

S9 / L3

# THREAT INTELLIGENCE & IOC

Riccardo Agostino Monti



# INDICE

- Scopo del test 01
- Analisi Cattura 02
- Potenziali Vettori di Attacco 03
- Remediaton 04

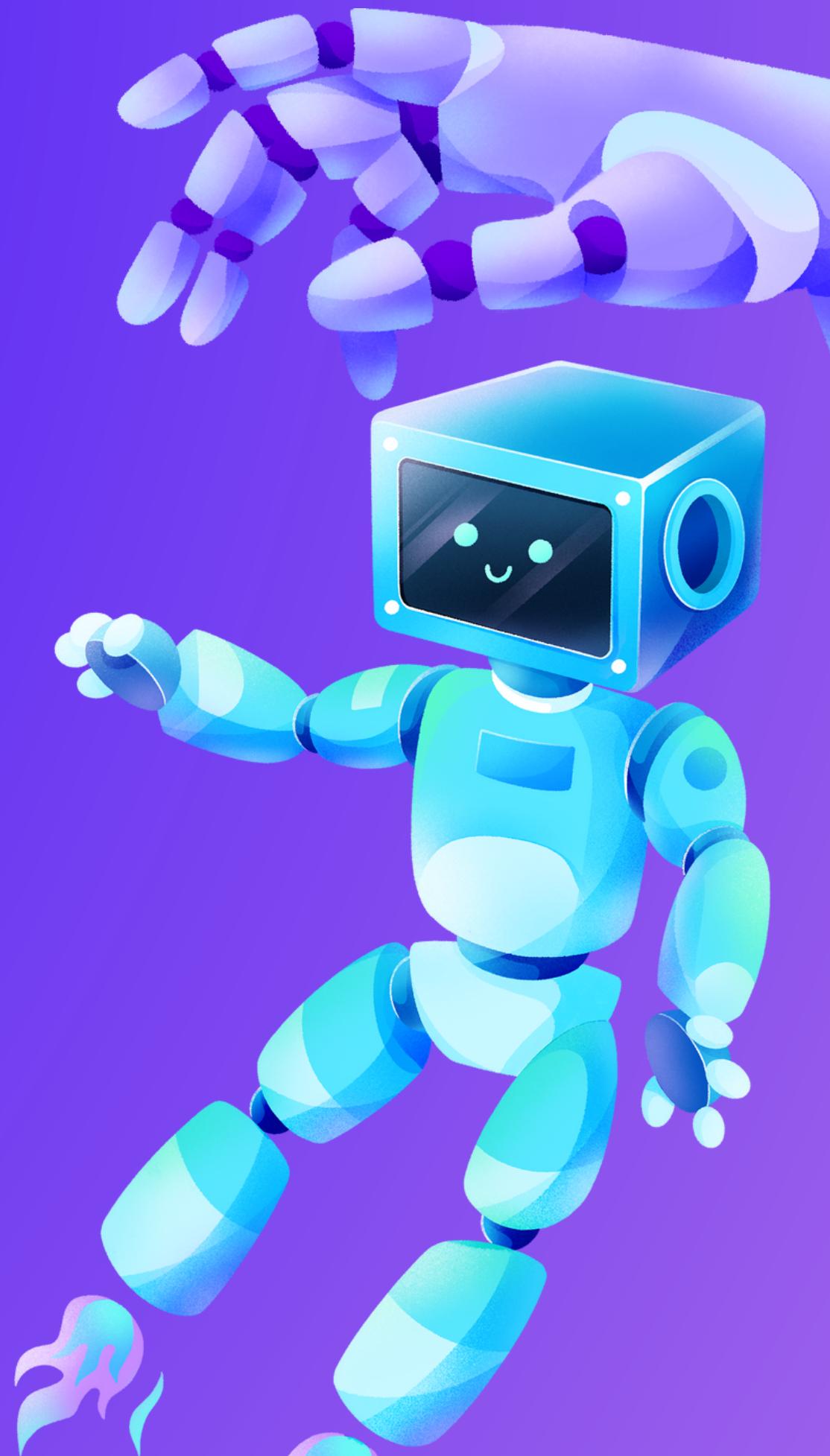


# SCOPO DEL TEST



L'esercizio di oggi prevede l'analisi di una cattura effettuata con WireShark, rispondendo poi ai seguenti quesiti:

- Identificare eventuali IOC, ovvero evidenze di attacchi in corso In base
  - In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
  - Consigliate un'azione per ridurre gli impatti dell'attacco
- 



