2016

Accessible Remote Testbed for Cyber-Physical Systems Security of the Smart Grid

Sujatha Krishnaswamy
Iowa State University

Accessible remote testbed for cyber-physical systems security of the smart grid

by

Sujatha Krishnaswamy

A thesis submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Major: Computer Engineering

Program of Study Committee:

Manimaran Govindarasu, Major Professor

Doug Jacobson

Venkataramana Ajjarapu

Iowa State University

Ames, Iowa

2016

DEDICATION

Dedicated to my beloved mother (Mrs. Rajalakshmi Subramanian), grandfather (Mr. Subramanian Iyer) and grandmother (Mrs. Saraswathi Subramanian) …

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENTS

I would like to express my sincere thanks to Dr. Manimaran Govindarasu and Aditya Ashok for their guidance and support throughout the course of this research. I would like to thank my committee members, Dr. Doug Jacobson and Dr. Venkataramana Ajjarapu for consenting to be a part of Program of Study committee.

In addition, I would also like to thank my colleagues, the department faculty and staff for making my time at Iowa State University a wonderful experience. I want to also offer my appreciation to those who were willing to participate in my surveys and observations, without whom, this thesis would not have been complete.

ABSTRACT

With growing concerns for cyber security of critical infrastructures like the power grid, Cyber-Physical Systems (CPS) security testbeds are essential in providing controlled testing environments for evaluating and validating novel CPS security tools and technologies, thereby accelerating the transition of research to industrial practice. The engineering of such testbeds requires significant investments in money, time and modeling efforts to provide a scalable, high-fidelity, realistic attack/defense platform. Therefore, there is a strong need in research community, academia and industry to create remotely accessible testbeds that enable access to a broader user community through frameworks that support a range of use-cases such as vulnerability assessments, impact analysis, product testing, attack-defense exercises, and operator training. This thesis will focus on remote access framework that has been implemented on PowerCyber - CPS security testbed for Smart Grid at Iowa State University.

Firstly, this thesis introduces the motivation for enabling remote access on PowerCyber by reviewing state-of-the-art work in the area along with engineering challenges. Secondly, the thesis elaborates on fundamental building blocks that enable remote experimentation, such as the front-end user interface, backend experiment automation and also describes the architecture, overall design flow and story-board constructs of the remote access framework. Thirdly, the thesis describes a case study of coordinated cyber-attack/defense experimentation on a wide-area power system protection scheme called Remedial Action Scheme using PowerCyber remote access framework. Details of how the remote access framework facilitated diverse user community engagement is included with survey results, use-case studies and user feedback. Finally, the thesis concludes by identifying future work to broaden the scope and features of PowerCyber remote access framework developed.

CHAPTER 1

INTRODUCTION

1.1 Smart Grid – A Cyber-Physical System

Cyber-Physical systems(CPS) are smart systems that consist of computational and physical components that are seamlessly integrated through highly networked communications. These components involve a high degree of complexity at numerous spatial and temporal scales which closely interact to sense the changing state of the real world [6]. Cyber-Physical systems provide the foundation of critical infrastructures such as electric power generation and delivery, personalized health care, emergency response, traffic flow management, etc. These systems form the basis of emerging and future smart services, and improve quality of life in many existing areas as well as many other areas being envisioned. Popular CPS technologies include: Smart Grid, Smart Cities, Internet of Things (IoT), Industrial Internet, etc. [24]

An increasing demand for reliable energy and numerous technological advancements motivated the development of smarter electric grids. The smart grid is an automated, widely distributed, cyber-physical energy production and delivery system integrated with communications and information technology, characterized by two-way flow of electricity and information [7, 25]. Smart grid modernization initiative involves deployment of a variety of individual technical initiatives such as Advanced Metering Infrastructure (AMI), Distribution Automation (DA), Demand Response (DR), Wide-Area Monitoring, Protection and Control systems (WAMPAC) based on Phasor Measurement Units (PMU), large scale renewable integration in the form of Wind and Solar generation, and Plug-in Hybrid Electric Vehicles (PHEV). Of these initiatives, AMI and WAMPAC depend heavily on the cyber infrastructure as data is transported through several communication protocols to utility control centers and the consumers [26]. The remainder of this section will provide an overview of AMI which is associated with the distribution system, and WAMPAC which is associated with the bulk power system.

Advanced Metering Infrastructure (AMI)

AMI is an integrated system of smart meters, communication networks and data management systems (DMS) that enables two-way communication between the utility and the customers. The main goal of AMI is enhancing reliability of electricity generation and distribution while maintaining cost effectiveness. AMI's are used by utilities to collect current usage information, perform remote meter readings, send real-time pricing data to consumers, detect outages remotely, offer prepaid options to customers and analyze faults within the distribution system. On the other hand, smart meters provide the customers with granular control over their consumption and also facilitate increased integration of Distributed Energy Resources (DER). Demand Side Management (DSM) enabled by AMI exercises direct/indirect control over consumer power consumption [26, 27].

Wide-Area Monitoring, Protection and Control (WAMPAC)

Wide Area Monitoring, Protection and Control systems (WAMPAC) are used to accurately analyze the flow of electricity through bulk power system. WAMPAC leverages the Phasor Measurements Units (PMUs) which provides high sampling rates and accurate GPS-based timing to gain real-time awareness of current grid operations and provide real-time protection and control functions such as Special Protection Schemes (SPS) and Automatic Generation Control (AGC). These are also used by other emerging applications such as oscillation detection, and transient stability predictions. WAMPAC can be subdivided further into its constituent components namely, Wide-Area Monitoring Systems (WAMS), Wide-Area Protection Systems (WAP), and Wide-Area Control Systems (WAC) [26, 27].

- **Wide-Area Monitoring Systems**

  The full potential of PMU data cannot be realized without sharing readings. WAMS provide monitoring techniques by utilizing PMU measurement data that are shared among utilities and other regulators. NASPInet (North American Synchro-Phasor Initiative Network) serves as an example of WAMS deployment, where a separate network was developed for the transmission and sharing of real-time control data [26, 27].

- **Wide-Area Protection**

  Wide-Area Protection (WAP) prevents propagation of larger disturbances by collecting system wide information over a wide geographic area to perform fast decision-making and switching actions. One of the most common Wide-Area Protection scheme is Special Protection Schemes (SPS) which is an automation system designed to detect system abnormalities, take corrective actions such as isolating faulted components and maintaining system reliability [28].

- **Wide-Area Control**

  Automatic Generation Control (AGC) is a major Wide-Area Control mechanism in the power grid which corrects system generation with respect to load changes to maintain grid frequency at 60 Hz. The AGC functions with the help of tie line flow measurements, frequency and generation data obtained from Supervisory Control and Data Acquisition (SCADA) infrastructure. Other WAC applications such as secondary voltage control, static VAR compensator, inter-area oscillation which use PMU data are still in their nascent stages [26].

1.2 Smart Grid Cyber Threats

As the electric grid evolves into a Smart Grid to provide a reliable, secure and resilient electricity transmission and distribution system, the dependence on cutting edge automation and networking technologies has increased tremendously. The advent of high accuracy, time synchronized, high data rate synchrophasor measurements and other modern substation automation systems over the grid, which are deployed to monitor, control and protect the power grid, have resulted in increased network connectivity to corporate IT networks. These connections were often created without an understanding of the potential consequences and thereby, have increased the attack surface of the system. Though attacks targeted at these systems are not frequent, their physical, economic and social impacts can be quite severe if successful [8, 11]. Several authoritative government reports and technical literature have documented increasing concerns for highly sophisticated, advanced persistent cyber threats on critical infrastructures, especially the power grid.

- McAfee study on “Critical Infrastructure in the age of Cyber War” [1] highlights that Critical infrastructure owners and operators have reported that their networks and control systems are under repeated cyberattack, often from high level adversaries like foreign nation-states. Assaults run the gamut from massive DDoS attacks designed to shut down systems all the way to stealthy efforts to enter networks undetected.
- “W32. Stuxnet Dossier” released by Symantec Security Response [2], describes Stuxnet as a malware primarily written to target industrial control systems (ICS) which are used in power plants and gas pipelines. End goal of Stuxnet was to reprogram industrial control systems (ICS) by modifying code on programmable logic controllers (PLCs) to make them work in a manner the attacker intended and to hide those changes from the operator of the equipment.

- On December 23, 2015 a regional Ukrainian electricity distribution company reported service outages to customers due to a third party's illegal entry into the company's computer and SCADA systems. This cyberattack disconnected seven 110 kv and twenty-three 35 kv substations for three hours, impacted additional portions of the distribution grid and forced operators to switch to manual mode. The attack resulted in outages that caused approximately 225,000 customers to lose power across various areas [31].
- A jointly commissioned summary report of the North American Electric Reliability Corporation and the U.S. Department of Energy [3], focuses on High-impact, Low-Frequency (HILF) events such as pandemic illness, coordinated cyber, physical, or blended attack on the system, extreme solar weather, and the high-altitude detonation of a nuclear weapon with the potential to cause long-term, catastrophic damage to the bulk power system.
- U.S. Government Accountability Office (GAO) assessment [4, 5] addresses key cybersecurity requirements in each Critical Infrastructure Protection (CIP) sectors, cybersecurity technologies which can be applied to CIP and implementation issues associated with using cybersecurity technologies for CIP, including policy issues such as privacy and information sharing.
- National Institute of Standards and Technology (NIST) released a "Guide to Industrial Control Systems (ICS) Security" [29] which identifies adversarial threats to ICS to emphasize the necessity to create a defense in depth strategy for the ICS.

Thus there is a growing need in academia, industry and research community to develop and validate novel security tools and algorithms for securing the smart grid and making it attack-resilient.

1.3 CPS Security Testbeds

Attempts to research smart grid cyber security enhancements are constrained by the availability of realistic cyber-physical environments. Testbeds that integrate both cyber and physical components provide ideal environments to perform and evaluate research efforts [9]. Cyber-Physical Systems (CPS) security testbeds provide controlled testing environments for realistic, attack/defense experimentation and also serve as a platform for evaluating and validating novel CPS security tools and technologies, thereby accelerating the transition of state-of-the-art research to industrial practice. CPS security testbeds capture computation, communication and physical system dynamics appropriately through a combination of simulated, emulated and physical system components respectively. In the past decade, several educational institutions and national labs have been developing CPS security testbeds for validating and evaluating the various cyber security tools and technologies, and also to provide realistic test environments for attack/defense experimentation. In this section, few prominent CPS security testbeds are identified along with a brief discussion of the use-cases they support and their capabilities to enable remote experimentation.

1.3.1 DETER Testbed

The DETER testbed at University of Southern California's Information Sciences Institute, is a large-scale testbed for cyber security experimentation [16]. DETER is a multi-user testbed that provides remote users the tools to create custom experiments by provisioning appropriate computing resources such as virtual machines on the dedicated server clusters. Users can configure their experiments by choosing from a set of available computing nodes, and by specifying network topologies to interconnect these nodes. DETER also provides automated scripting features to orchestrate complex experiments, however, it lacks CPS resources, specific to the power grid such as Supervisory Control and Data Acquisition (SCADA) software, Remote Terminal Units (RTU), relays and phasor measurement units, to perform hardware-in-the-loop experimentation in conjunction with its computing resources.

1.3.2 powerNET Testbed

The powerNET testbed at Pacific Northwest National Laboratory is an ongoing research effort that goes beyond the capabilities of the DETER testbed to provide a multi-user, remotely configurable testbed environment for research on multiple areas including CPS security experimentation [17]. The powerNET testbed leverages emerging open source cloud computing platforms such as OpenStack, in conjunction with its Industrial Control Systems hardware such as relays, PMUs, real-time power system simulator, and the associated SCADA software such as Energy Management Systems, to enable hardware-in-the-loop cyber security experimentation. However, the testbed has not yet been made available to the research community as some of its features are under development.

1.3.3 National SCADA Testbed (NSTB)

The National SCADA Testbed (NSTB) at Idaho National Laboratory (INL) is a collaborative research effort by several Department of Energy National labs across the U.S to create a CPS security testbed for the Smart Grid. The NSTB consists of physical and cyber system resources to perform vulnerability assessments and impact analysis studies [18]. Though the NSTB was utilized to perform vulnerability assessments, product testing, and red team - blue team training exercises, open, remote access to the testbed resources was not one of the project's priorities.

1.3.4 WSU Smart Grid Testbed

Washington State University(WSU) includes two currently interconnected testbeds, the Smart City Testbed and Smart Grid Demonstration Research Investigation Laboratory (SGDRIL). The testbeds are designed to perform detailed Cyber-Physical System simulations and to evaluate smart grid cybersecurity technologies within realistic environments. The testbeds span both transmission and distribution domains, included control system software, various embedded control devices, and real-time simulation capabilities [23].

1.3.5 NREL (National Renewable Energy Laboratory) Smart Grid Testbed

NREL’s Secure Distribution Grid Management (DGM) testbed runs DGM use cases using a combination of virtual grid and real power systems assets to evaluate critical cybersecurity vulnerabilities and the effectiveness of risk mitigations through sound network design, stringent security controls through firewalls, access control lists on network switches and cutting edge cybersecurity technologies [30]. One of the key areas of focus in the testbed is the integration of Information Technologies (IT) and Operations Technologies (OT) side of a typical distribution utility. It is a major effort for utilities to integrate these two areas to support cross-cutting Smart Grid applications while maintaining a strong cybersecurity posture.

1.3.6 ISU PowerCyber Testbed

The Cyber-Physical Power Grid Testbed, ***PowerCyber,*** is a hardware-in-the-loop hybrid test platform (real, simulation, and emulation) [9]. The SCADA portion of the testbed composed of industry-grade hardware/software from Siemens that include substation automation system (SICAM PAS), control center software (Power TG), SCADA and substation communication protocols (DNP, IEC 61850), and security technologies (Scalance: Firewall, VPN), and multifunction protection relays (7SJ610, 7SJ82). The testbed also has been integrated with three SEL 421 PMUs and Phasor Data Concentrator (PDC). **ISERink** is a virtual environment for cyber defense competitions, and attack-defense evaluations.

1.3.7 Other CPS Security Testbeds

Several other notable CPS security testbeds have been developed in the recent years, such as the Virtual Control System Environment testbed at Sandia National Laboratory [19], Virtual Power System Testbed at the University of Illinois at Urbana-Champaign [20], SCADA security testbed at Mississippi State University [21] and SCADA testbed at University College, Dublin [22]. These CPS security testbeds have been used to perform vulnerability assessments on SCADA devices communication protocols, and software, impact analysis for realistic cyber-attack scenarios, and developing defense measures such as anomaly/intrusion detection, besides several other related topics.

1.3.8 Comparison of Testbed capabilities

✓ - Existing Capabilities ☑ - Capabilities enabled by this thesis work

Table 1.1 *Testbed capability comparison*

Capabilities/Resources	**ISU Testbed**	**WSU Testbed**	**NREL Testbed**	**DETER Testbed**
Diversity of ICS Devices (Substation Automation, RTUs, Relays, PMUs)	✓	✓	✓	
Diversity of ICS Protocols (ICCP, DNP3, Modbus, IEC 61850, IEEE C37.118)	✓	✓	✓	
Cyber Systems (SCADA EMS, DMS)	✓	✓	✓	
Physical Systems (Real-time Simulation)	✓	✓	✓	
Advanced Networking (Stub Intranet, Internet connections)	✓			✓
Federation of Resources	✓			✓
Cyber System Virtualization	✓	✓		✓

✓ - Existing Capabilities ☑ - Capabilities enabled by this thesis work

Table 1.1 *(continued)*

Virtualization of ICS Devices				
Experiment Orchestration	☑			✓
Remote Accessibility and Configuration	☑			✓
Multi-user Support				✓
Cyber Security Toolsets & Devices			✓	✓
Sandboxing of ICS devices				
Support for Performance Evaluation	✓	✓	✓	✓
Cyber Defense Exercises	✓			✓

1.4 Thesis Motivation

Development process of CPS Security Testbeds is not well established due to the complexity of integrating cyber and physical resources while also incorporating simulation mechanisms to model power systems, cyber network dynamics, and security events [9]. The engineering of CPS security testbeds requires significant investments in time, money and modeling efforts to provide a scalable, high-fidelity, real-time attack/defense platform. Therefore, there is a strong need in the research community to create remotely accessible CPS security testbeds that enable access to a broader user community through open, remote access frameworks that support a range of use-cases pertaining to CPS security of the grid, including vulnerability assessments, impact analysis, product testing, attack-defense exercises, and operator training. From the literature survey it is clearly evident that remote access to a broad user community has not been addressed in any of the testbed efforts except DETER which lacks CPS resources. Thus there is an immediate need to develop remotely accessible CPS Security Testbeds for the benefit of research, academia and industry. However, the engineering of a scalable, flexible, multi-user, remote access testbed for CPS security experimentation has a broad spectrum of challenges. The reminder of this section identifies such challenges and wherever possible, potential solutions to overcome some of the challenges are identified and discussed.

- **Scalability**

One of the most critical challenges in creating a scalable remote access is scalability. As we increase the scale of the power system model, the associated cyber system model increases. This translates to increased resource requirements for performing real-time simulations with hardware-in-the-loop experimentation. Therefore, power system scalability would be limited to the maximum system size that the power system simulator can support for a real-time simulation. Scalability in cyber system VM's could be easily overcome with deploying additional computing resources such as server racks, however, increasing power system simulation capabilities at the same level is prohibitively expensive. To some extent, this could be handled by abstracting and equivalencing parts of the system model that are not directly involved in the experiment. This also would help to minimize the amount of physical hardware devices that need to be mapped into the real-time simulation. Though scalability for physical components like relays and PMU's are also comes at a price, to some extent we can get around device scalability with relay emulators, which replicate the entire communication behaviors that are essential to cyber security experimentation.

- **Concurrency and Isolation**

One of the main differences between the implementation of a remote access framework for a CPS security testbed vs. a regular cyber security testbed setup like DETER would be the problem of concurrent, multi-user experiments. There exist several options to virtualize and compartmentalize computing resources like VM's to provide isolation, security for multiple-concurrent users. However, the problem of sharing expensive, limited physical components such as relays, PMU's, and real-time power system simulators between multiple concurrent users is much more complicated and requires additional research and development effort.

- **Flexibility**

Extending the discussion on concurrency, the flexibility of a CPS security testbed is much lesser when compared to a traditional cyber security testbed. Specifically, the configuration of physical components such as relays and PMU's need to be changed dynamically based on user inputs for different types of experiments. Some of the software that are used to program these devices are based on a graphical user interface and therefore are not very amenable to automated scripting. While there are command line tools that automate mouse clicks on GUI, this approach is not very flexible and suitable for a wide range of scenarios.

- **Troubleshooting**

Troubleshooting remote, automated experiments when things don't work as expected presents tough challenges on any type of testbed. Especially, in CPS environments, with SCADA devices, and communication protocols, this challenge is even harder to overcome due to inherent design weaknesses in terms of security, and the heterogeneity of devices. Typically, SCADA devices have been built with usability, reliability as a preference over security. This leads to unexpected failure modes in devices during cyber-attack/defense experimentation. Consequently, failures are hard to debug in an automated manner. Therefore, it is extremely important to test all scenarios thoroughly for possible failure modes manually before completely automating them. Also, due to these limitations, the remote access provided to users would be mostly driven by a template-based experiment model, rather than allowing complete customization of the experiments.

1.5 Thesis Organization

The main contribution of this thesis is enabling remote accessibility, configuration and experiment orchestration on PowerCyber testbed by implementing remote access framework. This thesis is structured as follows

- **Chapter 2** introduces PowerCyber testbed with architecture details and use cases. The chapter explains the implementation details of remote access framework with architecture and design flow.
- **Chapter 3** discusses remote access framework story board constructs with details of how the remote access framework was used to perform a coordinated attack/defense experiment case study on wide-area protection scheme with step-by-step screenshots and explanation.
- **Chapter 4** explains details of academic and industrial user community engagement with use case studies evaluating the remote access framework.
- **Chapter 5** concludes the thesis by identifying future work in this direction to broaden the scope and features of PowerCyber remote access framework.

CHAPTER 2

PowerCyber - REMOTE ACCESS FRAMEWORK

2.1PowerCyber: Testbed Overview

The PowerCyber testbed at Iowa State University, consists of a hybrid mix of industry standard hardware and software, emulated components and real-time power system simulators for hardware-in-the-loop CPS security experimentation for the Smart Grid. The PowerCyber test-bed provides a virtual critical infrastructure environment wherein realistic experiments on wide area monitoring, wide area control and distributed decision making in the smart grid environment can be carried out.

2.1.1 PowerCyber Testbed Architecture

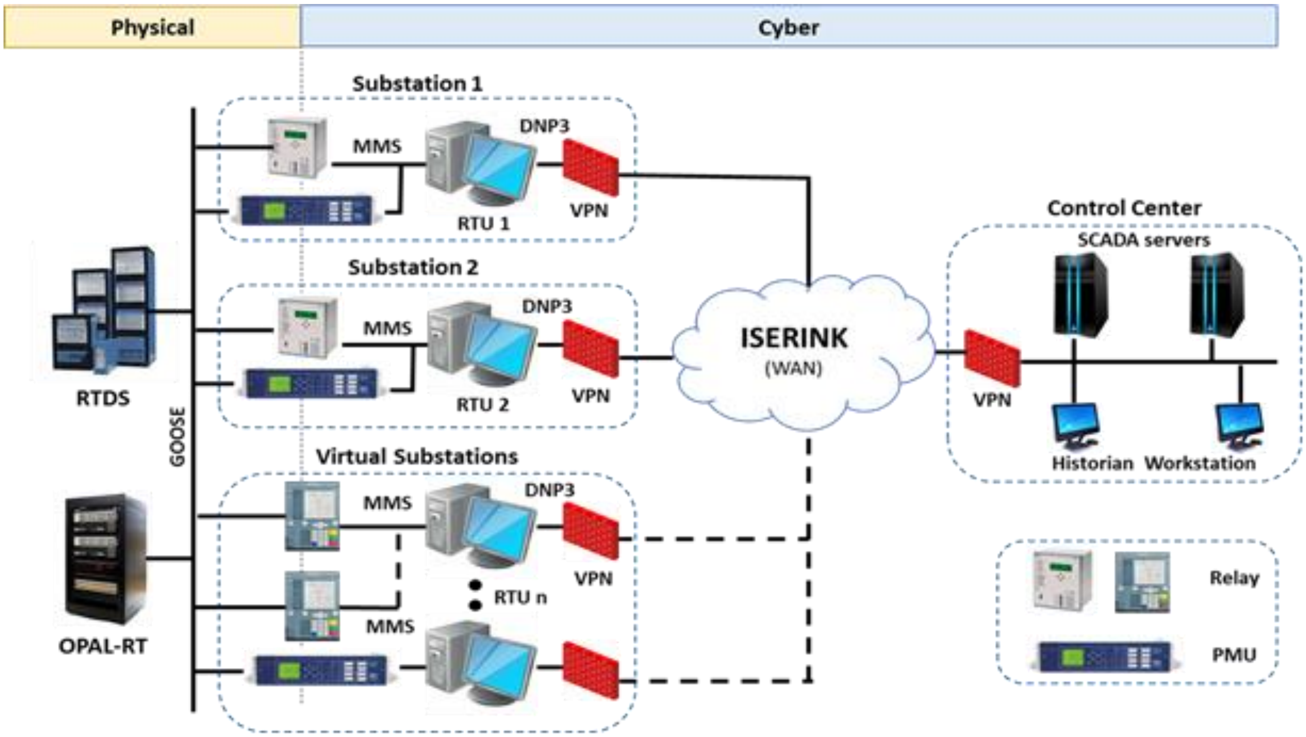


Figure 2.1 *PowerCyber CPS Security Testbed Architecture*

Figure 2.1 shows the current architecture of the PowerCyber CPS Security testbed at ISU. The testbed consists of SCADA hardware/software with emulation and simulation techniques that include substation automation system (SICAM PAS), control center software (Power TG), SCADA and substation communication protocols (DNP3, IEC 61850, IEEE C37.118), and security technologies (Scalance: Firewall, VPN), four multifunction protection relays (7SJ610, 7SJ82), three SEL 421 Phasor Measurement Units (PMU) and a Phasor Data Concentrator (PDC) to provide an accurate electric grid cyber infrastructure. The testbed employs virtualization technologies to address scalability concerns and reduce development cost. The testbed has also been integrated with the Internet Scale Event and Attack Generation Environment (ISEAGE) project at Iowa State to provide wide-area network emulation and advanced attack simulation. Power simulations are performed using Real Time Digital Simulator (RTDS), Opal-RT for real time evaluations and DIgSILIENT PowerFactory software for non-real time analysis [9].

