NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

LEARNING OBJECTIVE BASED DEVELOPMENT OF CYBERCIEGE INSTRUCTIONAL VIDEO GAME SCENARIOS

by

Terrel J. Richardson Jr.

June 2021

Thesis Advisor: Michael F. Thompson
Co-Advisor: Cynthia E. Irvine

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2021	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE LEARNING OBJECTIVE BASED DEVELOPMENT OF CYBERCIEGE INSTRUCTIONAL VIDEO GAME SCENARIOS	**5. FUNDING NUMBERS**
6. AUTHOR(S) Terrel J. Richardson Jr.	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Network security analysis has evolved as cyber threats have grown and adapted to new technologies and protocols. With the spread of networked technology, the need for network security knowledge has become more vital to keep networks secure and resilient. CyberCIEGE is a network construction and resource management simulation platform designed to educate users ranging from high school students to Department of Defense personnel on network security practices. One challenge to the effectiveness of CyberCIEGE is that its existing embedded questions and feedback lacked the perspective of an experienced educator and may not be responsive to the student's understanding of the material. This may inhibit feedback intended to help students overcome learning obstacles encountered during its use.

This work analyzed and revised two related CyberCIEGE scenarios with a goal of ensuring the learning objectives are met through the use of embedded assessments and help tips at key points in the scenarios. An objective has been to develop a process with which scenario designers can review a scenario to identify obstacles players may encounter and how they can be overcome. The assessment-enhanced scenarios are intended to serve as examples of how to analyze and adapt scenarios to provide effective dynamic feedback.

14. SUBJECT TERMS CyberCIEGE, learning objectives, dynamic assessment, network security education, scenarios	**15. NUMBER OF PAGES** 97
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

LEARNING OBJECTIVE BASED DEVELOPMENT OF CYBERCIEGE INSTRUCTIONAL VIDEO GAME SCENARIOS

Terrel J. Richardson Jr.
Lieutenant, United States Navy
BA, Brigham Young University, 2009
MA, University of Arizona, 2010

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
June 2021

Approved by: Michael F. Thompson
Advisor

Cynthia E. Irvine
Co-Advisor

Gurminder Singh
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Network security analysis has evolved as cyber threats have grown and adapted to new technologies and protocols. With the spread of networked technology, the need for network security knowledge has become more vital to keep networks secure and resilient. CyberCIEGE is a network construction and resource management simulation platform designed to educate users ranging from high school students to Department of Defense personnel on network security practices. One challenge to the effectiveness of CyberCIEGE is that its existing embedded questions and feedback lacked the perspective of an experienced educator and may not be responsive to the student's understanding of the material. This may inhibit feedback intended to help students overcome learning obstacles encountered during its use.

This work analyzed and revised two related CyberCIEGE scenarios with a goal of ensuring the learning objectives are met through the use of embedded assessments and help tips at key points in the scenarios. An objective has been to develop a process with which scenario designers can review a scenario to identify obstacles players may encounter and how they can be overcome. The assessment-enhanced scenarios are intended to serve as examples of how to analyze and adapt scenarios to provide effective dynamic feedback.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ACRONYMS AND ABBREVIATIONS

ACL	Access Control List
DMZ	Demilitarized Zone
LAN	Local Area Network
LO	Learning Obstacle
MO	Mechanics Obstacle
PCA	Professional Croquette Association
SDL	Scenario Definition Language
SDT	Scenario Development Tool
SSH	Secure Shell Protocol

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I wish to express my gratitude to Michael Thompson and Professor Cynthia Irvine for their guidance and mentorship throughout this thesis process. Their support, patience and feedback were instrumental to the completion of this research, and I wish them continued success as they build upon this research and other aspects of the CyberCIEGE video game.

I also wish to thank my program officer, LCDR Eric Regnier, who supported my family and me through all the twists and turns that my education took during the two years I was at Naval Postgraduate School.

Finally, this could not have been possible without my wife, Jennifer, who sacrifices so much for our family. During my time at NPS, Jenn never stopped working to take care of our family and to allow me the time to work and concentrate on my studies. She ended up taking on the additional role of educator to three of our children during the pandemic of 2020, taught preschool for two more of our kids, and gave birth to our sixth child. Her never-ending drive never ceases to amaze me, and I am grateful for her being by my side.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

Keeping networks safe from malicious attacks and maintaining resiliency of the network requires secure and up-to-date network security systems and individuals who have been trained to make them work. Originally, this was done by qualified network security system administrators, but small networks, such as home networks that may include Internet-of-Things devices, are pervasive. These networks may include equipment through which users access enterprise-level systems. Thus, network security now must be understood by those who wish to keep their networks safe. CyberCIEGE was developed at the Naval Postgraduate School with the intent of teaching network security basics to average users as well as to those going into network and computer security and to support instruction on more advanced topics, such as public key infrastructure and virtual private networks. CyberCIEGE is used as a training and education tool by U.S. government agencies and by education institutions from high school to university level.

Computer and network security education faces the challenge of teaching concepts along with their practical application. There are very few teaching environments that allow students to experiment with abstract concepts and make mistakes, both of which are essential to learning, without harming an actual system. CyberCIEGE is a simulation that provides students with the ability to construct information technology networks and manage resources through different scenarios. The scenarios build on each other and confront the student with new challenges that force the student to identify vulnerabilities and secure the network with physical systems, software, encryption, access controls, and procedural policies.

CyberCIEGE is designed to allow new scenarios to be built based on the needs of the educator. The scenarios take the student through a series of phases, each having a set of objectives requiring the student to have made appropriate choices. By the time the student completes the final phase of a scenario, we expect they have met the scenario's learning objectives (i.e., the student understands and is able to apply selected cybersecurity concepts.)

CyberCIEGE scenarios may include true-false and multiple-choice questions for two distinct purposes: "quiz questions to assess student knowledge following scenario phases and "guide questions" to help the student overcome obstacles using leading questions. The focus of this research is the use of guide questions and other dynamic feedback to help overcome obstacles a player may experience during gameplay. This research will also develop methods to identify the student's understanding of the material to dynamically provide feedback to help ensure the learning objectives are met by correct completion of the scenarios.

My hypothesis is that analysis of CyberCIEGE game state and the student's responses to leading questions can provide an assessment of the student's understanding of currently available choices in the context of scenario learning objectives. That assessment can then be used to dynamically provide feedback to help the student understand consequences of their choices. The intent is to increase the overall effectiveness of the education gained from playing CyberCIEGE. There are two types of obstacles that a player may experience during gameplay that can prevent the player from completing the phase or achieving the learning objectives: understanding of game mechanics and challenges in conceptual understanding. The game mechanics barrier may occur when the player understands the concept being evaluated but does not know how to implement that concept in the game. The conceptual understanding problem involves the concept itself; the player does not understand the concept necessary to successfully complete that part of the scenario. The revisions we propose to two selected scenarios will serve to overcome these barriers. If assessment and feedback we added to the scenarios can help the player overcome these two barriers, then they can move on in the game to more scenarios and concepts, achieving a deeper understanding of cybersecurity.

B. THESIS SCOPE

The scope of the thesis is divided into two main areas.

1. Learning Objectives

The first major question to be answered was "what are the learning objectives for the subset of existing scenarios." To answer this question, we looked at the Instructor's Notes, the lab manuals, and the game itself to identify the learning objectives associated with each phase. In most cases, the learning objective was explicitly stated in one of these resources. However, in a few cases, the objective was derived from analysis of the game and in discussion with the scenario designer.

To expound further on the questions of learning objectives, we attempted to identify prerequisite knowledge needed for each scenario. Many of the scenarios are designed in a way to build off of earlier scenarios. The learning objectives from the initial scenarios are not directly addressed in the secondary scenarios, but the knowledge gained from the first is necessary for completion of the second.

Finally, we assessed whether the learning objectives were actually achieved during the scenario in its current state and if completion of a scenario implies understanding of the concepts. For the majority of the learning objectives, the game was sufficiently programmed for the average player to achieve the learning objective. For a few objectives, we made additions or revisions to the game to ensure the player could understand the objective.

2. Obstacles Encountered

Our primary purpose in analyzing the scenarios in CyberCIEGE was to determine if a player encountered any obstacles that prevented them from either completing the scenario or achieving the learning objectives. Again, as with the learning objectives, the majority of the obstacles we identified are already handled by the current game design. However, we determined there were a few points in the scenarios that presented obstacles that average users could not overcome without additional help. After identifying these obstacles, we determined how best to help the player overcome them.

To help with this, we identified the CyberCIEGE game components and game engine functions that are available for assessing the game state and student choices. We then used those functions to recognize points in the game where either questions or help messages (helptips) were needed to help guide the player through the scenario.

