ISEStorm

In coordination with the Information Assurance Center and ISU Information Technology Services

Steff Bisinger | Kristin Clemens | Sophia Preston | Chris Read | Megan Solleveld

Advisor Dr. Doug Jacobson

ISEStorm

Project Plan

Senior Design Group: May1638

Project Plan > Problem Statement

- Setup
  - Responsibility for the ISU network and services is spread across multiple disparate ITS teams
- Scenario
  - Significant events occur, resulting in network or service compromises
- Problem
  - Progress toward recovery is severely impeded due to limited knowledge-share of ITS members

Problem Statement

Solution?

ISEStorm provides a way for ITS to train employees to respond as a team!

Project Plan > Important Terms

- Tabletop Exercise
  - A discussion among team members regarding their roles during an emergency
  - Typically led by a facilitator who guides the team through one or more operations
  - Also referred to as a **Game**
- Operation
  - A set of Events
- Event
  - An isolated incident that results in a specific problem which compromises the network or services
- ISERink
  - A virtual laboratory environment that allows hands-on activities focused on networking, cyber security, and penetration testing

Project Plan > Important Terms

- White Team
  - The group running the Game, providing support
- Blue Team
  - The users in the Game who are trying to keep services running or to bring them back online
- Red Team
  - The group of computers attacking the Blue Team's network in the Game
- Player
  - Anyone participating in the Game
  - In most cases, referencing a member of the Blue Team

Project Plan > Key Functional Requirements

- ISEStorm Web Application
  - Secure login, logout, and system access
  - Creation, modification, and execution of Events and Operations
  - Assignment of Events to Operations
- ISEStorm Back-End
  - Ability to model ISU infrastructure
  - Ability to modify and append infrastructure

Project Plan > Key Nonfunctional Requirements

- Extensibility
  - Modular design for “plug and play” introduction of new Events to the system
- Reusability
  - Can be adapted for use beyond ISU
- Scalability
  - Should be able to handle incrementally greater usage

Facts, Assumptions, and Constraints

- ISEStorm will exist in an isolated environment while still maintaining limited access to the public internet
- ISEStorm will not have access to any real data and information stored on university systems
- Events and operations may be designed in part by ITS or other future users of ISEStorm
- Any authentication system used will need to be approved (and possibly designed) by ITS and future users for their own use

Project Plan > Potential Risks & Mitigation

- Risks
  - Part of the ISEStorm network is public-facing
  - ISEStorm network could become susceptible to outside attackers
  - If outside attackers go undetected on the ISEStorm network, they would have a blueprint for the real Iowa State network
- Mitigation
  - ISEStorm networks are protected with complex passwords and have a 3600 second timeout after 10 incorrect attempts to gain access
  - Disabled root SSH login to ESXi
  - Attackers cannot directly access the real Iowa State network from ISEStorm's network

Project Plan > Resource / Cost Estimate

- The server being used has been repurposed from the ISEAGE Lab
- ITS has discussed providing servers for future expansion of the project

Cost:

$0.00

ISEStorm

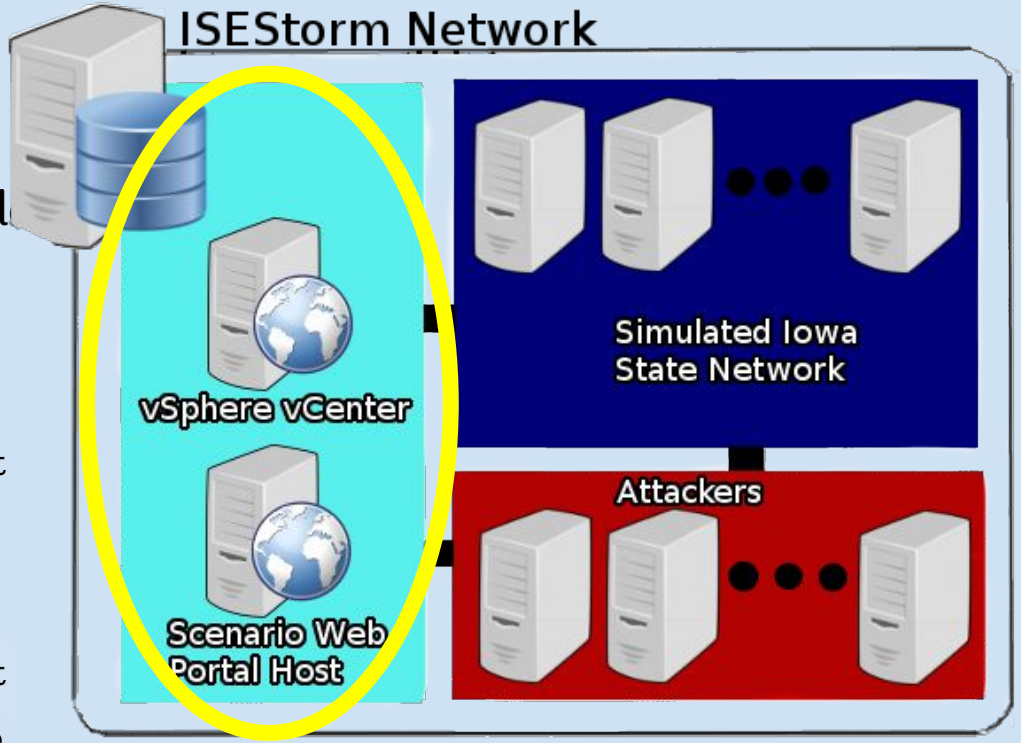
System Design

Senior Design Group: May1638

System Design > Functional Decomposition

"White Net"

