

ICS010 ICS Lab 2 Scanning and Enumerating

Lab Objective

The objective of this lab use scanning and enumeration techniques to discover control devices on an internal network.

In the previous we lab, access to the wireless network was obtained. For this lab, you will use Zenmap to discover Modbus devices on the network. Modubus is a popular communication technology used in today's control systems.

In this lab, you will learn to:

- Scan and enumerate devices on an internal network

Lab Environment

This lab requires a wireless laptop with Kali Linux flash drive and ICS lab kit.

Lab Duration

25 minutes

Lab Tasks

Use ZenMap to identify Modbus devices on a network.

Background

Zenmap is the GUI version Nmap (*Network Mapper*). Zenmap is a security scanner originally used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Zenmap sends specially crafted packets to the target host and then analyzes the responses. The software provides a number of features for probing computer networks, including host discovery and service and operating system detection.

Lab Scenario

Once network access is obtained, a scanning and enumeration tool must be used to identify devices on the network. In this lab, you will scan a network for the Modbus protocol that operates on port 502 using Zenmap.

Lab Procedure-Scanning and Enumeration in Zenmap

1. Once connected to the wireless network, the IP addressing scheme can be discovered using *ifconfig* in Kali Linux. Ifconfig provides IP addressing information assigned to your laptop from the wireless access point.
 - Open a Terminal window in Kali and type *ifconfig*. Fig. 1

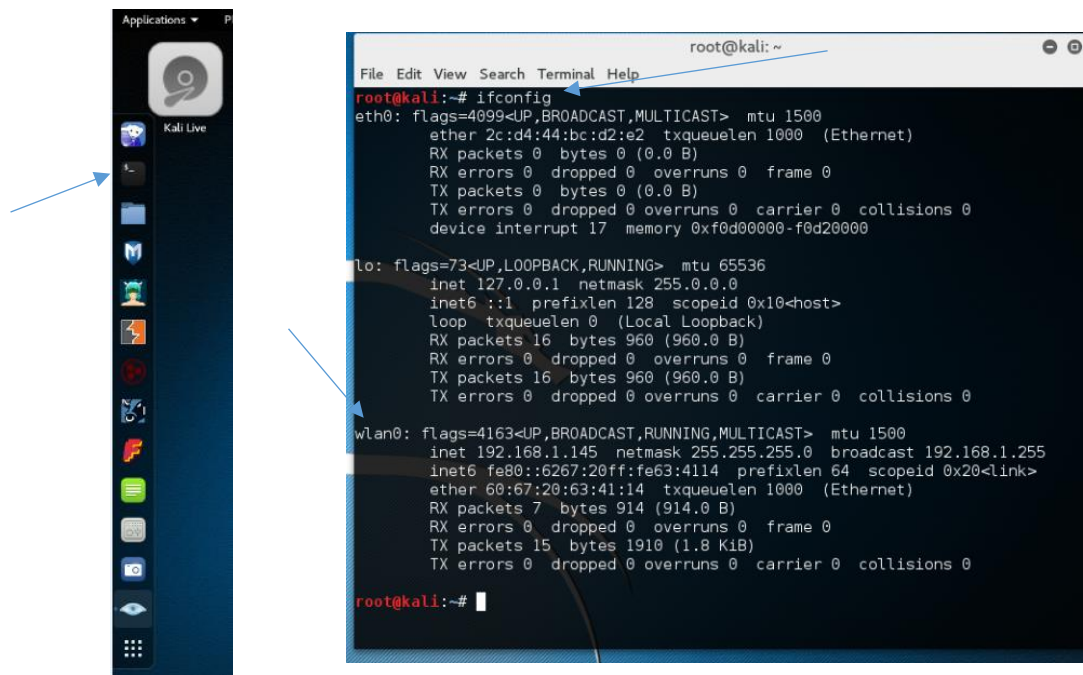


Fig. 1

- Note your IP address and subnet mask for your wireless adapter **wlan0**. You will need this information to complete a Zenmap scan.