The last question addressed in our research was whether we could create a process that could be applied to additional scenarios. The scope of this research was limited to two specific scenarios, but there are over twenty total scenarios and the game is designed in a way for more scenarios to be added as deemed necessary. Our objective has been to enable others to analyze and revise the remaining scenarios to ensure learning objectives are achieved and obstacles to game play can be overcome.

C. ORGANIZATION

This thesis is comprised of the following chapters:

- Chapter I provides the problem statement, defines the objectives and the scope of the research and gives an overview of the chapters.

- Chapter II describes the CyberCIEGE game and introduces its components. It discusses the need for improved assessment techniques and why they are important in the context of CyberCIEGE.

- Chapter III describes the approach we took in the conduct of this research. It describes how we chose which game scenarios to include in the work and how we identified decision points in those scenarios where learning objectives can be evaluated. It also discusses how we identified barriers players might encounter. Finally, it discusses how we determined which techniques should be used for assessment and overcoming the obstacles.

- Chapter IV provides the results of our research into the design objectives of the scenarios and how each scenario achieves its learning objective. This chapter also reviews the gameplay and implementation of the current scenarios. Finally, it discusses the results of our efforts to identify potential barriers to achieving the objectives and how students can be guided through those barriers.

- Chapter V: provides a conclusion and reviews lessons learned during this research and suggestions for future development of CyberCIEGE.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND AND MOTIVATION

This chapter provides a brief description of CyberCIEGE and its components. It then delves into the motivation behind this research and how we expect to revise given scenarios to ensure the player can complete the scenario and realize the learning objectives.

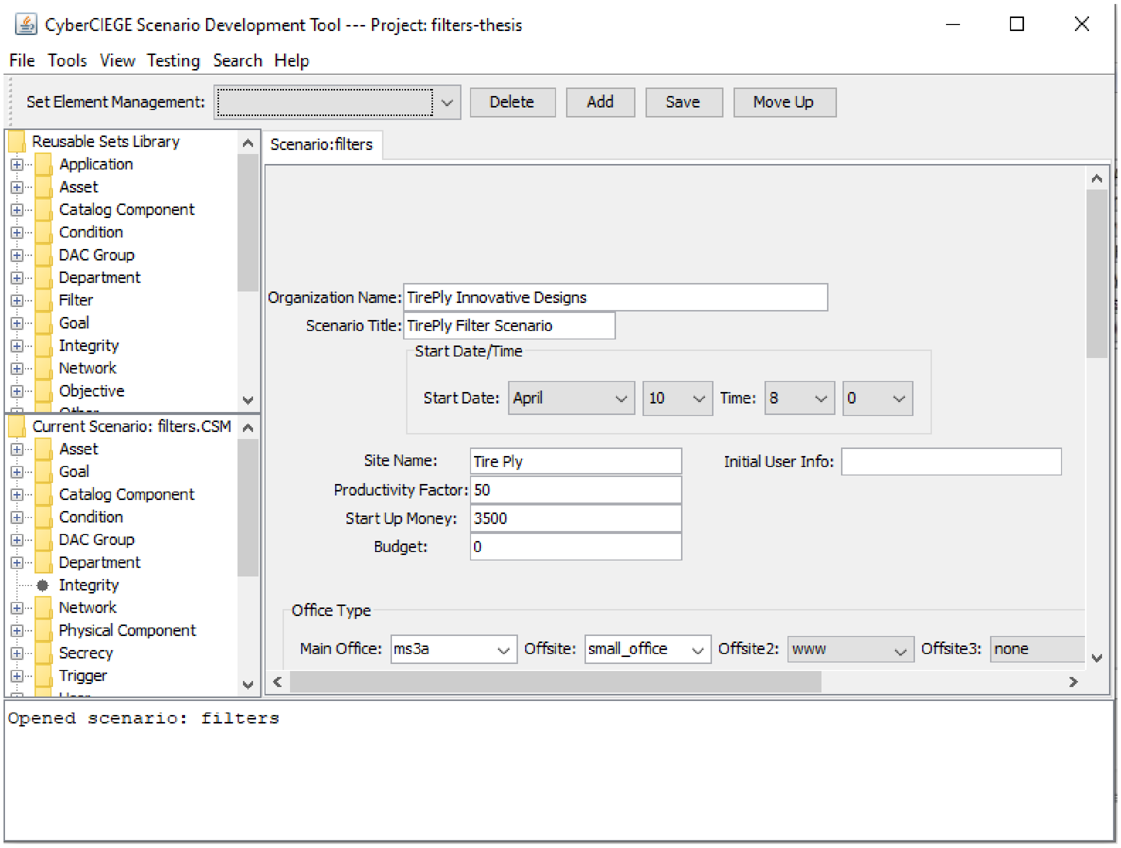
A. CYBERCIEGE

Traditionally, cybersecurity education was only offered to the system administrators and IT personnel within a company. However, the average worker does not have the necessary knowledge to identify and mitigate threats and system vulnerabilities, nor does the decision maker within a company have an understanding of what decisions need to be made to keep a network secure. "As a result, human errors and actions continue to demonstrate that we are the weakest links in cybersecurity" [1]. Security awareness education is becoming more essential for all users, but most importantly for system administrators and the upper management who approve and manage the security management plan. In his book *Digital Game-based Learning [2]*, Marc Prensky noted that as businesses and organizations rely more heavily on network infrastructure and digital technologies, a robust security awareness education program can effectively enhance the organization's overall information assurance posture. A couple challenges that network administrators encounter are the vast scope of all network security practices and communicating about those practices with the company executives who approve the finances for the equipment and training as well as with typical personnel within the organization. Video games have been proposed to be an effective learning tool that engages the audience, and still achieves the overall learning objectives [2].

CyberCIEGE is a video game platform, designed to teach network security principles. It is an on-going project designed and maintained by the Center for Cybersecurity and Cyber Operations at the Naval Postgraduate School. The game play places the player in a scenario, where simulated events illustrate the consequences and results of player choices in defending the assigned network and information assets. One of the primary objectives of the game is to support training and education in network and computer security. The game is used to teach students from high school through professional organizations with diverse backgrounds, including U.S. government and non-government agencies and over 400 educational institutions worldwide [3], [4]. The current twenty plus scenarios are designed to teach principles such as router configuration, use of firewalls, encryption, VPNs, how to protect against malware and other valuable network security topics.

B. CYBERCIEGE COMPONENTS

CyberCIEGE is composed of several building blocks: a unique simulation engine, a domain-specific Scenario Definition Language (SDL), a Scenario Development Tool (SDT), and an encyclopedia enhanced with video instructions [5]. Scenario designers create scenarios using the SDT, which provides a user interface that makes it easy to add the necessary features for a functioning scenario. A screenshot of the SDT can be seen in Figure 1. The SDT then converts the forms-based scenario expression into a scenario definition language. A collection of these forms then define the scenario and the game uses a combination of conditions and triggers to help the player achieve the scenario objectives [4]. The game simulation engine interprets the language and presents the player with the scenario defined by the language. The engine then performs vulnerability assessment, network topology parsing, and determines if the player is achieving the scenario objectives. The simulation can assess if a scenario objective has been met through identified trigger points, which will be discussed later.



Organization Name: TirePly Innovative Designs

Scenario Title: TirePly Filter Scenario

Start Date/Time

Start Date: April 10 Time: 8 0

Site Name: Tire Ply

Initial User Info:

Productivity Factor: 50

Start Up Money: 3500

Budget: 0

Office Type

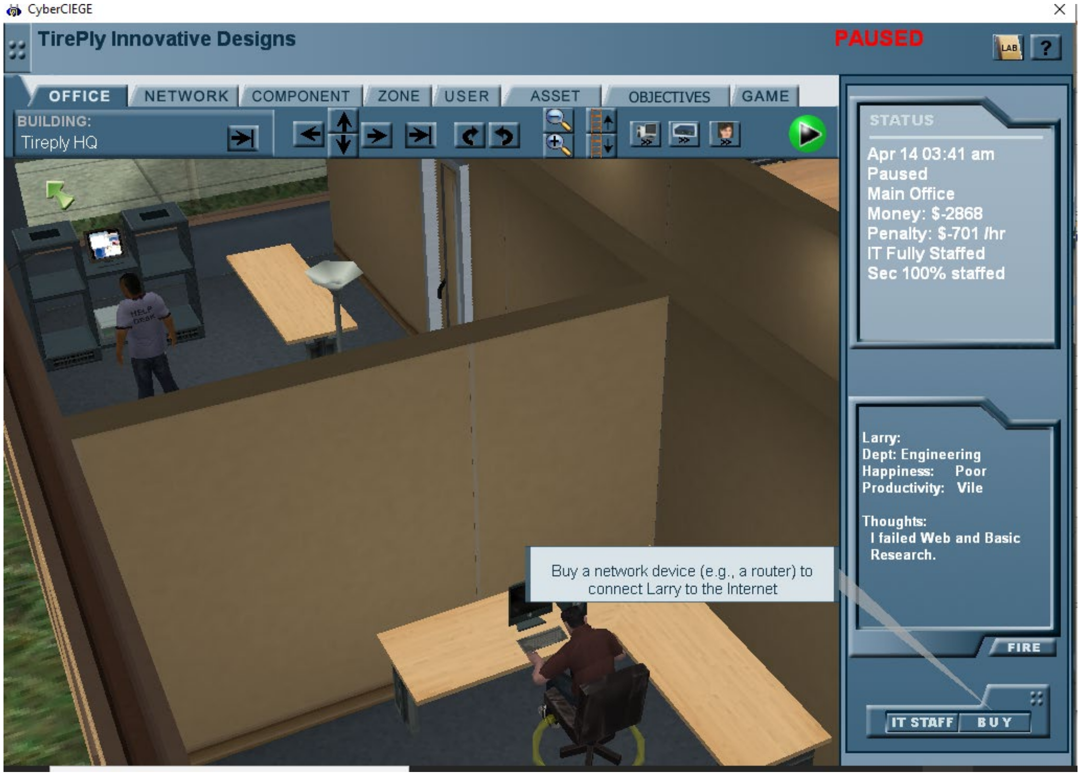
Main Office: ms3a Offsite: small_office Offsite2: www Offsite3: none

```
Opened scenario: filters
```