2.1.2 PowerCyber Supported Use Cases

PowerCyber has been leveraged to support the following types of use cases that are relevant to cyber physical security experimentation for the grid.

2.1.2.1 Vulnerability Assessment

PowerCyber supports vulnerability assessment of industry grade SCADA software and hardware platforms, network protocols and configurations to detect unknown vulnerabilities based on standard vulnerability databases. Several unknown vulnerabilities were discovered and a responsible disclosure process was followed to disclose them to vendors and appropriate regulatory authorities [10].

2.1.2.2 Impact Analysis and Mitigation Research

PowerCyber provides a realistic virtual critical infrastructure environment wherein realistic experiments on wide-area monitoring, protection, and control in the smart grid environment can be carried out. Specifically, the testbed has been used to evaluate coordinated attacks on Remedial Action Schemes [9], and data integrity attacks on automatic generation control [11]. Also, the testbed allows the implementation of defense measures such as firewalls, intrusion detection systems, software patches, etc., to also evaluate the performance of various mitigation strategies.

2.1.2.3 Testbed Federation

Recently, the PowerCyber testbed was successfully federated with the DETER testbed and the ISERINK platform, as part of Smart America Challenge and NIST Global City Teams Challenge to create a large-scale, high-fidelity CPS security testbed environment. The federated testbed was used to demonstrate proof-of-concept attack/defense experimentation on a wide-area protection scheme [12, 13]. Additional use cases to showcase the utility of CPS testbed federation are currently being explored.

2.1.2.4 Attack-Defense Exercises & Operator training

The PowerCyber testbed and the ISERINK platform for cyber defense competitions [14] had been recently integrated to conduct realistic cyber-attack/defense training exercises for utility practitioners at the NERC GridSecCon 2015 conference [15]. Also, PowerCyber has been used every year as part of an industry workshop to provide hands-on training sessions.

2.1.2.5 Model Development

PowerCyber testbed is currently developing a repository of standardized models and experimental datasets for power systems and associated cyber systems to facilitate researchers in leveraging the testbed capabilities for cyber security experimentation.

2.1.2.6 Remote Access

In order to engage and enable a broad user community to perform a variety of power grid related cyber security experimentation, a remote access framework has been developed on the PowerCyber testbed.

2.2 Remote Access Framework

The remote access framework interacts with the remote users via a Front-end Web server, which provides a web-based user interface that allows users to configure the relevant parameters needed for the automated attack/defense experimentation. The front-end web server is integrated tightly to a backend orchestration framework, which is written in Python. The backend framework orchestrates the creation/configuration of the necessary cyber resources such as the SCADA virtual machines, manages the interaction with the power system simulators and physical devices such as the relays and PMUs, coordinates various attack actions and defense measures depending on the user input, and also provides a way for the users to collect relevant simulation artifacts from the cyber system and the physical system in the form of log files, packet captures, plots, etc., Figure 2.2 shows the overall framework for enabling remote CPS security experimentation.

The Real-Time Grid Simulation module performs actions such as model compilation, loading, and execution on a real-time power system simulator and appropriately maps components such as relays and PMUs on the power system model based on user selection. The SCADA configuration module spawns SCADA virtual machines such as the control center VM's that house the Energy Management Systems (EMS) software, substation RTU VM's, and connects these VM's according to user specified communication topology. The module also appropriately initializes SCADA communications between the various devices and verifies communications between the SCADA VM's and the hardware devices that are mapped into the experiment. Based on the user's selection, the attack orchestration module coordinates and triggers attack actions on appropriate SCADA components. The attack module spawns attacker virtual machines once all the initializations have been performed appropriately. The attack script includes user selected attack actions from the attack template library.

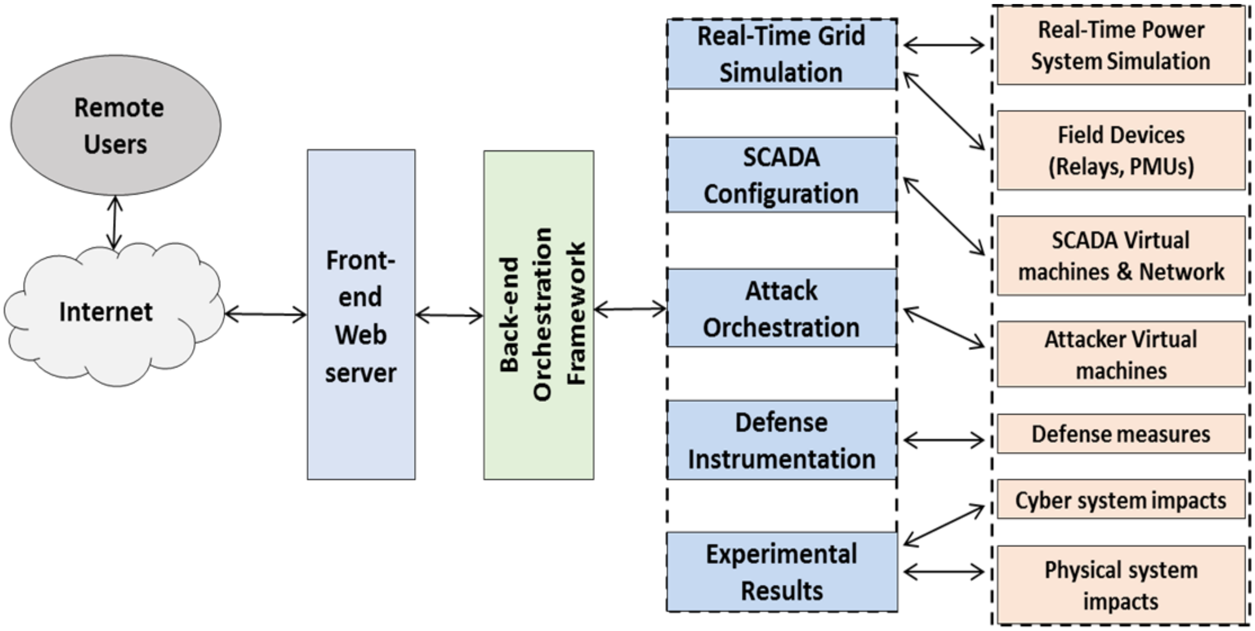


Figure 2.2 *Remote Access Framework*

The defense instrumentation module implements host based or network based mitigation mechanisms such as firewall rules, and intrusion/anomaly detection systems appropriately based on user input. Depending on the experimental scenario chosen by the user, appropriate inputs are obtained for the scenario with respect to the power system model, hardware device mapping, communication network topologies, attack parameters and defense parameters. This allows the users to run their own experiments within the limitations of the template experimental scenarios that are provided as initial inputs. As the capabilities of the remote access framework mature, more flexibility would be available to the users to select their own experimental scenarios by using custom power system models, relay/ PMU configurations, attack vectors, and defense mechanisms such as anomaly/intrusion detection algorithms. The following sections present a detailed description of the implementation methodology of the remote access framework.

2.2.1 Implementation Architecture

Figure 2.3 shows the implementation architecture of the PowerCyber remote access framework that was described earlier. The architecture describes remotely accessible PowerCyber testbed that consists of several interconnected VM's (SCADA, power system control, attack, defense, gateway), power system simulators, and physical devices such as relays and PMU's for performing hardware-in-the-loop experimentation.

The implementation architecture of the remote access CPS security testbed consists of three fundamental building blocks.

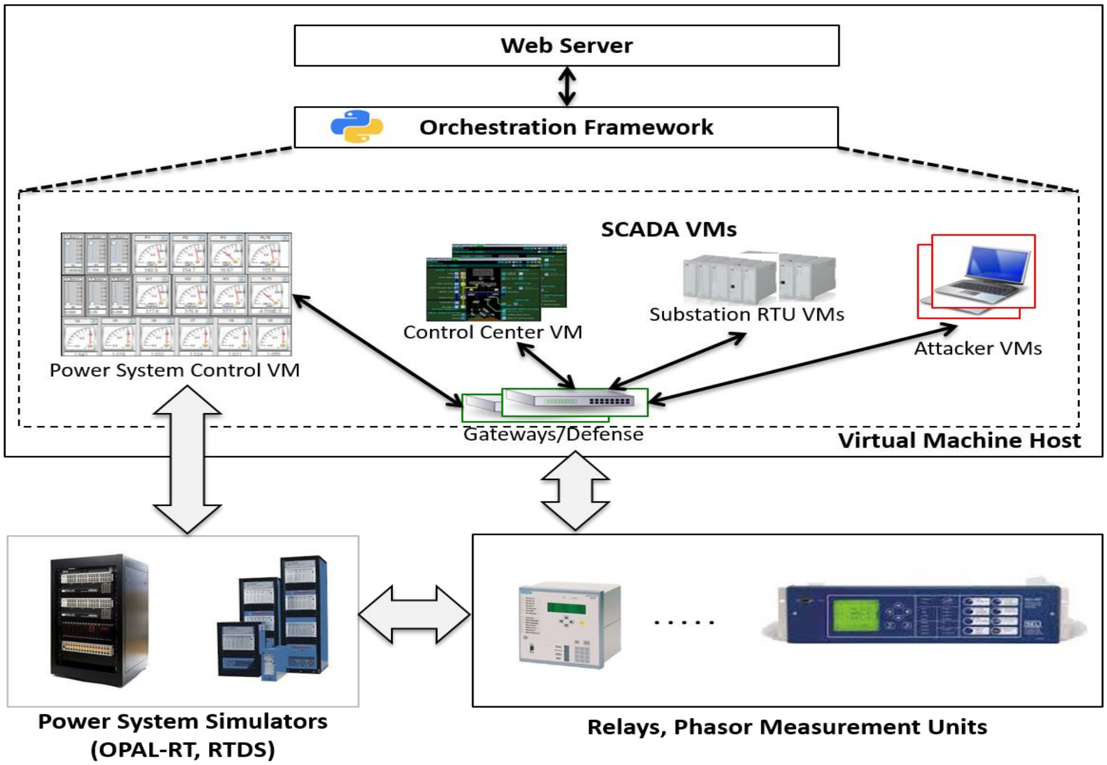


Figure 2.3 *Remote Access Framework – Implementation Architecture*

2.2.1.1 Front-end Web Server

The front-end web server interacts with the user through a web-based user interface. It provides options to select and customize experimental scenarios and also provides options to collect experimental results.

2.2.1.2 Backend Orchestration Framework

The back-end orchestration framework performs various tasks to automate the experimental scenario chosen, and interacts with the front-end web server to collect inputs and provide experimental results.

2.2.1.3 Models and Libraries

In order to provide standard experimental scenarios as part of the remote access web interface a library of commonly used power system models need to be developed. This includes models with appropriate WAMPAC applications modeled, commonly used attack vectors, defense measures, etc.,

The front-end web server and backend orchestration framework are hosted inside a virtual machine host, and would spawn the various virtual machines that are required as part of the experiment in the ESXi server. The front-end web server pushes user inputs as parameters to the backend orchestration framework, which is scripted using Python. The master backend script triggers multiple slave scripts which perform different functions along different stages in the design flow of the remote experimentation. The SCADA configuration script spawns control center VM and substation VM's depending on the experiment. The SCADA VM's are configured in a user specified network topology using virtual switches and gateways. Also, the backend scripts ensure that the virtual machines communicate with physical relays and PMU's that would be mapped into the experiment through the appropriate power system model. The power system simulation automation script spawns a power system control node VM, which interacts with the Power System Simulators such as OPAL-RT, RTDS. This script provides the capability to compile/load a power system model on the simulator and allows interaction with the model to perform run-time control actions either through script or GUI and also view real-time power system impacts or obtain results in the form of data files or plots respectively. The defense script configures network based defense measures such as firewall rules or intrusion detection system rules on the virtual gateway, and/or host based defense measures on user specified components in the SCADA VM's. The attack script spawns attacker virtual machines, which would be triggered by the master script once all the initializations have been performed appropriately. The attack script includes user selected attack actions from the attack template library. Once the experiments are performed, the master script can pull cyber system artifacts such as firewall and intrusion detection log files, network packet captures, network performance statistics, etc., from the various SCADA VM's and the gateway/defense nodes. Also, as mentioned previously, the master script interacts with the power system control scripts to pull relevant physical system simulation artifacts.

2.2.2 Design Flow

The following list represents key steps in the overall design flow for performing automated, cyber-attack/defense experimentation:

- **Power system configuration**

  The first stage involves the selection of the power system model to be used for the experiment. For example, the standard IEEE system models such as 39 bus, 118 bus, etc.,

- **WAMPAC experiment selection**

  Once the power system model has been selected, the next stage is to identify the Wide-Area Monitoring, Protection and Control (WAMPAC) experiment that is to be used for the experiment.

This stage would also involve an identification of how the physical components are mapped to the power system model.

- **Cyber system configuration**

This stage involves actions to appropriately spawn SCADA VM's such as Control Center, Substation VM's depending on the WAMPAC experimental scenario chosen, and ensuring that the appropriate network topology is setup between the various VM's and the hardware devices that are mapped as part of the scenario.

- **Defense configuration**

After the power system and cyber system configuration steps are performed, the next stage involves actions to spawn defense measures. The defense measures could be setup either in the communication gateway nodes or on the individual hosts depending on the experimental scenarios and user inputs.

- **Attack Configuration**

Once all the systems are configured and initialized, the next stage is to spawn the attacker VM's and execute the attack vector on specified targets in coordination with the backend orchestration framework.

- **Collecting Cyber System Results**

After the execution of the specified attack scenario, the next stage involves the collection of experimental artifacts on the cyber layer such as log files, packet captures, network performance metrics from the various systems.

- **Collecting Physical System Results**

The last stage involves the collection of power system simulation artifacts in the form of datasets, or plots of system states such as voltages, power flow and frequency.

The following subsections describe in detail the various activities that are performed as part of the overall design flow with respect to user interface (front-end) and experiment automation (back-end).

2.2.2.1 User Interface Design

The user interface provides the user with an array of templates to select from and configure the system to perform a specific type of cyber-attack/ defense experiment. Figure 2.4 shows the various activities with respect to the design flow for remote experimentation pertaining to the user interface. The user interface allows the user to select the power system model that is to be used from a list of choices such as IEEE 39 bus model IEEE 118 bus model, etc., As part of Step 2, the user can select the WAMPAC experimental scenarios to be used. For example, the list of available scenarios could be Remedial Action Schemes, Automatic Generation Control, State Estimation, etc.,

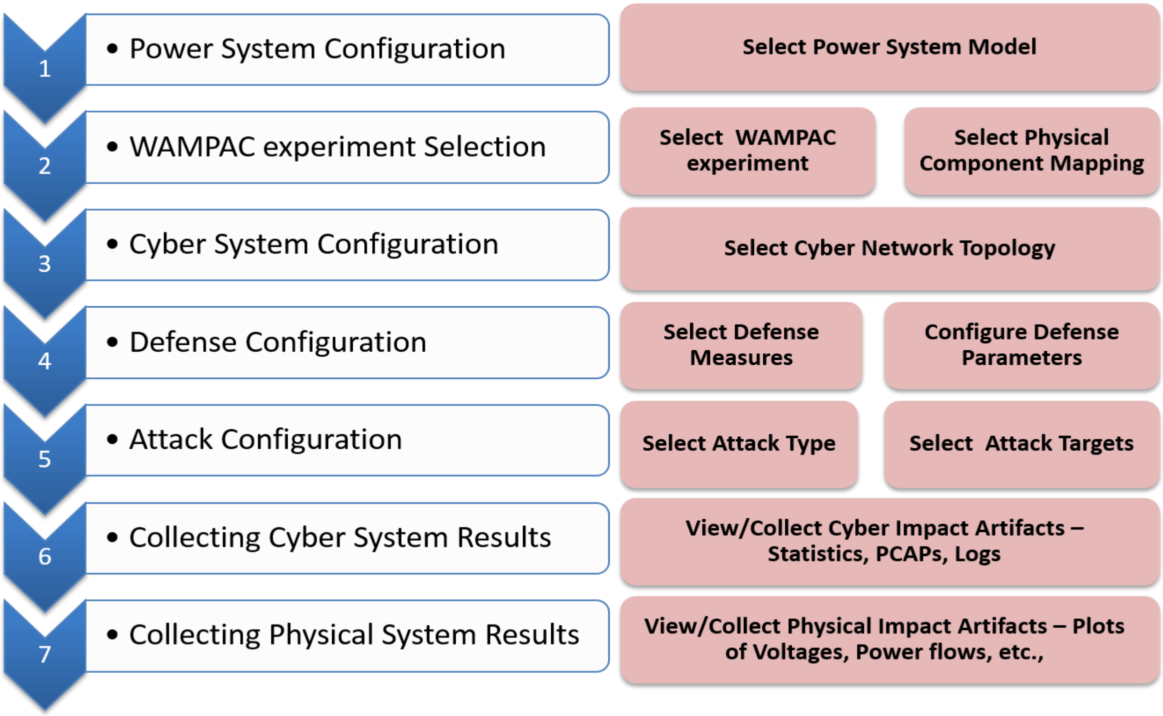

1
• Power System Configuration
Select Power System Model
2
• WAMPAC experiment Selection
Select WAMPAC experiment
Select Physical Component Mapping
3
• Cyber System Configuration
Select Cyber Network Topology
4
• Defense Configuration
Select Defense Measures
Configure Defense Parameters
5
• Attack Configuration
Select Attack Type
Select Attack Targets
6
• Collecting Cyber System Results
View/Collect Cyber Impact Artifacts – Statistics, PCAPs, Logs
7
• Collecting Physical System Results
View/Collect Physical Impact Artifacts – Plots of Voltages, Power flows, etc.,

Figure 2.4 *Design Flow for User Interface*

Each one of these WAMPAC applications correspond to a specific scenario and based on the user input they will be presented with subsequent web pages to select and map physical components such as relays and PMUs appropriately into their experiment, and also it determines the type and number of SCADA VM's needed. For the cyber system configuration, the user interface provides user with options to select the network topology in which SCADA components should be connected.

As part of defense measures, the user can select from either host based defense or network based defense. Based on their inputs, user interface provides options to select from defense methodologies such as firewall, intrusion detection and prevention based defense, etc., for implementation. For orchestrating the attack, the user interface provides a list of attack vectors such as DOS attack, Command injection attack, coordinated attack to choose from, along with options to choose the attack locations on the system selected. The user interface has a visualization component where remote users can observe the status of the physical devices that are part of the attack on the cyber layer, and also simultaneously observe the power system impacts on the real-time power system simulator through real-time simulation plots. Once the experiment has been performed, the user interface facilitates the collection of cyber system impacts such as downloading packet captures, log files etc., during attack phase. As part of power system impacts, the user interface provides the option of data collection relevant to power system parameters such as voltage and power flow plots.

2.2.2.2 Experiment Automation

Figure 2.5 lists the various activities as part of the design flow that relate to experiment automation. Each of the activities are implemented using the backend orchestration framework through appropriate slave scripts that communicate to a master script. With respect to the power system configuration, the automation tasks involve loading, compilation of the appropriate power system model such as the IEEE 9 bus system model simulator, initializing the runtime interface, and ensuring that the model has reached its steady state operating condition before any attack actions are started.

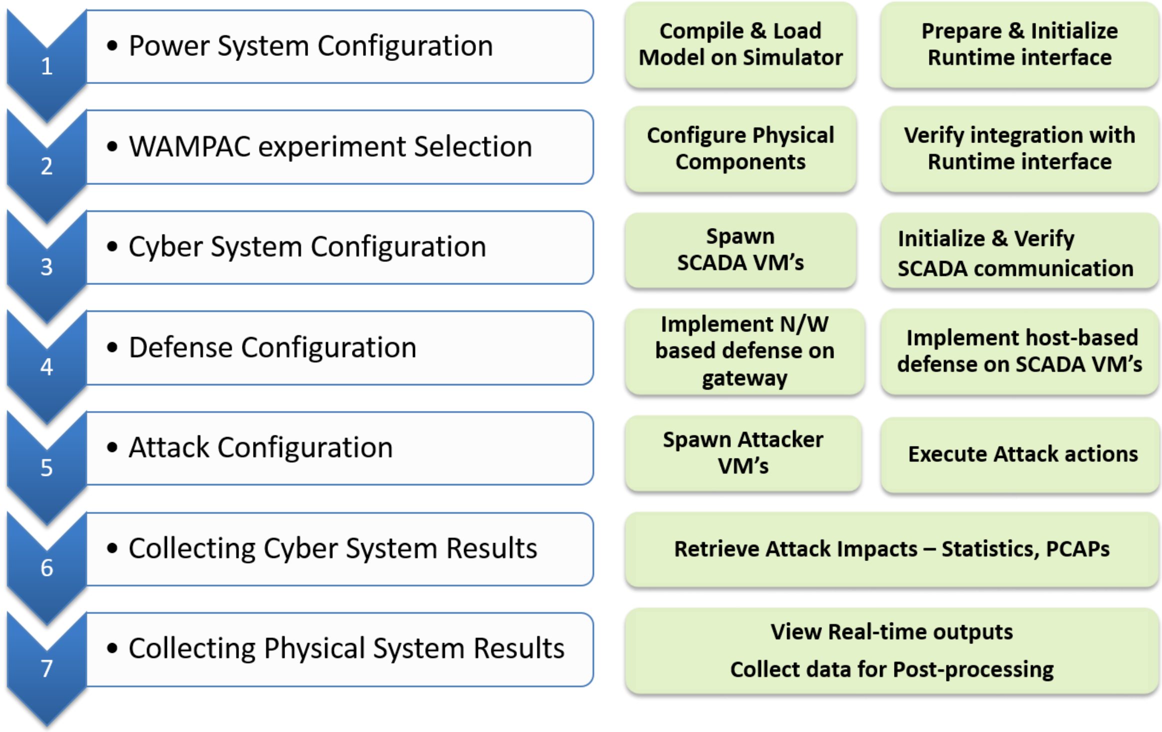

1
• Power System Configuration
Compile & Load Model on Simulator
Prepare & Initialize Runtime interface
2
• WAMPAC experiment Selection
Configure Physical Components
Verify integration with Runtime interface
3
• Cyber System Configuration
Spawn SCADA VM's
Initialize & Verify SCADA communication
4
• Defense Configuration
Implement N/W based defense on gateway
Implement host-based defense on SCADA VM's
5
• Attack Configuration
Spawn Attacker VM's
Execute Attack actions
6
• Collecting Cyber System Results
Retrieve Attack Impacts – Statistics, PCAPs
7
• Collecting Physical System Results
View Real-time outputs
Collect data for Post-processing

Figure 2.5 *Design Flow for Experiment Automation*

Depending on the WAMPAC experiment selection made, the backend automation scripts would configure physical components accordingly so that they could be mapped into the power system model for hardware-in-the-loop experiments, and also verify their integration with the runtime interface. With respect to automating the cyber system, the back-end configuration module spawns control center and substation VM's appropriately, and initializes the VM's in a specific network topology. Also, the scripts verify if inter-device communication is successful before proceeding further. Based on user selection, the backend scripts implement and initialize network based or host based defense measures such as firewalls, or intrusion detection systems on gateway nodes or on the hosts such as substation VM's. As part of attack orchestration, the backend scripts would spawn attacker VM's, which have a library of pre-defined attack modules. Based on the experiment scenario, the master script coordinates and triggers the specific attack scripts on these VM's.

