DoS Attacks on SCADA Systems

# Objective

A Denial-of-Service (DoS) attack is when an attacker causes a temporary or indefinite service disruption by flooding the target with a massive traffic. This exercise has four parts to design and implement DoS attacks on a SCADA system.

1. Use Hping3 to perform a LAND attack and a SYN flood attack.
2. Use Metasploit to conduct a SYN flood attack.
3. Analyze the performance of a SYN flood with Hping3 and with Metasploit.

# Before Starting

It is essential that you use the system you have created from the previous assignments on this homework. You will need Wireshark on your attacker machine for this assignment.

## Network Architecture Requirement

You must have the network architecture below before starting this assignment:



# Using Hping3 to create DoS attacks

Your goal is to create a DoS attack against the PLC using Hping3 and observe the results in Wireshark. Kali Linux comes with Hping3 pre-installed; so, you **do not** need to install it. **You will need to perform these tasks to answer the post exercise questions.**

## Create a LAND attack

Your DoS attack should follow these requirements:

1. This DoS attack will send 3000 packets.
2. Set the size of the payload to be 100 bytes.
3. Make sure the packet type is SYN.
4. The attack will occur on port 502 and the source port will be equal to 80.
5. You want to preserve the source port and to spoof the attacker address.
6. Open the terminal and conduct an Hping3 DoS attack.
7. Open Wireshark choose eth0 and check your results.

## Create a SYN flood attack

Using the same tool as Part #1 (Hping3), your goal is to perform a SYN flood attack against the PLC. Open Wireshark choose eth0 and check your results.

# Using Metasploit to create a DoS attack

Metasploit is a powerful framework that you can use to perform many types of attacks. Your task is to execute a SYN flood attack against the PLC using this tool. **You will need to perform these tasks to answer the post exercise questions.**

1. Kali Linux comes with Metasploit pre-installed; so, you **do not** need to install it.
2. Open Wireshark choose eth0 and check your results.

# Post Exercise Report

## What is a LAND attack? What can this do to a system?

## If a computer is a victim of a LAND attack how would you recover? How can we prevent this attack? Justify your answer.

## You created two DoS attacks in part 3. Briefly describe what you observed in Wireshark.

## Note any differences between what you saw in Wireshark for part 3 and part 4. If there are not any, clearly state so.

## In parts 3 and 4, you have performed the same attack using two different tools. In both cases, you verified the success of the attacks using Wireshark. During each attack, does the HMI in ScadaBR appear to still run? Explain.

# Exercise Rubric

| **Questions + Criteria** | **Full marks** | Mostly correct, missing one or two considerations | Partially correct, missing many considerations | Partially correct, explanation is lacking details | Missing or does not explain answers |
| --- | --- | --- | --- | --- | --- |
| 1. LAND attack questions | **25** | 22.5 | 15 | 5 | 0 |
| 1. LAND question on countermeasures | **20** | 17.5 | 10 | 3 | 0 |
| 1. DoS attack descriptions + observations | **15** | 12.5 | 7.5 | 3 | 0 |
| 1. Comparison in parts 3 and 4 | **15** | 12.5 | 7.5 | 3 | 0 |
| 1. Questions on SYN flood and HMI behavior | **25** | 22.5 | 15 | 5 | 0 |