Figure 1. Scenario Development Tool screenshot for building new CyberCIEGE scenarios.

The core of CyberCIEGE is its sophisticated game simulation engine. The game engine interprets the Scenario Definition Language (SDL) and presents the player with the resulting interactive scenario. The game engine is programmed with information assurance concepts and can simulate sophisticated environments that contain multiple threats and vulnerabilities. The game engine can then assess the network vulnerabilities, conduct attacks on the network and notify the player of the attacks that occur. The game engine also manages the in-game economy [6]. The economy is the net loss or gain of financial resources based on company productivity or lack thereof over time. The player can then use the financial resources to purchase equipment, hire personnel or provide training to the employees.

During game play, the player is presented with different choices that can affect the security of the network assets [4]. Players make decisions on how to better secure the network, and try to meet a series of objectives, which help advance the player through the scenario. Each scenario presents the player with a new in-game economy that suffers when players fail goals. The players identify vulnerabilities in the network and in overall cybersecurity. They work to mitigate these problems with cybersecurity-based strategies and tools based on the principles they learn during game play. Figure 2 is a screenshot of the Network Filters scenario.



Apr 14 03:41 am
Paused
Main Office
Money: $-2868
Penalty: $-701 /hr
IT Fully Staffed
Sec 100% staffed

Larry:
Dept: Engineering
Happiness: Poor
Productivity: Vile

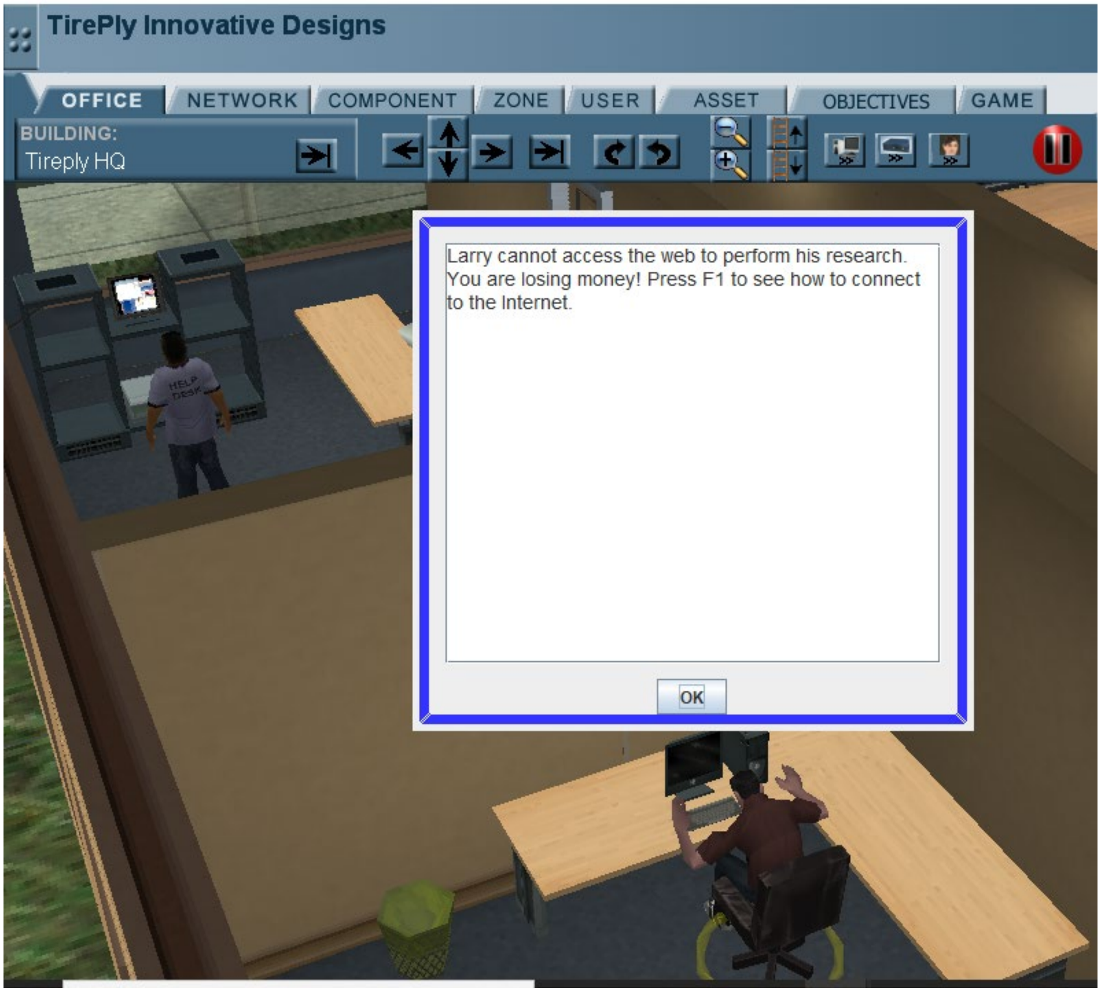
Thoughts:
I failed Web and Basic Research.

Buy a network device (e.g., a router) to connect Larry to the Internet

Figure 2. Screenshot of the CyberCIEGE game in the network filters scenario.

C. CONDITIONS AND TRIGGERS IN CYBERCIEGE

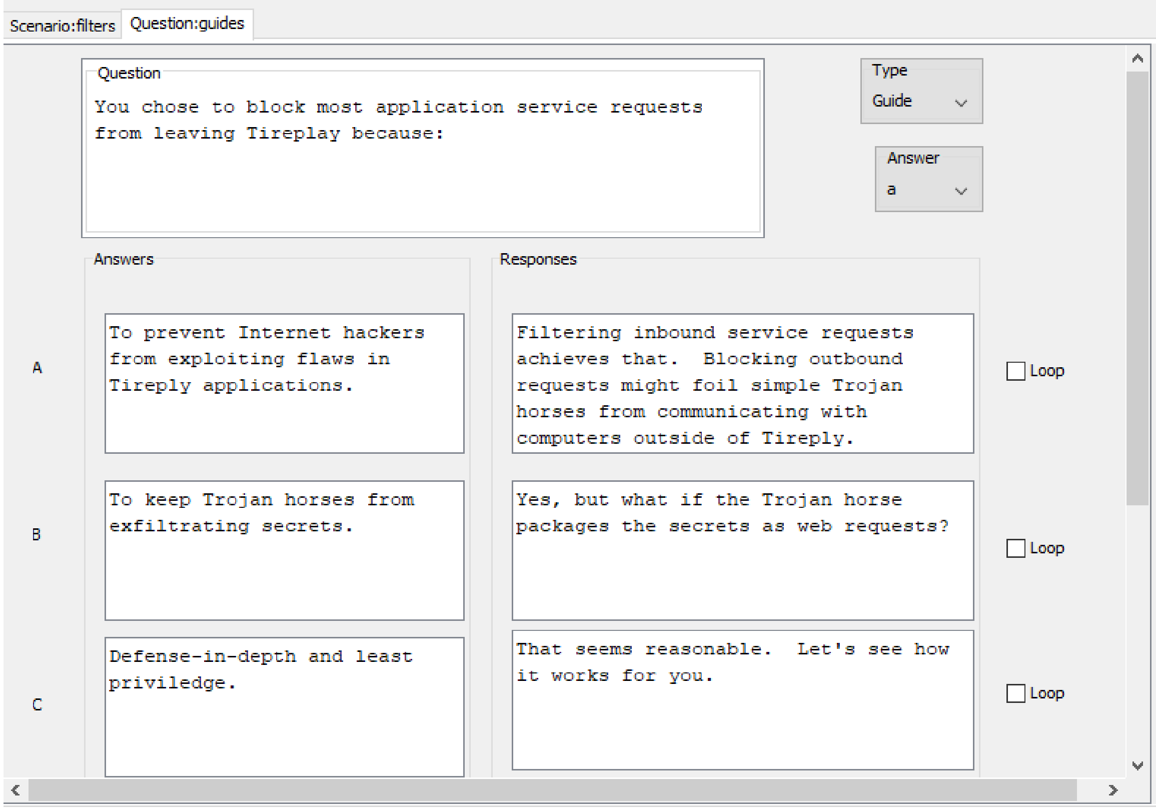
As a player moves through a scenario, (s)he is presented with a series of objectives that must be completed in order to move to the next part of the scenario. The CyberCIEGE SDL allows the designers to assess the active game state "conditions" and respond with "triggers" [4]. Conditions can include such things as "the passing of time, whether users are achieving their goals, computer configuration settings and whether attackers have compromised assets" [4]. "Scenario designers can then cause triggers to fire based on a Boolean expression of the current game state" [7]. "Active triggers include popup messages, brief movies, changes in user goals, commencement of attacks, and user feedback to the player via balloon speech" [7]. Figure 3 is an example of popup message during game play.



