1. Identificare eventuali IOC, ovvero evidenze di attacchi in corso:

Indicatori di Compromissione (IOC):

- **Scansione delle porte**: L'host `192.168.200.100` invia molte richieste **TCP SYN** a porte diverse dell'host `192.168.200.150`. L'host target risponde con **SYN-ACK** (porta aperta) o **RST-ACK** (porta chiusa), indicando un tentativo di mappare i servizi attivi.

2. In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati:

Ipotesi sui vettori di attacco:

- **Port scan**: L'attaccante sta probabilmente utilizzando uno strumento di scansione automatizzato (come Nmap) per identificare porte e servizi aperti, primo passo per un possibile attacco futuro.

3. Consigliate un’azione per ridurre gli impatti dell’attacco:

Azioni consigliate:

- **Bloccare l'IP**: Configurare una regola firewall per bloccare il traffico da `192.168.200.100`.
- **Hardening del sistema**: Disabilitare servizi non necessari, aggiornare quelli attivi e implementare un sistema IDS/IPS per monitorare attività sospette.
- **Whitelisting e rate limiting**: Limitare l'accesso solo a IP autorizzati e ridurre il numero di connessioni per mitigare le scansioni.