Once the experiment has successfully begun, the backend scripts periodically poll the status of various devices involved in the experiment in the cyber layer, and update a run-time visualization screen on the front-end web server. Simultaneously, the web-based interface can also provide another screen with the run-time interface on the power system control VM to see the impact of the attacks on the power system. Depending on the type of power system simulator selected and the type of outputs requested by the user (i.e. real-time outputs vs. offline plots), the automation scripts would be adapted to provide real-time outputs or data files that are collected for the experimental scenario accordingly. As part of collecting the results on the cyber layer, the back-end scripts would pull log files from the VM's where defense measures were deployed such as firewall and IDS logs, and packet captures from the gateway node, besides other network performance statistics. Similarly, the scripts on the power system control node would pull power system simulation artifacts such as data files or plots and make them available to the user as experimental results.

CHAPTER 3

STORY-BOARDS & CASESTUDY

3.1 Story-Board Constructs

The PowerCyber remote access framework has been implemented using story board based approach. This implementation facilitates ease of use for a versatile community of users with different expertise and also serves as an educational platform that allows users to learn about the importance and criticality of cyber security of critical infrastructures such as smart grid. The remote access framework supports the following story board constructs [32].

3.1.1 Story-Board 1 - Cascading outage through a coordinated attack on power system protection scheme

In this scenario, the attack involves a combination of two coordinated attack actions on a power system protection scheme known as Remedial Action Scheme (RAS). Typically, RAS are intended to take specific protective measures to prevent the spread of large disturbances under heavy system loading conditions. However, the attacker intelligently triggers the operation of this RAS by creating a data integrity attack on unencrypted communication between the substation and the control center that uses the DNP3 protocol. In order to create a cascading outage, the attacker also blocks the communication between the protection relays that are involved in the RAS through a targeted Denial of Service (DoS) attack on one of the protection controllers. This prevents the successful operation of the RAS and in turn initiates secondary protection to be tripped to avoid thermal overload on the impacted transmission line. As a result of this coordinated attack involving data integrity attack to trip a breaker and a DoS attack on RAS communications, the overall system frequency is also affected as it causes the islanding of a generator from the rest of the system.

3.1.2 Story-Board 2 - Manipulating AGC measurements/controls to affect system frequency

In this scenario, the attack involves a stealthy manipulation of measurements/controls used in Automatic Generation Control (AGC) algorithm to destabilize and affect the frequency of the power grid. This attack is a version of the classic Man-in-the-Middle attack, where the attacker intercepts the communication between the control center and the remote substations and chooses to stealthily modify either the frequency or tie-line measurements going to the control center, or the AGC control commands going to the generating stations. This is achieved by executing an ARP poisoning attack first, which tricks the remote substation to forward the data to the attacker before sending it to the external gateway. The attacker then selects the appropriate information that is to be replaced and modifies it appropriately using custom attack scripts and forwards it to the external gateway. As a result of this manipulation, there is a steady frequency deviation in the system. Eventually, this frequency deviation causes the load in the system to be shed in an attempt to restore frequency. A sustained attack could potentially lead to a major portion of the load in the power system to be unserved.

3.1.3 Story-Board 3 - Manipulating SCADA measurements to affect situational awareness in State Estimator

In this scenario, the attack involves a careful manipulation of the measurements (analog and status) that come from the substation remote terminal units (RTU) to the control center for State Estimation. 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 forward all its data to the attacker's 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’s Bad Data Detectors. This does not cause any bad data alarms in the control center and consequently, the attacker succeeds in impeding the situational awareness capabilities of the operator. Consequently, all applications that rely on State Estimator would be affected such as Contingency Analysis, Power Markets, etc., Also, this attack could be used to further trigger other attacks that could cause additional damage such as opening/overloading critical transmission lines.

3.1.4 Story-Board 4 - Using unencrypted RTU communication to send arbitrary commands to trip breakers

The attacker gains physical access to the process WAN, on which he is able to gain a network address. As the data flows between RTUs and SCADA are not encrypted the attacker is able to read any transmitted data in clear text. The attacker uses this opportunity to perform an ARP spoof attack and position himself between an RTU and the PCU (i.e., a man-in-the-middle attack). As such, the attacker is able to both send malicious requests to the RTU and hide to the operator the real events. The attacker uses this for an unauthorized opening of a distribution feeder breaker feeding a major manufacturing industry connected directly on the 40 kv level. The attacker’s intention is to create a power outage that will severely disturb or stop the production in a continuously operated plant in order to create economical and/or physical damage.

3.1.5 Story-Board 5 - Denial of Service attack on RTU/protection devices communication to blind SCADA

The attacker has physical access to the RTU communication network and is as such able to connect his own equipment to the network using a switch in an unmanned substation. From this point the attacker floods a number of logical connections with a continuous stream of packets, which creates an overload in the Front-End applications and blinds the operators to what is happening in the grid. The attacker has chosen a time for the attack when a severe snow and ice storm is expected and the control operators are unable to counteract the loss of physical devices created by the storm. This leads to an overload of power lines feeding the capital city and this also goes unnoticed in the control center. The blind SCADA severely delays the power restoration efforts to reenergize the capital city.

3.1.6 Story-Board 6 - Exploiting Social Engineering to gain access to Energy Management Systems/ Substation Workstations

An uninformed operator in the control room connects his workstation to Internet during a night shift. He does this to be able to use Facebook to chat with his friends and to surf on Internet. This operator has the tendency to accept any friend request on Facebook and add as his friend. The attacker uses this to request the operator to add him as a friend. In a chat, his Facebook friend sends him a link that was created by an attacker. Without becoming suspicious, the operator clicks on the link and gives the attacker access to his control room workstation. The attacker is now able to remotely connect to this system and he can open a shell with root privileges on the compromised system. From his own location the attacker is now able to open SCADA displays containing real-time information from the grid and to execute commands. He uses this to open HV breakers in the power grid, which leads to cascading events that causes a total blackout of the high voltage grid.

3.1.7 Story-Board 7 - Manipulating protection settings using Substation Automation tools

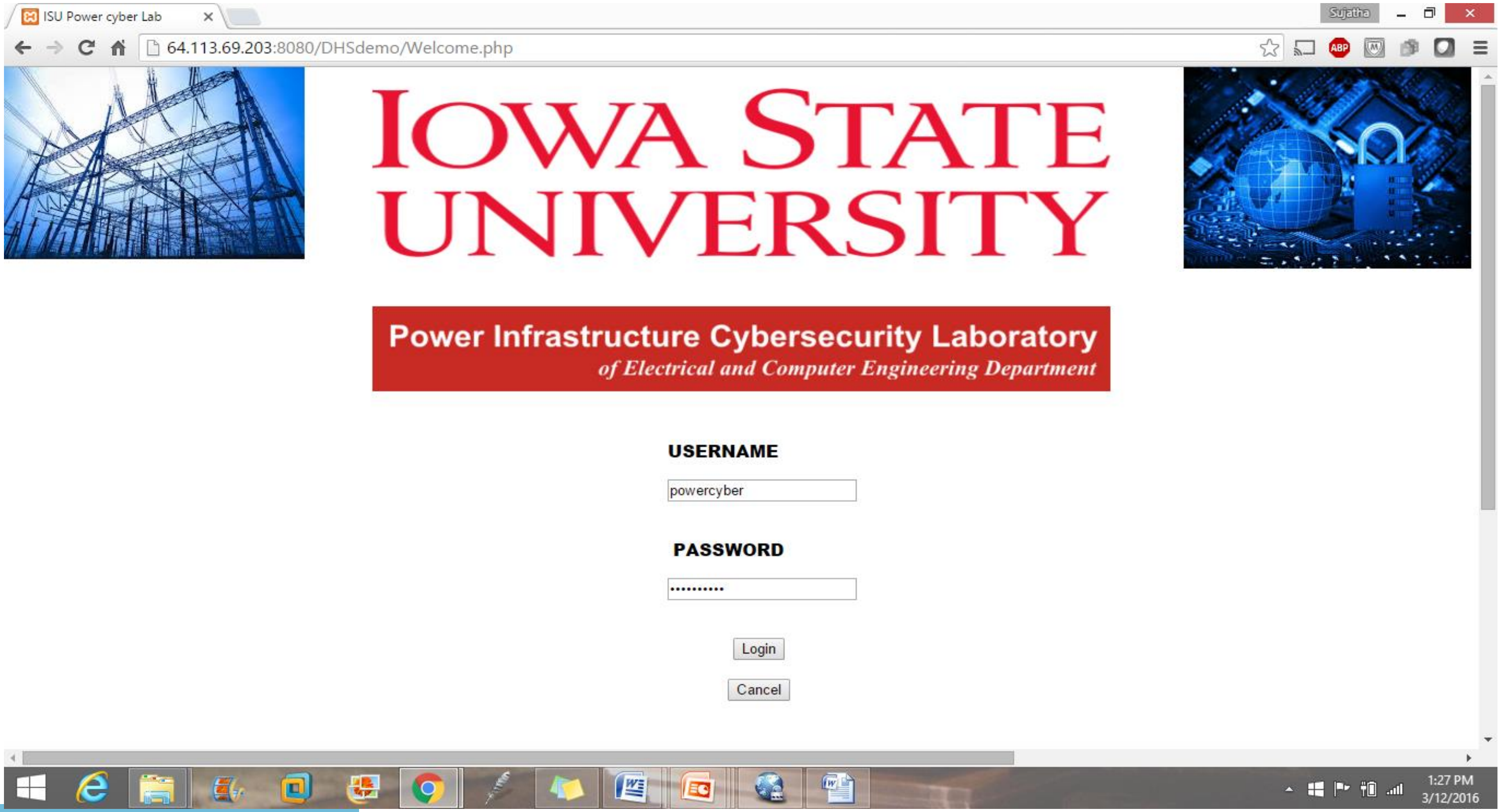
The attacker is an employee of the attacked utility and he has access to substations and to substation engineering tools. He uses the engineering tools for the substation protection devices to set line protection parameters to default values. The default values in the protection devices are defined at such low limits that the protection devices will trip all power lines also at a normal operating state. The attack is done in a central HV/MV substation on the MV side and it will cause a total blackout in the capital city.

3.2 Case Study

This section describes how the remote access CPS security testbed was used to perform a coordinated attack/defense experiment on a wide-area protection scheme. The experimental scenario involves a coordinated cyber-attack on a Remedial Action Scheme (RAS), which is a commonly used Wide-Area Protection scheme, as specified in [9]. Once the remote users login by providing their credentials, the user interface collects various information. For this case study, the IEEE 9-bus power system model was chosen, and RAS scheme was chosen as the WAMPAC experimental scenario. The web interface presents a set of options for mapping the RAS onto the generators in the 9 bus system model. As part of the back-end orchestration framework, the power system control VM is spawned and the runtime interface of the real-time power system simulator is triggered. The IEEE 9-bus model with RAS is then initialized on the run-time interface of the real-time power system simulator. The back-end framework triggers the SCADA configuration module, which spawns SCADA VM’s corresponding to power system simulation and checks network connectivity between devices. Upon successfully spawning the SCADA VM's, the user is provided with options to perform reconnaissance and enumeration followed by list of attack options such as gaining foothold in the internal SCADA network, data integrity attack, DoS attack etc., In this case study, a coordinated attack is chosen. The first part of the coordinated attack involves a data integrity attack by executing a malicious command injection to the substation RTU at bus 7 to trip one of the physical relays involved in the RAS. The second element in the coordinated attack involves a DoS attack on the RAS controller, which is another physical relay to block communication between the RAS controller and the generator controller. The users can select whether a defense measure is to be implemented as part of the experimental scenario. For this experimental scenario, the possible defense measures include a firewall rule at the substation gateway node to whitelist communication into the substation and updating security patches. This prevents the data integrity attack from succeeding and also prevents attacker infiltration into the internal SCADA network. Also, the users can select to implement throttling of the network traffic on the substation gateway to ensure that the impact of the DoS attack is minimized. The cyber layer visualization system constantly updates the status of the physical relays on the experiment to show the attack impacts. In addition to the visualization, as a part of post-attack data collection, the framework allows users to download capture of communication packets between all devices (cyber & physical). These packet captures can be used to analyze and understand the communication flow in the system before and after attack implementation which might be useful in design of anomaly detection algorithms. The power system run-time interface provides the users with real-time power system outputs as the attack is being executed. Also, it provides the users to interact with the power system model by applying manual control actions directly through the GUI. The framework provides two options for analyzing the power system impacts: real-time outputs for the users to observe vs. data files that could be processed offline. For this case study, only the real-time outputs option has been shown. As an additional feature, the framework will provide an option in the future to collect data files corresponding to appropriate power system parameters in the system model such as voltages, power flows and system frequency.

The reminder of this section captures the sample case study with step-by-step explanations and corresponding screen shots.

Step 1: To gain access to remote access framework, the users connect to PowerCyber laboratory virtual private network (VPN). This is done by downloading VPN clients such as OpenVPN, Viscosity or Tunnelblick and providing certificates and credentials for VPN access. Upon successful connection to VPN, the remote users connect to PowerCyber remote access framework URL and provide credentials to log into the framework.


ISU Power cyber Lab
Sujatha
64.113.69.203:8080/DHSdemo/Welcome.php
IOWA STATE UNIVERSITY
Power Infrastructure Cybersecurity Laboratory
of Electrical and Computer Engineering Department
Login
Cancel
1:27 PM
3/12/2016

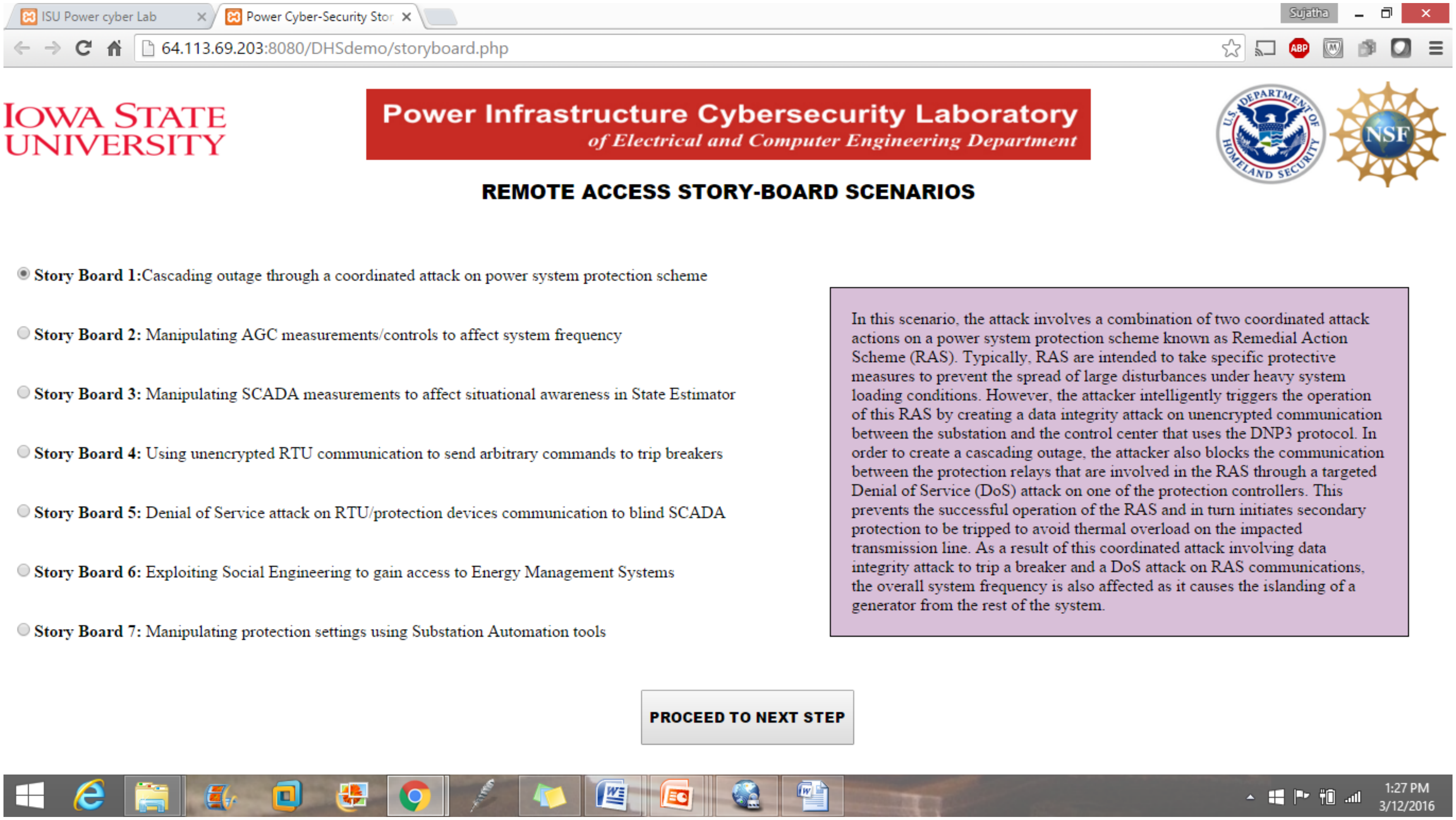
USERNAME

powercyber

PASSWORD

••••••••••

Step 2: Upon succesfull login, the interface provides story board scenarios for the remote users to choose from. A detailed description of story board scenario selected is displayed to the user. The screenshot below captures the description of Story Board 1: Cascading outage through a coordinated attack on power system protection scheme.


ISU Power cyber Lab
Power Cyber-Security Stor
Sujatha
64.113.69.203:8080/DHSdemo/storyboard.php
IOWA STATE UNIVERSITY
NSF
1:27 PM
3/12/2016

Power Infrastructure Cybersecurity Laboratory
of Electrical and Computer Engineering Department

REMOTE ACCESS STORY-BOARD SCENARIOS

● **Story Board 1:**Cascading outage through a coordinated attack on power system protection scheme

○ **Story Board 2:** Manipulating AGC measurements/controls to affect system frequency

○ **Story Board 3:** Manipulating SCADA measurements to affect situational awareness in State Estimator

○ **Story Board 4:** Using unencrypted RTU communication to send arbitrary commands to trip breakers

○ **Story Board 5:** Denial of Service attack on RTU/protection devices communication to blind SCADA

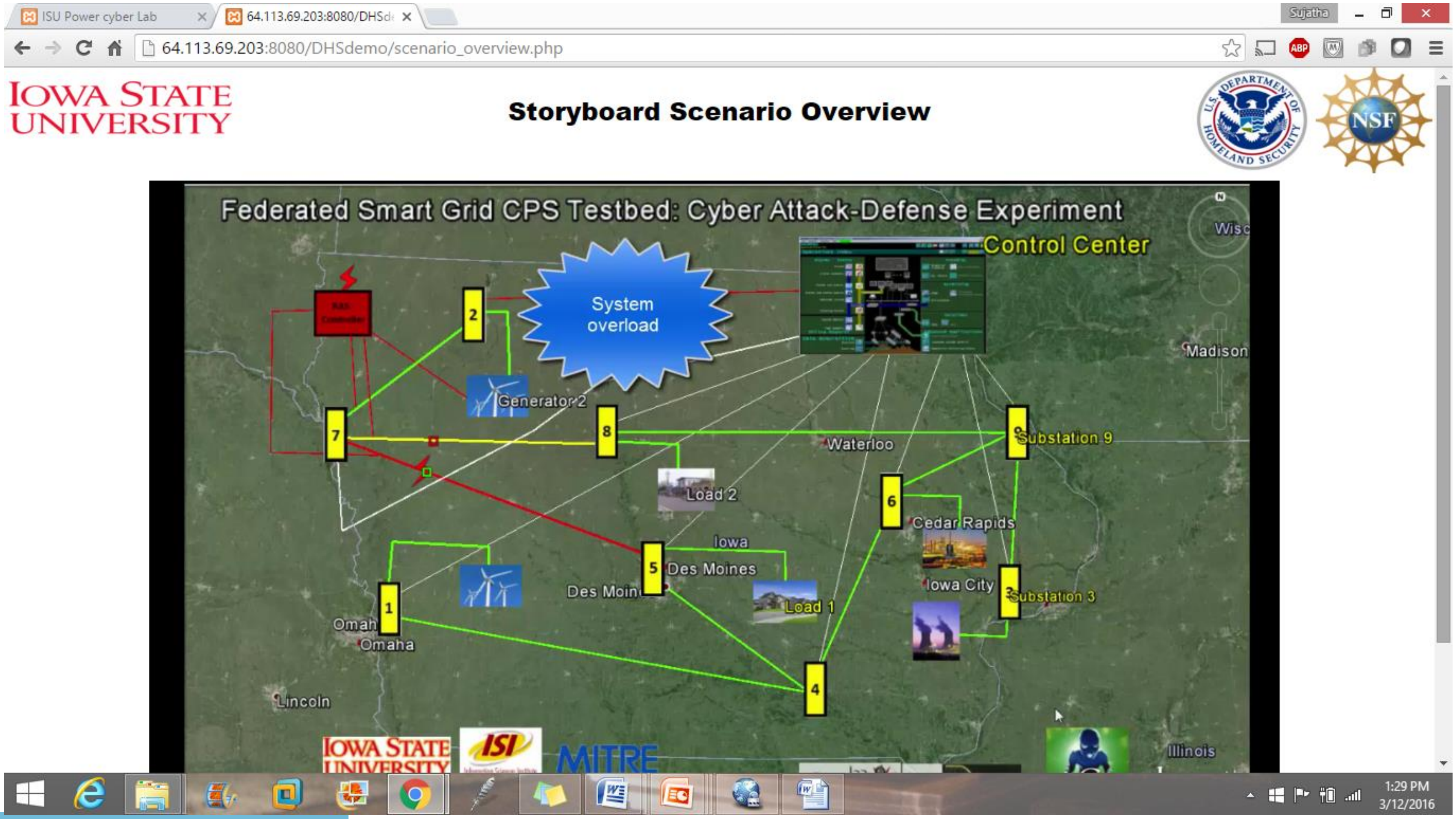
○ **Story Board 6:** Exploiting Social Engineering to gain access to Energy Management Systems

○ **Story Board 7:** Manipulating protection settings using Substation Automation tools

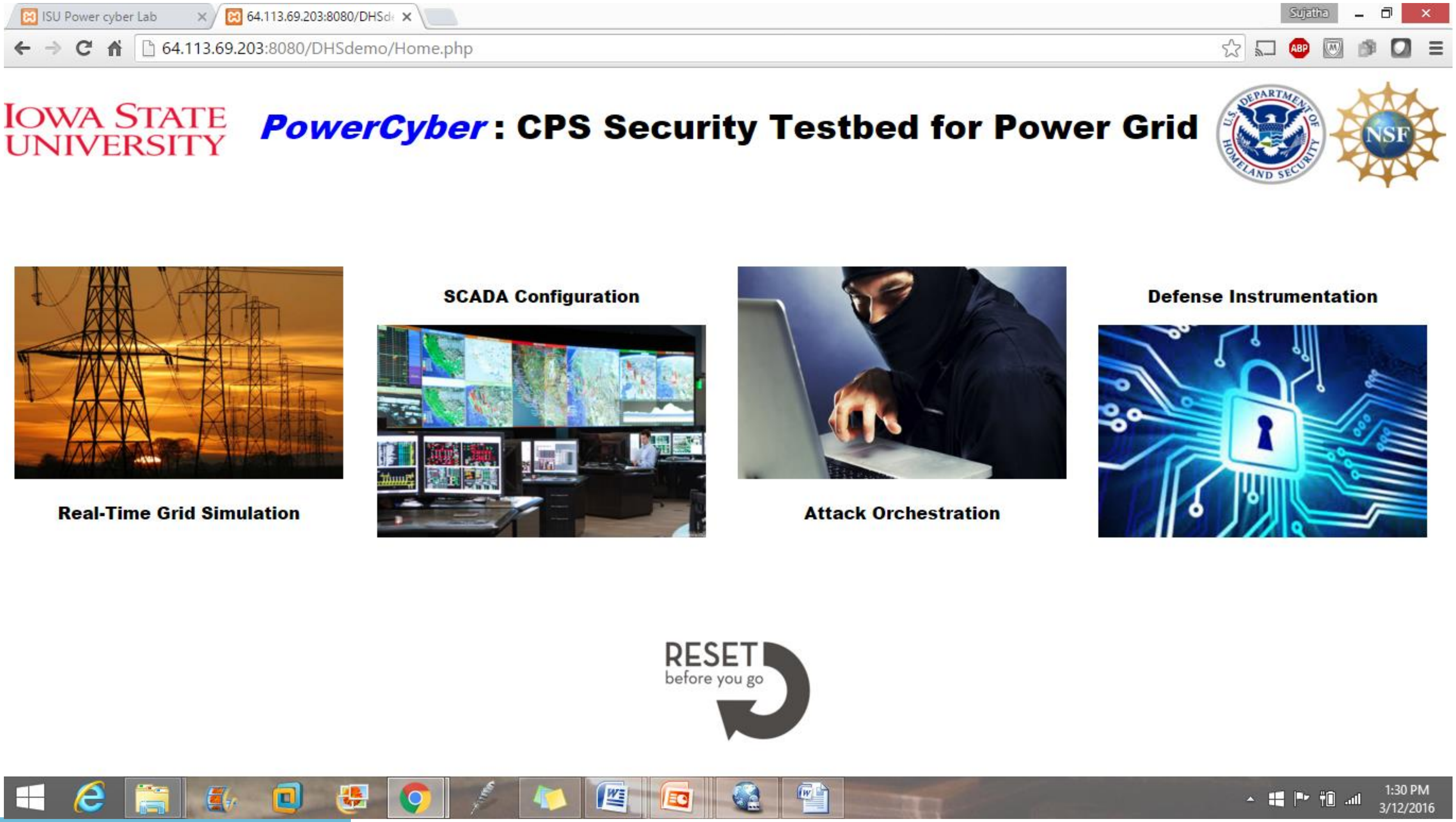
In this scenario, the attack involves a combination of two coordinated attack actions on a power system protection scheme known as Remedial Action Scheme (RAS). Typically, RAS are intended to take specific protective measures to prevent the spread of large disturbances under heavy system loading conditions. However, the attacker intelligently triggers the operation of this RAS by creating a data integrity attack on unencrypted communication between the substation and the control center that uses the DNP3 protocol. In order to create a cascading outage, the attacker also blocks the communication between the protection relays that are involved in the RAS through a targeted Denial of Service (DoS) attack on one of the protection controllers. This prevents the successful operation of the RAS and in turn initiates secondary protection to be tripped to avoid thermal overload on the impacted transmission line. As a result of this coordinated attack involving data integrity attack to trip a breaker and a DoS attack on RAS communications, the overall system frequency is also affected as it causes the islanding of a generator from the rest of the system.

