

Preliminary steps before starting the experiment:

- 1) Click the Launch button to start the experiment.

The screenshot shows the Power Cyber Labs website interface. At the top, there is a red navigation bar with the text "POWER CYBER LABS" on the left and "ABOUT TESTBED EXPERIMENTS PUBLICATIONS DOWNLOADS THE TEAM" on the right. Below the navigation bar, the page is divided into two main sections: "Cyber Storyboards" and "ICS Storyboards".

Cyber Storyboards:

- C1: Network Discovery with Port Scanning** (highlighted in red):
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 measurements.
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 appropriately certain targeted measurements to avoid detection by the State Estimator Bad Data Detectors.
Buttons: LAUNCH (orange), MANUAL (red)
- C2: Vulnerability Assessment with OpenVAS** (red)
- C3: Wireshark, Scripting and Replay Attack** (red)
- C4: Pfsense Firewall Configuration** (red)
- C5: DoS Attack (upcoming)** (grey)

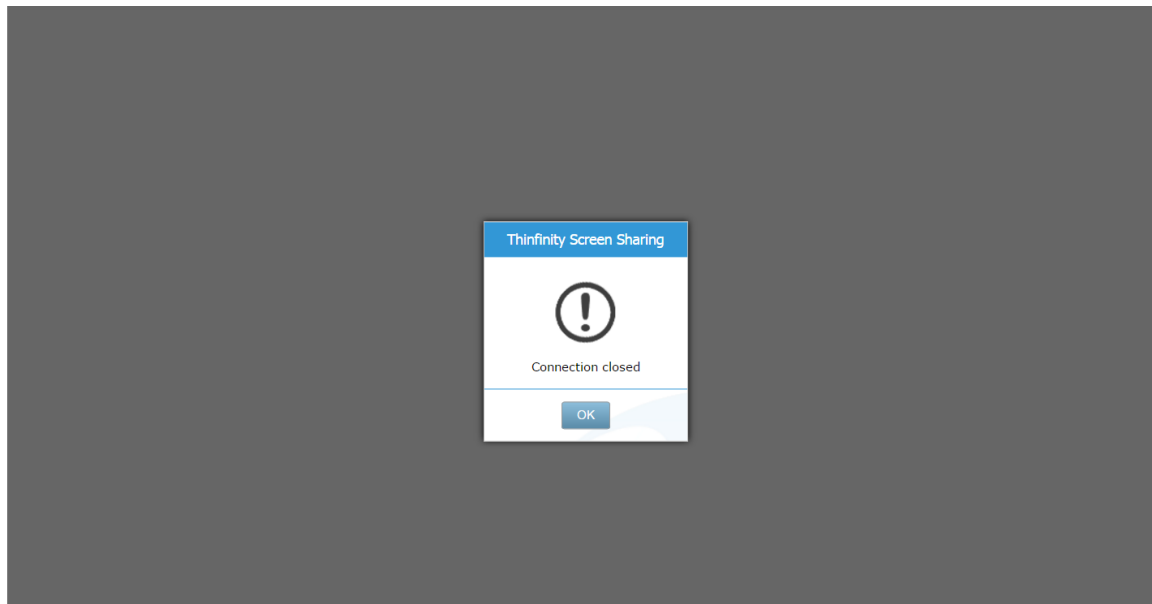
ICS Storyboards:

- ICS1: Attack and defense on a Remedial Action Scheme (automated)** (green)
- ICS2: Attack and defense on a Remedial Action Scheme (interactive)** (green)
- ICS3: Attack and Defense on Model-based AGC (automated)** (green)
- ICS4: Attack and Defense on Model-based AGC (interactive)** (green)
- ICS5: Ukraine Style Attack and Defense Experiment** (green)
- ICS6: Settings Manipulation (upcoming)** (grey)
- ICS7: State Estimation (upcoming)** (grey)

At the bottom left of the screenshot, there is a small URL: 64.113.69.210:8080/powercyber/portscan.php