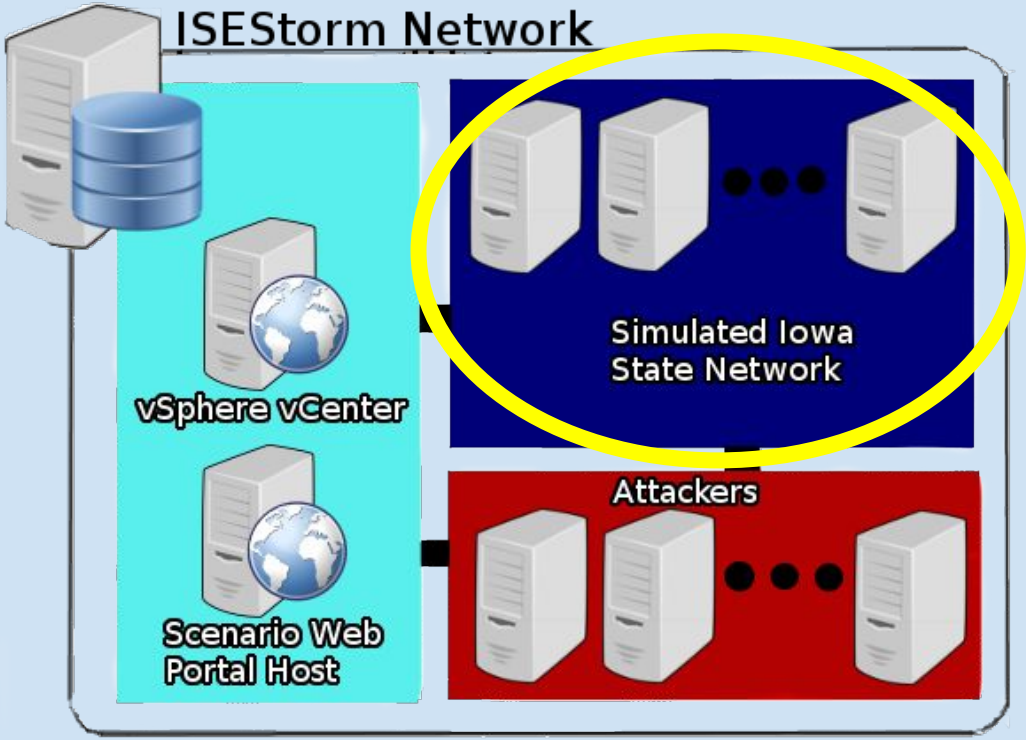
- Manages other servers; ad
  hosts
- Operation Web Portal
  - Contains user-defined Event scripts to control threats on the Red Net
  - Contains user-defined Event scripts to break areas of the Blue Net



System Design > Functional Decomposition

“Blue Net”

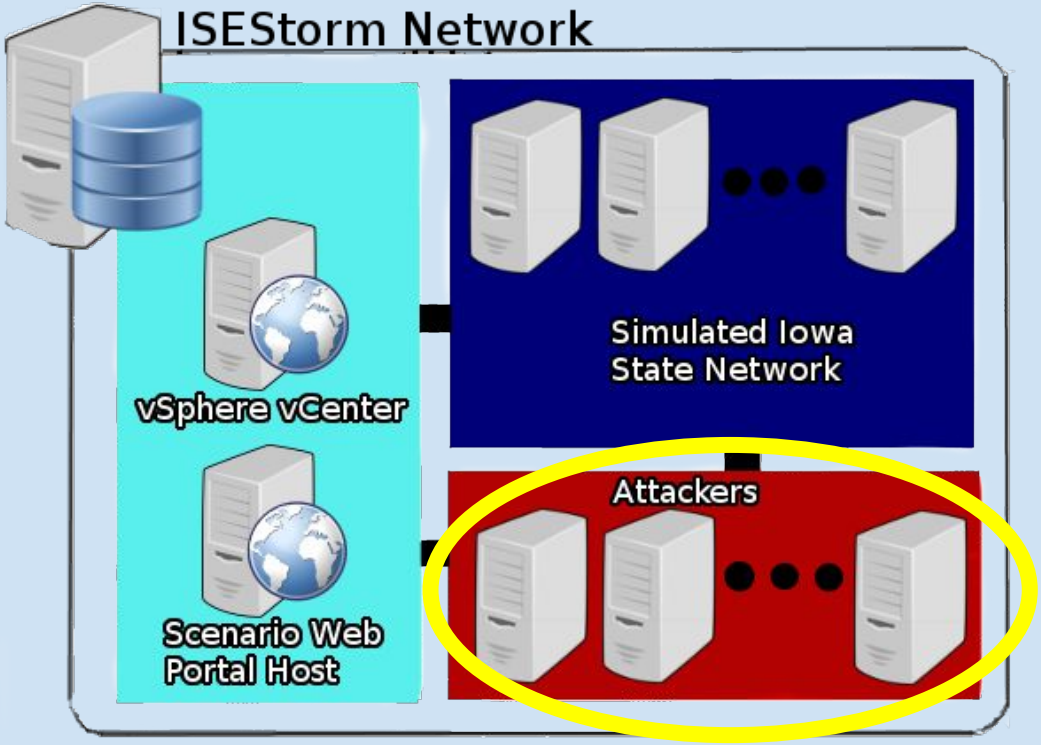
- Controlled using scripts from the White Net
- Acts as the game board
- Players access the game by connecting securely to this network from their workstations