2. Begin Zenmap by typing **zenmap** in a terminal or by clicking the Zenmap icon in the Applications menu. Fig 2

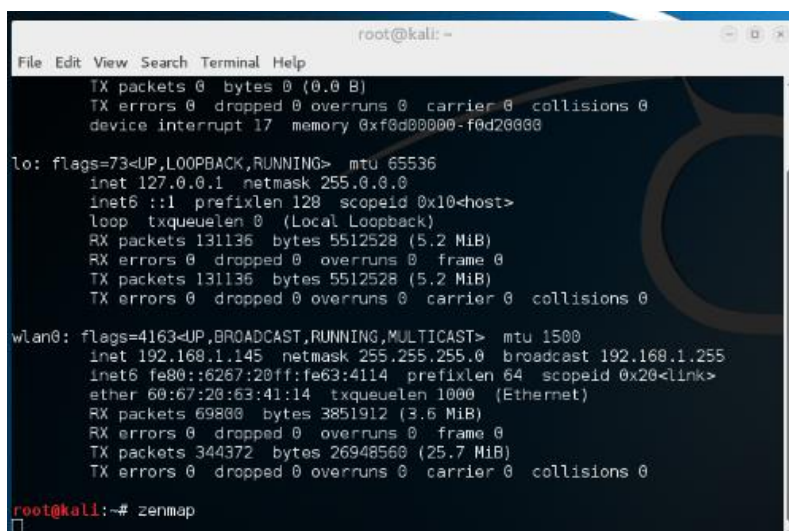


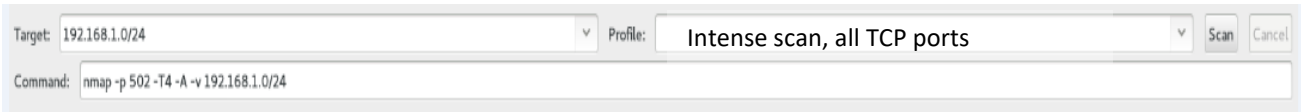
Fig 2

- The IP address is 192.168.11.x (x being the host address of your laptop). The subnet mask is 255.255.255.0. The subnet mask describes how many bits are assigned to the

network ID and how many bits are assigned to the host ID. 192.168.11.0 255.255.255.0 or /24 tell us that the first 3 octets (24 bits) are reserved for the network ID and the last octet is reserved for host addresses.

- Since we do not know exactly which address the control device is using, we should scan the entire subnet.

3. Enter the following scanning information into Zenmap. Fig 3



The screenshot shows the Zenmap configuration window. The 'Target' field is set to '192.168.1.0/24'. The 'Profile' dropdown is set to 'Intense scan, all TCP ports'. The 'Command' field contains the command 'nmap -p 502 -T4 -A -v 192.168.1.0/24'. There are 'Scan' and 'Cancel' buttons on the right.

Fig 3

1. **Target:** 192.168.11.0/24
2. **Profile:** intense scan, all TCP ports

- Note: For the scan, we are targeting control devices that use Modbus TCP communication on port 502. In the **command** area change port ranges from **1-65535** to **502**. Fig 4

- Command explanation:

Command: nmap -p 502 -T4 -A -v 192.168.1.0

- p port or ports to be scanned
- T4 caps the scan time to 10ms
- A Aggressive scan
- v verbosity level