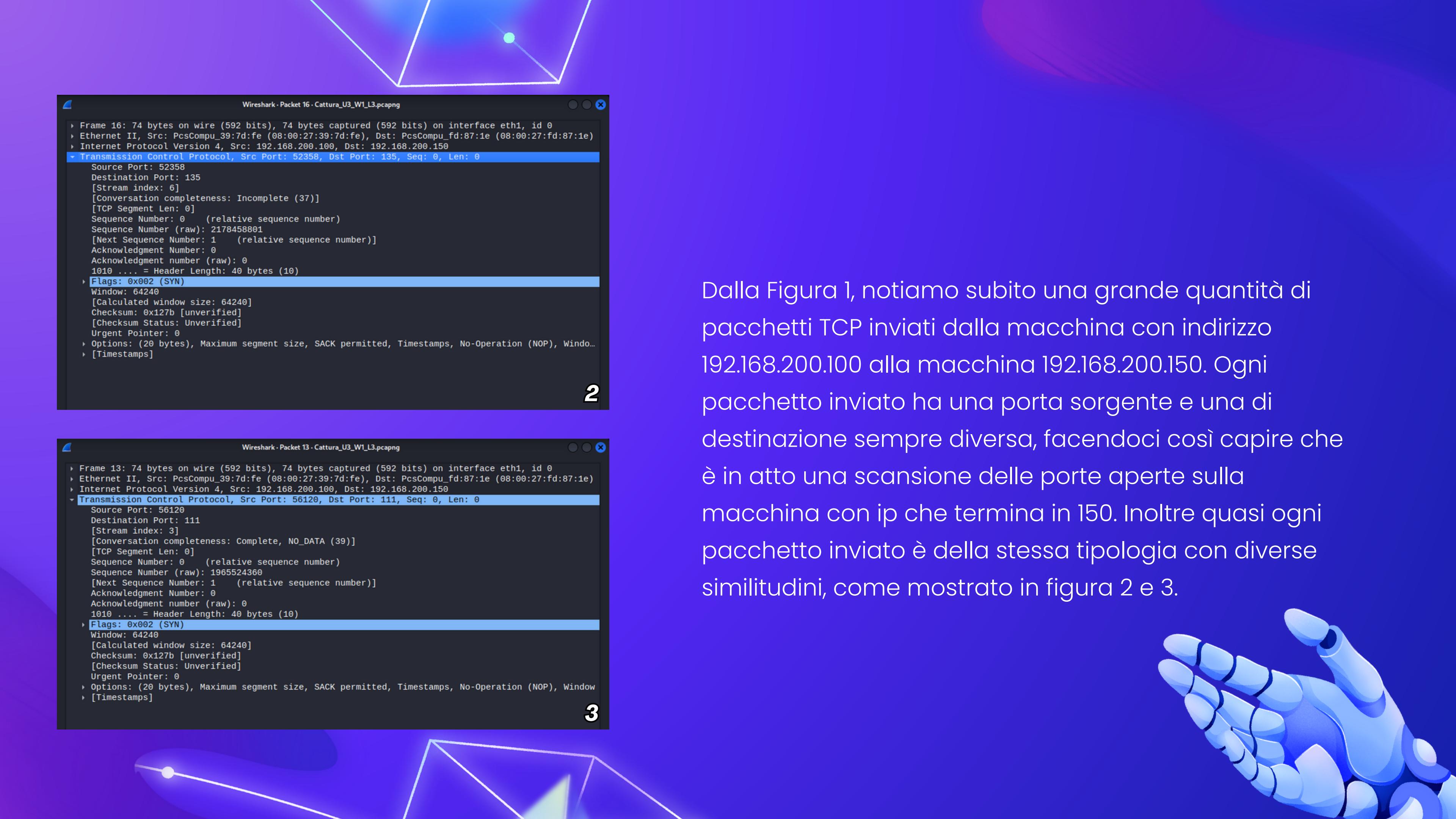
ANALISI  
CATTURA



Per analizzare la cattura dei pacchetti, importiamo prima il file fornito su Kali Linux (utilizzando una cartella condivisa) e successivamente apriamolo effettuando un doppio click sinistro. A schermo dovrebbe mostrarsi una schermata simile a quella in figura 1.