PROCEED TO NEXT STEP

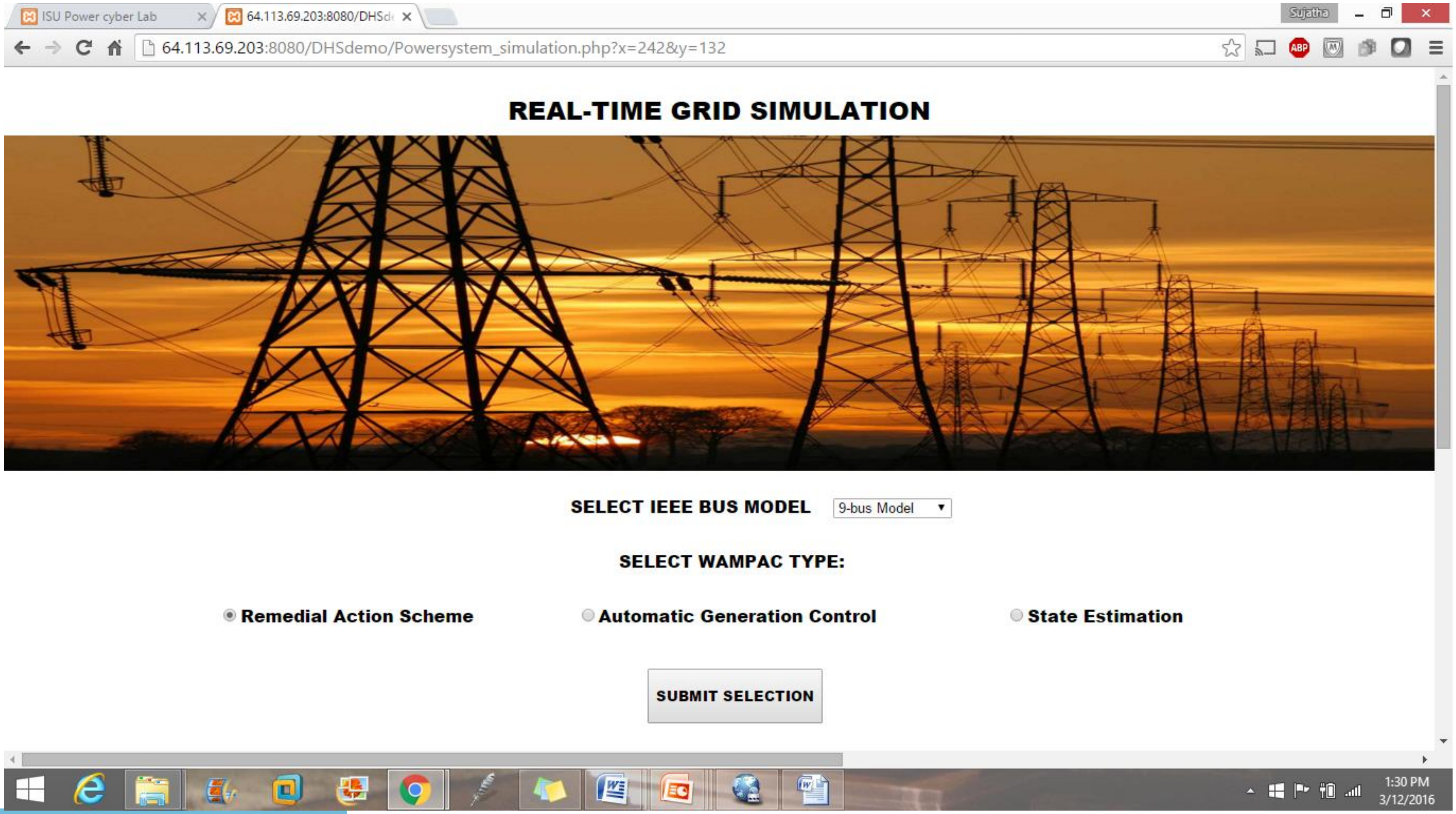
Step 3: The next webpage provides an overview video snippet of the scenario described in Story Board 1 [12]. The video demonstarates the impact of coordinated attack (data integrity and denial of service) on IEEE 9-bus system distributed across the state of IOWA. The video uses OPC server interfacing with SICAM and Google earth interface for visualizing the scenario decribed.



Step 4: The next webpage is the home page which is categorized into four main modules: Real-Time Grid Simulation, SCADA Configuration, Attack Orchestration and Defense Instrumentation. These four modules are the fundamental building blocks for orchestrating attack/defense experimentation in PowerCybed testbed environment.



Step 5: The real-time grid simulation module involves selection of IEEE Bus Model (such as 9-bus, 39-bus, etc.) from a drop down menu followed by selection of WAMPAC(Wide-Area Monitoring, Protection and Control) systems. The framework provides three WAMPAC types for selection, namely: Remedial Action Scheme (Wide-Area Protection scheme), Automatic Generation Control (Wide-Area Control scheme) and State Estimation (Wide-Area Monitoring scheme).


ISU Power cyber Lab
64.113.69.203:8080/DHSd
Sujatha
64.113.69.203:8080/DHSdemo/Powersystem_simulation.php?x=242&y=132
1:30 PM
3/12/2016

REAL-TIME GRID SIMULATION

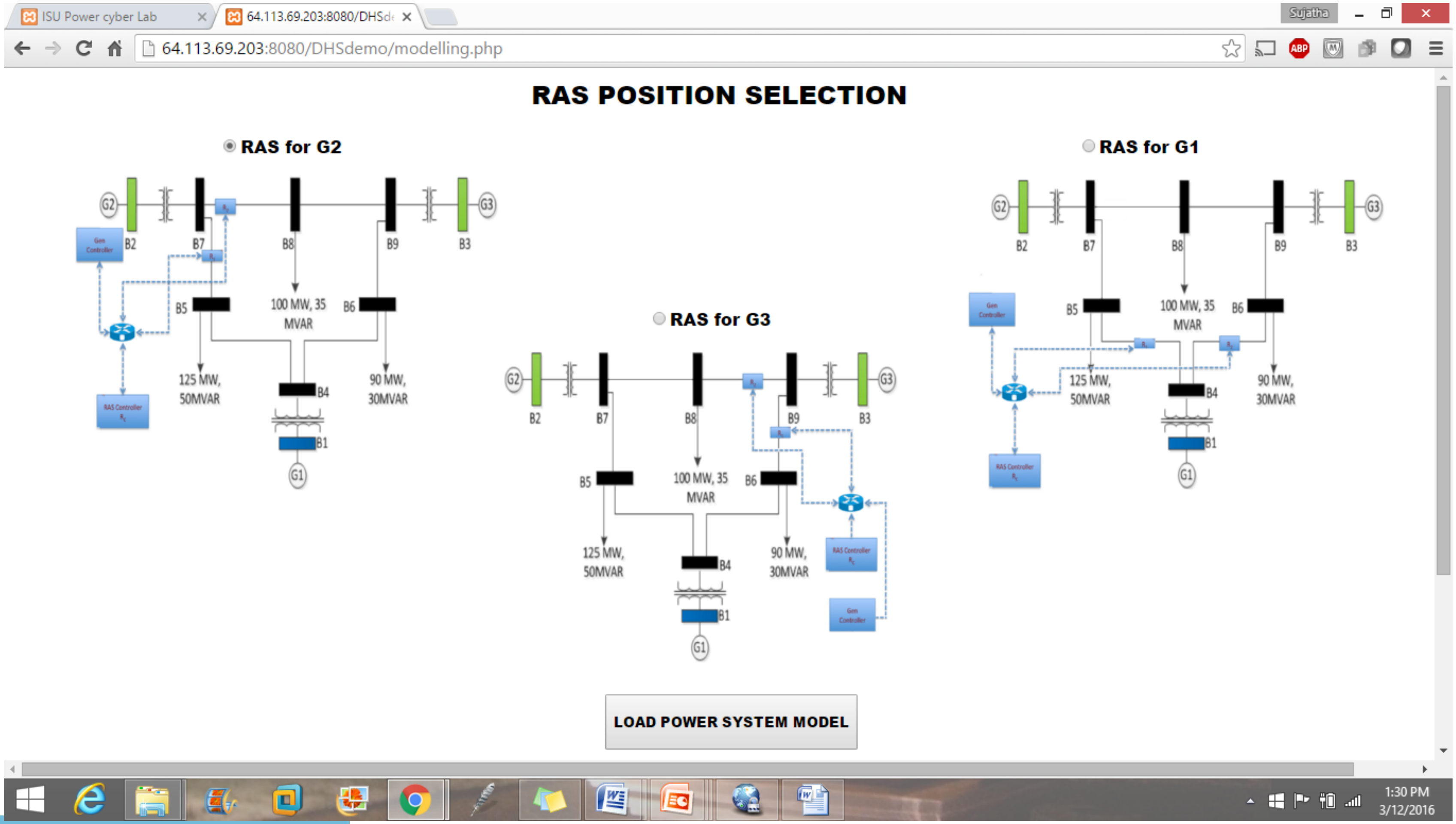
SELECT IEEE BUS MODEL 9-bus Model ▾

SELECT WAMPAC TYPE:

● Remedial Action Scheme ○ Automatic Generation Control ○ State Estimation

SUBMIT SELECTION

Step 6: For enhancing user programmability, second step in real-time grid simulation module involves identification of how the physical components should be mapped to the power system model. In particular, this case study identifies three possible positions for placing Remedial Action Scheme on IEEE 9-bus system, namely: Remedial Action Scheme for Generator 2, Remedial Action Scheme for Generator 1 and Remedial Action Scheme for Generator 3.



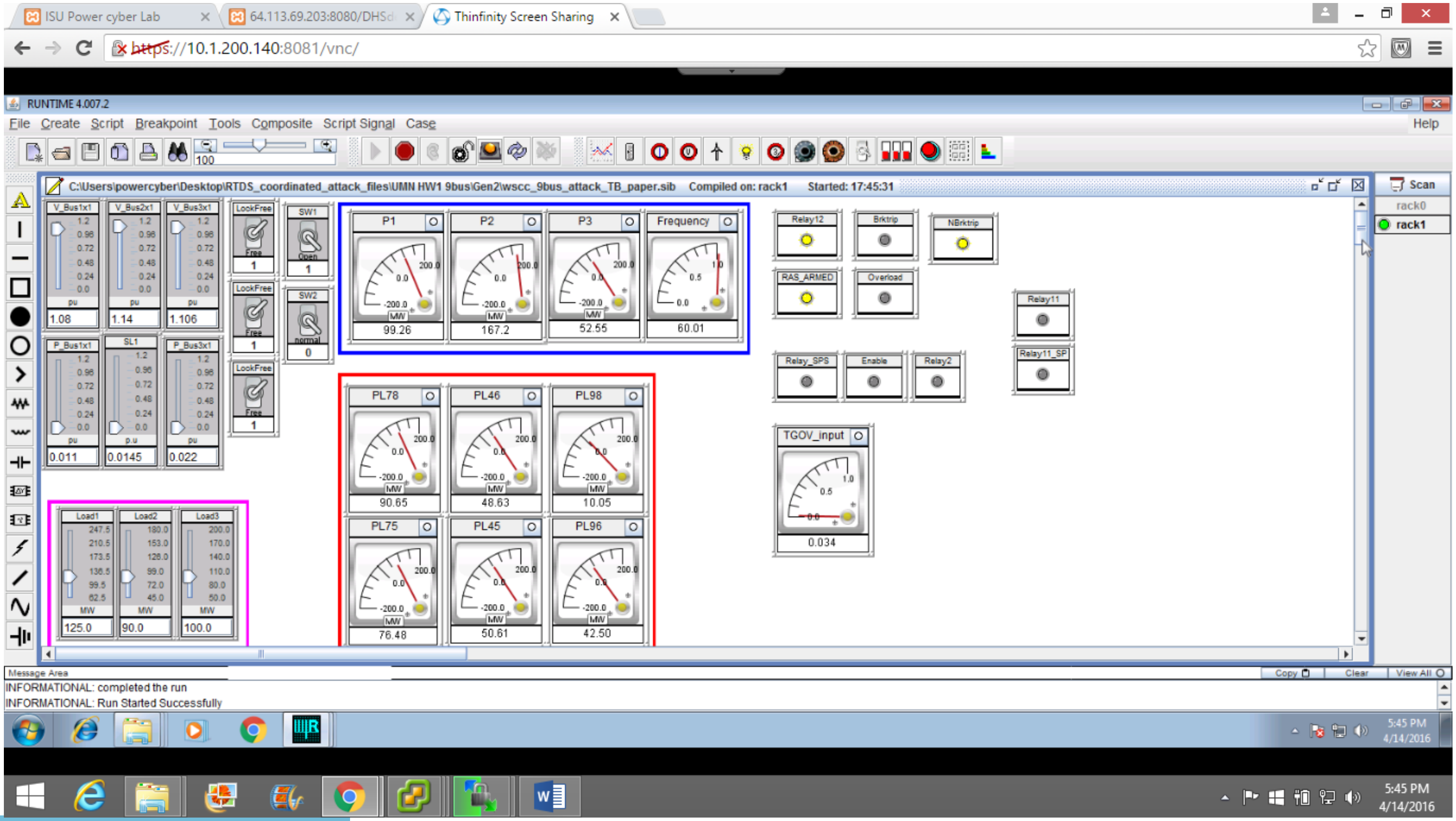
RAS POSITION SELECTION

● RAS for G2

○ RAS for G1

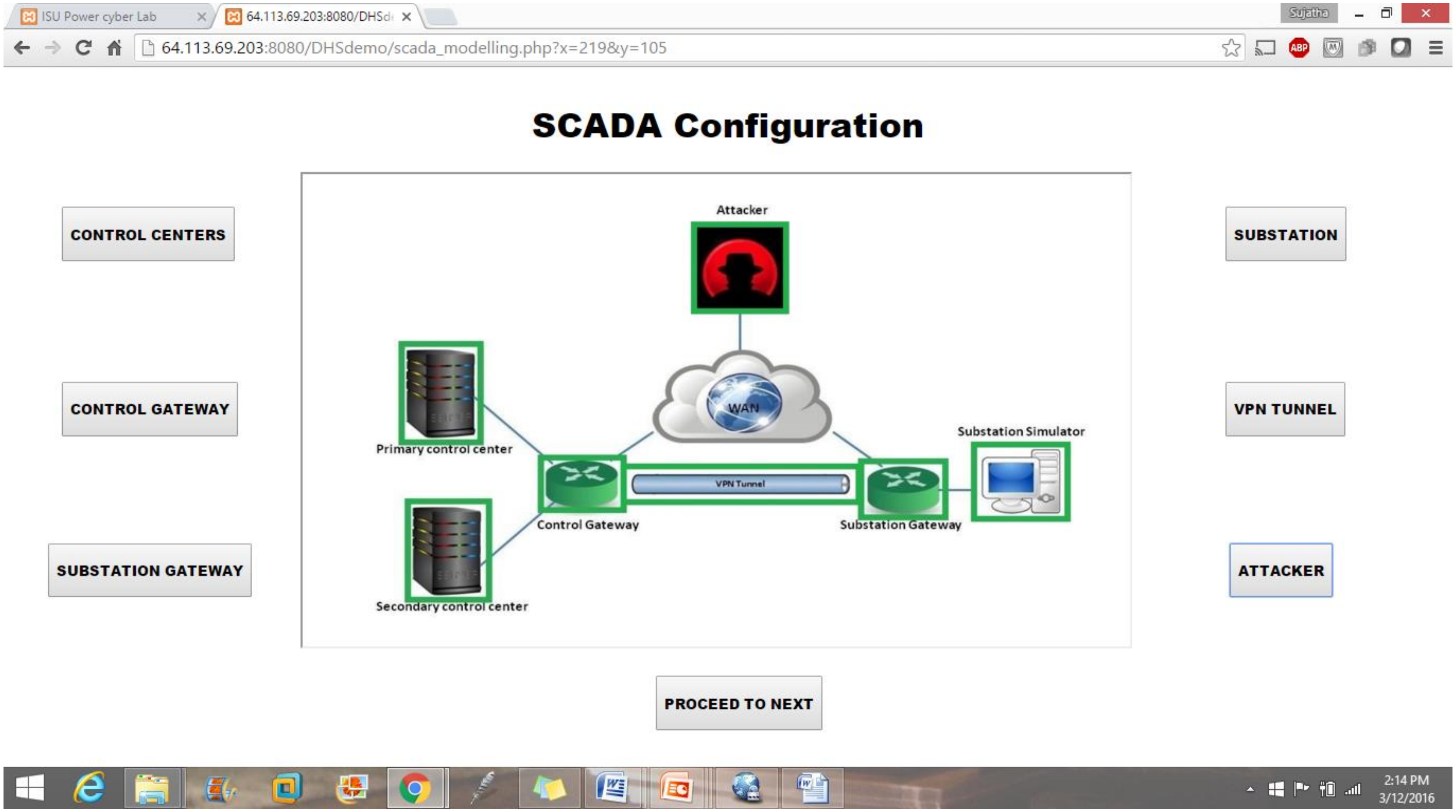
○ RAS for G3

Step 7: The model selected by remote user is compiled, loaded and executed on the real-time power system simulator and the run time visualization environment is provided to the user. The environment provides meters representing generation levels, overall system frequency, tie-line flows of transmission lines, bus voltages and loads to clearly capture the state of power system model before and after cyber-attack, defense simulation.



INFORMATIONAL: completed the run
INFORMATIONAL: Run Started Successfully

Step 8: The SCADA configuration module is responsible for spawning SCADA virtual machines and communication topology on the DELL PowerEdge ESXi server at PowerCyber Lab.



Specifically, the topology spawned for story board 1 consists of three networks: SCADA Control network, SCADA Substation Network and Wide Area Network (WAN). Virtual switches(vSwitch) were spawned in ESXi server (one each for each network) to create network topologies required for experimentation.

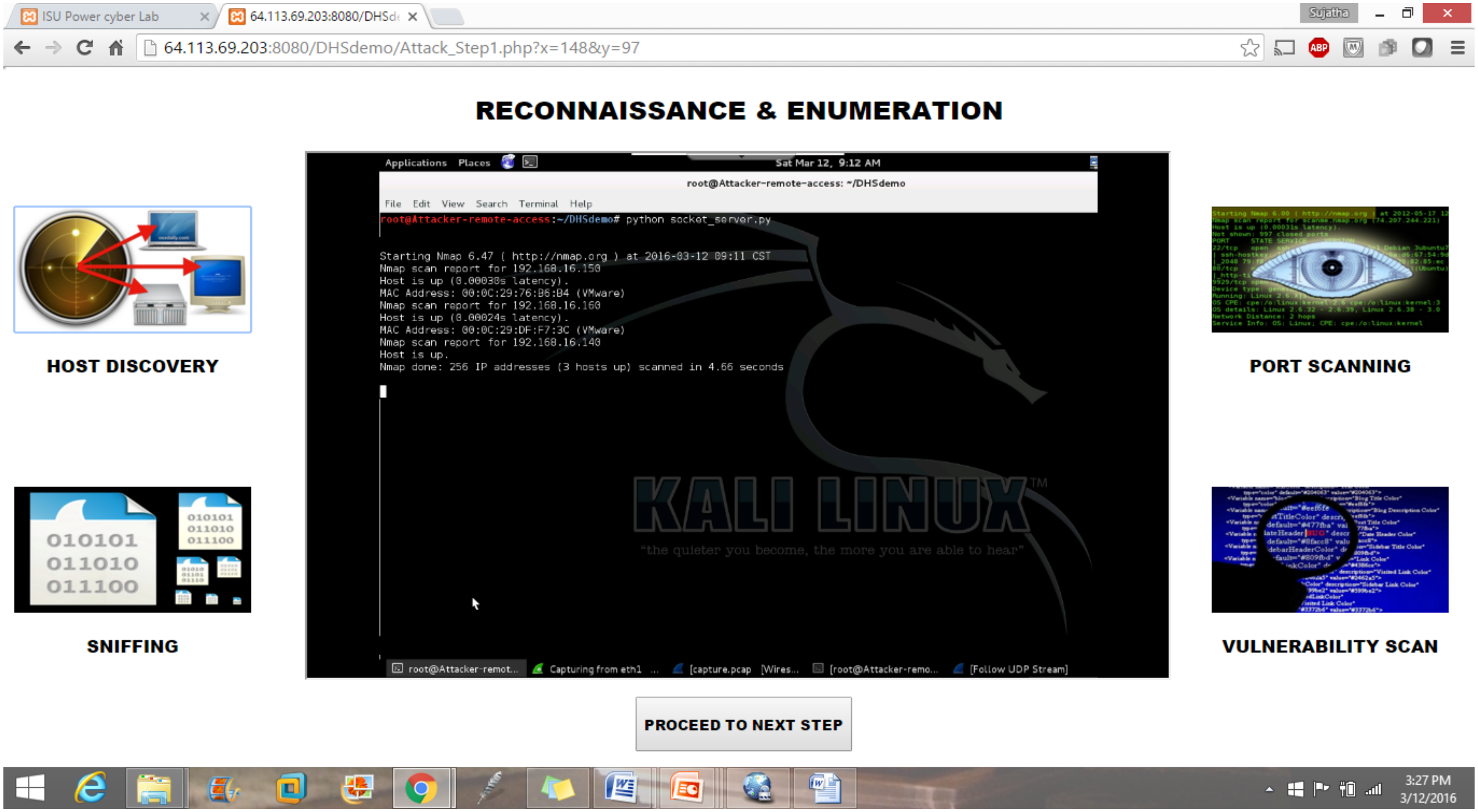
1. SCADA Control network (10.1.1.0/24) – consists of Primary control center (10.1.1.10/24), Secondary control center (10.1.1.20/24), and Control gateway (10.1.1.1/24).