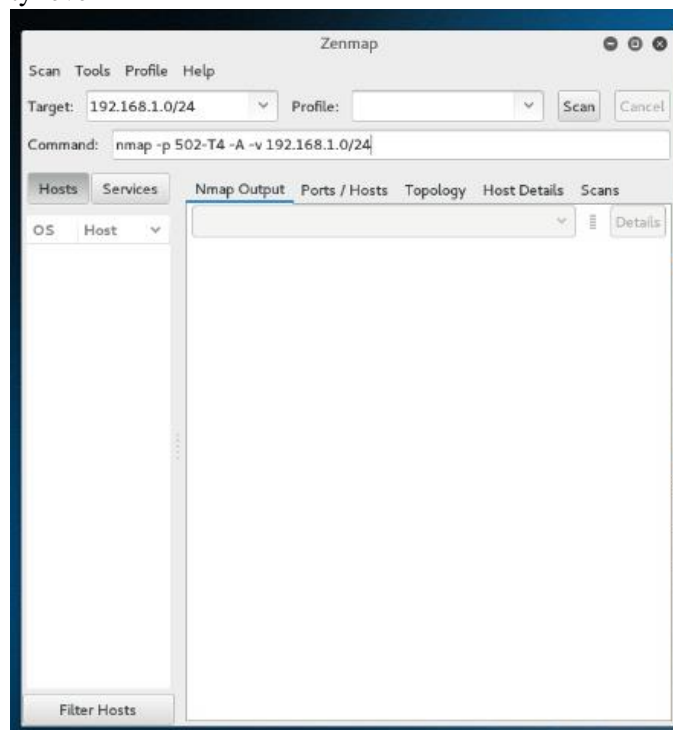


Fig 4

4. After the scan completes, the output status of each live host is displayed. See Fig 5 below.

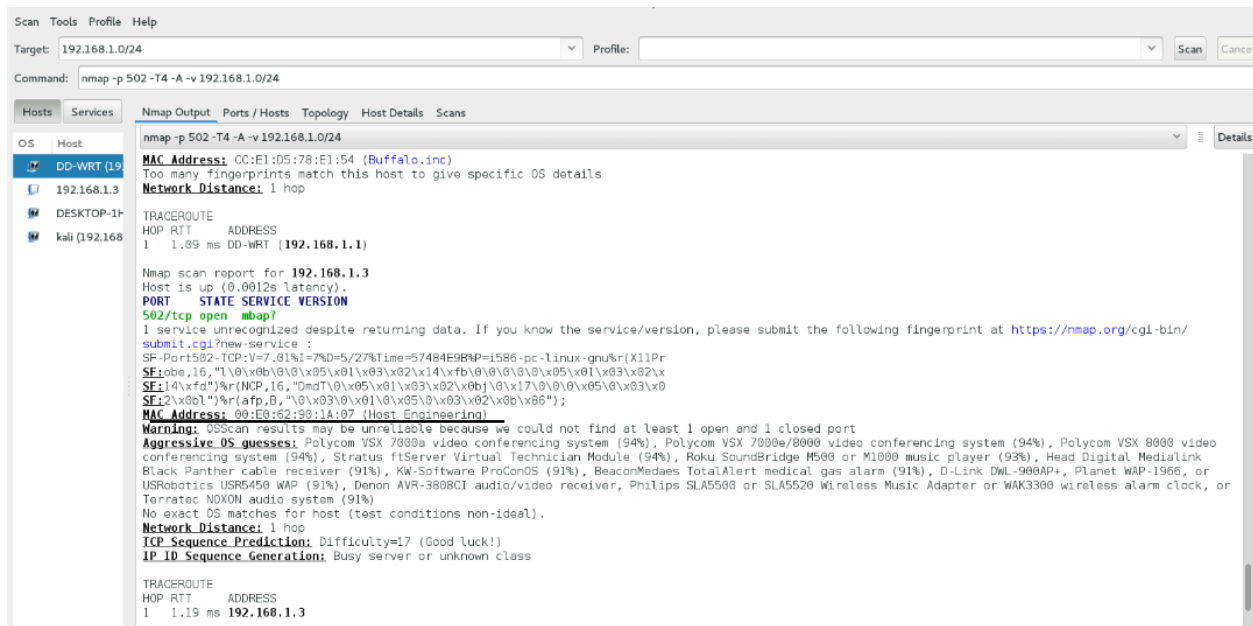


Fig. 5

- A quick search of the MAC address determines that IP address 192.168.1.3 is using a Host Engineering Ethernet port, which is found on DoMore PLCs or the Direct Logic 205 PLC.



5. We have now enumerated a DoMore PLC on the network. The next step in the process is to capture packets from the PLC with Wireshark to attempt to take control of the device.