No.	Time	Source	Destination	Protocol	Length	Info
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 TSval=810535439 TSecr=4294952466
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 TSval=810535439 TSecr=4294952466
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=1 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=1 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=1 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=1 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=1 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=1 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=1 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=1 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=1 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=1 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=1 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] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 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=1 TSval=4294952466 TSecr=810535440 WS=64
58	36.776904922	192.168.200.150	192.168.200.100	TCP	60	256 → 49814 [RST, ACK] Seq=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=1 TSval=4294952466 TSecr=810535440 WS=64
60	36.776905004	192.168.200.150	192.168.200.100	TCP	60	143 → 33206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61	36.776905043	192.168.200.150	192.168.200.100	TCP	74	25 → 60632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64
62	36.776905082	192.168.200.150	192.168.200.100	TCP	60	110 → 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63	36.776905123	192.168.200.150	192.168.200.100	TCP	74	53 → 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64
64	36.776905162	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=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] Seq=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=1 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=1 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=1 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=1 TSval=810535441 TSecr=0 WS=128
74	36.777430632	192.168.200.150	192.168.200.100	TCP	60	707 → 56990 [RST, ACK] Seq=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] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 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=1 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] Seq=1 Ack=1 Win=0 Len=0





Wireshark - Packet 16 - Cattura\_U3\_W1\_L3.pcapng

```
> Frame 16: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth1, id 0
> Ethernet II, Src: PcsCompu_39:7d:fe (08:00:27:39:7d:fe), Dst: PcsCompu_fd:87:1e (08:00:27:fd:87:1e)
> Internet Protocol Version 4, Src: 192.168.200.100, Dst: 192.168.200.150
-> Transmission Control Protocol, Src Port: 52358, Dst Port: 135, Seq: 0, Len: 0
  Source Port: 52358
  Destination Port: 135
  [Stream index: 6]
  [Conversation completeness: Incomplete (37)]
  [TCP Segment Len: 0]
  Sequence Number: 0      (relative sequence number)
  Sequence Number (raw): 2178458801
  [Next Sequence Number: 1      (relative sequence number)]
  Acknowledgment Number: 0
  Acknowledgment number (raw): 0
  1010 .... = Header Length: 40 bytes (10)
-> Flags: 0x002 (SYN)
  Window: 64240
  [Calculated window size: 64240]
  Checksum: 0x127b [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
-> Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window...
-> [Timestamps]
```

2

Wireshark - Packet 13 - Cattura\_U3\_W1\_L3.pcapng

```
> Frame 13: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth1, id 0
> Ethernet II, Src: PcsCompu_39:7d:fe (08:00:27:39:7d:fe), Dst: PcsCompu_fd:87:1e (08:00:27:fd:87:1e)
> Internet Protocol Version 4, Src: 192.168.200.100, Dst: 192.168.200.150
-> Transmission Control Protocol, Src Port: 56120, Dst Port: 111, Seq: 0, Len: 0
  Source Port: 56120
  Destination Port: 111
  [Stream index: 3]
  [Conversation completeness: Complete, NO_DATA (39)]
  [TCP Segment Len: 0]
  Sequence Number: 0      (relative sequence number)
  Sequence Number (raw): 1965524360
  [Next Sequence Number: 1      (relative sequence number)]
  Acknowledgment Number: 0
  Acknowledgment number (raw): 0
  1010 .... = Header Length: 40 bytes (10)
-> Flags: 0x002 (SYN)
  Window: 64240
  [Calculated window size: 64240]
  Checksum: 0x127b [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
-> Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window...
-> [Timestamps]
```

3

Dalla Figura 1, notiamo subito una grande quantità di pacchetti TCP inviati dalla macchina con indirizzo 192.168.200.100 alla macchina 192.168.200.150. Ogni pacchetto inviato ha una porta sorgente e una di destinazione sempre diversa, facendoci così capire che è in atto una scansione delle porte aperte sulla macchina con ip che termina in 150. Inoltre quasi ogni pacchetto inviato è della stessa tipologia con diverse similitudini, come mostrato in figura 2 e 3.



# POTENZIALI VETTORI DI ATTACCO



## Analisi dei pacchetti

Analizzando meglio i pacchetti in figura 1 notiamo inoltre che probabilmente è stato utilizzato il tool nMap per effettuare la scansione, tale tool è infatti solitamente utilizzato per scopi del genere, dalle analisi possiamo anche trarre che se è stato utilizzato nMap, l'attaccante ha usato lo switch `-sT` per effettuare una scansione Two-Hand-Shake visto l'utilizzo di Syn-Ack nei pacchetti analizzati.

REMEDIATION





Per evitare altre scansioni future è consigliata l'implementazione di un firewall configurato in modo da far risultare le porte scannerizzate come "Filtered" così da non fornire informazioni all'attaccante che effettua la scansione. Ricordiamo inoltre che solitamente la scansione delle porte attive è il primo passo verso un attacco informatico vero e proprio, per questo motivo è consigliato chiudere le porte superflue e utilizzare per i servizi installati sulla macchina porte oltre la 1024, solitamente scannerizzate solo in un secondo momento.

Inoltre, visto che l'attaccante è entrato in possesso di informazioni importanti per un possibile attacco, è opportuno bloccare l'indirizzo ip dell'attaccante tramite firewall.