THREAT INTELLIGENCE & IOC

NET. REBELS.

MICHELANGELO BORROMEO

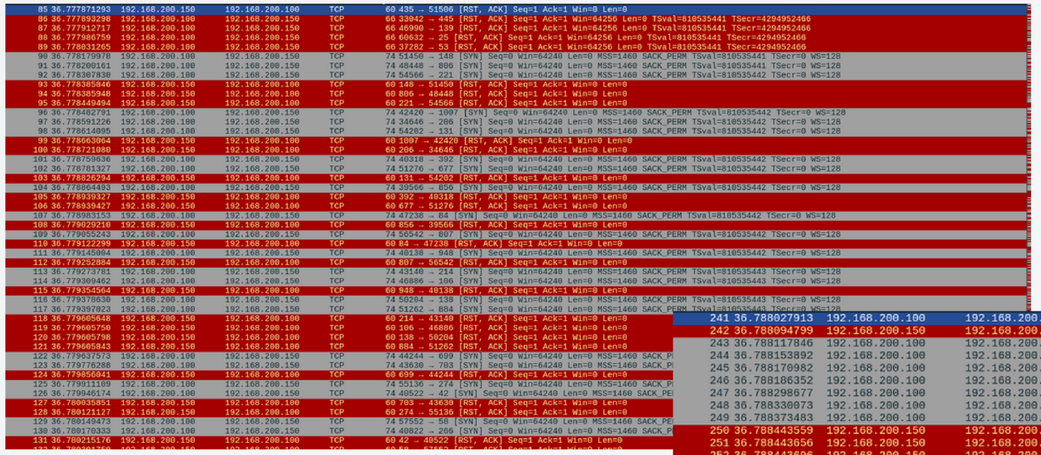
TRACCIA

1) Identificare eventuali IOC, ovvero evidenze di attacchi in corso In base agli IOC trovati.

2) fate delle ipotesi sui potenziali vettori di attacco utilizzati

3) Consigliare un’azione per ridurre gli impatti dell’attacco

WIRESHARK



85	36.777871293	192.168.200.150	192.168.200.100	TCP	60 435 → 51506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
86	36.777893298	192.168.200.100	192.168.200.150	TCP	66 33942 → 445 [RST, ACK] Seq=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] Seq=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	36.778307838	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	36.778760536	192.168.200.100	192.168.200.150	TCP	74 40318 → 302 [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] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
103	36.778826294	192.168.200.150	192.168.200.100	TCP	60 131 → 54202 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
104	36.778864493	192.168.200.100	192.168.200.150	TCP	74 60566 → 856 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
105	36.778939327	192.168.200.150	192.168.200.100	TCP	60 392 → 40318 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
106	36.778939427	192.168.200.150	192.168.200.100	TCP	60 677 → 51276 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
107	36.778983153	192.168.200.100	192.168.200.150	TCP	74 47238 → 82 [SYN] Seq=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	60 856 → 39566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
109	36.779055243	192.168.200.100	192.168.200.150	TCP	74 56542 → 807 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
110	36.779122295	192.168.200.150	192.168.200.100	TCP	60 82 → 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] Seq=1 Ack=1 Win=0 Len=0
113	36.779272713	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	36.779370550	192.168.200.100	192.168.200.150	TCP	74 59204 → 318 [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	60 138 → 50204 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
121	36.779605843	192.168.200.150	192.168.200.100	TCP	60 884 → 51262 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
122	36.779707078	192.168.200.100	192.168.200.150	TCP	74 44244 → 699 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P
123	36.779776288	192.168.200.100	192.168.200.150	TCP	74 43630 → 703 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P
124	36.779856041	192.168.200.150	192.168.200.100	TCP	60 699 → 44244 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
125	36.779931169	192.168.200.100	192.168.200.150	TCP	74 50136 → 274 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P
126	36.779946174	192.168.200.100	192.168.200.150	TCP	74 40522 → 42 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PE
127	36.780035851	192.168.200.150	192.168.200.100	TCP	60 703 → 43630 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
128	36.780121127	192.168.200.150	192.168.200.100	TCP	60 274 → 55196 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
129	36.780149473	192.168.200.100	192.168.200.150	TCP	74 57552 → 58 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PE
130	36.780170333	192.168.200.100	192.168.200.150	TCP	74 40822 → 266 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P
131	36.780215170	192.168.200.150	192.168.200.100	TCP	60 42 → 40522 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