Larry cannot access the web to perform his research. You are losing money! Press F1 to see how to connect to the Internet.

Figure 3. Example of popup message after trigger event.

There are multiple types of triggers in the game engine. The Scenario Development Tool Guide [7] explains the triggers. Designers can implement question triggers to test a player's understanding with two different types of questions: quiz or guide. Quiz questions are for testing the knowledge of the player. Guide questions are Socratic questions, meant to help guide the player to think about the response and to then test the response in the simulated environment. The player's responses help the game engine determine which follow-on feedback to provide to the player [7]. Quiz questions can be used to test if a player has the knowledge to complete a task, but guide questions help the player learn how to apply that knowledge into a situation. In application of these principles, network administrators and company decision makers no longer have to communicate about system security based on facts from a textbook or manual. Instead, they gain the experience necessary to discuss a problem and decide what is the best course of action for their company to take.



Question: You chose to block most application service requests from leaving Tireplay because:

Type: Guide

Answer: a

	Answers	Responses
A	To prevent Internet hackers from exploiting flaws in Tireply applications.	Filtering inbound service requests achieves that. Blocking outbound requests might foil simple Trojan horses from communicating with computers outside of Tireply.
B	To keep Trojan horses from exfiltrating secrets.	Yes, but what if the Trojan horse packages the secrets as web requests?
C	Defense-in-depth and least priviledge.	That seems reasonable. Let's see how it works for you.

Figure 4. Example of guide question from SDT.

Figure 4 displays how the Socratic method is applied within the game play. None of the answers are necessarily wrong, but the responses to the answers motivate the player to think if there is maybe a better way to configure the network filter. The question posed at the top of Figure 4 is triggered in a very specific condition when an asset is connected to the Internet, but outbound connections are blocked. The player is asked why certain types of messages are blocked. There could be multiple reasons the player chose such a filter. The responses to the questions force the player to think about additional consequences of the actions taken, then moves the scenario forward. In this case, there is a better course of action for system functionality and security, but that is not discussed in the guide question. The resulting scenario will show the player that the security is not complete as a Trojan Horse enters the system, disguised as a web request.

D. SCENARIOS

CyberCIEGE gameplay is designed so that the player goes through each scenario in one or more phases, each intended to help the player achieve the learning objectives intended by the scenario designer. Each scenario covers one or more cybersecurity related concepts for the player to focus on and each scenario has its own set of learning objectives. In addition, scenarios may build on knowledge and experience gained in previous scenarios.

In each scenario, the player is placed in a work environment and given a task to accomplish within their assigned job responsibility. Scenarios are divided into phases that guide the player to the overall learning objective. Each phase has a set of objectives that must be met before the player can move on to the next phase. At any point, players may click on the Objectives tab to read and review the phase and scenario objectives to understand what they need to accomplish. Figure 5 displays the tabs that a player can select during game play. The Objective tab is second from the right.

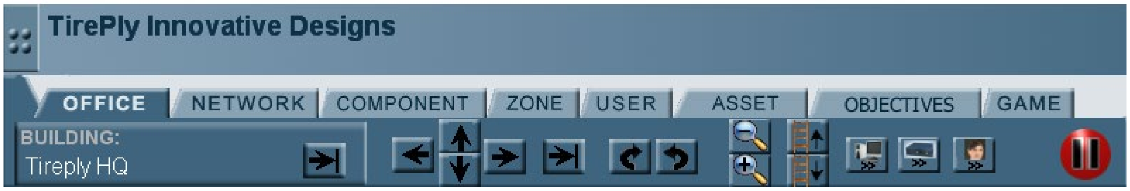


Figure 5. Screenshot of the tabs available to the player during game play.

E. MOTIVATION FOR THIS WORK

In a traditional classroom setting, a teacher may observe the students' performance and gauge understanding. This can be done through in class exercises, homework, assessments and even through facial expression and body language while the material is being presented. In a virtual educational environment such as that offered by CyberCIEGE, no teacher is present to recognize the level of understanding of the player. With our backgrounds in education, we find the task of overcoming learning obstacles and assessing understanding is vital to the overall success of the educational program. Patricia Cross wrote "continuous feedback is necessary for improvement in both teaching and learning. Teachers need to assess learning so that they may provide feedback to students on their progress as learners. And teachers need to receive continuous and accurate feed-back on the impact of their teaching on the students in their classrooms, so that they may improve their teaching" [8]. In communication with the game's designers, we determined that bringing in someone with a teaching background, who could apply knowledge of assessment techniques and purposes could prove valuable to the effectiveness of CyberCIEGE.

When a student is participating in virtual education, there are simple indicators, such as quiz questions or failed objectives, that show the student cannot proceed with the current level of knowledge. In that case, a computer program could keep sending the student back to the beginning with a failed score, leaving the player in a cycle of failure. A teacher, however, can sit with the student to determine if there are other challenges. It is possible that the student actually does understand the material presented but does not understand the game mechanics of required to apply the knowledge. It is also possible that the scenario-based learning environment is not sufficient for the student to learn the material. Either way, the student-player's needs are not being met and completion of the learning or scenario objectives is hindered. By identifying possible learning obstacles in the gameplay and evaluating and improving CyberCIEGE's trigger-condition-driven feedback, CyberCIEGE can be improved ensure the player has a better chance of achieving the game objectives.

F. USE OF ASSESSMENT AS AN EDUCATIONAL TOOL

Dr. Cross continued in her article, “feedback plays different roles in two current modes of assessment that are frequently contrasted as assessment-for-accountability and assessment-for-improvement.” The assessment-for-improvement mode would apply to the educational goals of the CyberCIEGE video game. She continued, “the role of feedback in the assessment-for-improvement model is to provide a continuous flow of information that is useful in shaping the process of teaching and learning while it is in process. This is generally referred to as ‘formative evaluation’” [8].

Most research that has been conducted on assessment techniques and feedback to improve student learning centers on traditional classroom settings, such as the Dr. Cross article cited and the top ten results from a Google scholar search on “assessment in education.” CyberCIEGE is far from a traditional learning setting, but we hypothesize that, with the use of conditions and triggers, we can create an environment that assesses the game state and dynamically presents questions or help as necessary to give the student-player the best chance of overcoming educational barriers.

In addition to a dynamic set of triggers and conditions to create a formative evaluation environment, developing Socratic questions, as already discussed, can help the player to learn the material and apply it into an actual situation. The combination of the two methods of learning and assessment can place a balance between the educator (in this case the CyberCIEGE game engine) and the student. As the student learns from mistakes and experience, the language programmed into the game engine will evaluate the conditions and triggers and adjust accordingly.

CyberCIEGE was developed by programmers with an emphasis placed on developing the simulations to convey learning objectives. The developers have identified a path for future work in the game development. “Assessing the efficacy of CyberCIEGE is a challenge that we think would greatly benefit from participation of education researchers versed in formal methodologies for measuring the contribution of the hands-on activities to student understanding” [9].

