Reconnaissance Attacks

# Objective

A reconnaissance attack is when an attacker targets a victim’s system to gather information about its vulnerabilities. In this assignment, you will use three tools to perform tasks: NMAP, SHODAN and S-MOD. This exercise has three parts to design and implement a Reconnaissance attack on a SCADA system.

1. Perform a network scan (IP address & MAC) to find all the IP addresses and MAC addresses of your Virtual Network. Use NMAP to also find open ports in your virtual network.
2. Use S-MOD to identify registers, coils, and function codes available in a system.
3. Discover information about devices connected to the internet using SHODAN.

# Before Starting

## Install a Kali Linux VM

1. Make sure you have Kali Linux installed on a VM. If you don’t have it, please click on the below and go to part 5: <https://sites.google.com/uah.edu/openplctipsandtricks/initial-vm-setup>

An attacker gathers information about a system by observing system operations and listening in on the network communication. Therefore, the network architecture of this assignment is as follows:



# Network Scan with NMAP

## Find all IP addresses and MAC addresses on your Virtual Network

1. Kali Linux comes with some pre-installed tools such as NMAP. So, you **do not** need to install it.
2. Open the terminal and type the command: “**sudo** **nmap –sn [subnet/CIDR]**”.
3. *Using the information that you have found, answer the post-exercise questions.*

## Use NMAP to find open ports in your virtual network.

1. Open the terminal and type: **“sudo nmap -sT -p [range of ports] [subnet/CIDR]”.**
2. Close any other port that is does not use Modbus, ScadaBR and OpenPLC services. Type this command for each port you want to close:

“***sudo iptables -A INPUT -p tcp --destination-port [port number] -j REJECT”***

1. Type again the command **“sudo nmap -sT -p [range of ports] [subnet/CIDR]”** to verify if all the ports are closed except the ones cited above.
2. *Using the information that you have found, answer the post-exercise questions.*

# Using S-MOD to identify registers, coils, and function codes

## Initial Setup

1. Open Kali terminal and install S-MOD, type: **“sudo git clone https://github.com/theralfbrown/smod-1”**
2. Next, type: “**cd smod-1**”
3. Run smod-1: “**python smod-1**”
4. After you run, type **“show modules”** to get the list containing all the functions available using this tool.

## Use S-MOD to find the function codes

1. Type: “**use modbus/scanner/getfunc**” and configure the module if it needs some additional settings before running (Check Reconnaissance slide deck for instructions).
2. *You will need this task completed in order to answer the post-exercise questions.*

## Use S-MOD to read coils and register values

1. To read register values, use the steps from 5.2 except you type:  
   **use modbus/function/readHoldingRegister**
2. After you run, you need to know if the values you obtained are correct or not – register values should be in front of the registerVal list. To find out that**:**
   1. Go to your *HMI* and open *SCADABR*.
   2. Click on Data Sources.
   3. Click on the Edit icon for the Traffic Light.
   4. Under *Modbus read data,* choose *Holding Register* for Register range, change the number of registers to 8 and click on *Read data*.
   5. Note what you see and answer the post-exercise questions.
3. To read coil values, use the steps from 4.2 except you type:  
   **use modbus/function/readCoils**
4. After you run, you need to know if the values you obtained are correct or not – coil values should be in front of coilStatus list. To do this,
   1. Go to your *HMI* and open *SCADABR*.
   2. Click on Data Sources.
   3. Under *Modbus read data,* choose *Coil Status* for Register range, change the number of registers to 8 and click on *Read data*.
   4. *Note what you see and answer the post-exercise questions.*

# SHODAN

SHODAN is a search engine that lets users find certain types of computers connected to the Internet. Use SHODAN to answer the post-exercise questions.

# Post Exercise Report

Submit your answers to the following questions.

## Using what you found in section 3.1, please fill out the table below:

|  |  |  |
| --- | --- | --- |
| Node | IP ADDRESS | MAC ADDRESS |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Using what you found in section 3.2, please fill out the table below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Node | IP | MAC | Port | Service |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## What are the function codes used in your system?

## Is it possible to create a reconnaissance attack and change the values of registers or coils using function codes 5 through 16? Why or why not? Explain. HINT: Remember that the values are in decimal, but they are stored in binary/hexadecimal.

## For Section 4.3, you read the registers and coils. For each of them, compare what you see on the HMI with what you see using S-Mod. Are they the same? Why or why not? Explain. Hint: Consider how coils are read either in Little Endian or Big Endian.

## How many Modbus ports are found in the world?

## How many DNP3 ports can you find using SHODAN? Are they all real DNP3 ports? Justify your answer.

# 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. NMAP IP address table | 10 | 8 | 5 | 1 | 0 |
| 1. NMAP open ports table | 10 | 8 | 5 | 1 | 0 |
| 1. List of S-MOD function codes | 10 | 8 | 5 | 1 | 0 |
| 1. S-MOD read coils + recon attack question | 25 | 22.5 | 17.5 | 5 | 0 |
| 1. Comparing reading registers and coils | 25 | 22.5 | 17.5 | 5 | 0 |
| 1. Number of Modbus ports | 5 | 4 | 2.5 | 1 | 0 |
| 1. DNP3 ports using SHODAN | 10 | 8 | 5 | 1 | 0 |