39 36.775861964 192.168.200.100 192.168.200.150 TCP 66 41182 - 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 40 36.775975876 192.168.200.100 192.168.200.150 TCP 66 55656 - 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 41 36.776005853 192.168.200.100 192.168.200.150 TCP 66 53062 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 42 36.776179338 192.168.200.100 192.168.200.150 TCP 74 50684 - 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1 43 36.776233880 192.168.200.100 192.168.200.150 TCP 74 54220 - 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1 45 36.776330610 192.168.200.100 192.168.200.150 TCP 74 34648 - 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1 45 36.776402500 192.168.200.100 192.168.200.150 TCP 74 33042 - 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1 46 36.776402500 192.168.200.100 192.168.200.150 TCP 74 49814 - 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36-776451284 192.168.200.150 192.168.200.100 TCP 60 199 - 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len= 49 36.776478201 192.168.200.150 192.168.200.150 TCP 74 46990 - 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776496366 192.168.200.150 192.168.200.150 TCP 74 46990 - 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776496366 192.168.200.100 192.168.200.150 TCP 74 46990 - 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776512221 192.168.200.100 192.168.200.150 TCP 74 49654 - 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776512221 192.168.200.100 192.168.200.150 TCP 74 49654 - 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.7766712271 192.168.200.100 192.168.200.150 TCP 74 49654 - 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776671271 192.168.200.100 192.168.200.150 TCP 74 49654 - 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776671271 192.168.200.100 192.168.200.150 TCP 74 49654 - 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776671271 192.168.200.100 192.168.200.150 TCP 74 49654 - 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776671271 192.168.200.100 192.168.200.150 TCP 74 49654 - 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.77667127																				-				
39 36.775861964 192.168.200.100 192.168.200.150 TCP 66 41182 — 21 [RST, ACK] Seq=1 Ack=1 Win=64256 L 40 36.775975876 192.168.200.100 192.168.200.150 TCP 66 55656 — 22 [RST, ACK] Seq=1 Ack=1 Win=64256 L 41 36.776005853 192.168.200.100 192.168.200.150 TCP 66 53062 — 80 [RST, ACK] Seq=1 Ack=1 Win=64256 L 42 36.776179338 192.168.200.100 192.168.200.150 TCP 74 50684 — 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1 43 36.77633880 192.168.200.100 192.168.200.150 TCP 74 54220 — 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1 44 36.776330610 192.168.200.100 192.168.200.150 TCP 74 34648 — 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1 45 36.776385694 192.168.200.100 192.168.200.150 TCP 74 33042 — 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36.776451284 192.168.200.150 192.168.200.150 TCP 74 49814 — 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36.776451284 192.168.200.150 192.168.200.100 TCP 60 199 — 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=49 36.776478201 192.168.200.150 192.168.200.150 TCP 74 49814 — 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776496366 192.168.200.150 192.168.200.150 TCP 74 46990 — 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 51 36.776512221 192.168.200.100 192.168.200.150 TCP 74 60632 — 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776568606 192.168.200.100 192.168.200.150 TCP 74 49694 — 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776568606 192.168.200.100 192.168.200.150 TCP 74 49694 — 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776568606 192.168.200.100 192.168.200.150 TCP 74 49694 — 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.7765671271 192.168.200.100 192.168.200.150 TCP 74 49654 — 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 49654 — 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 49654 — 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 49654 — 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 49654 — 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.																			-					
40 36.775975876 192.168.200.100 192.168.200.150 TCP 66 55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 L 41 36.776005853 192.168.200.100 192.168.200.150 TCP 66 53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 L 42 36.776179338 192.168.200.100 192.168.200.150 TCP 74 50684 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1 43 36.77633860 192.168.200.100 192.168.200.150 TCP 74 54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1 45 36.776385694 192.168.200.100 192.168.200.150 TCP 74 34648 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1 45 36.776385694 192.168.200.100 192.168.200.150 TCP 74 33042 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1 46 36.776402500 192.168.200.100 192.168.200.150 TCP 74 49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36.776451284 192.168.200.150 192.168.200.100 TCP 60 199 → 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len= 49 36.776478201 192.168.200.150 192.168.200.150 TCP 74 46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776496366 192.168.200.100 192.168.200.150 TCP 74 46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 51 36.77657656806 192.168.200.100 192.168.200.150 TCP 74 49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 52 36.776568606 192.168.200.100 192.168.200.150 TCP 74 49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100																								
41 36.776005853 192.168.200.100 192.168.200.150 TCP 66 53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 L 42 36.776179338 192.168.200.100 192.168.200.150 TCP 74 50684 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1 43 36.776233880 192.168.200.100 192.168.200.150 TCP 74 54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1 44 36.776330610 192.168.200.100 192.168.200.150 TCP 74 34648 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1 45 36.776385694 192.168.200.100 192.168.200.150 TCP 74 33042 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1 46 36.776492500 192.168.200.100 192.168.200.150 TCP 74 49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36-776451284 192.168.200.150 192.168.200.100 TCP 60 199 → 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=48 36.776478201 192.168.200.150 192.168.200.100 TCP 60 995 → 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=49 36.776496366 192.168.200.150 192.168.200.150 TCP 74 46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776496366 192.168.200.100 192.168.200.150 TCP 74 33206 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1 51 36.776512221 192.168.200.100 192.168.200.150 TCP 74 60632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1 52 36.776568606 192.168.200.100 192.168.200.150 TCP 74 49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.																								