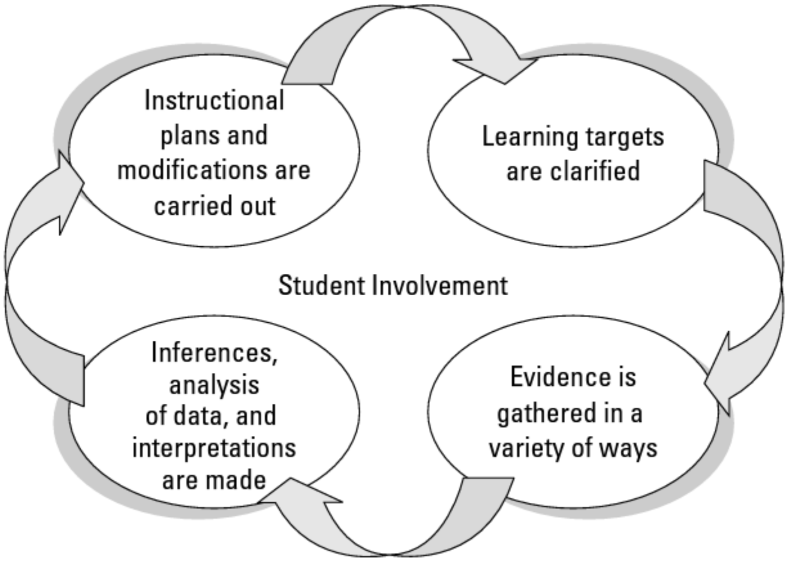

Instructional plans and modifications are carried out
Learning targets are clarified
Student Involvement
Inferences, analysis of data, and interpretations are made
Evidence is gathered in a variety of ways

Figure 6. Classroom assessment cycle. Source: [10].

Figure 6 is the classroom assessment cycle as identified in the *Teacher's Guide to Assessment* manual [10]. With proper conditions and assessment techniques, CyberCIEGE can implement all steps of this cycle. The learning targets can be clarified through communicated scenario objectives accessible at any time during game play. The instructional plans and modifications are easy to implement with the game engine's ability to understand the language implemented by the scenario designer. The biggest challenge in the assessment cycle will be knowing how to gather evidence of understanding, or better yet misunderstanding and using that to create the correct language for the game engine to present the material necessary for the player to move forward in the scenario. This is not dynamic adaptation of the game, but different execution paths programmed into the game based on current state and the user activity during game play.

As game play goes on, a variety of conditions and triggers can provide evidence of misunderstanding. For example, in the Network Filters scenario, completion of the first phase requires the player to purchase a router and connect it to the Internet. This objective is clearly communicated at the very beginning of the scenario. If a certain amount of time goes by and nothing has been purchased, it is very possible that game mechanics are preventing the player for accomplishing the task. In this situation, simple hints about how to purchase a router will help move the game along. If the player purchases, a router, but does not connect it to anything, there could be a lack of understanding of the purpose of a router, or game mechanics could be the problem. The player's response to a question posed by the game in this situation asking what a router connects to could tell the game engine to give instruction on the purpose of a router or give hints on how to connect the router. In a third execution of the scenario, the player purchases the router and only connects it to the local LAN. It is clear that the player then understands the purpose of a router and how it works. A simple reminder to connect the router to the external network would be sufficient to guide the player toward achieving the scenario's objectives. By modifying the basic programming of the scenario, it can be made to handle a variety of educational contingencies. In doing this, the overall product will then mirror, within the constraints of the overall CyberCIEGE design, a productive learning environment that better supports the learning of the player.

THIS PAGE INTENTIONALLY LEFT BLANK

III. APPROACH

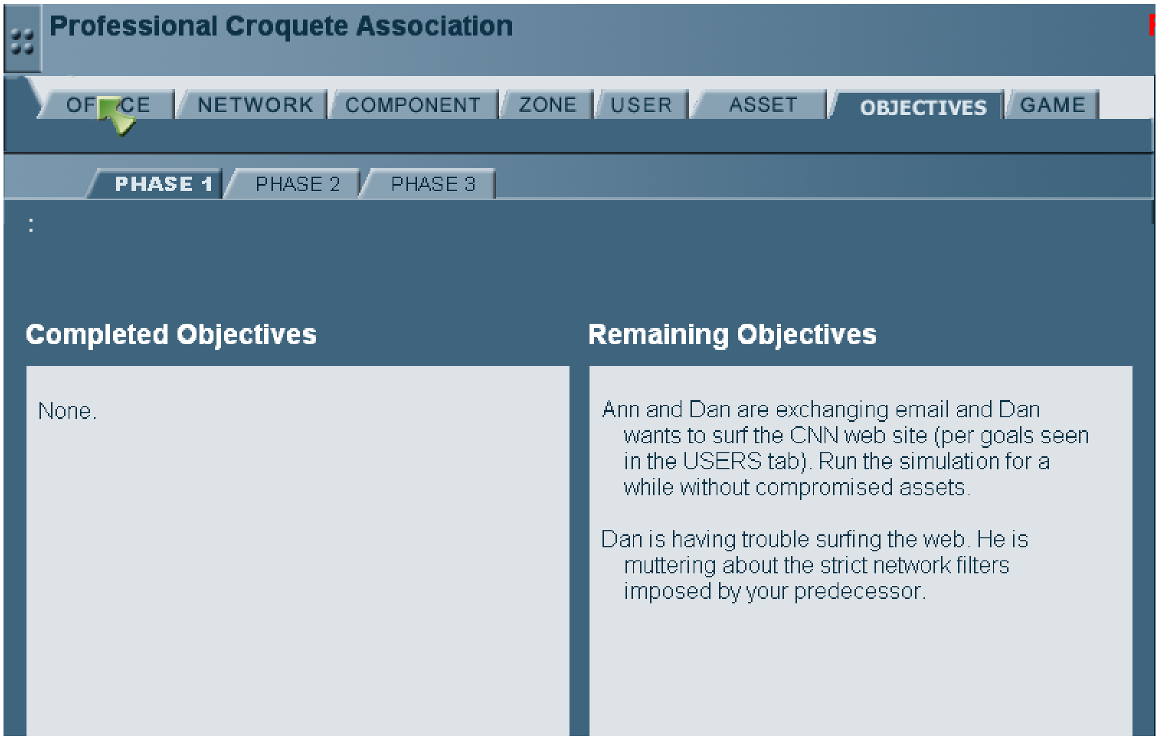
In this chapter, we review the approach used to identify whether learning objectives have been met. We will also discuss how to determine if there were obstacles a student might encounter in attempting to achieve scenario objectives. The obstacles could be a barrier to learning and understanding the material, or they could be a result of gameplay mechanics that prevents the player from accomplishing the required task.

A. DETERMINING SECTIONS FOR RESEARCH

The purpose of this research was to determine a method for identifying obstacles to the completion of learning and scenario objectives. Our objective was to create a general-purpose process for CyberCIEGE. This process was developed in the context of two actual scenarios: the Network Filters scenario and the demilitarized zone (DMZ) scenario. These scenarios were recommended by the primary CyberCIEGE developer, Michael Thompson, as a good starting point for the research. The Network Filters scenario is an introductory-level scenario that can be played when first opening the game. Other scenarios require completion of another prerequisite scenario before it is unlocked and made available for play. The DMZ scenario builds on the lessons learned and only unlocks after completion of the Network Filters scenario. By using these two scenarios, the obstacles the player faces from the very beginning of game play can be determined, and the lessons learned while overcoming those obstacles can help the player overcome new challenges in a more advanced scenario.

B. SCENARIO AND LEARNING OBJECTIVES

As discussed in a previous chapter, CyberCIEGE scenarios are divided into smaller phases. Moving from one phase to the next depends upon the completion of objectives communicated to the player at the beginning of each phase. At any point during game play objectives can be accessed by selecting the Objectives tab. Figure 7 shows the Objectives tab for the first phase of the DMZ scenario. These scenario and phase objectives are determined by the scenario designer.



Completed Objectives

None.

Remaining Objectives

Ann and Dan are exchanging email and Dan wants to surf the CNN web site (per goals seen in the USERS tab). Run the simulation for a while without compromised assets.

Dan is having trouble surfing the web. He is muttering about the strict network filters imposed by your predecessor.

Figure 7. Screenshot of objectives tab during CyberCIEGE game play. These two scenario objectives must be met before the player can move on to the Phase 2 objectives.

Identifying learning objectives requires more analysis than does identification of the scenario objectives. The learning objectives are the lessons that the player should be able to understand and apply at the completion of the scenario. Learning objectives are used by educators to track progress of students and make sure that educational requirements are met. The CyberCIEGE game does not provide an explicit list of learning objectives for each scenario. Rather, educators can identify the learning objectives through additional documentation such as the instructor notes and the lab manuals. Additionally, review of the topics covered in each scenario in the game encyclopedia and the associated tutorial videos can help educators determine the learning objectives addressed by the scenario designer [11].

The instructor notes start with an explanation of what the students should be able to understand to complete the scenario [12]. These are some of the basic learning objectives. A comprehensive list of the learning objectives for the two scenarios is provided in Chapter IV.

An example, though, is found in the DMZ Scenario instructor notes which begins as follows: "The scenario is intended to illustrate the use of a DMZ to protect internal systems, including internal email servers, from attack by deploying externally accessible email servers to a DMZ. The scenario also requires deployment of a web server to the DMZ and permitting that web server to access an internally located database server" [13].