2. SCADA Substation network (10.2.2.0/24) – consists of Substation simulator (10.2.2.10/24) and Substation gateway (10.2.2.1/24). The Substation simulator is in turn connected to the physical Siemens and Schweitzer relays in PowerCyber testbed environment.

3. Wide Area Network (WAN) (192.168.16.0/24) - connects the Control gateway (192.168.16.160/24) and Substation gateway (192.168.16.150/24) using a site-to-site OPEN VPN tunnel which encrypts two-way SCADA communication between control centers and substation. The Attacker virtual machine (192.168.16.140/24) running Kali Linux operating system is also connected to the Wide Area Network for providing the remote user with capabilities to perform penetration testing in PowerCyber testbed SCADA environment.

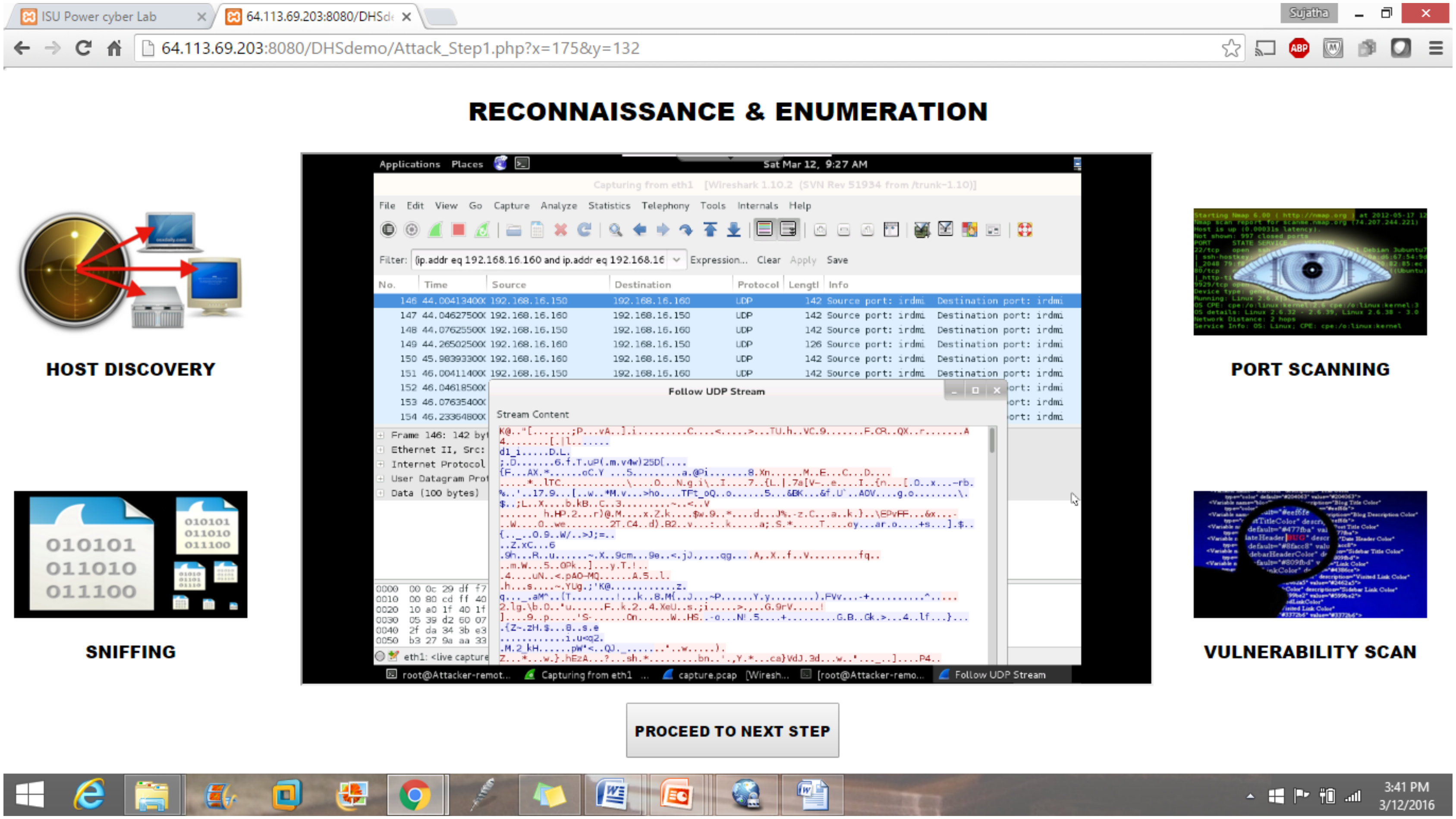
Step 9: The Attack orchestration module involves two steps: 1. Reconnaissance and Enumeration 2. Vulnerability Exploitation. Each of these steps are subdivided into four steps respectively. During reconnaissance phase, interesting information about the target is collected which is used during enumeration phase to identify possible entry points into the internal network. In vulnerability exploitation phase, the identified security weaknesses are exploited to gain access into the internal SCADA communication network which results in manifestation of SCADA virtual machines causing physical impacts on power system models.

Step 9.1: During host discovery, the attacker tries identifying internet facing hosts on the target 192.168.16.0/24 network using nmap command which performs ping sweep and prints out available hosts that responded to host discovery probes. In this scenario, 192.168.16.160 (Control gateway) and 192.168.16.150(Substation gateway) are identified as being live.



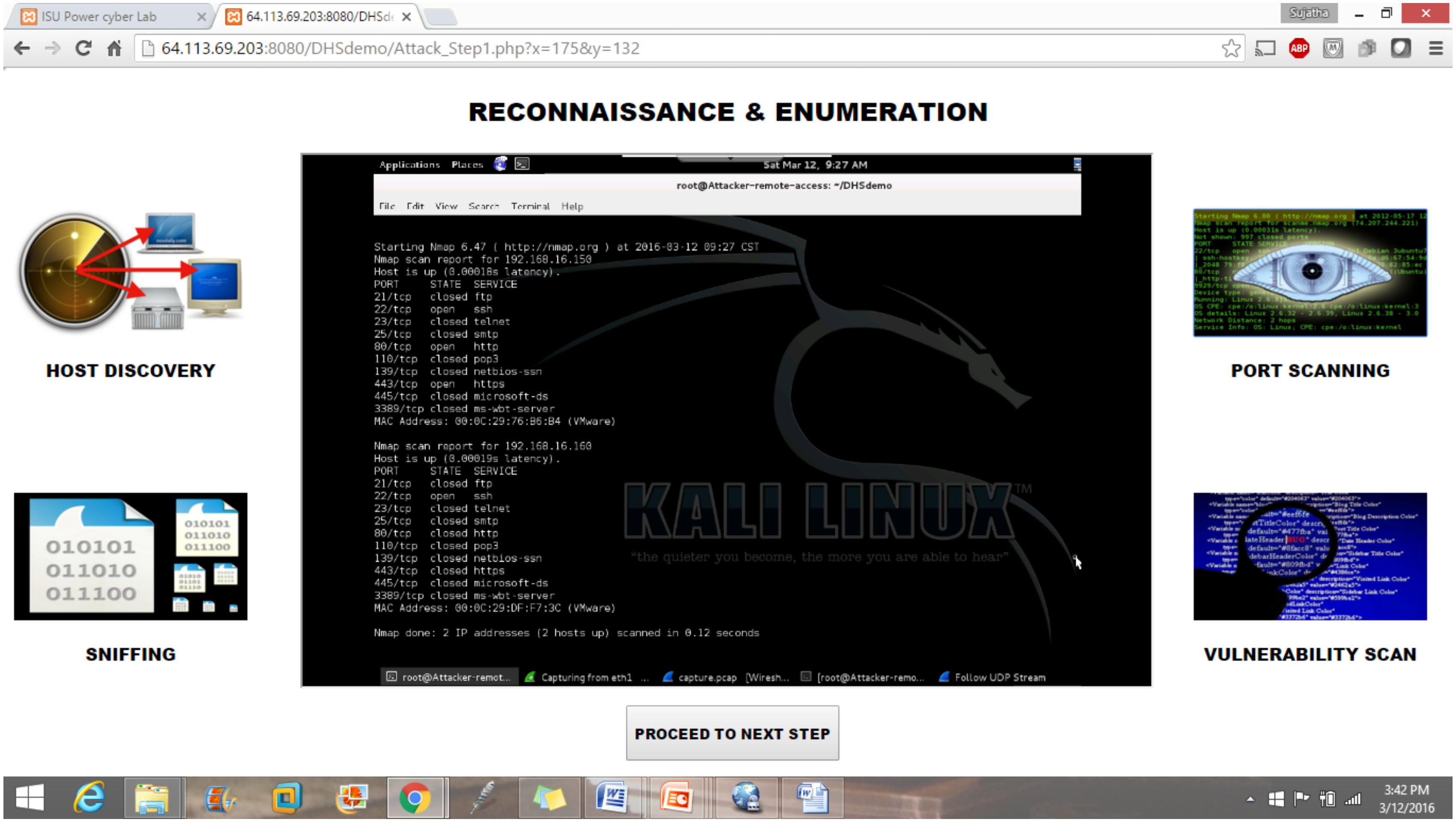
```
root@Attacker-remote-access:~/DHSdemo# python socket_server.py

Starting Nmap 6.47 ( http://nmap.org ) at 2016-03-12 09:11 CST
Nmap scan report for 192.168.16.150
Host is up (0.00030s latency).
MAC Address: 00:0C:29:76:B6:B4 (VMware)
Nmap scan report for 192.168.16.160
Host is up (0.00024s latency).
MAC Address: 00:0C:29:DF:F7:3C (VMware)
Nmap scan report for 192.168.16.140
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 4.66 seconds
```

Step 9.2: In network sniffing phase, the attacker captures all traffic between the discovered hosts 192.168.16.160 and 192.168.16.150. Due to the presence of site-to-site VPN tunnel between the Control gateway and Substation gateway, the Attacker is unsuccessful in decrypting the contents of packets exchanged between the Control Center and Substation. The attacker now tries identifying backdoor techniques to penetrate into the internal network.


ISU Power cyber Lab
64.113.69.203:8080/DHSde
64.113.69.203:8080/DHSdemo/Attack_Step1.php?x=175&y=132
RECONNAISSANCE & ENUMERATION
HOST DISCOVERY
PORT SCANNING
SNIFFING
VULNERABILITY SCAN
PROCEED TO NEXT STEP
Applications Places
Sat Mar 12, 9:27 AM
Capturing from eth1 [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
Follow UDP Stream
Stream Content
3:41 PM
3/12/2016

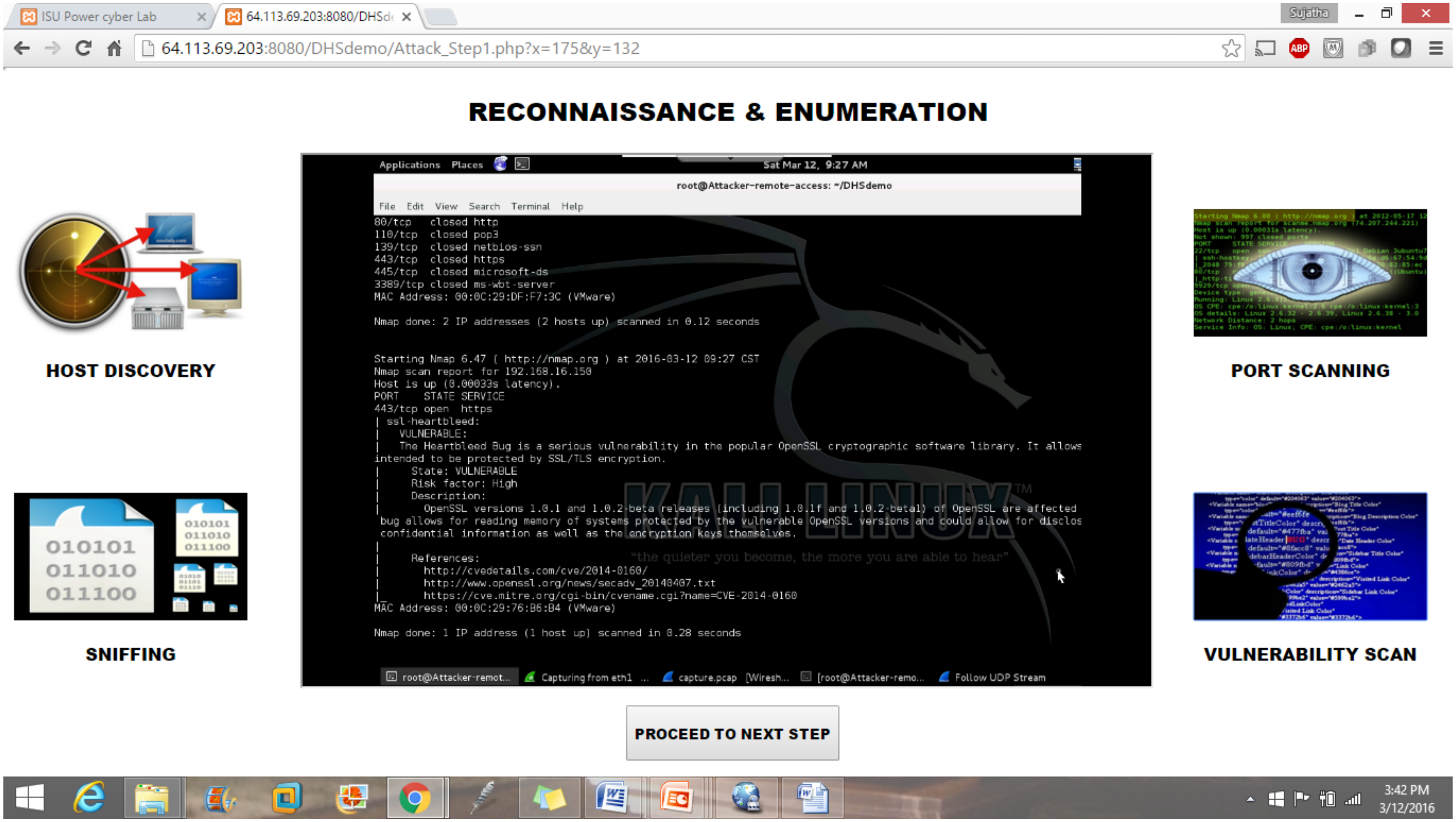
```
Filter: (ip.addr eq 192.168.16.160 and ip.addr eq 192.168.16

No.  Time        Source          Destination     Protocol Lengtl Info
 146 44.00413400( 192.168.16.150 192.168.16.160  UDP         142 Source port: irdmi  Destination port: irdmi
 147 44.04627500( 192.168.16.160 192.168.16.150  UDP         142 Source port: irdmi  Destination port: irdmi
 148 44.07625500( 192.168.16.150 192.168.16.160  UDP         142 Source port: irdmi  Destination port: irdmi
 149 44.26502500( 192.168.16.160 192.168.16.150  UDP         126 Source port: irdmi  Destination port: irdmi
 150 45.98393300( 192.168.16.160 192.168.16.150  UDP         142 Source port: irdmi  Destination port: irdmi
 151 46.00411400( 192.168.16.150 192.168.16.160  UDP         142 Source port: irdmi  Destination port: irdmi
 152 46.04618500(
 153 46.07635400(
 154 46.23364800(

⊞ Frame 146: 142 byt
⊞ Ethernet II, Src:
⊞ Internet Protocol
⊞ User Datagram Prot
⊞ Data (100 bytes)
```

Step 9.3: The attacker next performs intense port scanning to identify top ten TCP ports which are open on the target hosts using nmap commands. In this scenario, TCP port running SSH service and TCP port running HTTPS are identified by the attacker as being open on the target hosts.



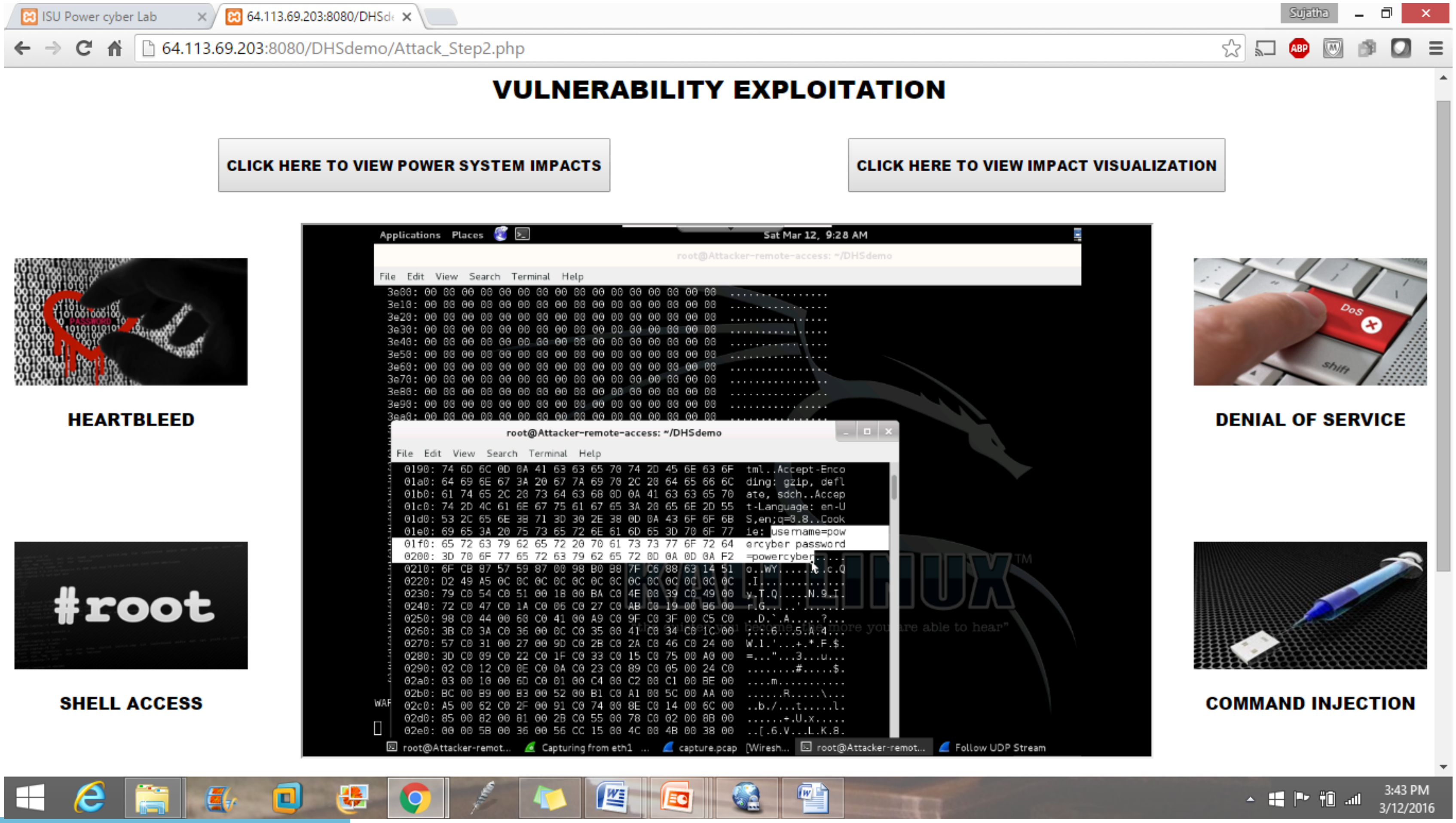
```
Starting Nmap 6.47 ( http://nmap.org ) at 2016-03-12 09:27 CST
Nmap scan report for 192.168.16.150
Host is up (0.00018s latency).
PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   open   ssh
23/tcp   closed telnet
25/tcp   closed smtp
80/tcp   open   http
110/tcp  closed pop3
139/tcp  closed netbios-ssn
443/tcp  open   https
445/tcp  closed microsoft-ds
3389/tcp closed ms-wbt-server
MAC Address: 00:0C:29:76:B6:B4 (VMware)

Nmap scan report for 192.168.16.160
Host is up (0.00019s latency).
PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   open   ssh
23/tcp   closed telnet
25/tcp   closed smtp
80/tcp   closed http
110/tcp  closed pop3
139/tcp  closed netbios-ssn
443/tcp  closed https
445/tcp  closed microsoft-ds
3389/tcp closed ms-wbt-server
MAC Address: 00:0C:29:DF:F7:3C (VMware)

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.12 seconds
```

Step 9.4: Vulnerability scanning identifies that the Substation gateway is vulnerable to Heartbleed bug which is a serious vulnerability in OpenSSL cryptographic software library that allows the attacker to steal information protected by the SSL/TLS encryption used to secure the internet.