241	36.788027913	192.168.200.100	192.168.200.150	TCP	74 50612 → 470 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
242	36.788094799	192.168.200.150	192.168.200.100	TCP	60 234 → 59932 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
243	36.788117846	192.168.200.100	192.168.200.150	TCP	74 36266 → 180 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
244	36.788153892	192.168.200.100	192.168.200.150	TCP	74 51844 → 855 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
245	36.788170982	192.168.200.100	192.168.200.150	TCP	74 45726 → 232 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
246	36.788186352	192.168.200.100	192.168.200.150	TCP	74 52724 → 904 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
247	36.788298677	192.168.200.100	192.168.200.150	TCP	74 49480 → 835 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535452 TSecr=0 WS=128
248	36.788330073	192.168.200.100	192.168.200.150	TCP	74 41098 → 602 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535452 TSecr=0 WS=128
249	36.788373483	192.168.200.100	192.168.200.150	TCP	74 54196 → 291 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535452 TSecr=0 WS=128
250	36.788443559	192.168.200.150	192.168.200.100	TCP	60 709 → 59046 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
251	36.788443656	192.168.200.150	192.168.200.100	TCP	60 271 → 44414 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
252	36.788443696	192.168.200.150	192.168.200.100	TCP	60 470 → 50612 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
253	36.788443736	192.168.200.150	192.168.200.100	TCP	60 180 → 36266 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
254	36.788443776	192.168.200.150	192.168.200.100	TCP	60 855 → 51844 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
255	36.788443816	192.168.200.150	192.168.200.100	TCP	60 232 → 45726 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
256	36.788443857	192.168.200.150	192.168.200.100	TCP	60 904 → 52724 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
257	36.788443896	192.168.200.150	192.168.200.100	TCP	60 835 → 49480 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
258	36.788490564	192.168.200.150	192.168.200.100	TCP	60 602 → 41098 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
259	36.788490603	192.168.200.150	192.168.200.100	TCP	60 291 → 54196 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
260	36.788511936	192.168.200.100	192.168.200.150	TCP	74 48350 → 956 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535452 TSecr=0 WS=128
261	36.788567765	192.168.200.100	192.168.200.150	TCP	74 36542 → 773 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535452 TSecr=0 WS=128
262	36.788600279	192.168.200.100	192.168.200.150	TCP	74 51396 → 514 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535452 TSecr=0 WS=128
263	36.788677629	192.168.200.100	192.168.200.150	TCP	74 56758 → 224 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535452 TSecr=0 WS=128
264	36.788716758	192.168.200.100	192.168.200.150	TCP	74 48824 → 183 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535452 TSecr=0 WS=128
265	36.788805799	192.168.200.150	192.168.200.100	TCP	60 956 → 48350 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
266	36.788805893	192.168.200.150	192.168.200.100	TCP	60 773 → 36542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
267	36.788805940	192.168.200.100	192.168.200.150	TCP	74 514 → 51396 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952467 TSecr=810535452 WS=64
268	36.788833247	192.168.200.100	192.168.200.150	TCP	66 51396 → 514 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535452 TSecr=4294952467
269	36.788954711	192.168.200.150	192.168.200.100	TCP	60 224 → 56758 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
270	36.789081011	192.168.200.100	192.168.200.150	TCP	74 40182 → 361 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535452 TSecr=0 WS=128
271	36.789254102	192.168.200.150	192.168.200.100	TCP	60 183 → 48824 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
272	36.789378458	192.168.200.150	192.168.200.100	TCP	60 361 → 40182 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
273	36.789681130	192.168.200.100	192.168.200.150	TCP	66 51396 → 514 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535453 TSecr=4294952467
274	36.789840070	192.168.200.100	192.168.200.150	TCP	74 36046 → 617 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535453 TSecr=0 WS=128
275	36.789887828	192.168.200.100	192.168.200.150	TCP	74 34868 → 62 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535453 TSecr=0 WS=128
276	36.790032784	192.168.200.150	192.168.200.100	TCP	60 617 → 36046 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
277	36.790062742	192.168.200.100	192.168.200.150	TCP	74 47720 → 8 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535453 TSecr=0 WS=128
278	36.790152859	192.168.200.150	192.168.200.100	TCP	60 62 → 34868 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
279	36.790152966	192.168.200.150	192.168.200.100	TCP	60 8 → 47720 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
280	36.790171438	192.168.200.100	192.168.200.150	TCP	74 37560 → 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535453 TSecr=0 WS=128
281	36.790198841	192.168.200.100	192.168.200.150	TCP	74 58384 → 121 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535453 TSecr=0 WS=128
282	36.790247212	192.168.200.100	192.168.200.150	TCP	74 59884 → 186 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535453 TSecr=0 WS=128
283	36.790263750	192.168.200.100	192.168.200.150	TCP	74 49848 → 344 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535454 TSecr=0 WS=128
284	36.790407394	192.168.200.150	192.168.200.100	TCP	60 978 → 37560 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
285	36.790435700	192.168.200.100	192.168.200.150	TCP	74 59258 → 168 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535454 TSecr=0 WS=128
286	36.790470966	192.168.200.100	192.168.200.150	TCP	74 44832 → 416 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535454 TSecr=0 WS=128
287	36.790531361	192.168.200.150	192.168.200.100	TCP	60 121 → 58384 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