During game play, the player can press F1 to access the CyberCIEGE Encyclopedia. This resource provides instruction and guidance on all topics addressed during game play. There are also tutorial videos on selected topics that give background information on necessary topics, such as software patches and network filters. In combination, the information contained in the encyclopedia and the videos covers the material the game designer intended the player to learn or understand in CyberCIEGE. There is not, however, a specific mapping of topics in the encyclopedia to scenarios as the concepts are often addressed in multiple scenarios. Further discussion with the scenario designer revealed additional learning objectives that were intended to be met in each scenario.

C. IDENTIFYING BARRIERS TO OBJECTIVE COMPLETION

Our initial approach to analyzing a scenario was to play it multiple times, attempting to complete each phase's objectives, while noting challenges encountered during play. We then created a roadmap, or a visual representation of choices a player could make during each phase of the scenario (see Appendix A). At the start of each roadmap was the game state after completion of the previous phase. The end of a roadmap was the completion of the objective necessary to complete the phase. Figure 8 shows an example of the Phase 1 roadmap for the Network Filters scenario.

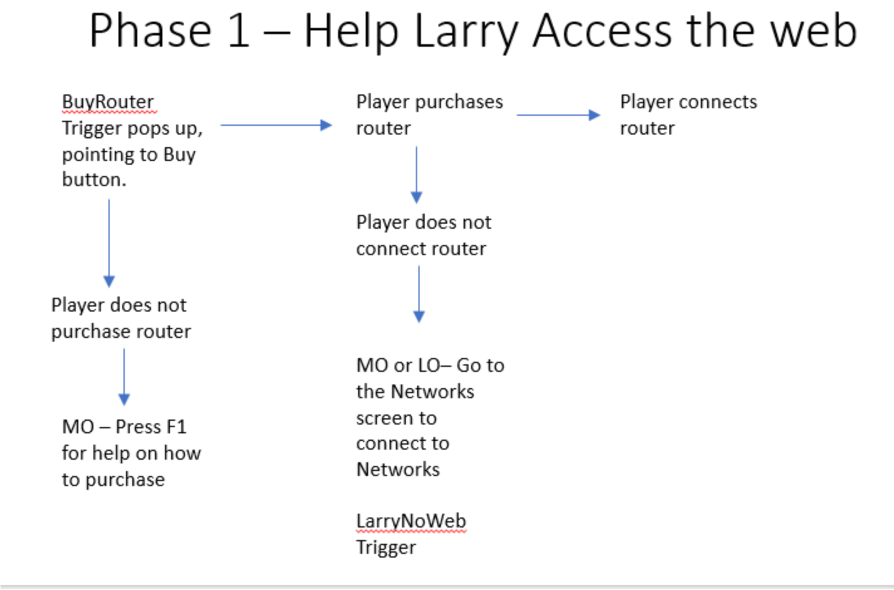
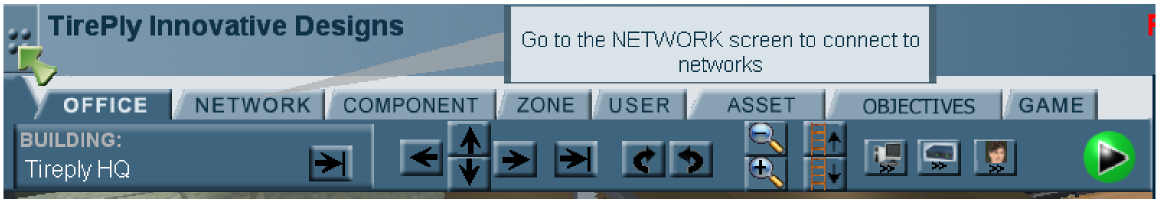

Phase 1 – Help Larry Access the web
BuyRouter Trigger pops up, pointing to Buy button.
Player purchases router
Player connects router
Player does not connect router
Player does not purchase router
MO – Press F1 for help on how to purchase
MO or LO– Go to the Networks screen to connect to Networks
LarryNoWeb Trigger

Figure 8. Roadmap for network filters scenario Phase 1.

The beginning of the roadmap is "BuyRouter Trigger pops up, pointing to Buy button." The phase ends with "Player connects router." All of the steps in between the beginning and end of the map show possible choices a player could take while working to achieve the objective of the phase. This could lead to numerous possibilities, as players could have various notions about security and what is necessary to complete the objective. When identifying these possibilities, it is important to try to assume the level of understanding of a beginning player who may or may not be familiar with network security concepts but is diligently trying to complete the phase by following the helptips that may be introduced during game play.

During this process, we identified two main types of obstacles a player could encounter during game play: game mechanics obstacles (MO) and learning obstacles (LO), where the latter are challenges with learning and understanding the information necessary to complete the scenario objective. Initially, the obstacles could be either MO or LO, since the player has never experienced any of the game mechanics and may not know how to interact with the game. MOs could be addressed by providing pop up helptips explaining exactly what to click and where to look to overcome the MO. A point in gameplay where a student could make a choice that did not lead to achieving the scenario objective and where numerous helptips had already been programmed into the game, was labeled as having a LO. If a point in the game was determined to have insufficient helptips and where the game play mechanics had not been explained in a previous phase, then the obstacle was assigned a MO label.



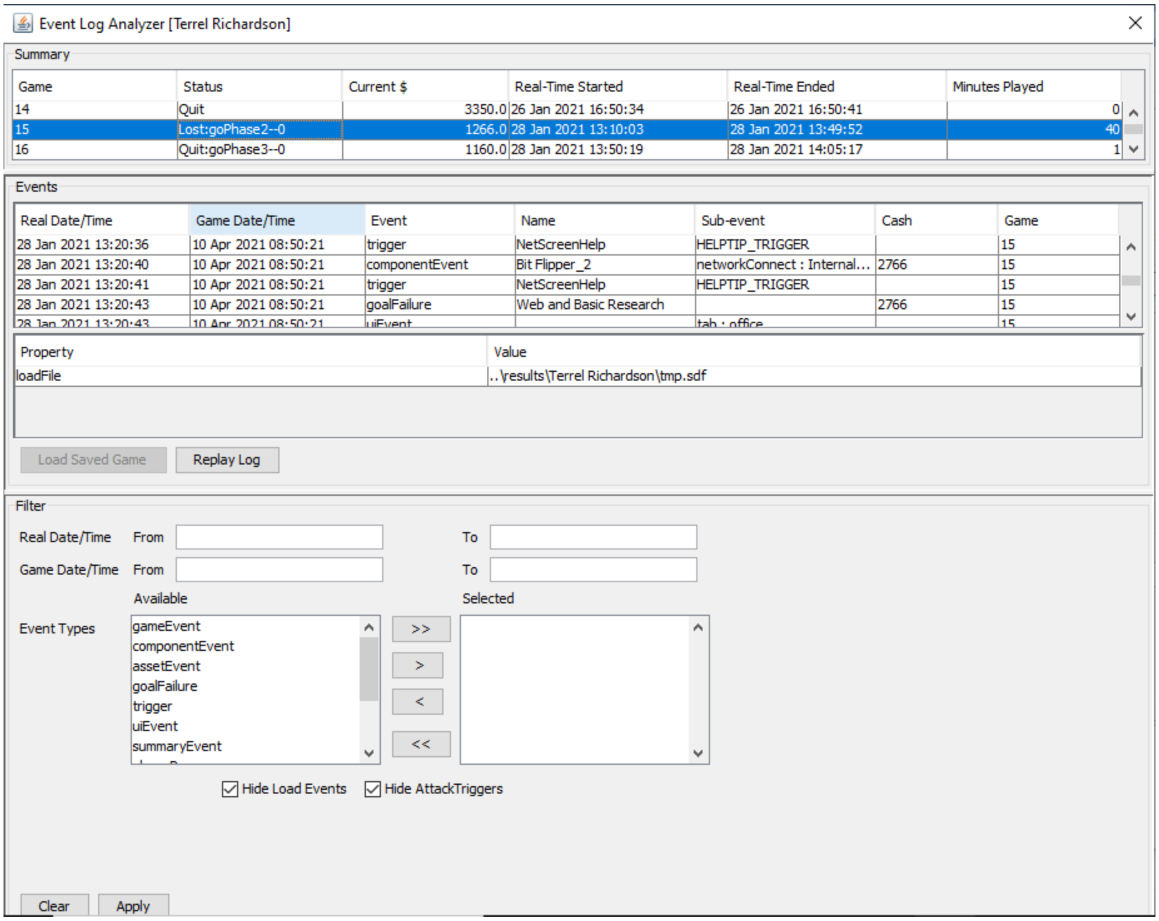
Go to the NETWORK screen to connect to networks

Figure 9. Screen shot of helptip instruction the player how to access the network screen to configure a router.