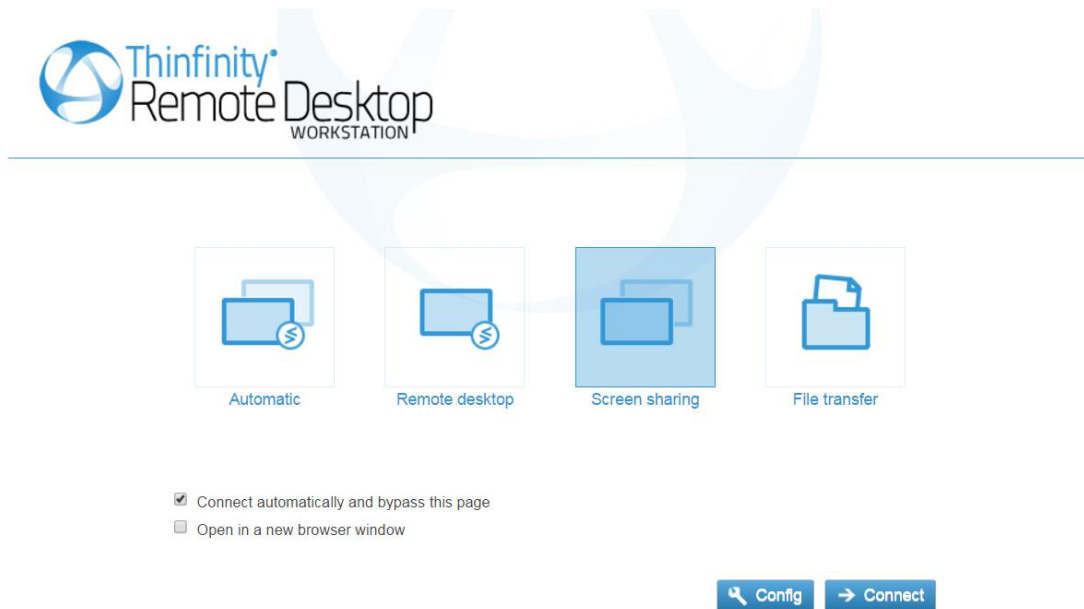
- 2) Click OK to create a new session

Attacker



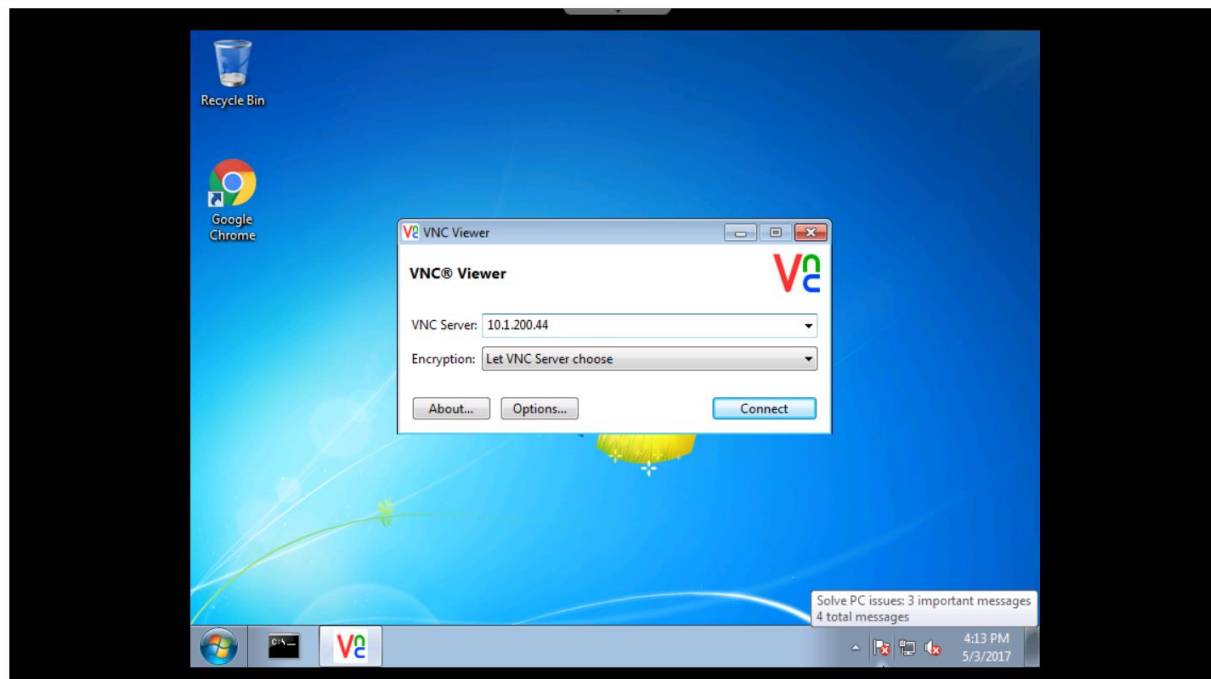
- 3) Click the **Screen Sharing** option and click connect to establish the session

Attacker



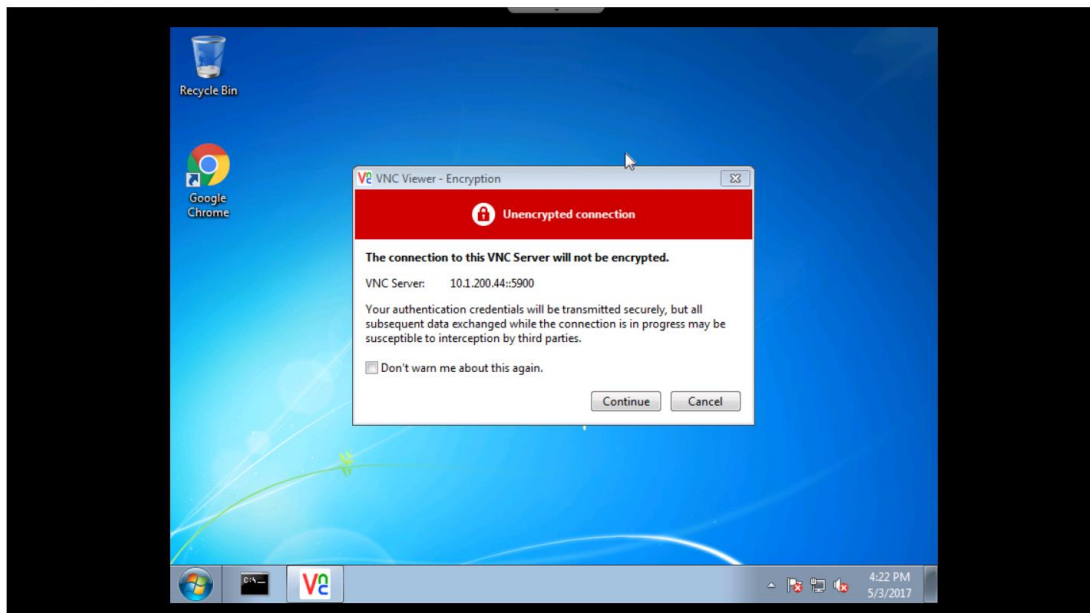
- 4) Click the **VNC viewer** button on the taskbar of the Windows 7 host that opens soon after and enter **10.1.200.44** as the ip address of the VNC server. Click connect to establish the session

Attacker



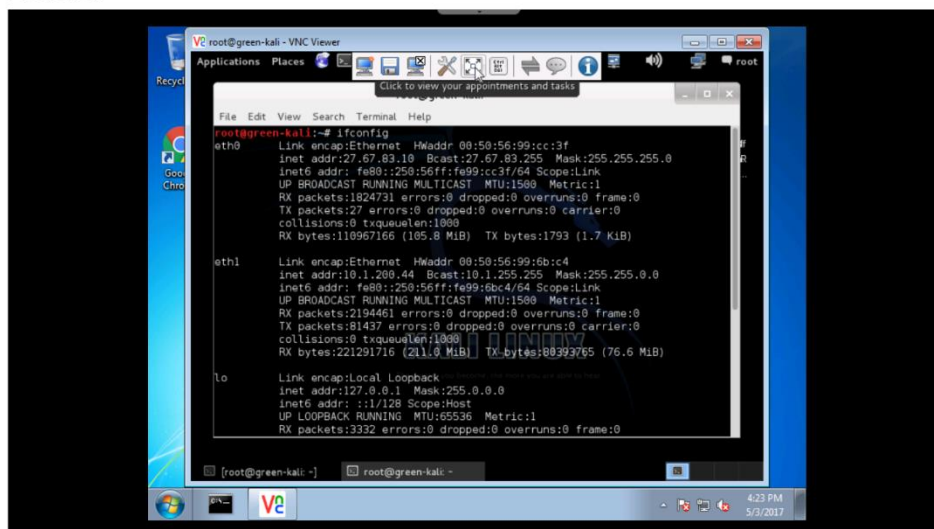
- 5) Click Continue to connect to the kali box.

Attacker



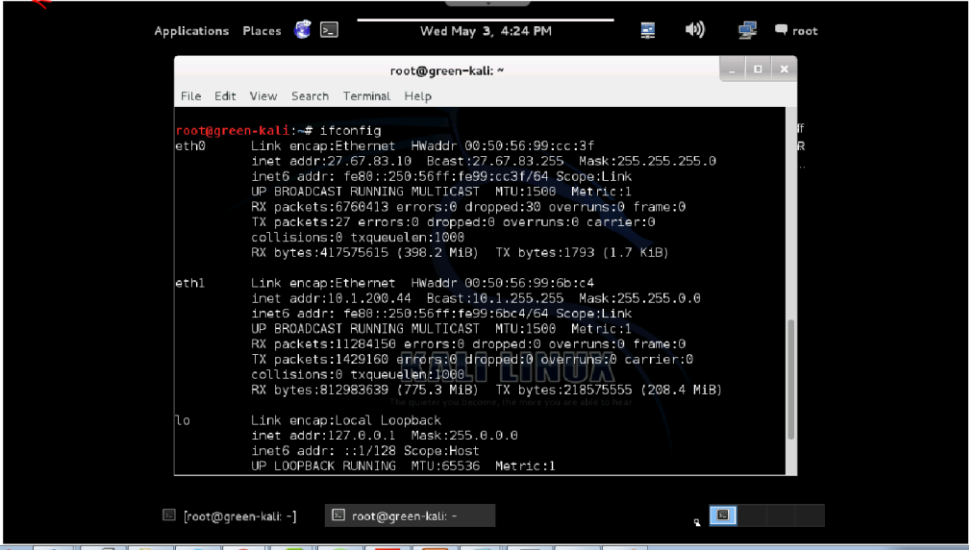
- 6) Gently hover over the center of the VNC viewer window to find the menu with options. Click the **Full Screen View** button (fifth from the left) for a better experience.

Attacker



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

Attacker



```
root@green-kali: ~  
File Edit View Search Terminal Help  
root@green-kali:~# ifconfig  
eth0      Link encap:Ethernet  HWaddr 00:50:56:99:cc:3f  
          inet addr:27.67.83.10  Bcast:27.67.83.255  Mask:255.255.255.0  
          inet6 addr: fe80::250:56ff:fe99:cc31/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:6766413  errors:0  dropped:30  overruns:0  frame:0  
          TX packets:27  errors:0  dropped:0  overruns:0  carrier:0  
          collisions:0  txqueuelen:1000  
          RX bytes:417575615 (398.2 MiB)  TX bytes:1793 (1.7 KiB)  
  
eth1      Link encap:Ethernet  HWaddr 00:50:56:99:6b:c4  
          inet addr:10.1.200.44  Bcast:10.1.255.255  Mask:255.255.0.0  
          inet6 addr: fe80::250:56ff:fe99:6bc4/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:11284156  errors:0  dropped:0  overruns:0  frame:0  
          TX packets:1429160  errors:0  dropped:0  overruns:0  carrier:0  
          collisions:0  txqueuelen:1000  
          RX bytes:812983639 (775.3 MiB)  TX bytes:21857555 (208.4 MiB)  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
```

Actual Experiment:

Network Discovery with Port Scanning

Learning Outcomes

- Learn how an attacker uses port scanning to gather information that can be used later for an attack.
- Be able to discover what hosts are alive on a network and what services are running on them.

Port Scanning is the process of making connection attempts to another networked computing device in order to gain information about what services are running on the machine.

The most common tool to perform this operation is called Nmap. Nmap, and its graphical counterpart Zenmap, allow an individual to scan vast networks and to discover what machines are on the network and what services are being offered.

More exactly, Nmap performs these functions by sending different types of requests, or probes, to the target host and observes what data, if any, is sent back.

Ping Scan

When scanning a network, the first thing to do is to determine which hosts are “alive” on a network. This process is known as host discovery.

Nmap has a vast amount of methods for performing host discovery. In this module, we will discuss only one, the basic “ping” scan. As an example, to perform a ping scan against the network 10.0.0.1/24 (10.0.0.1-10.0.0.254), one would issue the following command:

```
nmap -sn 10.0.0.1/24
```

similarly, if you want to only target a single host, you could issue the following command:

```
nmap -sn host_ip_address
```

These scans should report back telling you whether they are up or not.

Your Turn

Use nmap to discover which hosts are alive on the corp, control center, and substation networks. Create a list of IP addresses in a text file that are up on the networks.

corp: A.A.A.0/24

control center: B.B.B.0/24

substation: C.C.C.0/24

Where A.A.A is your corp network range, etc.

*You may ignore the host with IP address as A.A.A.254 (similarly, B.B.B.254 and C.C.C.254), it's a VM in ISERINK and not of as much interest. The number of hosts you should be able to find is 7.

Service Scan

After you have discovered which hosts are on the various networks of interest, we then want to interrogate those machines with a deeper scan. This is where the nmap service scan comes into play.

To do a service scan against the IP addresses in a file called `hosts`, issue the following command:

```
nmap -iL hosts -sV
```

Your Turn

Now do the same for the list of IP addresses that you collected from the ping scan. Take note of key services that are running on each host.

Extras

If you have extra time, try some of the other scan techniques shown in the nmap help.

Just type “nmap” with no arguments to list the help information.

Report

- 1) Note down the command you used and the corresponding information collected.

2) Analyze the information that you get and comment on what potential attacks could happen to your fleet.

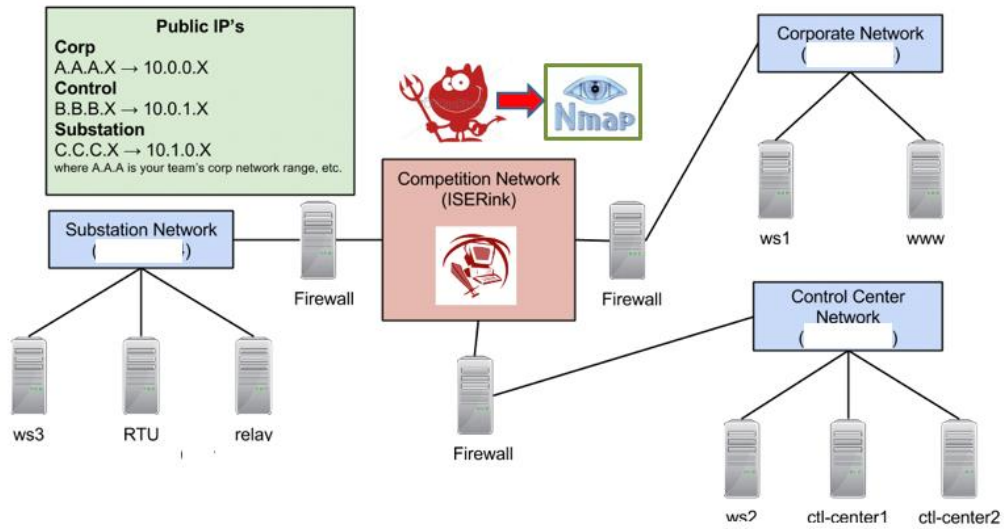


Fig1. Overall topology for your reference.