42 36.776179338 192.168.200.100 192.168.200.150 TCP 74 50684 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1 43 36.776233880 192.168.200.100 192.168.200.150 TCP 74 54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1 44 36.776330610 192.168.200.100 192.168.200.150 TCP 74 34648 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1 45 36.776385694 192.168.200.100 192.168.200.150 TCP 74 33042 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1 46 36.776402500 192.168.200.100 192.168.200.150 TCP 74 49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36.776451284 192.168.200.150 192.168.200.100 TCP 60 199 → 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len= 49 36.776478201 192.168.200.150 192.168.200.100 TCP 60 995 → 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len= 49 36.776478201 192.168.200.100 192.168.200.150 TCP 74 46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776496366 192.168.200.100 192.168.200.150 TCP 74 33206 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1 51 36.776512221 192.168.200.100 192.168.200.150 TCP 74 60632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1 52 36.776568606 192.168.200.100 192.168.200.150 TCP 74 49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 54 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 54 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 54 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 54 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 54 36.776671271 192.168.200.100 192																								
43 36.776233880 192.168.200.100 192.168.200.150 TCP 74 54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1 44 36.776330610 192.168.200.100 192.168.200.150 TCP 74 34648 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1 45 36.776385694 192.168.200.100 192.168.200.150 TCP 74 33042 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1 46 36.776402500 192.168.200.100 192.168.200.150 TCP 74 49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36.776451284 192.168.200.150 192.168.200.100 TCP 60 199 → 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=48 36.776451357 192.168.200.150 192.168.200.100 TCP 60 995 → 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=49 36.776478201 192.168.200.150 192.168.200.150 TCP 74 46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776496366 192.168.200.100 192.168.200.150 TCP 74 46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 51 36.776512221 192.168.200.100 192.168.200.150 TCP 74 60632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1 52 36.776568606 192.168.200.100 192.168.200.150 TCP 74 49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 42 53 [SYN] Seq=0									_				Т	СР										
45 36.776385694 192.168.200.100 192.168.200.150 TCP 74 33042 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1 46 36.776492500 192.168.200.100 192.168.200.150 TCP 74 49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1 47 36.776451284 192.168.200.150 192.168.200.100 TCP 60 199 → 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=48 36.776451357 192.168.200.150 192.168.200.100 TCP 60 995 → 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=49 36.776478201 192.168.200.150 192.168.200.150 TCP 74 46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776496366 192.168.200.100 192.168.200.150 TCP 74 33206 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1 51 36.776512221 192.168.200.100 192.168.200.150 TCP 74 60632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1 52 36.776568606 192.168.200.100 192.168.200.150 TCP 74 49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.		43 3	36.77	6233880	192	2.168.2	200.	100		192.	168.200	9.150	Т	СР										
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$		44 3	36.77	6330610	192	2.168.2	200.	100		192.	168.200	9.150	Т	CP	74	34648	→ 587	[SYN]	Seq=	9 Win=	64240	Len=6	MSS=	1460
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$		45 3	36.77	6385694	192	2.168.2	200.	100		192.	168.200	9.150	Т	CP	74	33042	→ 445	[SYN]	Seq=	0 Win=	64240	Len=6	MSS=	1460