WIRESHARK PACKET STRUCTURE ANALISYS

Porta Vittima

La porta di destinazione

Vittima

Indirizzo IP di destinazione

Attaccante

Indirizzo IP dalla quale parte la connessione

Protocollo

Tipologia di connessione utilizzata **TCP**

Porta Attaccante

La porta dalla quale parte il pacchetto

Flag

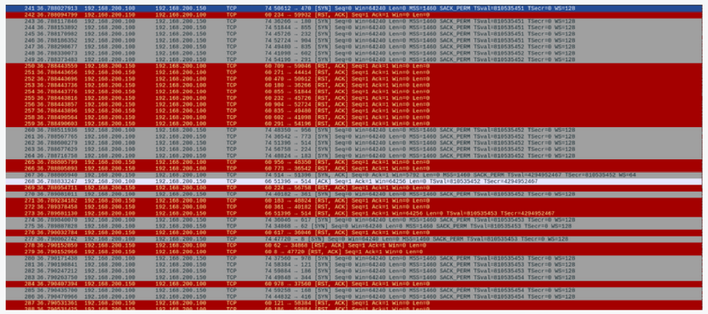
Flag utilizzate dal protocollo **TCP**

IOC ANALISYS

(INDICATOR OF COMPROMISSION)

```
86 36.777893298  192.168.200.100      192.168.200.150      TCP      66 33042 → 445 [RST, ACK] Seq=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] Seq=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
```

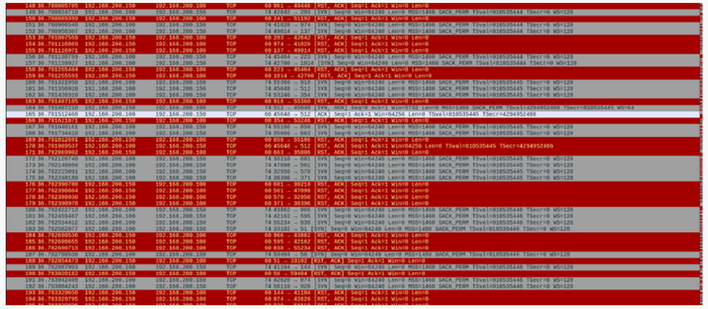
L'IP 192.168.200.150 sta inviando una serie di pacchetti con i flag RST e ACK all'IP 192.168.200.100.



