Lab 5 Outline

Background:

IEC 62433 series of standards and NIST 800-82 outline cybersecurity standards for securing industrial control systems(ICS) using modern IT cybersecurity practices. This lab outlines introductory practices to secure ICS networks, or operational technology(OT), by pentesting via network reconnaissance tools and common IT/OT implementations. Use of these tools on networks without permission is advised against before notifying IT/OT professionals and internet service providers(ISP). This is a secure network environment where IEDs do not have direct access to sensitive systems and lives are not in danger. Use in real SCADA systems can cause adverse damage to equipment and bodily harm/injury.

Introduction:

In most cases, when penetration testing a network, we want to avoid damages to devices on the network and possible down time that can result from our tests. In order to do so, this lab will be broken up into two sections. The first of which is doing reconnaissance in the form of network mapping/routing and port/packet sniffing to see what is available and secure from different points in our OT network.

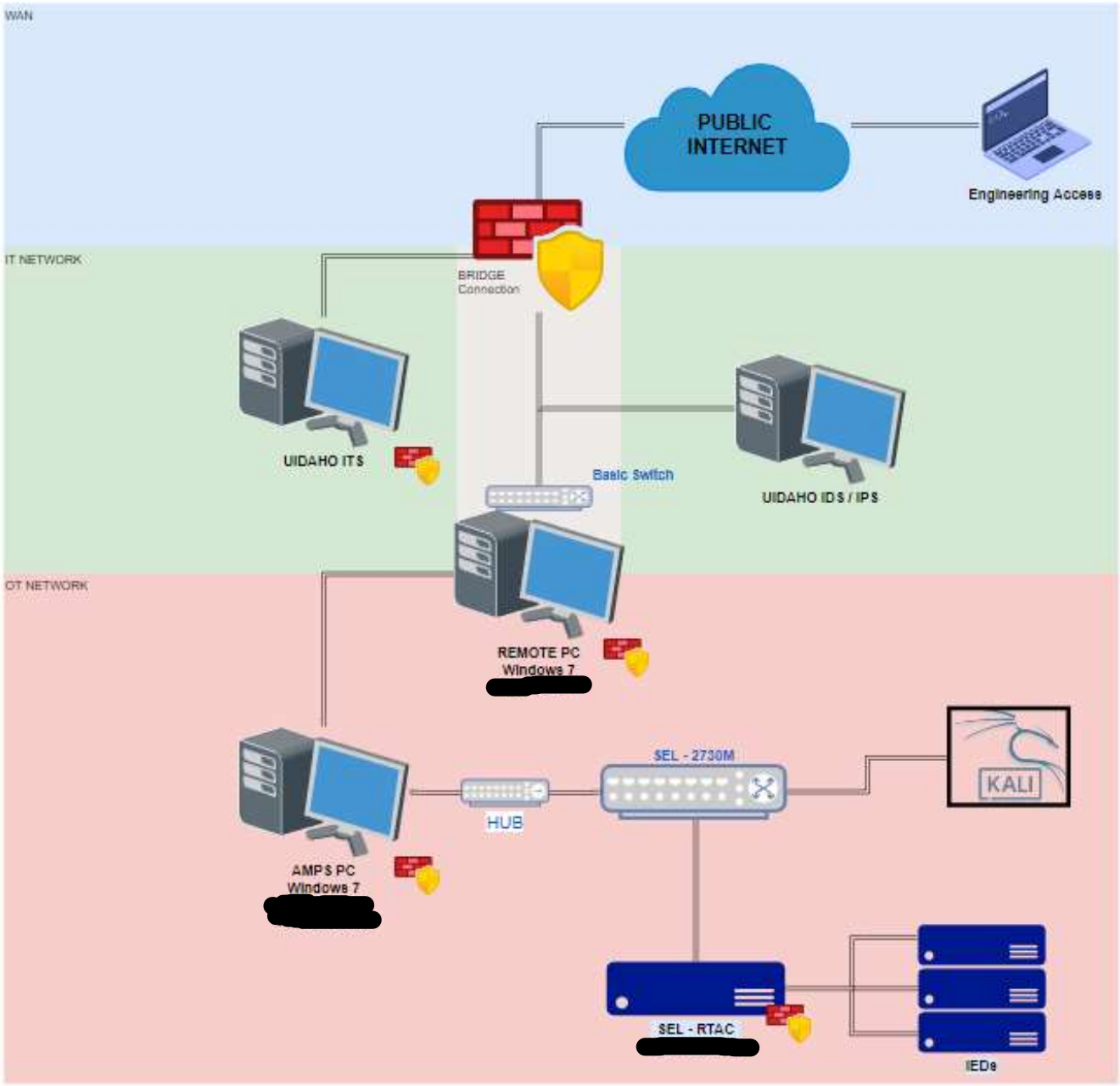
Then the second is an optional section that takes an in-depth view of virtual networking and modeling. These resources use VMware Workstation with a simulated view of our lab setup to test and implement open-source security options. Taking a virtual configuration lets us safely test and develop cybersecurity options that can later be used to increase the security of our current network without disrupting ICS/SCADA routines.