48 36.776451357 192.168.200.150 192.168.200.100 TCP 60 995 → 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len= 49 36.776478201 192.168.200.100 192.168.200.150 TCP 74 46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1 50 36.776496366 192.168.200.100 192.168.200.150 TCP 74 33206 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1 51 36.776512221 192.168.200.100 192.168.200.150 TCP 74 60632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1 52 36.776568606 192.168.200.100 192.168.200.150 TCP 74 49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1 53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1 42 TCP 74		46 3	36.77	6402500	192	2.168.2	200.	100		192.	168.200	9.150	Т	CP	74	49814	→ 256	[SYN]] Seq=(0 Win=	64240	Len=6	MSS=	1460
$\begin{array}{cccccccccccccccccccccccccccccccccccc$										192.	168.200	9.100	T	CP	60	199 →	50684	[RST	, ACK]	Seq=1	Ack=:	1 Win=	0 Len	=0
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		48 3	36.77	6451357	192	2.168	200.	150		192.	168.200	9.100	T	CP	60	995 →	54220	[RST	, ACK]	Seq=1	Ack=	1 Win=	0 Len	i=0
$\begin{array}{cccccccccccccccccccccccccccccccccccc$										192.	168.200	9.150	Т	CP	74	46990	→ 139	[SYN]] Seq=(9 Win=	64240	Len=0	MSS=	1460
$52\ 36.776568606\ 192.168.200.100\ 192.168.200.150\ TCP\ 74\ 49654\ \rightarrow\ 110\ [SYN]\ Seq=0\ Win=64240\ Len=0\ MSS=14500.776671271\ 192.168.200.100\ 192.168.200.150\ TCP\ 74\ 37282\ \rightarrow\ 53\ [SYN]\ Seq=0\ Win=64240\ Len=0\ MSS=14500.150\ TCP\ 74\ 37282\ \rightarrow\ 53\ [SYN]\ Seq=0\ Win=64240\ Len=0\ MSS=14500.150\ TCP\ 74\ 37282\ \rightarrow\ 53\ [SYN]\ Seq=0\ Win=64240\ Len=0\ MSS=14500.150\ TCP\ 74\ 37282\ \rightarrow\ 53\ [SYN]\ Seq=0\ Win=64240\ Len=0\ MSS=14500.150\ TCP\ 74\ 37282\ \rightarrow\ 53\ [SYN]\ Seq=0\ Win=64240\ Len=0\ MSS=14500.150\ TCP\ 74\ 37282\ \rightarrow\ 53\ [SYN]\ Seq=0\ Win=64240\ Len=0\ MSS=14500.150\ TCP\ 74\ 37282\ \rightarrow\ 53\ [SYN]\ Seq=0\ Win=64240\ Len=0\ MSS=14500.150\ TCP\ 74\ 37282\ \rightarrow\ 53\ [SYN]\ Seq=0\ Win=64240\ Len=0\ MSS=14500.150\ TCP\ 74\ 37282\ \rightarrow\ 53\ [SYN]\ Seq=0\ Win=64240\ Len=0\ MSS=14500.150\ TCP\ 74\ 37282\ \rightarrow\ 53\ [SYN]\ Seq=0\ Win=64240\ Len=0\ MSS=14500.150\ TCP\ 74\ 37282\ \rightarrow\ 53\ [SYN]\ Seq=0\ Win=64240\ Len=0\ MSS=14500.150\ TCP\ 74\ 37282\ \rightarrow\ 53\ [SYN]\ Seq=0\ Win=64240\ Len=0\ MSS=14500.150\ TCP\ 74\ 37282\ \rightarrow\ 53\ [SYN]\ Seq=0\ Win=64240\ Len=0\ MSS=14500.150\ TCP\ TCP\ 74\ 37282\ TCP\ TCP\ TCP\ TCP\ TCP\ TCP\ TCP\ TCP$		50 3	36.77	6496366	192	2.168.2	200.	100		192.	168.200	9.150	Т	CP										
53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seg=0 Win=64240 Len=0 MSS=14 Frame 21: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth1, id 0 0000 08 00 27 39 7d		51 3	36.77	6512221	192	2.168.2	200.	100		192.	168.200	9.150	Т	CP										
Frame 21: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth1, id 0		52 3	36.77	6568606	192	2.168.2	200.	100		192.	168.200	9.150												
																			Sea=0	Win=6	4240	Len=0	MSS=1	460 S
Ethernet II. Src: PcsCompu_fd:87:1e (08:00:2) fd:87:1e), Dst: PcsCompu_39:7d:fe (08:00:27:39:7d:fe) 0010 00 28 00 00 40																								
																:fe (0	8:00:2	27:39:	7d:fe)					
Internet Protocol Version 4, Src: 192.168.200.150, Dst: 192.168.200.100 0020 c8 64 01 bb 84											_													_

Una volta aperto il file .pcap ci ritroveremo davanti alla situazione riportata nell'immagine, analizzando il traffico TCP possiamo notare che dall'indirizzo IP 192.168.200.100 avvengono molti tentativi di 3wayhandshake su svariate porte, andando poi a chiudere la connessione una volta ottenuta risposta. Questo potrebbe indicare che un attaccante stia cercando di eseguire una scansione ed enumerazione della nostra rete, in quanto se la porta risponderà risulterà di conseguenza aperta.

Per andare a risolvere questa situazione potrei agire in più modi:

- andando a creare una regola nel firewall che blocchi o limiti un determinato indirizzo IP.
- andando a limitare le richieste che un determinato indirizzo IP può effettuare in un certo lasso di tempo.
- Creare una ACL che vada a bloccare gli indirizzi IP automaticamente quando rileva attività sospette o che ci notifichi tale comportamento.