System Design > Functional Decomposition

“Red Net”

- Controlled by the Operation Web Portal via Event scripts
- Automated attacks sent against the Blue network from these servers



System Design > Challenges: Hardware

- Originally planned to use a decommissioned HP C7000 bladesystem provided by ITS
- Ran into multiple problems
  - No internal storage
  - Were not able to obtain external storage that would work
  - No drivers for ESXi 6.0

http://www8.hp.com/us/en/products/enclosures/product-detail.html?oid=1844065

System Design > Hardware

Currently using a single Dell R610

System Design > Software

- Django web application written in Python that allows the White Team to interact with the virtualized network via scripts
- Web App provides the ability to
  - create new Events and upload scripts for them
  - map Events to new Operations
  - simulate Events by running their ‘action’ scripts on the virtualized network
  - edit and delete Operations and Events

System Design > Software

- ESXi and VMware vSphere Client to create and manage the virtualized systems
- VMware vCenter Server and Web Client
- VMware PowerCLI
- MobaSSH

System Design > Software

- ISERink
  - Encapsulates the entire ISEStorm Game environment
  - Prevents students and attackers from accessing the virtualized network
- ISEFlow to control network traffic
  - Written by Dr. Doug Jacobson
  - Managed through config files

System Design > Challenges: Software

- Mapping Events to Operations
  - Originally, a list field of foreign keys in Operation
  - Django models do not allow this
  - **Solution:** Instead, created a new model EOMap that handles this
- Running Event actions
  - Originally, run actions as python scripts or similar on ISEStorm web server
  - Extra code for us to write
  - Web server is not the right tool for the job
  - **Solution:** Use VMWare PowerCLI on the vCenter server

System Design > Testing

- Behavior Driven Development and Testing (Benno Rice, et al.)
  - "… an agile software development technique that encourages collaboration between developers, QA and non-technical or business participants in a software project."
  - Establishing the goals of different stakeholders required for a vision to be implemented
  - Drawing out features which will achieve those goals using feature injection
  - Using examples to describe the behavior of the application, or of units of code
  - Automating those examples to provide quick feedback and regression testing

System Design > Testing

```
Feature: Fight or flight
  In order to increase the ninja survival rate,
  As a ninja commander
  I want my ninjas to decide whether to take on an
  opponent based on their skill levels

  Scenario: Weaker opponent
    Given the ninja has a third level black-belt
     When attacked by a samurai
     Then the ninja should engage the opponent

  Scenario: Stronger opponent
    Given the ninja has a third level black-belt
     When attacked by Chuck Norris
     Then the ninja should run for his life
```

System Design > Testing

Feature

In order to ensure uniqueness of events
As a user adding a new event
I want ISEStorm to prevent me from adding an event
with the same name as an existing event

Scenario

Event already exists
Given an event exists with a certain Name
When a user tries to add a new Event with the same Name
Then ISEStorm should prevent the new Event from being created
And ISEStorm should prompt the user to choose a different Name

- Each step is encoded and run separately, promoting reuse
- If any step fails, then that entire test scenario fails

Demo

ISEStorm > Recap

- Worked with ITS and Dr. Jacobson to determine the scope and requirements of the project
- Implemented primary behaviors of the web application
- Developed method of running scripts through the web application to carry out attacks on the Blue Network
  - Shut off the power to a server
  - Launch exploitation tools (e.g. Metasploit)
  - Generate large amounts of network traffic

ISEStorm > What Next?

- In the near future…
  - UI showing status of VMs following the running of a script
  - Feedback on result of running script
  - Virtualize the Iowa State website

- Eventually…
  - Statewide adoption of ISEStorm as basis for expanded tabletop games

Questions?