Configuration:

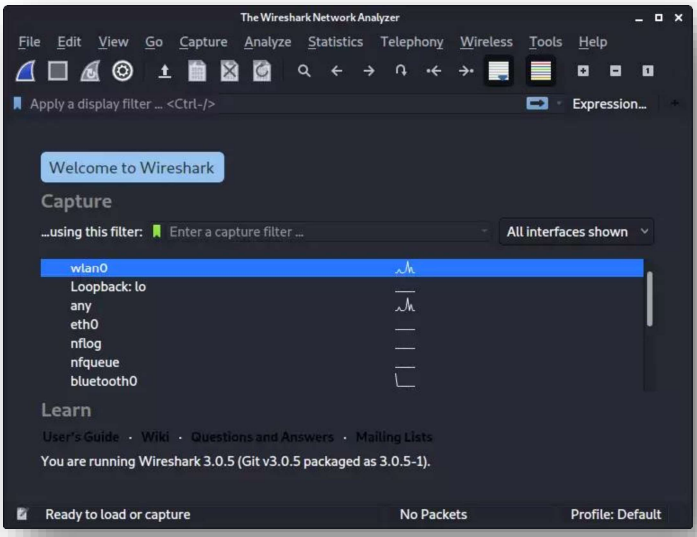
<u>Section 1</u>
SEL-3622(NSG)
SEL-2730M
SEL-3530(RTAC)
Multiple SEL IEDs
AMPS PC
Raspberry Pi(RPi)
    Insert Kali SD card into RPi C from previous labs and use same setup.

<u>Optional Section 2</u>
Kali Linux
    Install:
    Netdiscover
    Nmap
    Wireshark
VMware Workstation Pro 15
Virtual Machine Configuration Files

Initial Network Diagram



OT Network:



I Network Scanning:

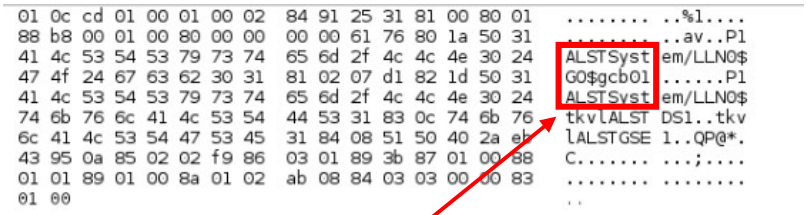
1. Log onto the Kali Linux RPi
   a. Username/Password -[redacted]
2. Make sure that the RPi is connected to a port on the Hub
3. Open terminal windows
4. Use *ifconfig*
   a. Locate your IP Details
      - IPv4, Subnetmask, and Default Gateway
      - Subnetting Videos

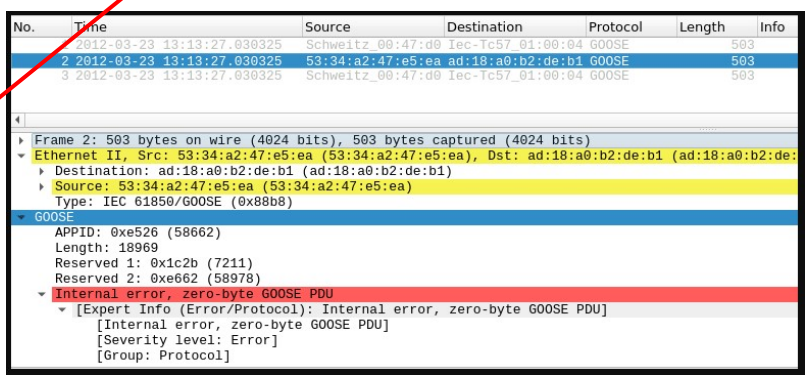
Online Devices

1. Use command netdiscover -h
2. Use command *sudo netdiscover*
   a. Let cycle through till[redacted] (All IP addresses under subnet[redacted])
      - Netdiscover actively sends ARP requests as-well-as passively monitors these packets
   b. Press Q to stop search
      - Set list aside for reference
        - Take note of different devices on network
3. Open another terminal window
   a. Use command *sudo wireshark*
   b. Select eth0
   c. Select File > Start Capture
      - Stop after 15 seconds
   d. Type in filter bar
      - GOOSE
        - Try other protocols TCP, UDP, ARP
        - You can also combine filters w/ 'and'
      - ip.addr == xxx.xxx.xxx.xxx
        - View traffic filtered using some IPs from netdiscover list
   e. Search GOOSE in filter
   f. Select GOOSE packet > Ethernet II dropdown
      - View Destination MAC Address
      - View Source Address

      If unencrypted, we can view the manufacturer, destination, and source addresses, and sometimes the specific model of device

      What are some devices you see?





Nmap on ICS devices

4. Open a third terminal window
   a. Use command *sudo su*
      - *Password -* [redacted]
   b. Use command *nmap -h*
      - Look through list of possible commands
      - Nmap cheat sheet
   c. Use command *nmap -Pn -sT -p502 --script modbus-discover <target>*
      - Try on [redacted]
        - SEL - RTAC
      - From wireshark traffic
        - Known devices trying to communicate
        - Filter wireshark using ip.addr == [redacted]
   d. Use command *nmap -Pn -sT -p502 --script modbus-discover* [redacted]
      - The asterisk is a wildcard and will search throughout all 256 ports.
        - May take a while.
        - Press enter to check progress.
   e. Use command *nmap -Pn -sT --scan-delay 1s --max-parallelism 1 -p *
   *80,102,443,502,530,593,789,1089-1091,1911,1962,2222,2404, *
   *4000,4840,4843,4911,9600,19999,20000,20547, *
   *34962-34964,34980,44818,46823,46824,55000-55003 *
   <target>
        - Will take significantly more time

Common scan types

- *-sS(Stealth scan)*
  - In the three-way TCP/IP handshake, this will not complete the handshake.
- *-Pn(Disable Ping Return)*
- *-sT(TCP Scan)*
- *-sV(Version of service on device)*
- *-O(OS Detection)*
- *-T#(Timing and Performance)*
  - *# = 0-5*
    (i) *T0/1 IDS Evasion*
    (ii) *T2-5 Depending on network speeds*

Perform vulnerability scan of network

f. Use Command *nmap -sV --script nmap-vulners/ <target>*

- List vulnerabilities
  - Vulnerable to ____ DDoS, ____ MiTM, etc.
  - List open ports(Holes in the network)

VMware
Workstation Pro 15.

Optional Section 2