Attacco DoS (Denial of Service)

1. Identificazione della Minaccia

- **Cos'è un attacco DoS e come funziona:**
  Un **attacco DoS (Denial of Service)** è un tentativo malevolo di rendere un sistema informatico (come un server o sito web) non disponibile per gli utenti legittimi. Questo viene fatto sovraccaricando la rete o il sistema con un volume eccessivo di richieste, fino a esaurire le risorse disponibili.

- **Come compromette la disponibilità dei servizi aziendali:**

  - I server diventano **non responsivi**.

  - I clienti non riescono ad accedere ai servizi online.

  - Si possono verificare **perdite di vendite** o **danni reputazionali**.

2. Analisi del Rischio

- **Impatto potenziale sull'azienda:**

  - **Perdita di produttività interna** per indisponibilità di sistemi.

  - **Interruzione del servizio** per clienti e partner.

  - **Possibili danni finanziari** se l'attività è legata a e-commerce o a servizi digitali.

- **Servizi critici compromessi:**

  - Server web aziendali.

  - Applicazioni gestionali interne (ERP/CRM).

  - Infrastruttura cloud o VPN.

  - Sistemi email e comunicazioni.

3. Pianificazione della Remediation

Per rispondere a un attacco DoS, il piano dovrebbe includere:

- **Identificazione delle fonti dell'attacco:**
  Utilizzare strumenti come **Wireshark** o firewall per monitorare il traffico anomalo e identificare IP sospetti (es. IP 192.168.1.1 e 192.168.1.2 nei pacchetti TCP indirizzati a 10.0.0.1).

- **Mitigazione del traffico malevolo:**
  Reindirizzamento, throttling o filtraggio tramite firewall, rate-limiting o strumenti di difesa (es. Cloudflare, WAF, ecc.).

4. Implementazione della Remediation

Azioni pratiche per mitigare la minaccia:

- **Bilanciamento del carico (Load Balancing):**
  Distribuire le richieste in arrivo tra più server per evitare il sovraccarico.

- **Servizi di mitigazione DoS di terze parti:**
  Cloudflare, AWS Shield, Akamai Kona: proteggono automaticamente contro attacchi volumetrici.

- **Regole firewall per bloccare traffico sospetto:**

    - Bloccare gli IP identificati come origine dell'attacco (es. IP 192.168.1.1).

    - Bloccare protocolli o porte specifiche.

    - Limitare il numero di connessioni al secondo da ogni IP.

5. Mitigazione dei Rischi Residuali

Misure preventive per futuri attacchi:

- **Monitoraggio continuo del traffico:**
  Sistemi IDS/IPS (come Snort o Suricata) per rilevare attività anomale in tempo reale.

- **Collaborazione con il team di sicurezza:**
  Analisi congiunta e simulazioni periodiche per migliorare la difesa.

- **Test di resilienza periodici:**
  Simulazioni di attacco (penetration testing, red teaming) per verificare la tenuta dell'infrastruttura.

- L'attacco è stato rilevato tra le **06:51:17** e le **06:51:26** con numerosi pacchetti TCP della stessa lunghezza.

- **Origine sospetta:** IP 192.168.1.1 e 192.168.1.2.

- **Azione correttiva:** Bloccare tali IP via firewall e aumentare la soglia di rilevamento nel sistema IDS.