ISU Power cyber Lab
64.113.69.203:8080/DHSd
Sujatha
64.113.69.203:8080/DHSdemo/Attack_Step1.php?x=175&y=132
RECONNAISSANCE & ENUMERATION
HOST DISCOVERY
PORT SCANNING
SNIFFING
VULNERABILITY SCAN
Applications Places
Sat Mar 12, 9:27 AM
root@Attacker-remote-access: ~/DHSdemo
File Edit View Search Terminal Help
root@Attacker-remot... Capturing from eth1 ... capture.pcap [Wiresh... [root@Attacker-remo... Follow UDP Stream
PROCEED TO NEXT STEP
3:42 PM
3/12/2016

```
80/tcp   closed http
110/tcp  closed pop3
139/tcp  closed netbios-ssn
443/tcp  closed https
445/tcp  closed microsoft-ds
3389/tcp closed ms-wbt-server
MAC Address: 00:0C:29:DF:F7:3C (VMware)

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.12 seconds


Starting Nmap 6.47 ( http://nmap.org ) at 2016-03-12 09:27 CST
Nmap scan report for 192.168.16.150
Host is up (0.00033s latency).
PORT    STATE SERVICE
443/tcp open  https
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows
intended to be protected by SSL/TLS encryption.
|     State: VULNERABLE
|     Risk factor: High
|     Description:
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected
 bug allows for reading memory of systems protected by the vulnerable OpenSSL versions and could allow for disclos
 confidential information as well as the encryption keys themselves.
|
|     References:
|       http://cvedetails.com/cve/2014-0160/
|       http://www.openssl.org/news/secadv_20140407.txt
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
MAC Address: 00:0C:29:76:B6:B4 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

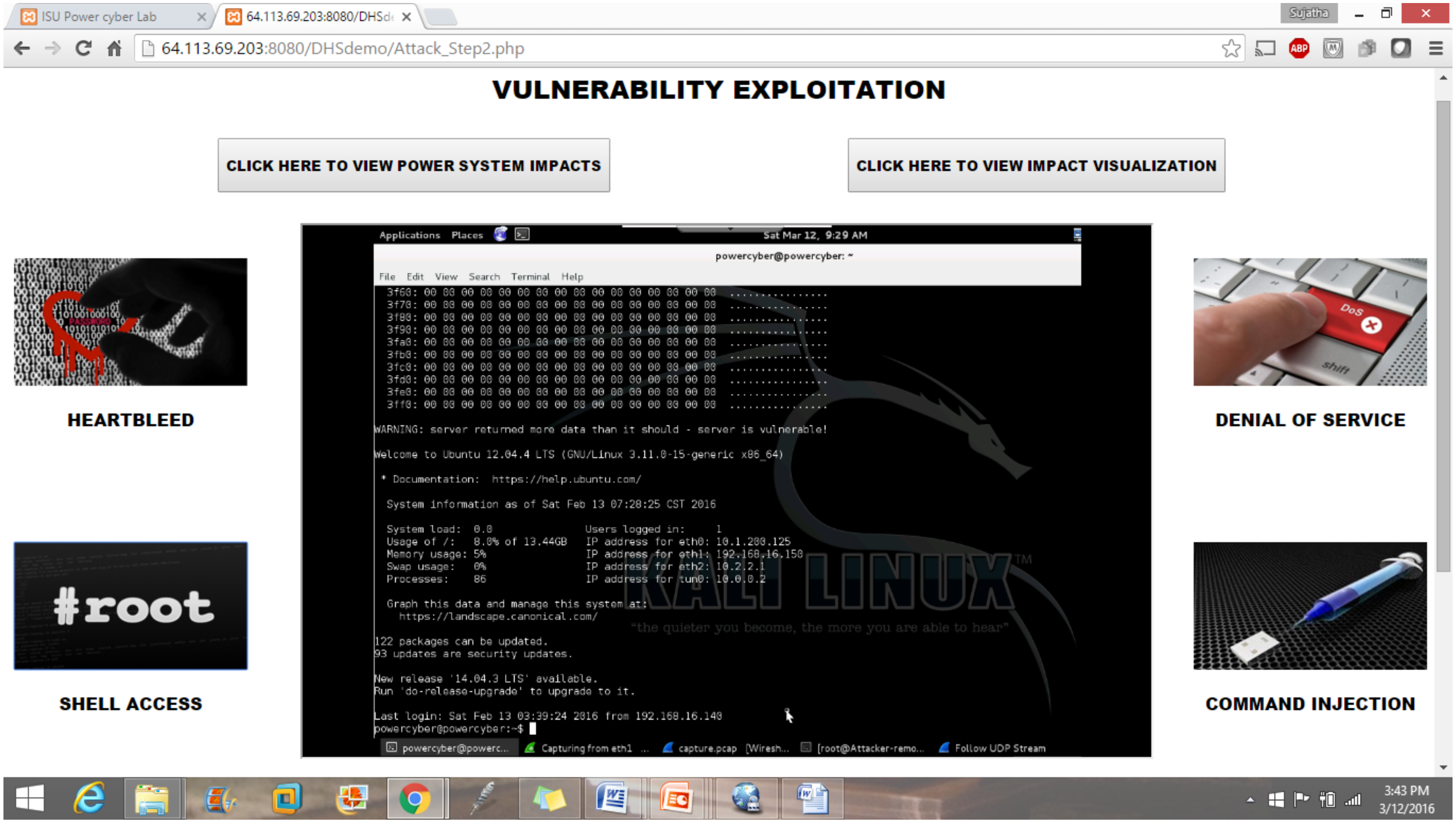
Step 9.5: In vulnerability exploitation phase initially, the remote attacker exploits Heartbleed vulnerability which allows the attacker to obtain up to 64 KB of unencrypted sensitive data from the memory of a vulnerable OpenSSL server. In this scenario the credentials (username and password) of the Substation gateway vulnerable to Heartbleed is extracted by the attacker using packets that trigger a buffer over-read.



```
3e00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
3e10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
3e20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
3e30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
3e40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
3e50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
3e60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
3e70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
3e80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
3e90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
3ea0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

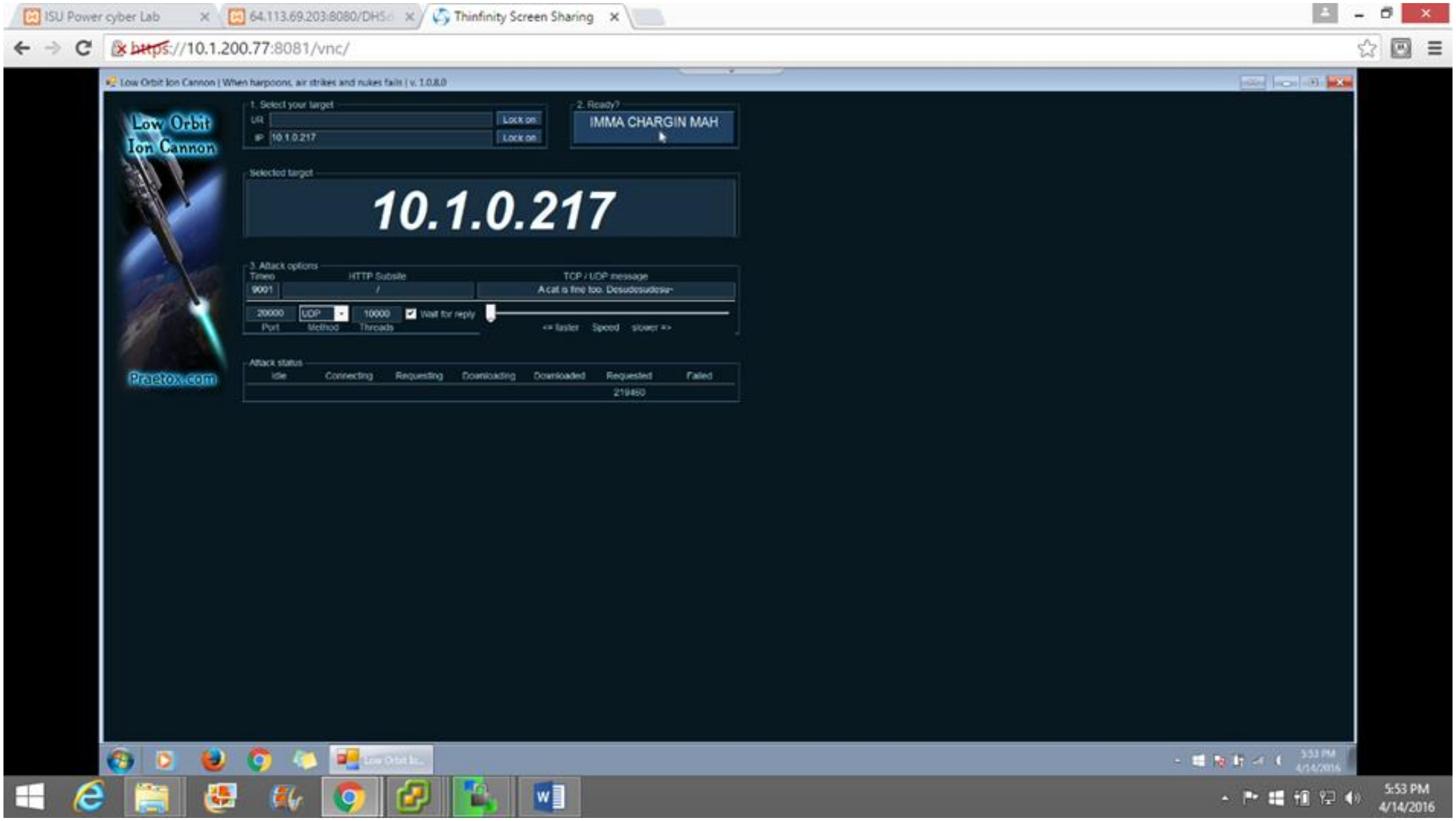
```
0190: 74 6D 6C 0D 0A 41 63 63 65 70 74 2D 45 6E 63 6F   tml..Accept-Enco
01a0: 64 69 6E 67 3A 20 67 7A 69 70 2C 20 64 65 66 6C   ding: gzip, defl
01b0: 61 74 65 2C 20 73 64 63 68 0D 0A 41 63 63 65 70   ate, sdch..Accep
01c0: 74 2D 4C 61 6E 67 75 61 67 65 3A 20 65 6E 2D 55   t-Language: en-U
01d0: 53 2C 65 6E 3B 71 3D 30 2E 38 0D 0A 43 6F 6F 6B   S,en;q=0.8..Cook
01e0: 69 65 3A 20 75 73 65 72 6E 61 6D 65 3D 70 6F 77   ie: username=pow
01f0: 65 72 63 79 62 65 72 20 70 61 73 73 77 6F 72 64   ercyber password
0200: 3D 70 6F 77 65 72 63 79 62 65 72 0D 0A 0D 0A F2   =powercyber.....
0210: 6F CB 87 57 59 87 00 98 B0 88 7F C6 88 63 14 51   o..WY........c.Q
0220: D2 49 A5 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C   .I..............
0230: 79 C0 54 C0 51 00 18 00 BA C0 4E 00 39 C0 49 00   y.T.Q.....N.9.I.
0240: 72 C0 47 C0 1A C0 06 C0 27 C0 AB C0 19 00 B6 00   r.G.....'.......
0250: 98 C0 44 00 60 C0 41 00 A9 C0 9F C0 3F 00 C5 C0   ..D.`.A.....?...
0260: 3B C0 3A C0 36 00 0C C0 35 00 41 C0 34 C0 1C 00   ;.:.6...5.A.4...
0270: 57 C0 31 00 27 00 9D C0 2B C0 2A C0 46 C0 24 00   W.1.'...+.*.F.$.
0280: 3D C0 09 C0 22 C0 1F C0 33 C0 15 C0 75 00 A0 00   =..."...3...u...
0290: 02 C0 12 C0 0E C0 0A C0 23 C0 89 C0 05 00 24 C0   ........#.....$.
02a0: 03 00 10 00 6D C0 01 00 C4 00 C2 00 C1 00 BE 00   ....m...........
02b0: BC 00 B9 00 B3 00 52 00 B1 C0 A1 00 5C 00 AA 00   ......R.....\...
02c0: A5 00 62 C0 2F 00 91 C0 74 00 8E C0 14 00 6C 00   ..b./...t.....l.
02d0: 85 00 82 00 81 00 2B C0 55 00 78 C0 02 00 8B 00   ......+.U.x.....
02e0: 00 00 5B 00 36 00 56 CC 15 00 4C 00 4B 00 38 00   ..[.6.V...L.K.8.
```

Step 9.6: The attacker makes use of credentials obtained using Heartbleed vulnerability to gain SSH access into the substation gateway. This in turn allows the attacker to obtain root access with administrator privilege and capture two-way SCADA communication traffic between control center and substation. This step serves as the stepping stone for performing a successful coordinated attack on the power system model.



```
  3f60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  3f70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  3f80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  3f90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  3fa0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  3fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  3fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  3fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  3fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  3ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................

WARNING: server returned more data than it should - server is vulnerable!

Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

  System information as of Sat Feb 13 07:28:25 CST 2016

  System load:  0.0               Users logged in:     1
  Usage of /:   8.0% of 13.44GB   IP address for eth0: 10.1.200.125
  Memory usage: 5%                IP address for eth1: 192.168.16.150
  Swap usage:   0%                IP address for eth2: 10.2.2.1
  Processes:    86                IP address for tun0: 10.0.0.2

  Graph this data and manage this system at:
    https://landscape.canonical.com/

122 packages can be updated.
93 updates are security updates.

New release '14.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sat Feb 13 03:39:24 2016 from 192.168.16.140
powercyber@powercyber:~$
```

Step 9.7: The attacker now triggers the Denial of Service attack which is the first step towards execution of successful coordinated attack. Button click opens up Low Orbit Ion Canon (LOIC) front-end simulation in a new tab where DOS attack parameters such as target IP Address, port, method, threads and throttle are configured and the attack is successfully triggered.



~~https~~://10.1.200.77:8081/vnc/

Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.8.0

1. Select your target
IP: 10.1.0.217

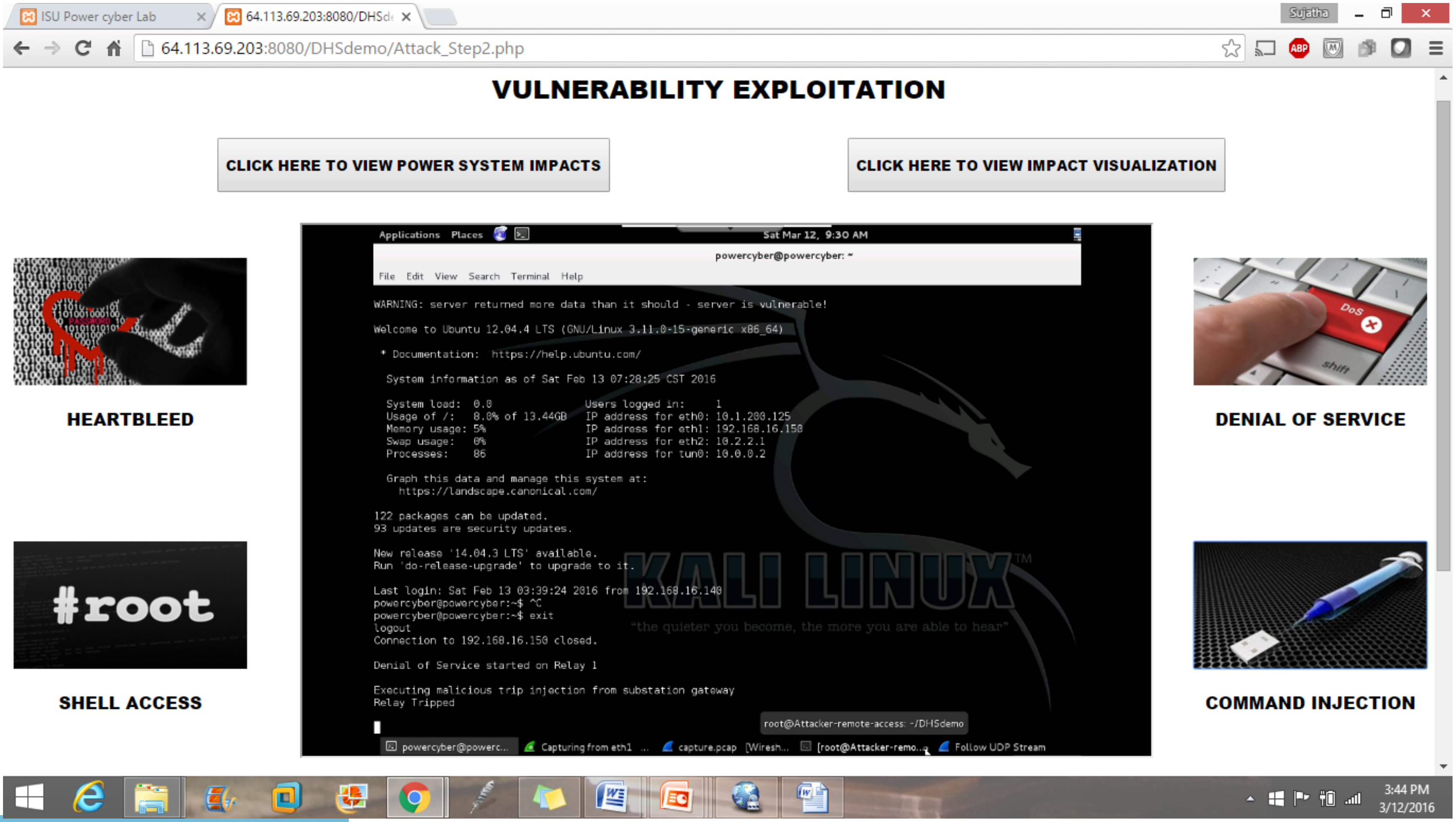
Selected target: 10.1.0.217

3. Attack options
Timeo: 9001
HTTP Subsite: /
TCP / UDP message: A cat is fine too. Desudesudesu~
Port: 20000
Method: UDP
Threads: 10000
☑ Wait for reply

Attack status

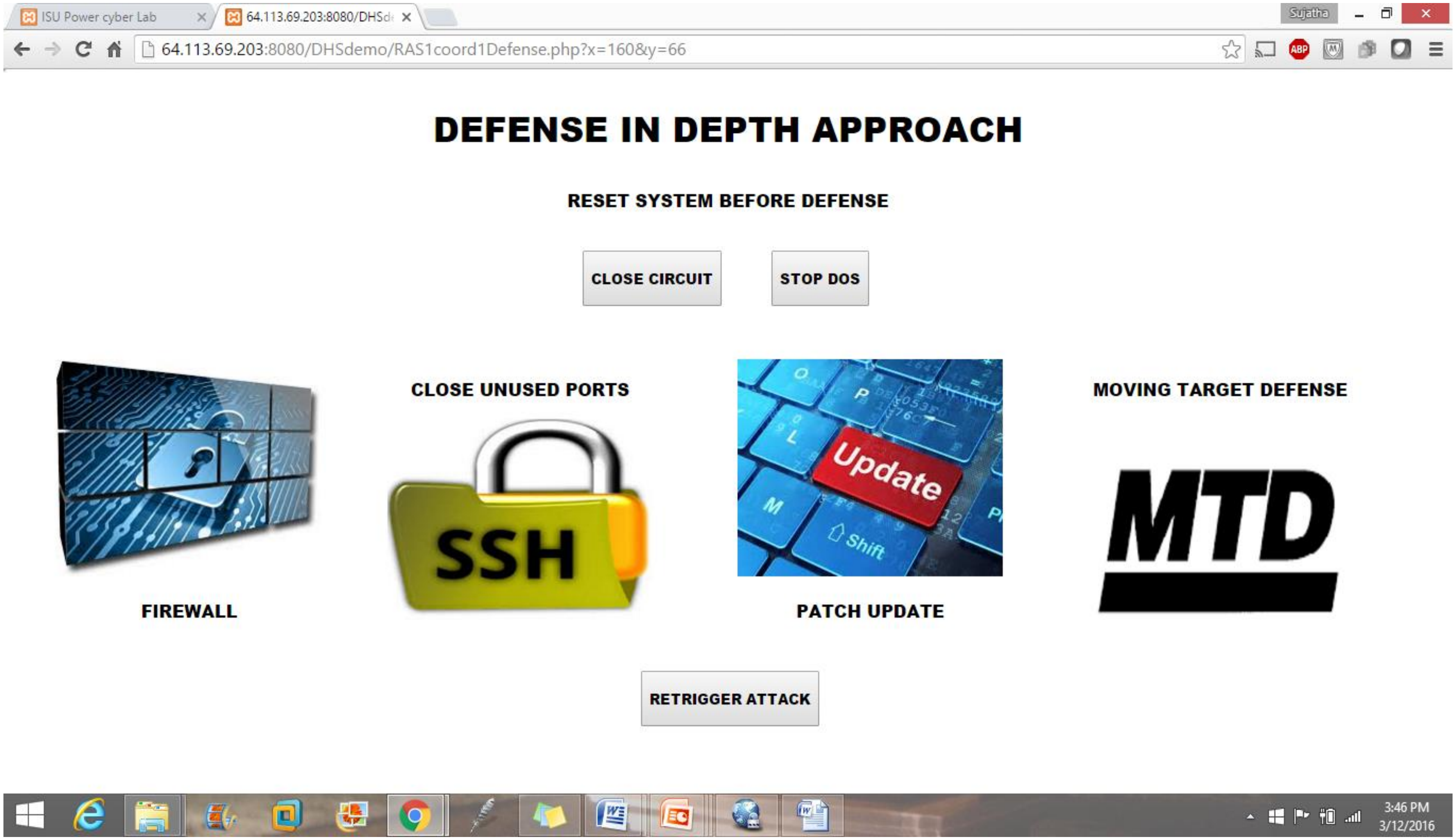
Idle	Connecting	Requesting	Downloading	Downloaded	Requested	Failed
					219460	

Step 9.8: The attacker now triggers the command injection attack which is the second step towards execution of successful coordinated attack. Button click triggers a python script in the backend which establishes socket connection to substation simulator and sends malicious DNP3 control packet to the substation. This Denial of service and command injection together cause cascading outage in the underlying power system model.

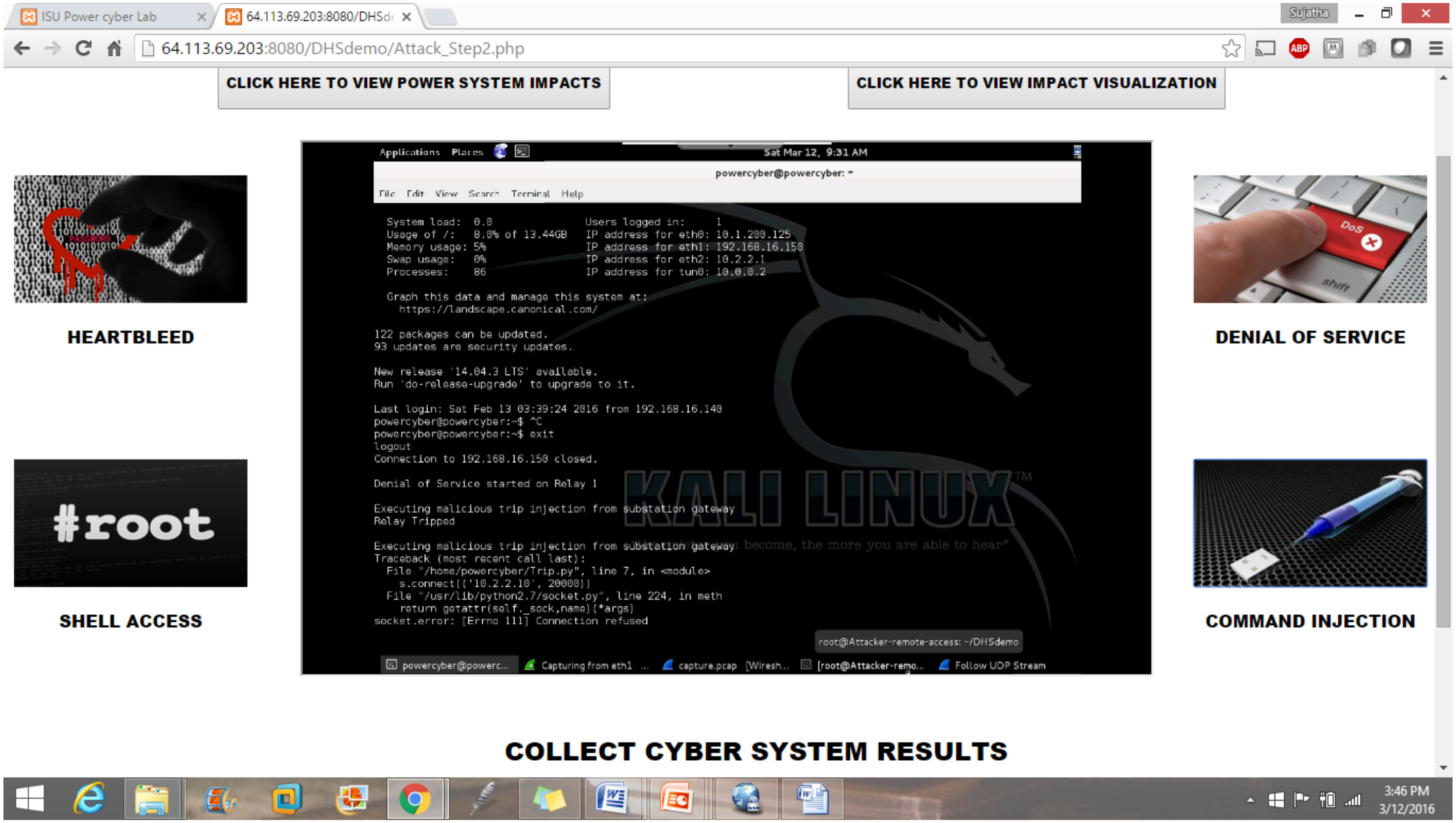


```
WARNING: server returned more data than it should - server is vulnerable!

Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

  System information as of Sat Feb 13 07:28:25 CST 2016

  System load:  0.0               Users logged in:     1
  Usage of /:   8.0% of 13.44GB   IP address for eth0: 10.1.200.125
  Memory usage: 5%                IP address for eth1: 192.168.16.150
  Swap usage:   0%                IP address for eth2: 10.2.2.1
  Processes:    86                IP address for tun0: 10.0.0.2

  Graph this data and manage this system at:
    https://landscape.canonical.com/

122 packages can be updated.
93 updates are security updates.

New release '14.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sat Feb 13 03:39:24 2016 from 192.168.16.140
powercyber@powercyber:~$ ^C
powercyber@powercyber:~$ exit
logout
Connection to 192.168.16.150 closed.

Denial of Service started on Relay 1

Executing malicious trip injection from substation gateway
Relay Tripped
```

Step 10: The Defense Instrumentation module provides basic defense options such as firewall configuration, closing unused ports, patching updates, etc.

