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-fine-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 Connection closed |
|--|
| |

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

Attacker

Attacker

| C Thir Rei | n <mark>finity"</mark> mote Desl | COD | | | |
|----------------------|---|-------------------------------|----------------|------------------|--|
| | Automatic | Remote desktop | Screen sharing | File transfer | |
| | Connect automatically ar Open in a new browser v | id bypass this page vindow | 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

| | · · · · | | |
|---------------|-----------------------------------|--------------------|---------------------|
| Recycle Bin | | | 7 |
| S rock | | | |
| Chrome | V2 VNC Viewer | | |
| | VNC® Viewer | Ve | |
| | VNC Server: 10.1.200.44 | | |
| | Encryption: Let VNC Server choose | • | |
| | About Options | Connect | |
| | - Aline | | |
| | | | |
| 1 | | Solve PC issues: 3 | important messages |
| () | Ve | 4 total messages | 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.



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



Repeat steps 2 and 3 for the Control Center virtual machine, the Substation-RTU virtual machine and the Substation-Workstation virtual machine respectively.

Actual Experiment:

pfsense Firewall Configuration

Learning Outcomes

- Learn to configure firewall rules to meet certain security requirements.
- Learn how to restrict access to various devices connected based on the requirements.

Accessing the pfsense Firewall

pfsense uses a web-based interface to configure the various settings on the firewall. This web interface can only be accessed from the LAN side of the firewall.

We have created a workstation machine inside each network, that is running Windows 7, for the purpose of configuring each firewall.

To configure a certain pfsense firewall, first access the workstation machine that is on the same network as the firewall. (e.g.) If one wants to manage the firewall in the **Substation** network, he would access the workstation named **teamX_substation-workstation3-win7**.

The login credentials for that machine are:

Username: alice Password: whoami On the workstation, open a web browser and enter the IP Address of the LAN side of the pfsense firewall. (e.g.) to access the pfsense firewall on the corporate network enter the IP "10.0.0.1".



The login credentials for all the firewalls are as follows:

username: admin password: pfsense

Viewing the Port Forward Configuration

From the pfsense web interface, go to Firewall \rightarrow NAT



Here you will see how each of WAN IP Addresses are being forwarded to corresponding LAN IP addresses on corresponding ports.

| | If | Proto | Src. addr | Src. ports | Dest. addr | Dest. ports | NAT IP | NAT Ports | Description |
|---|-----|---------|-----------|------------|------------|--------------|-----------|-----------|-------------|
| ω | WAN | ТСР | * | * | 64.39.3.30 | 1 - 10000 | 10.0.0.30 | 1 - 10000 | |
| | - | 2407050 | - | - | | No. Services | | | |
| 8 | WAN | TCP | * | * | 64.39.3.10 | 1 - 10000 | 10.0.0.10 | 1 - 10000 | |
| 8 | WAN | ICMP | * | * | 64.39.3.10 | * | 10.0.0.10 | * | |
| 8 | WAN | ICMP | * | * | 64.39.3.30 | * | 10.0.30 | * | |

Viewing the Firewall Rule Configurations

To view the firewall rules that are automatically generated from the above NAT port forwarding settings, go to Firewall \rightarrow Rules

| 😵 pfS | ense.lo 0.0.0.1, | caldoma /firewall_ | i <mark>in - Fire</mark> nat.php | e × | + | | | Q Search | |
|----------------------------|----------------------|-----------------------|-------------------------------------|-----------------|--------------|--|----------------|-------------|----------|
| Firewa Port Forv | SC all: N vard | ► Sys | tem Port | ▶ Inter Forw | faces ard | ▼ Firewa Aliases NAT Rules Schedule Traffic S | ll → Servio | ces ► VPN | ▶ Status |
| | If | Proto | Src. a | ddr | Src. po | Virtual II | ^o s | Dest. ports | NAT IP |
| | WAN | ТСР | * | | * | 6 | 4.39.3.30 | 1 - 10000 | 10.0.30 |

| PfSense.loc | aldomain - Fi | re × + | | | | | | | |] @ | |
|-------------|------------------|--------------|------------|------------------|----------|----------------------------|-------------|------------|------|-----|--|
| | firewall_rules.p | ohp | | ⊽ C ⁴ | C Search | | ☆自 | □ + | ⋒ | ø | |
| esense / | ▶ System | ▶ Interfaces | ▶ Firewall | Services | ► VPN | Status | Diagnostics | s ► Gold | ► He | lp | |

0 |

Firewall: Rules

| | ID | Proto | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | 0 |
|---|----|--------------|-------------------------------------|------|-------------|--------------|---------|-------|----------|------------------------|-----|
| 8 | | * | RFC 1918 networks | * | * | * | * | * | | Block private networks | 3 |
| 8 | | * | Reserved/not assigned by IANA | * | * | * | * | * | * | Block bogon networks | 23 |
| ۵ | | IPv4 TCP | * | * | 10.0.0.30 | 1 - 60000 | * | none | | NAT | 6 |
| ۵ | | IPv4 ICMP | * | * | 10.0.0.30 | * | * | none | | NAT | 800 |
| ۵ | | IPv4 TCP | * | * | 10.0.0.10 | 1 - 60000 | * | none | | NAT | 800 |
| ۵ | | IPv4 | * | * | 10.0.0.10 | * | * | none | | NAT | 6 |

- Is there something wrong with the way we are using the firewall?
- How could these rules have been written better?

Adding Firewall Rules to prevent Trip Script from unauthorized host

We want to configure the firewall on the **substation network** to **only allow** DNP3 traffic from the control center network NAT (the PFSense firewall). (IP address = x.x.x.1 where x.x.x is your control network) (Default port for DNP3 is 20000)

On the **substation workstation**, open a web browser and enter the IP Address of the LAN side of the pfsense firewall. (e.g.) to access the pfsense firewall on the substation network enter the IP "10.1.0.1".

Then navigate to the rules tab and click the plus sign at the bottom right side of the page.

| Sei | 150 | | Systematic | am 🕨 Interfa | ces) | Firewall > S | ervices | ▶ VPN | Status | Diagno | stics + Gold + H | elp |
|-----|-----|----|--------------------------------|-------------------------------------|-------|--------------|--------------|---------|----------------------------|----------|------------------------|-----|
| - | - | 1D | Proto | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | 18 |
| | 8 | | • | RFC 1918 networks | • | * | • | * | * | | Block private networks | 20 |
| | 83 | | * | Reserved/not assigned by IANA | * | * | • | * | * | * | Block bogon networks | 26 |
| | | | IPv4 TCP | • | * | 10.1.0.210 | 1 - 60000 | * | none | | NAT | |
| | • | | IPv4 TCP | * | * | 10.1.0.10 | 1 - 60000 | * | none | | NAT | |
| | ۵ | | IPv4 ICMP | • | • | 10.1.0.10 | • | • | none | | NAT | |
| | ۵ | | IPv4 ICMP | | * | 10.1.0.210 | * | * | none | | NAT | |
| | ٩ | - | IPv4 TCP | * | * | 10.1.0.218 | 1 - 60000 | * | none | | NAT | |
| | ۵ | | IPv4 ICMP | • | • | 10.1.0.218 | • | • | none | | NAT | |

Firewall Rule – Block port 20000 from all IPs except your control center host.

Action: Block Interface: WAN TCP/IP version: IPv4 Protocol: TCP Source – NOT: selected Source – Type: Single host or alias Source – Address: X.X.X.1 Destination – Type: Single host or alias Destination – Address: 10.1.0.210 Destination port range: to set the destination port, select other as the port range. In the from field, enter 20000 as the port number. Leave the from field blank.

Then click save.

| Edit Firewall rule | |
|--------------------|--|
| Action | Block Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. |
| Disabled | Disable this rule Set this option to disable this rule without removing it from the list. |
| Interface | WAN ÷ Choose which interface packets must be sourced on to match this rule. |
| TCP/IP Version | IPv4 ÷ Select the Internet Protocol version this rule applies to |
| Protocol | TCP ‡ Choose which IP protocol this rule should match. Hint: in most cases, you should specify TCP here. |
| Source | ✓ not Use this option to invert the sense of the match. Type: Single host or alias ‡ Address: 33.96.5.1 / 31 ▼ Advanced - Show source port range |

| Destination | not Use this option to invert the sense of the match. |
|------------------------|--|
| | Type: Single host or alias Address: 10.1.0.210 |
| Destination port range | from: (other) - 20000 |
| | to: (other) - 20000 Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port |
| Log | Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If you we consider using a remote syslog server (see the Diagnostics: System logs: Settings page). |
| Description | You may enter a description here for your reference. |

Click Apply changes to apply the firewall rule.

| The firewall rule configuration has been changed. You must apply the changes in order for them to take effect. | Apply changes |
|---|---------------|
| | |

We must now move the firewall rule we created to the top of the list so it gets applied first.

Click the *check mark* on the left side of the rule you just created.

| 2 | IPv4 TCP | ! 33.96.5.1 | * | 10.1.0.210 | 20000 | * | none | | |
|---|-------------|-------------|---|------------|-------|---|------|--|--|
| | | | | | | | | | |

Then scroll up and click the left arrow to insert the rule above the NAT rules but below the 2 block rules.

| | | ID | Proto | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | GE |
|---|----|----|-------------|-------------------------------------|------|-------------|--------------|---------|-------|----------|------------------------|------------------|
| | 8 | | • | RFC 1918 networks | • | | • | | • | | Block private networks | 20 |
| | 63 | | • | Reserved/not assigned by IANA | • | • | • | * | • | • | Block bogon networks | |
| E | ۵ | Γ | IPv4 TCP | • | | 10.1.0.210 | 1 - 60000 | • | none | | NAT | Refere this rule |
| C | ۵ | | IPv4 TCP | • | • | 10.1.0.10 | 1 - 60000 | • | none | | NAT | |
| | - | | 10.00 | | | 10.000 | | | 02200 | | ine. | 170.00 |

Then click Apply changes.

Your Task

1, Setup your whitelist in the substation firewall following above steps, and also try to create a blacklist in the similar way.

2, Once the firewall rules have been configured (either with your whitelist or blacklist enabled at one time), please verify that the changes made in pfsense does not adversely affect the normal functioning of the SCADA system. Try to switch your relay from CC and see if the controls can be done.

3, Test out whether the trip script is being blocked from the attacker Kali.

Other

Please submit the screenshots of the two firewall rules configuration. This time you should work in your own team, and the relays will be used in a time-multiplexing way. Check the following to find the two time slots when your team has a relay connected.

| | 03/03/2016 | 03/06/2016 | 03/08/2016 | 03/10/2016 |
|--------|--------------|------------|--------------|--------------|
| | 2pm to 5pm | 2pm to 5pm | 2pm to 5pm | 2pm to 5pm |
| Team 1 | \checkmark | | \checkmark | |
| Team 2 | \checkmark | | \checkmark | |
| Team 3 | \checkmark | | \checkmark | |
| Team 4 | \checkmark | | \checkmark | |
| Team 5 | | | | \checkmark |
| Team 6 | | | | \checkmark |
| Team 7 | | | | \checkmark |
| Team 8 | | | | \checkmark |

* Please remember to remove all firewall rules after testing them.