Each roadmap allowed us to better understand the flow of the game and the obstacles a player could experience, but the roadmaps did not help us determine how the player might overcome those obstacles. That depth of understanding could only be achieved by reviewing the triggers and conditions of the scenario.

D. IDENTIFYING TRIGGERS AND CONDITIONS FOR OBSTACLES

To identify conditions and triggers where learning objectives can be evaluated, we had to understand how the game engine interprets events in the game that satisfy particular conditions and result in the firing of associated triggers. Each game instance creates a log, which can be viewed in the SDT Event Log Analyzer, or by accessing the log files saved to the game directory folder upon each instance of play. Instructions on how to play a selected scenario and view the associated log files can be found in the SDT instructions [7]. Figure 10 displays a screenshot of the Event Log Analyzer and the events that occurred during that game play session.



Game	Status	Current $	Real-Time Started	Real-Time Ended	Minutes Played
14	Quit	3350.0	26 Jan 2021 16:50:34	26 Jan 2021 16:50:41	0
15	Lost:goPhase2--0	1266.0	28 Jan 2021 13:10:03	28 Jan 2021 13:49:52	40
16	Quit:goPhase3--0	1160.0	28 Jan 2021 13:50:19	28 Jan 2021 14:05:17	1

Real Date/Time	Game Date/Time	Event	Name	Sub-event	Cash	Game
28 Jan 2021 13:20:36	10 Apr 2021 08:50:21	trigger	NetScreenHelp	HELPTIP_TRIGGER		15
28 Jan 2021 13:20:40	10 Apr 2021 08:50:21	componentEvent	Bit Flipper_2	networkConnect : Internal…	2766	15
28 Jan 2021 13:20:41	10 Apr 2021 08:50:21	trigger	NetScreenHelp	HELPTIP_TRIGGER		15
28 Jan 2021 13:20:43	10 Apr 2021 08:50:21	goalFailure	Web and Basic Research		2766	15
28 Jan 2021 13:20:43	10 Apr 2021 08:50:21	uiEvent		tab : office		15

Property	Value
loadFile	..\results\Terrel Richardson\tmp.sdf

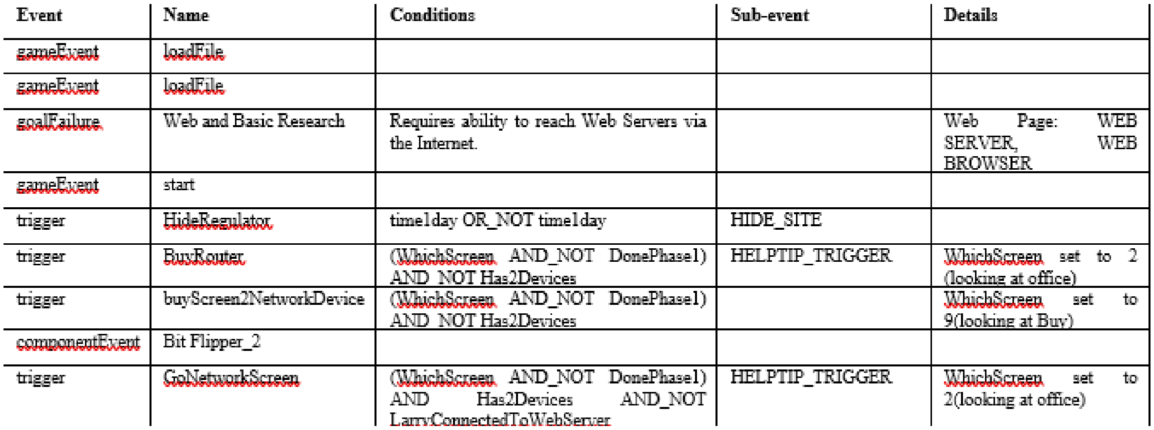
Figure 10. Screenshot of SDT event log analyzer.

The log file lists events in order of their occurrence during game play. Analyzing these events helped us understand the different components of the SDF. The SDT instructions explain what each component is, but to appreciate how they worked together, analysis of the triggers and conditions and how the game engine interpreted them to move game play along was useful. For example, the SteeltoInternet condition is referenced in multiple Triggers. The condition is listed in the SDT as an AssetToNetwork type condition. Further exploration of the condition shows the Asset referenced to be the Steel Formula. Analysis of the Steel Formula Asset showed us where the Asset was located, its intended Access Control List (ACL) and its actual ACL, how the Asset was instantiated by the game engine, as well as its value to the company. This analysis helped better explain why and how the condition containing the asset was assessed, thus leading certain triggers to fire.

Based on a review of the Event Log Analyzer, we created a simple process to analyze and dissect the triggers and conditions. The results of that process can be seen in Appendix B. This allowed us to understand how the triggers and conditions were interpreted based on the choice made during game play, creating a sense of cause and effect.

The process is as follows:

1. Create separate blank spreadsheets for triggers, conditions, assets and goals. The columns of the spreadsheet correlate to the columns in the log file for each new event. The rows of the spreadsheet are the individual triggers, conditions, assets, or goals. Figure 11 is an example of the triggers' spreadsheet. The first column describes the event logged. The second column is the name of the specific event. The third column is the conditions that were met to fire the event. The Sub-event is recorded if the event is a trigger and lists the type of trigger. The Details column gives amplifying information for the conditions that were met.



Event	Name	Conditions	Sub-event	Details
gameEvent	loadFile			
gameEvent	loadFile			
goalFailure	Web and Basic Research	Requires ability to reach Web Servers via the Internet.		Web Page: WEB SERVER, WEB BROWSER
gameEvent	start			
trigger	HideRegulator	time1day OR_NOT time1day	HIDE_SITE	
trigger	BuyRouter	(WhichScreen AND_NOT DonePhase1) AND_NOT Has2Devices	HELPTIP_TRIGGER	WhichScreen set to 2 (looking at office)
trigger	buyScreen2NetworkDevice	(WhichScreen AND_NOT DonePhase1) AND_NOT Has2Devices		WhichScreen set to 9(looking at Buy)
componentEvent	Bit Flipper_2			
trigger	GoNetworkScreen	(WhichScreen AND_NOT DonePhase1) AND Has2Devices AND_NOT LarryConnectedToWebServer	HELPTIP_TRIGGER	WhichScreen set to 2(looking at office)

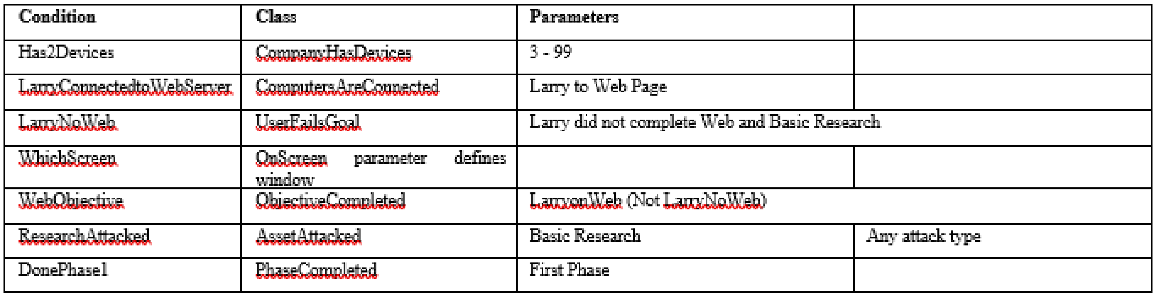
Figure 11. Example of triggers spreadsheet as taken from the events listed in the event log analyzer

2. Record each new trigger in the trigger spreadsheet.

3. Identify the class of the trigger, which is another name for Sub-event. The SDT Instructions explain each trigger class and the parameters values required for the trigger to fire [7].

4. List the conditions that cause trigger to fire. Conditions can be obtained by double clicking on the trigger name in the Event Log Analyzer.