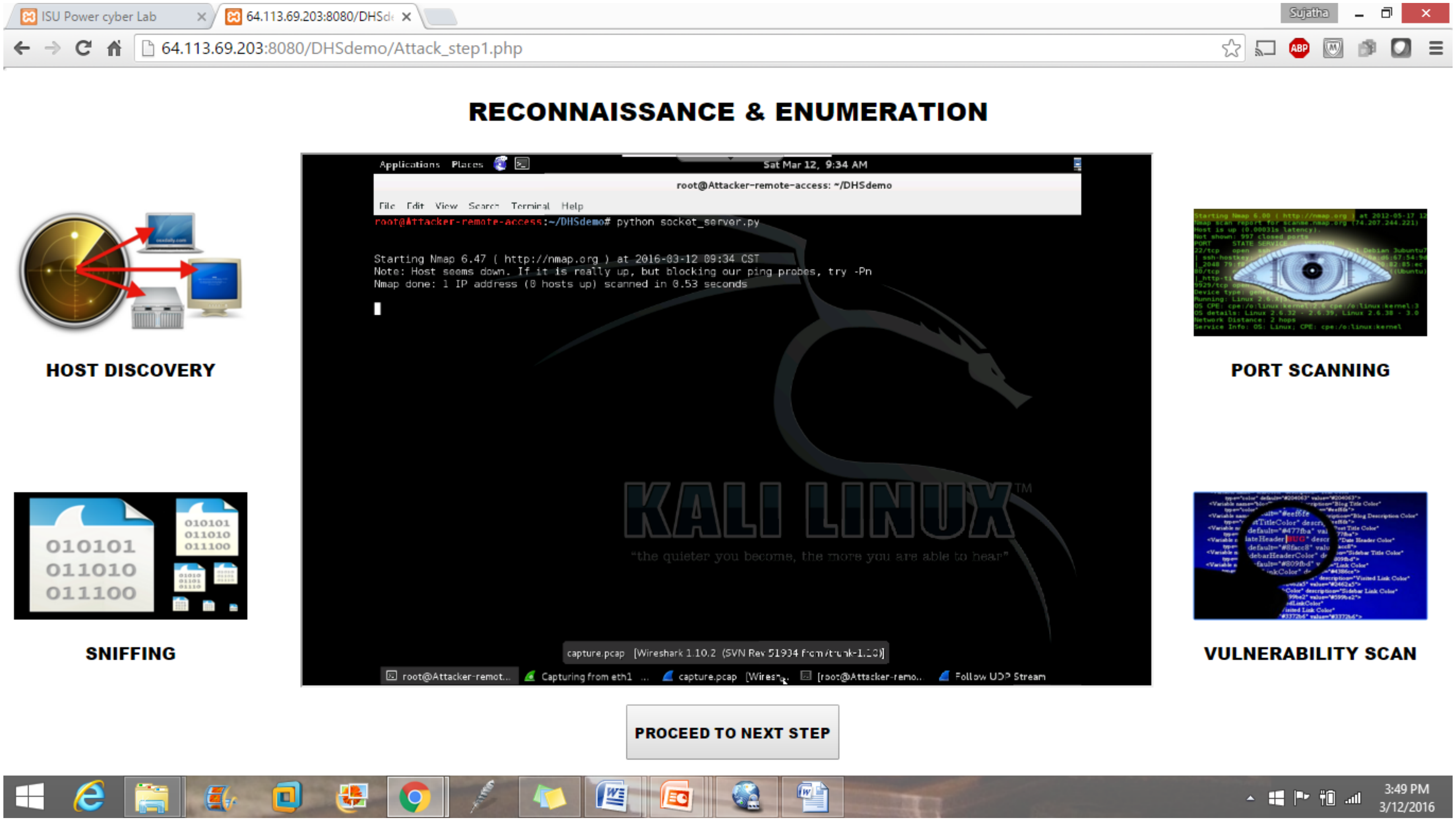


Step 10.1: SCADA network-flow based firewall implementation, blocks flow of DNP3 control commands to substation from hosts other than primary or secondary control centers. When, the attacker python script tries establishing socket connection to the substation on DNP3 port, the firewall blocks connections to port from non-control center hosts.



```
  System load:  0.0               Users logged in:     1
  Usage of /:   8.0% of 13.44GB   IP address for eth0: 10.1.200.125
  Memory usage: 5%                IP address for eth1: 192.168.16.150
  Swap usage:   0%                IP address for eth2: 10.2.2.1
  Processes:    86                IP address for tun0: 10.0.0.2

  Graph this data and manage this system at:
    https://landscape.canonical.com/

122 packages can be updated.
93 updates are security updates.

New release '14.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sat Feb 13 03:39:24 2016 from 192.168.16.140
powercyber@powercyber:~$ ^C
powercyber@powercyber:~$ exit
logout
Connection to 192.168.16.150 closed.

Denial of Service started on Relay 1

Executing malicious trip injection from substation gateway
Relay Tripped

Executing malicious trip injection from substation gateway
Traceback (most recent call last):
  File "/home/powercyber/Trip.py", line 7, in <module>
    s.connect(('10.2.2.10', 20000))
  File "/usr/lib/python2.7/socket.py", line 224, in meth
    return getattr(self._sock,name)(*args)
socket.error: [Errno 111] Connection refused
```

Step 10.2: Closing SSH port 22 on substation gateway interface facing wide-area network, prevents the attacker from penetrating into the substation internal network. Updating the OpenSSL library in the substation gateway patches Heart Bleed bug. This prevents the discovery and exploitation of this vulnerability.



RECONNAISSANCE & ENUMERATION

```
root@Attacker-remote-access:~/DHSdemo# python socket_server.py


Starting Nmap 6.47 ( http://nmap.org ) at 2016-03-12 09:34 CST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.53 seconds
```

CHAPTER 4

USER COMMUNITY ENGAGEMENT STUDIES

One of the most important goals of developing remote access framework was enabling access to a broader user community such as academia, research and industrial users interested in cyber security experimentation on cyber physical systems such as smart grid. This would allow enhancement and refinement of PowerCyber testbed features as well as remote access framework features going forward. This chapter will provide detailed descriptions about PowerCyber remote access framework user community engagement with use case studies.

4.1 Academic user engagement

4.1.1 Background

- **University of Minnesota – Duluth(UMND)**

As part of graduate level electrical engineering course EE5533 Grid: Resiliency, Efficiency & Technology offered by Dr. Desineni Subbaram Naidu, Minnesota Power Jack Rowe Endowed Chair, University of Minnesota, Duluth, PowerCyber testbed and remote access framework for PowerCyber were introduced to UMND students through guest lectures. A user manual explaining remote access framework usage was also provided to students. Access to remote access framework was made available to students interested in performing experimentation on PowerCyber testbed. In total, fourteen students from the course signed up for experimentation and used the PowerCyber remote access framework.

- **Iowa State University(ISU)**

As part of graduate level course CprE 539: Cyber Security for the Smart Grid offered by Dr. Manimaran Govindarasu, Mehl Professor and Associate Chair, Department of Electrical and

Computer Engineering, Iowa State University, the PowerCyber testbed and remote access framework for PowerCyber were introduced to ISU students. The students were asked to perform remote experimentation on PowerCyber testbed using the framework as part of course project. In total, the course had eight students with equal distribution power engineers and computer engineers.

4.1.2 Experimentation Overview

The main goal of the experimentation project was to allow students to characterize the impact of different types of cyber-attacks on different power system models using remote access framework to PowerCyber testbed. The students experimented different types of attack scenarios on 9 bus system model. The web interface presented a set of options for mapping the RAS in different positions onto the generators in the 9 bus system model. After compiling and loading the chosen power system model, the students were asked to note down pre-attack values such as generation level of generators G1, G2 and G3, overall system frequency, tie-line flows (active power) of all 6 transmission lines and bus voltages by referring to the power system run-time interface. The web interface also provided options for triggering different attack vectors such as command injection attacks, coordinated attack, Denial of service attack with handles for tweaking DOS throttles, etc. Upon successful execution of attacks, the students were asked to note down post-attack values from the power system run-time interface. The following scenarios were experimented by students to perform impact studies.

- **Scenario 1**

In scenario 1, the Remedial action scheme is mapped onto generator 2. The first attack, injects malicious command to the substation RTU at bus 7 to trip one of the physical relays involved in the RAS. In second attack, DoS attack on the RAS controller is triggered by setting DOS throttle to fastest and then malicious command is injected after approximately 10 seconds to the substation RTU at bus 7 to trip one of the physical relays involved in the RAS as depicted in Figure 4.1. This attack triggers a successful coordinated attack resulting in considerable drop in system frequency.

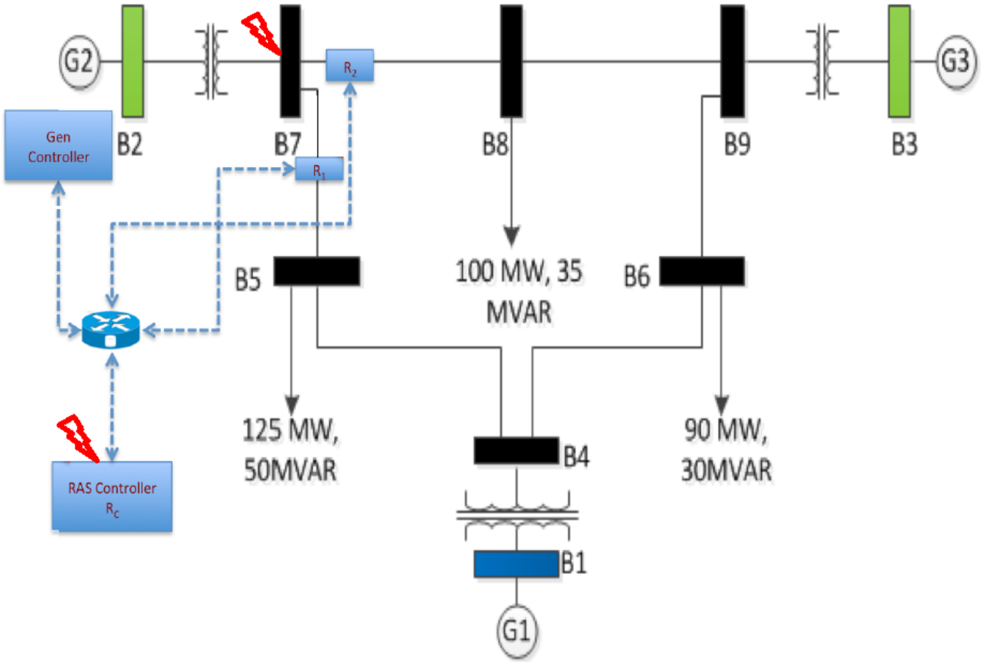


Figure 4.1 *RAS on G2 coordinated attack*

In third attack, DoS attack on the RAS controller is triggered by setting DOS throttle to slowest and then malicious command is injected after approximately 10 seconds to the substation RTU at bus 7 to trip one of the physical relays involved in the RAS. Due to slow DOS throttle, this attack results in unsuccessful coordinated attack creating impact similar to first attack.

- **Scenario 2**

In scenario1, the Remedial Action Scheme is mapped onto generator 1. The first attack, injects malicious command to the substation RTU at bus 4 to trip one of the physical relays involved in the RAS. In second attack, DoS attack on the RAS controller is triggered by setting DoS throttle to fastest and then malicious command is injected after approximately 10 seconds to the substation

RTU at bus 4 to trip one of the physical relays involved in the RAS as depicted in Figure 4.2. This attack triggers a successful coordinated attack resulting in considerable drop in system frequency.

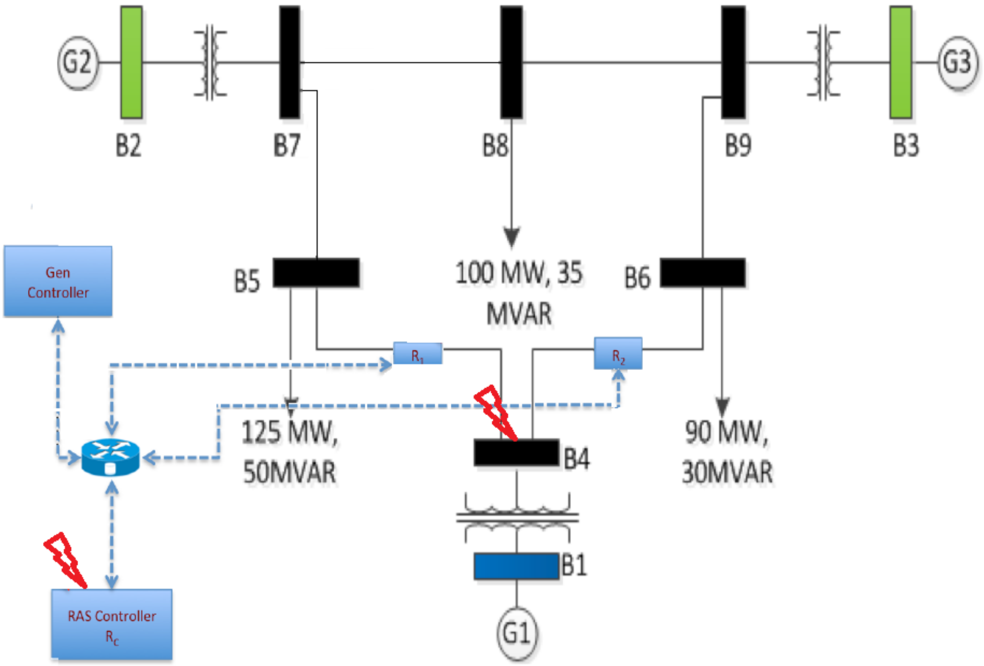


Figure 4.2 *RAS on G1 coordinated attack*

In third attack, DoS attack on the RAS controller is triggered by setting DoS throttle to slowest and then malicious command is injected after approximately 10 seconds to the substation RTU at bus 4 to trip one of the physical relays involved in the RAS. Due to slow DoS throttle, this attack results in unsuccessful coordinated attack creating impact similar to first attack.

- **Scenario 3**

In scenario1, the Remedial action scheme is mapped onto generator 3. The first attack, injects malicious command to the substation RTU at bus 9 to trip one of the physical relays involved in the RAS. In second attack, DoS attack on the RAS controller is triggered by setting DoS throttle to fastest and then malicious command is injected after approximately 10 seconds to the substation

RTU at bus 9 to trip one of the physical relays involved in the RAS as depicted in Figure 4.3. This attack triggers a successful coordinated attack resulting in considerable drop in system frequency.

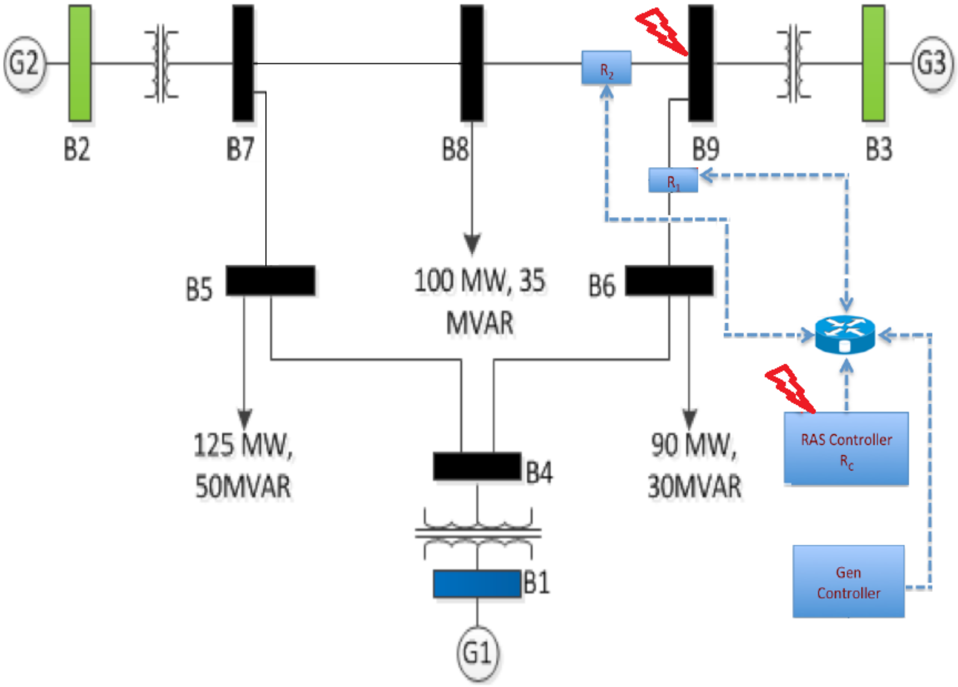


Figure 4.3 *RAS on G3 coordinated attack*

In third attack, DoS attack on the RAS controller is triggered by setting DoS throttle to slowest and then malicious command is injected after approximately 10 seconds to the substation RTU at bus 9 to trip one of the physical relays involved in the RAS. Due to slow DoS throttle, this attack results in unsuccessful coordinated attack creating impact similar to first attack.

Finally, the students were asked to compare pre-attack, post-attack values obtained in all three scenarios to identify the RAS position and type of attack which created maximum disturbance in the power system with reasoning.

4.1.3 User Survey & Evaluation

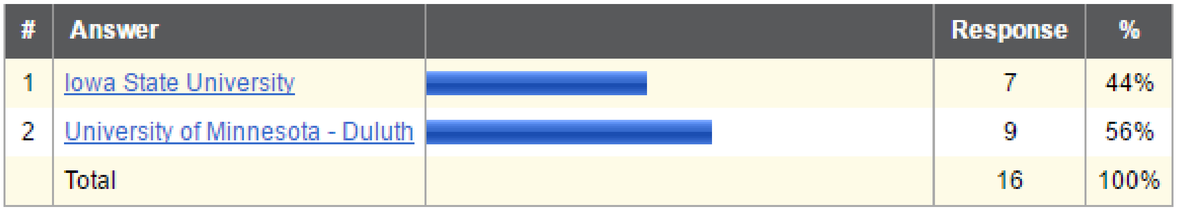
Upon successful completion of experimental project, the users were distributed a survey to help understand remote access framework usage experience and identify avenues for enhancing the framework for future users and returning users. The survey consisted of twelve questions in total which comprised of six ranking questions, three multiple choice questions and three text entry descriptive questions. The reminder of this section will provide details of the survey with corresponding results.

- **Question 1:**

  Select your University

  Responses:

Table 4.1 *University selection*



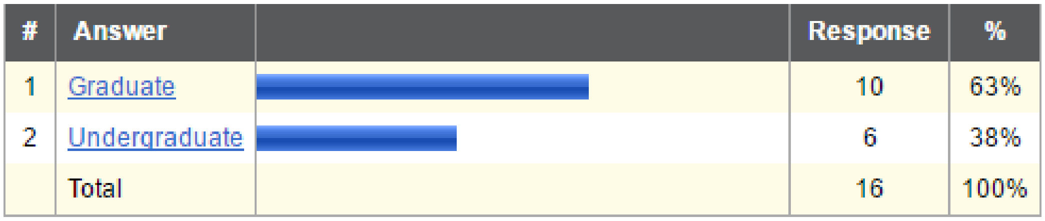
#	Answer		Response	%
1	Iowa State University		7	44%
2	University of Minnesota - Duluth		9	56%
	Total		16	100%

- **Question 2:**

  Please indicate level of education

  Responses:

Table 4.2 *Level of education*



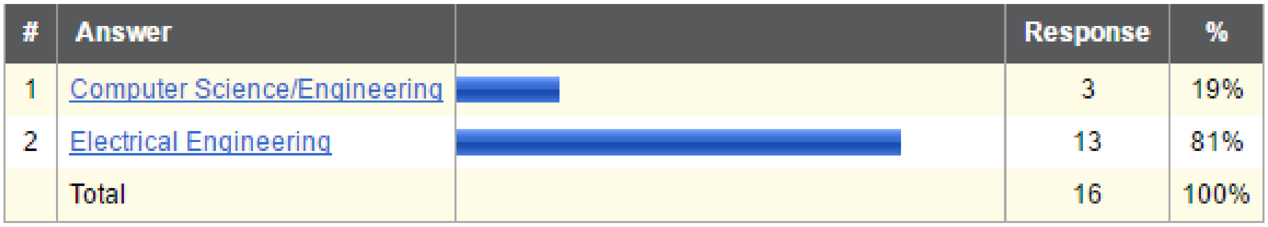
#	Answer		Response	%
1	Graduate		10	63%
2	Undergraduate		6	38%
	Total		16	100%

- **Question 3:**

Please indicate majors

Responses:

Table 4.3 *Majors selection*



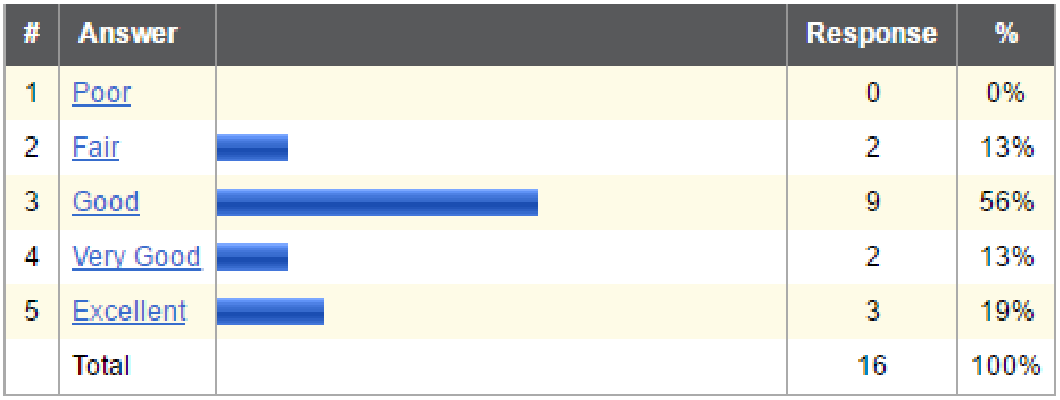
#	Answer		Response	%
1	Computer Science/Engineering		3	19%
2	Electrical Engineering		13	81%
	Total		16	100%

- **Question 4:**

Please indicate level of proficiency in cybersecurity concepts

Responses:

Table 4.4 *Cybersecurity proficiency*



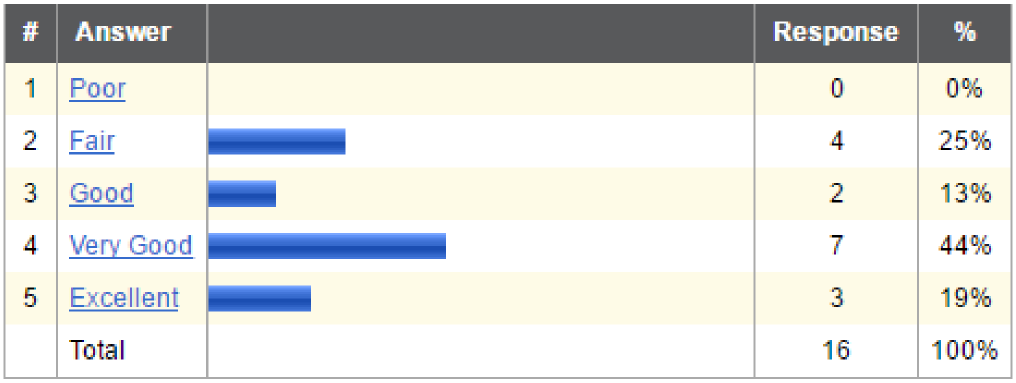
#	Answer		Response	%
1	Poor		0	0%
2	Fair		2	13%
3	Good		9	56%
4	Very Good		2	13%
5	Excellent		3	19%
	Total		16	100%

