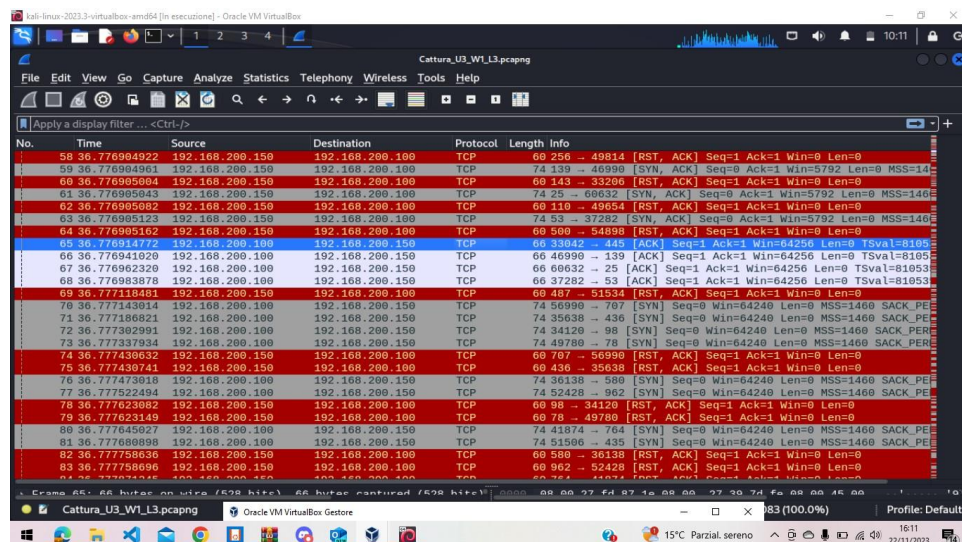


## Esercizio IOC

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



The screenshot shows a Wireshark capture of network traffic. The display filter is set to 'Cattura\_U3\_WI\_L3.pcapng'. The packet list shows a high volume of TCP RST (Reset) packets. The source IP is consistently 192.168.200.150, and the destination IP is 192.168.200.100. The packets are numbered from 58 to 83. The 'Info' column shows details for each packet, including sequence numbers, acknowledgment numbers, and window sizes. The status bar at the bottom indicates that 83 packets (100.0%) are displayed.

No.	Time	Source	Destination	Protocol	Length	Info
58	36.776994922	192.168.200.150	192.168.200.100	TCP	60	256 → 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59	36.776994961	192.168.200.150	192.168.200.100	TCP	74	139 → 46990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
60	36.776995084	192.168.200.150	192.168.200.100	TCP	60	143 → 33206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61	36.776995043	192.168.200.150	192.168.200.100	TCP	74	25 → 68632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
62	36.776995082	192.168.200.150	192.168.200.100	TCP	60	110 → 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63	36.776995125	192.168.200.150	192.168.200.100	TCP	74	53 → 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
64	36.776995162	192.168.200.150	192.168.200.100	TCP	60	500 → 54898 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65	36.776914772	192.168.200.100	192.168.200.150	TCP	66	33042 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=8185
66	36.776941020	192.168.200.100	192.168.200.150	TCP	66	46999 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=8185
67	36.776962320	192.168.200.100	192.168.200.150	TCP	66	68632 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=8185
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=8185
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_PER
71	36.777186021	192.168.200.100	192.168.200.150	TCP	74	35638 → 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
72	36.777392991	192.168.200.100	192.168.200.150	TCP	74	34120 → 98 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
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_PER
74	36.777436632	192.168.200.150	192.168.200.100	TCP	60	707 → 56990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75	36.777436741	192.168.200.150	192.168.200.100	TCP	60	436 → 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
76	36.777474016	192.168.200.100	192.168.200.150	TCP	74	30130 → 580 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
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_PER
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] Seq=1 Ack=1 Win=0 Len=0
80	36.777645027	192.168.200.100	192.168.200.150	TCP	74	41074 → 704 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
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_PER
82	36.777758636	192.168.200.150	192.168.200.100	TCP	60	580 → 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83	36.777758696	192.168.200.150	192.168.200.100	TCP	60	962 → 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Già da questo screen di alcuni pacchetti “sniffati” da wireshark notiamo già alcuni IOC o indicatori di essi

- Una grandissima quantità di richieste tcp (più di 2000) indice che siano sotto una scannerizzazione che può precedere un attacco
- Molte richieste tcp non hanno una effettiva stretta di mano a tre vie ma vi è il termine "RST" Quando un dispositivo invia un pacchetto con il flag "RST" impostato, sta segnalando all'altro dispositivo che la connessione deve essere reimpostata o resettata. Questo può verificarsi, ad esempio, in risposta a un errore o a una situazione anomala.
- Molte delle richieste sono su porte desuete o comunque porte superiori alle prime 1024 (well-known ports), queste porte usualmente non vengono utilizzate con frequenza, difficilmente un nostro collega di ufficio ci invierà una richiesta su una di esse, può anche essere sintomo della ricerca di un servizio spostato tramite rimappatura delle porte
- 

Ultimo fattore molto importante è che tutti questi pacchetti sono provenienti da un ip all'interno della nostra rete, da una semplice occhiata come la nostra non possiamo capire se si tratti un intruso fisico, da remoto o uno spoofing dell'ip ma si prospetta sicuramente una delle ipotesi peggiori ovvero un buco all'interno della nostra rete.

#### Alcuni consigli utili

- Isolamento del Sistema:
- Analisi Dettagliata:
- Monitoraggio Continuo:
- Implementazione di Firme IDS/IPS:
- Regole del Firewall:
- Aggiornamento e Patching:
- Controllo degli Account e delle Credenziali:
- Collaborazione con il Team di Sicurezza:
- Indagine Forense:
- Report alle Autorità Competenti: