Port Scans of Physical Access Control System Boards

The missing piece of the puzzle!

By Matt Bordelon
matt.bordelon@cleco.com

Thanks to Phillip Miller for his help
Presentation Targets

- What’s a PACS system?
- Typical configuration (Server- Processor – I/O – Doors)
- Things to consider/ concerns
- Configuring a test system (boards-laptop-OS)
- nmap command and parameters
- Example output
- UDP versus TCP
- Considering what to disable
Physical Access Control System

BCS PSP

CTOC PSP

ENERGY
OPS PSP

PACS
Server
Physical Access Control System

Processor Board

Input - Output Board

Input - Output Board

Corporate Network

TCP/IP

TCP/IP

TCP/IP

PACS Server

Located Remote to the PSP

Located local to the PSP

Within scope of Vulnerability Assessment

Serial

Serial

Hard Wired

Emergency Exit

Magnetic Lock

Card Reader

Outside

Inside

Physical Access Point (i.e. Door)

Emergency Exit

Located local to the PSP

TCP/IP
Running port scans on an embedded system board was not like running one on other machines

- Concerned over the lack of a high level operating system
  - Afraid to “Brick” the system - essentially making it unusable.
  - Would we possibly turn off something that was needed for the system to run or communicate to it?

- How would we run the port scan on a live system without affecting the CIP requirements of the PSP (i.e. what happens to the doors)?
Vital to communicate with your vendor- these are embedded systems

- If you have a contract for support, take advantage of it
  - Be specific in what you’re planning to do
  - The vendor may not be familiar with customers performing port scans on their boards
  - The vendor may have to ask their board supplier about the effects of running the scan- depends on who is writing the firmware
  - Find out how to reset your board to factory defaults in case a mistake is made
  - You will need to know which ports and services are essential to the system’s operation
  - Also will need to know the effects of disabling the non-essential ports and services. Some may not be able to be reset.
Weigh your options when it comes to performing a scan on a live system

- It’s best if you can run your scan on a live system, but you may not be able.

- You may have to configure a test system which accurately represents the environment of the processor boards
  - Acquire the same model processor boards used for each of the PSPs
  - Get a power supply
  - Mounted processor boards to a piece of plywood- not elegant, but hey it works
  - Wire boards together and to the power supply
  - Configure the boards just like they are in the field
Example of a Test setup

- Laptop
- Computer cable
- Power Supply
- Processor Boards
Read processor board documentation

- Need to find out how to connect to the processor boards via a laptop
  For this example:
  - Firmware allowed you to use a web browser over a http connection
  - Had to adjust the dip switches on board to connect and then switch them back again - be sure to power down each time
  - Configure the laptop to a specific IP Address
  - Also set a static IP Address of the board via the board’s web interface
Laptop

- Disabled the wireless interface
- Set the IP Address according to the board’s documentation
- Used a version of Linux to boot-up on- Kali Linux Live CD
  - Kali Linux is designed for use in Penetration Testing
  - Comes with nmap (used for port scan) as part of the distribution
  - Double checked the “eth0” network interface to make sure it matches the IP Address that is required by the board
- Connected the laptop to the TCP/IP connectors with a CAT-5 patch/crossover cable.
Right click on the network icon (red arrow). Then left click the edit connections menu.
Checking eth0 in Kali Linux

Network Connections window

Click on the wired connection name and choose edit. Choose the IPv4 Settings Tab and choose the Manual method and enter in the Laptop’s IP address, Netmask (typically 255.255.255.0), then the gateway (can be 0). Of course choose save at the end of the process.
“eth0” is the first network device (Ethernet card) connected to a computer that a Linux operating system identifies.

Check this out if are getting problems with running the nmap command- giving you a can’t find target error.

1. Right click on the network icon in the upper right of the Kali Linux display
2. Left click on “Edit connections”
3. Select “wired connection 1”
4. Click on “edit”
5. Select the “IPv4 Setting” tab on the pop-up display
6. Type in under address, xxx.xxx.xxx.xxx, this is the IP Address that we will give to eth0
7. Type in “255.255.255.000” for the subnet mask
8. Click on “add”
9. Click on “Save”
What’s nmap?

- Nmap (www.nmap.org)
  - Open source utility used in finding devices on your network and in device security audits - has many other uses
  - Supported by most operating systems - Linux is the most popular
  - Just type on a command line the nmap command and options - next slide
The nmap command used to run the port scan is as follows:

```
nmap –n –T3 –sS –sU –p1-65535 xxx.xxx.xxx.xxx | tee filename.txt
```

Breakdown:

- `-n` is no DNS resolution. No need because we are connecting directly to the board- speeds the process
- `-T3` adjustment to the overall speed of the command 0- very slow to 5- very fast
- `-sS` runs a scan of TCP ports in a “stealthy” fashion. Very popular and fastest way to scan TCP ports and works against all functional TCP stacks
- `-sU` runs a scan of your UDP ports. So scan will be of your TCP & UDP ports
- `-p1-65535` defines the port range of your scan. This one does from ports 1 through 65K which covers all your 16 bit addressing. Also can use –p- which covers all ports as well
- `xxx.xxx.xxx.xxx` is the Processor board IP Address the scan is running on

`| tee` “tee” will display on your screen the results of your scan and like a plumber’s tee will also direct it to a text file. In our example, it writes to the current directory.

`filename.txt` is the name of the text file you want your output to go to. You can also use `| tee` –a `filename.txt` if you want to append to the original file (in case you are running more than one scan and want the output in one file)
Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-19 09:33 UTC
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 4.41% done; ETC: 09:39 (0:05:47 remaining)
Stats: 0:00:20 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 5.27% done; ETC: 09:39 (0:05:42 remaining)
Stats: 0:22:56 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 32.38% done; ETC: 10:32 (0:36:04 remaining)
Stats: 0:22:59 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 32.46% done; ETC: 10:32 (0:36:02 remaining)
Stats: 0:23:00 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 32.48% done; ETC: 10:32 (0:36:02 remaining)
Stats: 0:23:00 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 32.49% done; ETC: 10:32 (0:36:01 remaining)
Stats: 0:23:00 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 32.50% done; ETC: 10:32 (0:36:00 remaining)
Stats: 0:23:01 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 32.50% done; ETC: 10:32 (0:36:00 remaining)
Stats: 0:23:00 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 32.51% done; ETC: 10:32 (0:36:01 remaining)
Stats: 0:23:01 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 32.52% done; ETC: 10:32 (0:36:00 remaining)
Stats: 0:23:01 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 32.53% done; ETC: 10:32 (0:35:59 remaining)
Stats: 0:23:01 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 32.53% done; ETC: 10:32 (0:35:59 remaining)
Stats: 0:23:01 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 32.53% done; ETC: 10:32 (0:36:00 remaining)
Stats: 0:23:31 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 33.44% done; ETC: 10:32 (0:35:31 remaining)
At the end of the scan we get what we were looking for

Nmap scan report for 192.168.0.151
Host is up (0.00081s latency).
Not shown: 131062 closed ports
PORT          STATE                   SERVICE
80/tcp        open                      http
443/tcp      open                      https
3001/tcp    open                      nessus
4001/tcp    open                      newoak
67/udp       open|filtered       dhcps
68/udp       open|filtered       dhcpc
161/udp     open|filtered       snmp
5353/udp  open|filtered       zeroconf
MAC Address: 02:0E:E5:A2:5E:DA (Mercury Security)

Nmap done: 1 IP address (1 host up) scanned in 3604.09 seconds
Possible Actions

- Ensure that default user names and passwords are changed
- Contact vendor about what you found and inquire about your options to disable non-essential services.
- Make sure that you identify the port and its service that is used to communicate with the server. Obviously this one should not be disabled.
- Consider leaving the port/service necessary to communicate with the board enabled
- Test the board reset procedure from your vendor. Make sure you can go back to factory defaults.
- Check with your vendor to see how and which services can be disabled.
  - User Interfaces may be your only option
- Run another scan after making changes to see that the ports/services have been disabled
nmap example output- Checking closed ports

Original

Nmap scan report for 192.168.0.151
Host is up (0.00081s latency).
Not shown: 131062 closed ports

<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>SERVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
</tr>
<tr>
<td>443/tcp</td>
<td>open</td>
<td>https</td>
</tr>
<tr>
<td>3001/tcp</td>
<td>open</td>
<td>nessus</td>
</tr>
<tr>
<td>4001/tcp</td>
<td>open</td>
<td>newoak</td>
</tr>
<tr>
<td>67/udp</td>
<td>open</td>
<td>filtered</td>
</tr>
<tr>
<td>68/udp</td>
<td>open</td>
<td>filtered</td>
</tr>
<tr>
<td>161/udp</td>
<td>open</td>
<td>filtered</td>
</tr>
<tr>
<td>5353/udp</td>
<td>open</td>
<td>filtered</td>
</tr>
</tbody>
</table>

MAC Address: 02:0E:E5:A2:5E:FA (Mercury Security)

Nmap done: 1 IP address (1 host up) scanned in 3604.09 seconds

Check

Nmap scan report for 192.168.0.101
Host is up (0.00077s latency).
Not shown: 131064 closed ports

<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>SERVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
</tr>
<tr>
<td>443/tcp</td>
<td>open</td>
<td>https</td>
</tr>
<tr>
<td>3001/tcp</td>
<td>open</td>
<td>nessus</td>
</tr>
<tr>
<td>4001/tcp</td>
<td>open</td>
<td>newoak</td>
</tr>
<tr>
<td>67/udp</td>
<td>open</td>
<td>filtered</td>
</tr>
<tr>
<td>68/udp</td>
<td>open</td>
<td>filtered</td>
</tr>
<tr>
<td>161/udp</td>
<td>open</td>
<td>filtered</td>
</tr>
</tbody>
</table>

MAC Address: 02:0E:E5:A2:5E:FA (Mercury Security)

Nmap done: 1 IP address (1 host up) scanned in 3605.13 seconds
As much as we would love for this PACS I/O board to run Nessus (CIP v5 compliant), this is not the case..

- Yes, the board has port 3001 open, but the listening service is not Nessus

- Actually, the vendor’s service associated with this port is used to communicate with the PACS server

- `/etc/services` contains the “general” services listening on a particular port. However this is not always correct
  - `/etc/services` is a file that lists ports and services normally associated with that port. If the scan sees the port is open it assumes this service is listening

- You will need to work with your vendor in order to help you identify these ports and their services
No, the I/O board is not running Nessus.

Port 3001?

Scan

OK
/etc/services file says you should be NESSUS

Could be any service

Hello!

Port 3001
PORT   STATE     SERVICE
67/udp open|filtered dhcps

- open|filtered means that Nmap didn’t get a response when the port was scanned
  - Ports are placed in this state when nmap doesn’t know if a port is open or filtered.
  - UDP open ports give no response
  - A “No response” could mean that a packet filter dropped the probe or any response it elicited.
  - Nmap doesn’t know if the port is open or the packet is being filtered
  - In this example the UDP protocol is used

- Closed TCP or UDP ports will normally respond with an ICMP* message (Destination unreachable)

*Internet Control Message Protocol- used by networked devices for sending error messages, diagnostics and controls
TCP Packet Scan

Send Port X scan packet

TCP Packet scan

Firewall

nmap knows the packet got to destination and for sure it’s open

SYN

SYN-ACK

Port X is open

Send Port X scan packet

nmap sees this as filtered

SYN

No response

Packet Blocked

Firewall

Send Port X scan packet

nmap sees this as closed

SYN

ICMP* Message Destination unreachable

Port X is closed

*Internet Control Message Protocol- used by networked devices for sending error messages, diagnostics and controls
UDP Packet Scan

nmap recognizes this as open|filtered but:
A) Did the packet get to the board?
B) Is the port really open?

nmap recognizes this as open|filtered

nmap sees this as closed

*Internet Control Message Protocol used by networked devices for sending error messages, diagnostics and controls
What did we learn here?

- How a Physical Access Control System works
- How one can setup an applicable test system
- How to use nmap to run the port scan
- What you see may not be what is actually running
- How nmap output responses differ between UDP and TCP ports
- Work with your vendor