RST = Questo flag indica che la connessione deve essere terminata immediatamente. Viene solitamente inviato quando un pacchetto viene ricevuto su una connessione che non esiste più o non è mai esistita. È una sorta di messaggio di errore che dice "termina questa connessione".

ACK = Questo flag viene utilizzato per riconoscere la ricezione di pacchetti nel protocollo TCP.

Una quantità enorme di richieste Syn potrebbe esaurire le risorse di memoria della macchina bersaglio, di conseguenza potrebbe portare un rallentamento del sistema o al blocco completo rendendo la macchina incapace di gestire le nuove connessioni legittime



Possiamo dedurre che questo è un attacco DoS ovvero Denial of Service

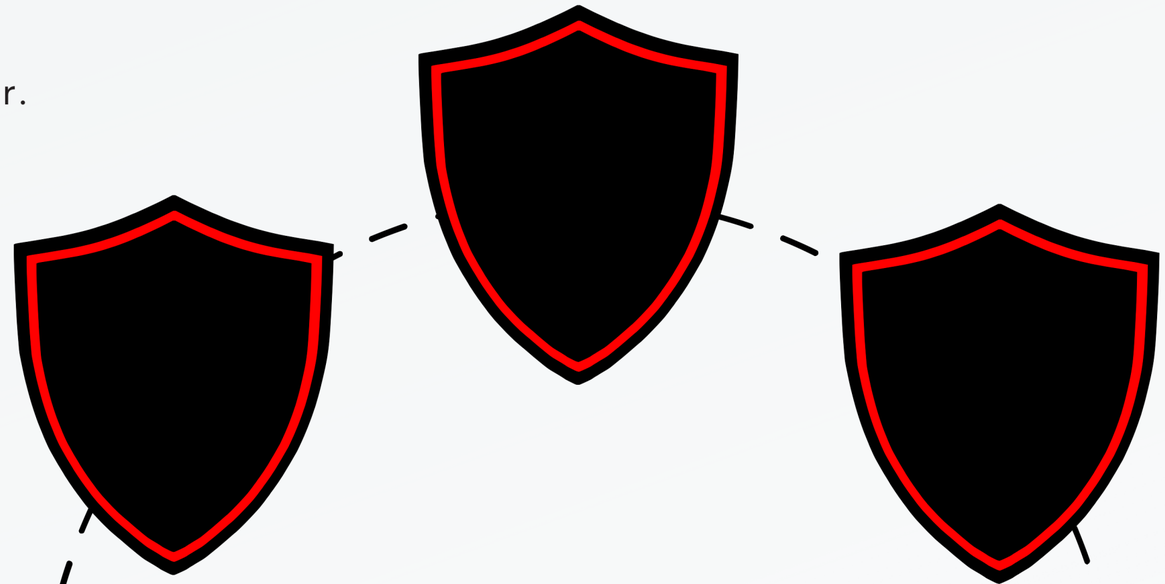
RIDUZIONE IMPATTO

Firewall

Utilizzare un firewall per limitare il numero di nuove connessioni da una singola origine. Questo può prevenire che un singolo attaccante sovraccarichi il server.

Reverse Proxy

Utilizzare un reverse proxy per filtrare il traffico prima che raggiunga il server principale.



IDS/IPS

Implementare sistemi di rilevamento e prevenzione delle intrusioni che possono identificare e bloccare automaticamente il traffico sospetto.