**🔍 1. Atak brute-force na SSH**

**Cel:** Symulacja łamania hasła do SSH.  
**Kroki:**

1. **Przeprowadź atak** (z Kali Linux):

hydra -l root -P /usr/share/wordlists/rockyou.txt -t 4 ssh://192.168.0.172

1. **Sprawdź blokadę** (na Ubuntu z CrowdSec):

sudo cscli decisions list

sudo cscli alerts list

1. **Odblokuj IP** (pełne czyszczenie po teście):

sudo cscli decisions delete --ip 192.168.0.177

sudo cscli alerts delete --ip 192.168.0.177

sudo iptables -F

sudo nft flush ruleset

sudo systemctl restart crowdsec

**🌐 2. Skanowanie portów (nmap)**

**Cel:** Wykrycie skanowania jako podejrzanej aktywności.  
**Kroki:**

1. **Skanuj porty** (z Kali Linux):

nmap -sV -T4 192.168.0.172

1. **Sprawdź alerty** (na Ubuntu):

sudo cscli alerts list

1. **Wyczyść decyzje**:

sudo cscli alerts delete --ip 192.168.0.177

**🕵️ 3. Próba dostępu do panelu admina (HTTP)**

**Cel:** Wykrycie próby dostępu do nieistniejących ścieżek.  
**Kroki:**

1. **Wyślij żądania HTTP** (z Kali Linux):

curl http://192.168.0.172/admin

curl http://192.168.0.172/wp-login.php

1. **Sprawdź logi CrowdSec**:

sudo tail -f /var/log/crowdsec.log | grep "http"

1. **Odblokuj IP**:

sudo cscli decisions delete --ip 192.168.0.177

**🧨 4. Atak DDoS (hping3)**

**Cel:** Wykrycie floodu pakietów.  
**Kroki:**

1. **Uruchom flood** (z Kali Linux):

sudo hping3 -S --flood -p 80 192.168.0.172

1. **Sprawdź decyzje** (na Ubuntu):

sudo cscli decisions list

1. **Zatrzymaj atak** (Ctrl+C w Kali) i odblokuj IP:

sudo cscli decisions delete --all