- **Question 5:**

Please indicate level of proficiency in power engineering concepts

Responses:

***Table 4.5** Power engineering proficiency*



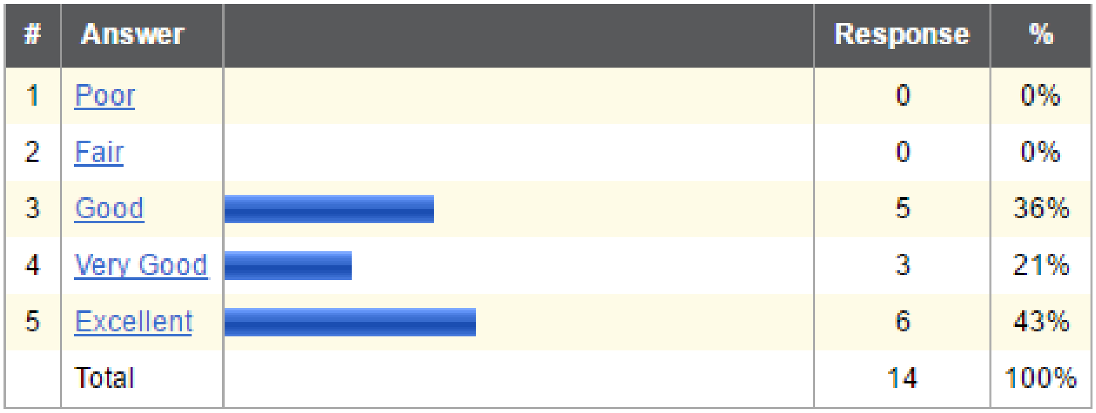
#	Answer		Response	%
1	Poor		0	0%
2	Fair		4	25%
3	Good		2	13%
4	Very Good		7	44%
5	Excellent		3	19%
	Total		16	100%

- **Question 6:**

Please rate the quality of instructions provided by the remote interface user manual

Responses:

***Table 4.6** User manual clarity*



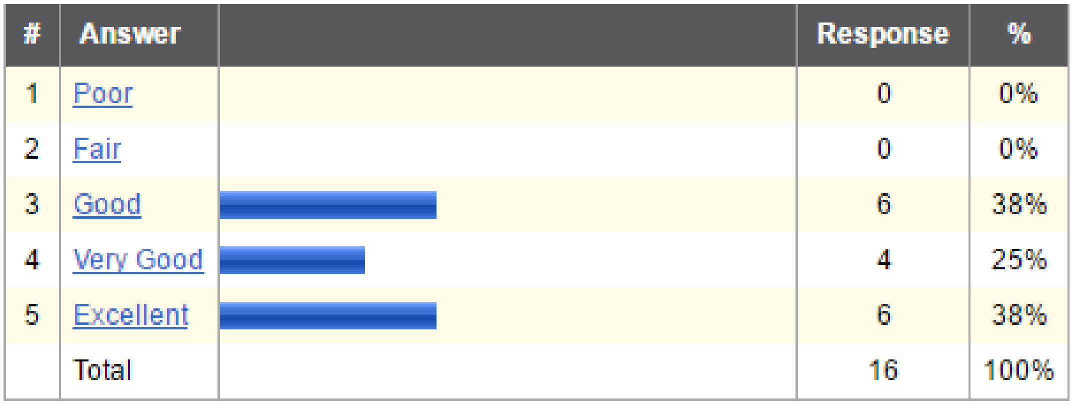
#	Answer		Response	%
1	Poor		0	0%
2	Fair		0	0%
3	Good		5	36%
4	Very Good		3	21%
5	Excellent		6	43%
	Total		14	100%

- **Question 7:**

Please rate clarity of instructions provided by the experimentation document

Responses:

Table 4.7 *Experiment documentation clarity*



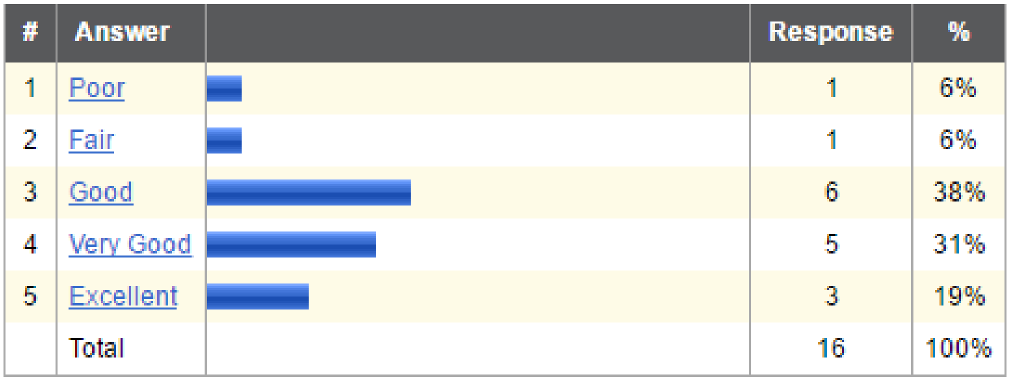
#	Answer		Response	%
1	Poor		0	0%
2	Fair		0	0%
3	Good		6	38%
4	Very Good		4	25%
5	Excellent		6	38%
	Total		16	100%

- **Question 8:**

Please rate ease of use of remote access framework in performing experimentation. Was the framework self-explanatory?

Responses:

Table 4.8 *Remote access framework – Ease of use*



#	Answer		Response	%
1	Poor		1	6%
2	Fair		1	6%
3	Good		6	38%
4	Very Good		5	31%
5	Excellent		3	19%
	Total		16	100%

- **Question 9:**

Please indicate improvisations which can be made to the remote access framework to enhance your usage experience

Responses:

Table 4.9 *Improvisation suggestions from users*

Text Response
It's fine just the way it is now.
We experienced server issues, but I am not sure how they could have been resolved.
Can't think of any
None
A better explanation of what's happening in the lab. At the moment, the user clicks a button and the grid has issues - there's not a whole lot of explanation of what's happening.
The experience has been excellent.
If somehow you can make the resetting possible for the remote user (without the help of in lab person) it would really help.
Better access
N/A
To be able to switch between RAS positions without having to go back to the homepage first.
We encountered some difficulty in executing the attack scenario, I hope it is being resolved by now.
I wish we did some more labs to get even better understanding
control and substation should be updated
It was fine.
According to me, the attacks can be made better visible using the UI.
Add something to allow for more experimentation and self-exploration of the systems.

- **Question 10:**

  Please indicate your takeaway from this experimentation

Responses:

Table 4.10 *Experimentation takeaway*

Text Response
The experiment let us know the power side impacts because of the cyber-attacks.
The cascading effects on the grid after a system disturbance.
was good
Learnt to perform different attacks on a cyber physical system
After this experience, I researched grid security and learned quite a bit about the security that's needed and the attacks that exist for it.
The experience has been excellent.
Well, I got a closer look what impact does a certain attack has on the grid.
Good
A better understanding of grid security
To give some insight as to how a cyber attack would be orchestrated so that such an attack might be stopped in the future.
The experiment was well designed and properly explained. It was easy to understand the difference in the impact of different attack scenario and thus value of a coordinated attack was highlighted. I was able to relate this with our course module and class discussions very much. It is good for a power engineer to find out research problems as in terms of placement of RAS, impact characterization etc.

Table 4.10 *(continued)*

I learned a lot practically.
good learning experience about cyber and power integration
The final project was a much more valuable learning tool that the remote interface.
I did the DOS attacks in the computer networks before but, the DOS attacks in the cyber lab made more sense and were very practical.
Having vulnerabilities in power grids can be devastating

- **Question 11:**

  If given an opportunity to reuse the testbed, please specify what kind of experimentation would you like to perform using PowerCyber remote access framework

  Responses:

Table 4.11 *Experimentation enhancement*

Text Response
Malware injection, Reverse TCP handling.
I honestly cannot say there is anything more I would include.
Defense
Simulation of larger power system models
I would like to watch the system while doing the attacks instead of switching platforms so I could watch any changes immediately.
Perhaps one more experiment with (previous) real-world cyber-attacks may be included.

Table 4.11 *(continued)*

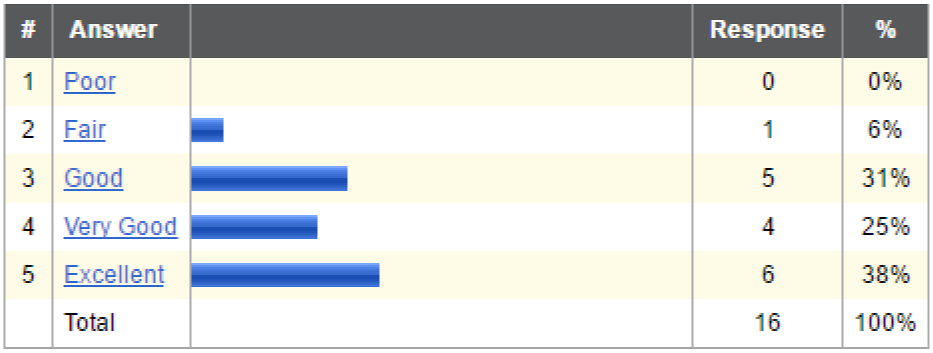
Something to determine/get access to the system (brute forcing password with rainbow tables, etc.). This would be a new direction for the lab
Coordinated
Nothing more than we did
I would like to do more variations of the DOS attack.
This experiment was good, if with time we increase the system size and variation in attack methods it would be more useful and good from learning point of view.
to know more about how to block bugs
malware based attack
N/A
I would experiment more on UDP attacks which are more effective and also would try to find out a way to identify and prevent UDP attacks.
The effects of attacking multiple generators at the same time

- **Question 12:**

  Please rate the overall quality of the experimentation and associated learning experience

  Responses:

Table 4.12 *Experimentation quality*



#	Answer		Response	%
1	Poor		0	0%
2	Fair		1	6%
3	Good		5	31%
4	Very Good		4	25%
5	Excellent		6	38%
	Total		16	100%

4.1.4 Testimonials

This section highlights few testimonials about the PowerCyber remote access framework.

"I completely realize that there has been lot of interest, effort and time put into the offering of guest lectures and working with students to conduct CPS security testbed for power grid experimentations via "remote access interface" with the Dept. of Electrical and Computer Engineering, Iowa State University (ISU). I want to express my sincere thanks and appreciation to both of you. Hopefully, the next time we offer, I will make sure all the students go through the lab experience. "

Dr. Desineni Subbaram Naidu

"Thanks again for allowing us to do this experiment, it was very informative! I am a very hands-on, visual type learner and this really helped clarify how the grid operates."

Maxwell Tesch, Student UMND

4.2 Industrial user engagement

4.2.1 Background

One of the most important use cases of PowerCyber testbed is providing controlled testing environments for evaluating and validating novel CPS security tools and technologies, thereby accelerating the transition of research to industrial practice. Symantec Corporation, an American technology company which develops security products and solutions to protect small, medium, and enterprise businesses from advanced threats, malware, and other cyber-attacks, expressed interest in utilizing PowerCyber testbed remotely for developing and validating their ICS, anomaly detection product in a close to realistic SCADA testbed such as the one provided by PowerCyber.

4.2.2 Product Overview

The Symantec product is a Java based solution which serves as a network based anomaly detection engine which learns all SCADA communication traffic in the control and substation networks to create a profiling of expected regular traffic flow in the SCADA environment. After successful profiling, the product actively segregates anomalous traffic from regular traffic.

4.2.3 Phase 1 Engagement (completed)

Initially, the engagement required capturing all possible SCADA traffic such as DNP3, IEC61850, etc. between control centers, substations and physical relays during normal operations and abnormal operations such as attack scenarios. For executing this requirement, an interface in the master network switch in PowerCyber testbed was made to listen and capture all traffic in promiscuous traffic. The regular traffic was captured continuously for four hours with attack traffic injected in regular intervals. This capture was used by Symantec to develop logic for their anomaly detection engine.

4.2.4 Phase 2 Engagement (ongoing)

Second phase of engagement required integration of Symantec anomaly detection product into PowerCyber testbed for validating the detection capabilities of the product.

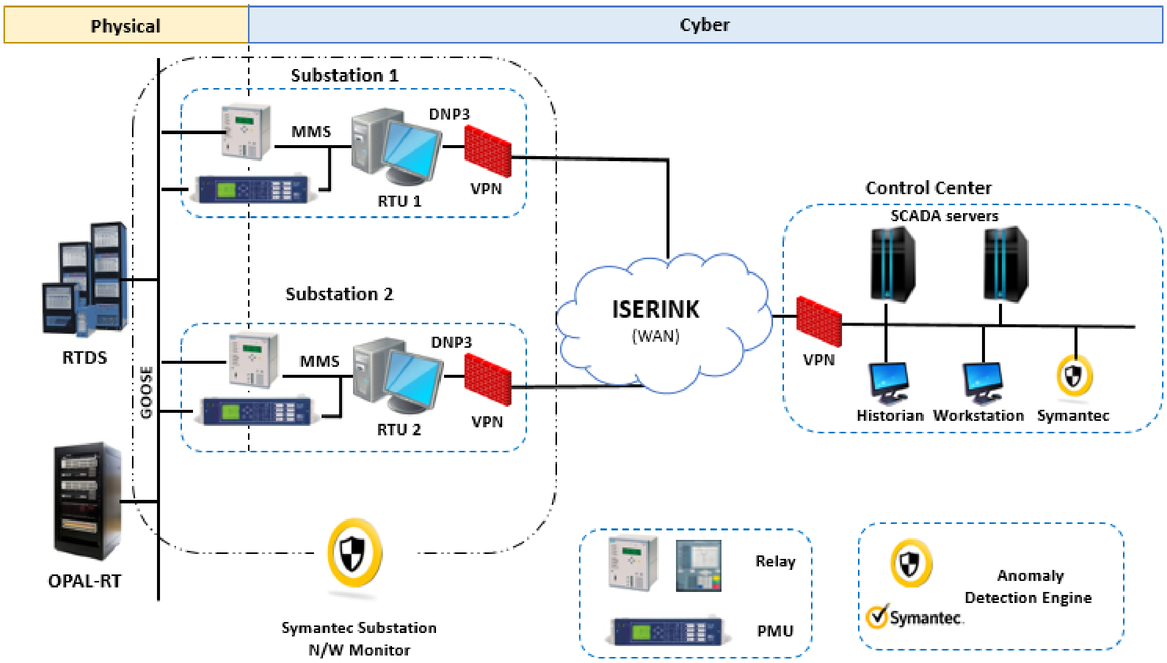


Figure 4.4 *Symantec Deployment topology*

For integration of the product, the Symantec collaborator was introduced to PowerCyber testbed architecture, remote access framework, remote access user manual, attack vectors and other relevant documentation along with demonstration sessions to provide an insight of the PowerCyber testbed capabilities and identify use cases relevant to Symantec. For building appropriate integration topology, many on call meetings were held to gather requirements which satisfies Symantec use cases. Consecutively, a topology for deploying Symantec product was developed and the product is currently being installed in PowerCyber testbed. Figure 4.4 captures the deployment topology of Symantec anomaly detection product in PowerCyber testbed.

Upon successful integration and execution of test cases in future, the Symantec anomaly detection product will be trained to profile normal and anomalous SCADA traffic using network traffic monitoring performed in PowerCyber testbed.

CHAPTER 5

CONCLUSION & FUTURE WORK

5.1 Conclusion

The need to enable remote access to CPS security testbeds is quite compelling in the context of accelerating research and development by enabling access to a broader research/ academic community. Existing research efforts on enabling remote access have been successful in providing infrastructure for regular cyber security experimentation [16]. However, they have several shortcomings when extended to CPS environments with a heterogeneous mix of simulated, emulated and physical components. There are promising ongoing efforts made to provide scalable, multi-user remote access CPS security testbeds for researchers and this thesis describes the architecture and capabilities of PowerCyber remote access framework for cyber physical security experimentation on Smart Grid applications, which is one such efforts. Though the implementation architecture described in this thesis is far from being perfect or comprehensive, it provides a solid foundation for further R&D in enabling remote experimentation and is also being actively refined. The thesis also articulates user community engagements and various engineering challenges in creating remote access testbeds along with some potential solutions that would serve to educate a broader research community. Due to some of the practical challenges faced, only a limited set of template-based scenarios have been implemented completely at this time.

5.2 Future Work

In order to broaden the scope and features of PowerCyber remote access framework, the following activities would be performed:

5.2.1 Developing a library of models, attack vectors

Additional power system models would be developed along with template attack scenarios for commonly used WAMPAC applications such as State Estimation, Automatic Generation Control, etc.,

5.2.2 Expanding user community

A user community would be developed for PowerCyber remote access framework and existing user community engagements will also be expanded by providing access to a broader research, academic and industrial community. This would also enable the refinement of the testbed's features going forward.

5.2.3 Improving the programmability

The programmability of the remote access framework would be improved by allowing more user customization of power system models and experimental scenarios, dynamic configuration/mapping of hardware devices, custom attack vectors, and defense measures.

5.2.4 Federation

The remote access framework would be expanded to address federated testbed resources to provide increased scalability, and multi-user experimental capabilities.

REFERENCES

[1] S. Baker, S. Waterman, and G. Ivanov. In the Crossfire: Critical Infrastructure in the Age of Cyber War. McAfee, 2009.

[2] N. Falliere, L. Murchu, and E. Chien. W32.Stuxnet Dossier, Version 1.3. Symantec, November 2010.

[3] Jointly-Commissioned Summary Report of the North American Electric Reliability Corporation and the U.S. Department of Energy. High-Impact, Low-Frequency Event Risk to the North American Bulk Power System, Nov. 2009.

[4] U.S. Government Accountability Office (GAO). Critical Infrastructure Protection Report, May 2004.

[5] U.S. Government Accountability Office (GAO). GAO-14-125: More Comprehensive Planning Would Enhance the Cybersecurity of Public Safety Entities' Emerging Technology, Jan 2014.

[6] National Institute of Standards and Technology workshop report on Foundations for Innovation in Cyber-Physical Systems, Jan. 2013.

[7] J. F. Keith Stouffer and K. Kent, "Guide to supervisory control and data acquisition (SCADA) and industrial control systems security—Recommendations of the national institute of standards and technology," Special Publication 800-82, Initial Public Draft Sept. 2006.

[8] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," Proc. IEEE, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[9] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," Smart Grid, IEEE Transactions on, vol. 4, no. 2, pp. 847–855, 2013.

[10] Industrial Control Systems (ICS) Computer Emergency Response Team (CERT). Advisory (ICSA-12-102-05): Siemens Scalance S Multiple Security Vulnerabilities, May 2013. URL: https://ics-cert.uscert.gov/advisories/ICSA-12-102-05.

[11] A. Ashok, P. Wang, M. Brown, and M. Govindarasu. Experimental evaluation of cyberattacks on automatic generation control using a cps security testbed. In Power Energy Society General Meeting, 2015 IEEE, pages 1–5, July 2015.

[12] Govindarasu, M. and Benzel, T. and Hahn, A. Smart Energy CPS – CPS Security Testbed Federation for Coordinated Cyber Attack/Defense Experimentation, June 2014. URL: http://smartamerica.org/news/iowastate-researchers-to-demonstrate-cyber-physical-security-testbed-forpower-grid-at-smartamerica-challenge-expo/.

[13] Iowa State University. Iowa State awarded NSF Global City Teams Challenge project, September 2015. URL:http://news.engineering.iastate.edu/2015/09/16/iowa-state-awardednsf-global-city-teams-challenge-project/.

[14] Iowa State University. ISERINK platform for Cyber Defense Competitions, 2015. URL: http://www.iserink.org/

[15] North American Electric Reliability Corporation (NERC). Training Workshop: CyDECS: Cyber Attack-Defense Training Exercise for Power Grid - Iowa State, October 2015. URL: http://www.nerc.com/pa/CI/CIPOutreach/Pages/GridSecCon-Training-Tracks.aspx.

[16] J. Mirkovic, T. Benzel, T. Faber, R. Braden, J. Wroclawski, and S. Schwab. The DETER project: Advancing the science of cyber security experimentation and test (https://www.isi.deterlab.net/index.php3). In Technologies for Homeland Security (HST), 2010 IEEE International Conference, 2010.

[17] Pacific Northwest National Laboratory (PNNL). Power Networking, Equipment and Technology (powerNET) Testbed, 2015.

[18] Idaho National Laboratory (INL). National SCADA Test Bed: Fact Sheet, 2009.

[19] Michael J. McDonald, Gregory N. Conrad, Travis C. Service, Regis H. Cassidy. SAND2008-5954: Cyber Effects Analysis Using VCSE, Promoting Control System Reliability. Sandia National Laboratories, September 2008.

[20] David C. Bergman, Dong Jin, David M. Nicol, Tim Yardley. The Virtual Power System Testbed and Inter-Testbed Integration. 2nd Workshop on Cyber Security Experimentation and Test, August 2009.

[21] B. Reaves and T. Morris. An open virtual testbed for industrial control system security research. International Journal of Information Security, 2012.

[22] J. Hong, S.-S. Wu, A. Stefano, A. Fshosha, C.-C. Liu, P. Gladyshev, and M. Govindarasu. An intrusion and defense testbed in a cyber-power system environment. In Power and Energy Society General Meeting, 2011 IEEE, July 2011.

[23] S. Biswas, F. Shariatzadeh, R. Beckstrom, and A. Srivastava. Real time testing and validation of smart grid devices and algorithms. In Power and Energy Society General Meeting (PES), 2013 IEEE, July 2013.

[24] National Institute of Standards and Technology, Cyber-Physical Systems Homepage URL: http://www.nist.gov/cps/

[25] Smart Grid Overview: National Renewable Energy Laboratory Director for Energy Systems URL: http://energy.gov/sites/prod/files/2013/10/f4/fupwg_fall12_kroposki.pdf

[26] Aditya Ashok , Adam Hahn, Manimaran Govindarasu. Cyber-Physical security of Wide-Area Monitoring, Protection and Control in a smart grid environment. Journal of Advanced Research, July 2014

[27] Adam Hahn. Cyber Security of the smart grid: Attack exposure analysis, detection algorithms, and testbed evaluation – Iowa State University Doctoral dissertation

URL: http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=4105&context=etd

[28] Terzija V, Valverde G, Cai D, Regulski P, Madani V, Fitch J, et al. Wide-area monitoring, protection, and control of future electric power networks. Proc IEEE 2011; 99(1):80–93

[29] National Institute of Standards and Technology: “Guide to Industrial Control Systems(ICS) Security” URL: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

[30] National Renewable Energy Laboratory’s: Secure Distribution Grid Management (DGM) testbed URL: http://www.nrel.gov/esif/

[31] Analysis of the Cyber Attack on the Ukrainian Power Grid by E-ISAC & SANS. URL: http://www.nerc.com/pa/CI/ESISAC/Documents/EISAC_SANS_Ukraine_DUC_18Mar2016.pdf

[32] Vital Infrastructure, NetworKs, Information and Control System ManaGement (VIKING) summary results by European Community 7th Framework Program URL: https://www.kth.se/polopoly_fs/1.407987!/Menu/general/columncontent/attachment/Final%20Project%20Report_WEB%20version.pdf