5. Record each new condition in the conditions' spreadsheet. See Figure 12 for example.

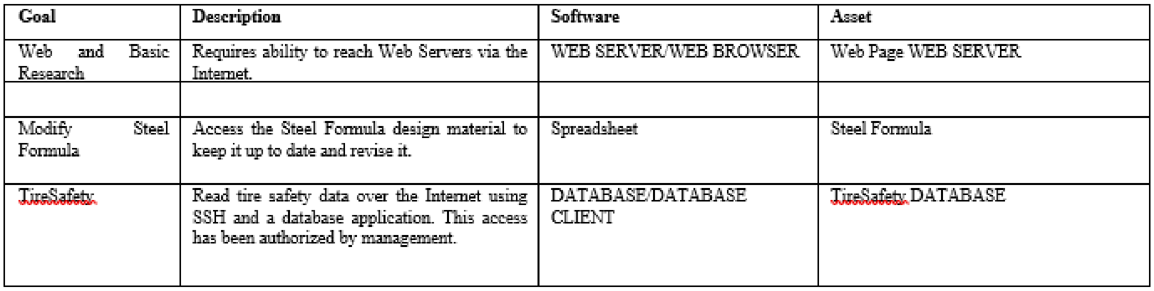


Condition	Class	Parameters	
Has2Devices	CompanyHasDevices	3 - 99	
LarryConnectedtoWebServer	ComputersAreConnected	Larry to Web Page	
LarryNoWeb	UserFailsGoal	Larry did not complete Web and Basic Research	
WhichScreen	OnScreen parameter defines window		
WebObjective	ObjectiveCompleted	LarryonWeb (Not LarryNoWeb)	
ResearchAttacked	AssetAttacked	Basic Research	Any attack type
DonePhase1	PhaseCompleted	First Phase	

Figure 12. Example of spreadsheet for conditions.

6. Identify the condition class and the parameters associated with that class for the specific scenario. The class is listed in the SDT. The SDT Instructions explain each condition class and the parameters associated with the class.

7. If the parameters reference an asset or a goal, record the asset or goal in the corresponding spreadsheet, along with the description of that asset or goal. See Figure 13 for an example of a Goals spreadsheet. The software column represents the software necessary to evaluate completion of the goal.



Goal	Description	Software	Asset
Web and Basic Research	Requires ability to reach Web Servers via the Internet.	WEB SERVER/WEB BROWSER	Web Page WEB SERVER
Modify Steel Formula	Access the Steel Formula design material to keep it up to date and revise it.	Spreadsheet	Steel Formula
TireSafety	Read tire safety data over the Internet using SSH and a database application. This access has been authorized by management.	DATABASE/DATABASE CLIENT	TireSafety DATABASE

Figure 13. Example of goals spreadsheet.

8. Move to the next trigger.

A limitation of this log file-based process is that no single time a player plays the game will include all the possible triggers. To overcome this, we used multiple log files that ended at different points in the game, starting with the file that ended in the earliest phase. Once the point at which the next logfile differed from the previous log file was identified, more lines were added to the spreadsheet with each new trigger, condition, etc., encountered. By the end of this process, there were very few remaining triggers in the SDF that had not been entered into the spreadsheet. The remaining triggers and conditions were identified by downloading the SDF for the scenario and comparing the listed triggers and conditions to the ones already in the spreadsheet. The SDF could have been used from the very beginning to identify all triggers, conditions, etc., but the process we took helped us understand which triggers would fire given assumptions made by us on how a player would move through the scenario. These trigger spreadsheets helped us to consider obstacles the player might experience that were not obvious in our initial review and roadmap. Those new obstacles were then added into the roadmap. It is important to note that the process described above could have been easily replaced by simply downloading the SDF and reviewing all the triggers and conditions in the scenario, but by following this process, we could simulate the gameplay of a novice user and come to a more thorough understanding of how the game engine moves the scenario along based off the player’s actions. Ultimately this allowed us to create a more structured progression of mitigations for the player.

E. OVERCOMING BARRIERS

Upon completion of the roadmap and analysis of all triggers and conditions in the scenario being analyzed, the next step was to identify methods to overcoming the barriers, both LOs and MOs. The CyberCIEGE developers had already implemented numerous helptips throughout the scenario to assist players in overcoming most of the MOs. In most cases, these helptips were sufficient. However, in some cases, more help was needed. By reviewing all the conditions, we could determine exactly which conditions had to be met at the points where obstacles had been identified in the roadmap. The next step was to review the given set of triggers to determine if there were already triggers in place to help the player overcome the obstacle. We also reviewed the log files to determine if previously developed triggers had indeed fired during the game play and if they helped the player progress to the next step of the roadmap.

The next step was to create ways to help the player to get through any remaining learning or game mechanics obstacles. Helptips were our preferred method for overcoming MOs, as these tips were already used in CyberCIEGE to address such barriers. Another advantage of helptips is that they do not slow down the pace of the game. Guide questions were selected as the means to help players overcome LOs. There were already guidance questions in the scenarios at various points, but we determined that additional questions were necessary at certain points. Guide questions are intended to help ensure the learning objectives were met and that the player has the requisite knowledge to complete the current scenario and any subsequent, dependent scenarios.

F. ADDITIONAL GUIDE AND QUIZ QUESTIONS TO ASSIST IN ACHIEVING LEARNING OBJECTIVES

During game play, the learning objectives are not explicitly stated. The player only understands the scenario objectives that must be reached to keep making progress. However, from an educator’s perspective there are times when evaluation is beneficial to ensure the student understands the material presented. Question triggers are implemented in CyberCIEGE to assess students during game play. The questions have been and should be used sparingly, as too many questions could make the player feel as if they are taking a test, rather than playing a game.

The two types of question triggers were discussed in Chapter II. It is important to note that they serve different purposes in the context of overcoming barriers. Specifically, guide questions are presented in a Socratic style, allowing the player to revisit the actions taken up to that point and can be used to help the player determine if those actions were the best for accomplishing the scenario objective. Quiz questions, on the other hand, are designed for formal assessment and the game play moves on to the next phase without revisiting the previous phase. In the context of overcoming LOs, quiz questions were most beneficial upon completion of a phase. Quizzes give the player has an intermediate feeling of success and can demonstrate that they have the knowledge to move forward. Note that in the current implementation of CyberCIEGE, the outcome of quiz question(s) does not affect the progress of the scenario and the player can move on to the next phase. When players answer correctly, they can move on with an affirmation, but if the answer is incorrect, then the response can further explain the material associated with the learning objective.

We determined through our process and in discussion with the game developer that guide questions are more beneficial than quiz questions in overcoming obstacles. They can be designed to trigger at any point, but are most useful when the player's choice leads them in a direction that does not accomplish the scenario objective. The answers to the guide questions can be designed to capture what the player may have been thinking when they made a particular choice. The guide question then responds to the player's answer. The responses can give the player enough information to see where (s)he erred, but not directly give them the correct answer. For example, if the game designer could predict a logical fallacy that players might make, it could be captured in a guide question. The response could then help explain where player's reasoning went awry. These follow the Socratic method as discussed previously, allowing the student to learn through consequences, good or bad, of the actions.

As we identified the different obstacles the player may experience, we tried to determine the best method to overcome them. A mix of helptips and guide questions was the preferred means to give the player enough information to accomplish the scenario objectives and to make sure that learning objectives were met along the way.

G. USE OF SDT FOR IMPLEMENTING IMPROVEMENTS TO SCENARIO

Identifying the obstacles during game play was just the first part of our research process. The second part was finding a way to overcome those obstacles. We have already discussed the use of helptips and different types of questions, but we needed a way to implement these changes by developing new triggers and by testing them to ensure the new triggers fired at the correct place during game play and that they actually helped overcome the obstacles.

To simplify debugging of scenarios, the SDT provides functions to replay previously performed scenarios by repeating the events captured in the game logs. We will not recount the exact directions for debugging and replaying as they are explicitly stated in the SDT Instructions in the section labeled "Debugging, Game Logs and Replaying Scenarios" [7]. This method of replaying a scenario proved invaluable, allowing us to develop a trigger and recreate the exact scenario sequence to ensure all conditions were controlled for testing the trigger. Once a scenario has been played, the log file of that specific session can be used to replay the scenario using the exact same conditions up to any stopping point identified in the SDT as a break point. During analysis of the Network Filters scenario, a trigger was identified that was not firing at a specific point, leading to a significant MO. Once the trigger was debugged, we could replay the scenario to get back to the same point and test if the trigger did indeed fire. This saved time and energy as it can be difficult to remember exactly how to get to a specific point in the scenario and have the exact same conditions met to fire a trigger.

IV. RESULTS

This chapter will discuss the results of our analysis of two CyberCIEGE scenarios: the Network Filters scenario and the DMZ scenario. During our analysis, we found that at several points during the game, obstacles to the student emerged, whether in learning or game mechanics. We will discuss how obstacles were identified and the methods used to overcome those obstacles. In a few situations, the obstacle was determined to be a bug in the game itself and was sent to the game designer for review.

A. DESIGN OBJECTIVES OF EACH SCENARIO

The following sections discuss the scenarios analyzed during our research. We will outline each phase of the scenario and the learning objectives associated with the phases.

1. Network Filters Scenario

The Network Filters Scenario takes place at the Tireply company, a small business that sells innovative car tire designs to major tire manufacturers [14]. The scenario consists of four phases:

Phase 1: Help Larry Access the web

Phase 1A: Configure the network filter

Phase 2: Protect the Steel Asset

Phase 3: Configure the network filter to allow Secure Shell Protocol (SSH) remote access.

In this section, we will outline the design objectives of each phase of the scenario. Any obstacles that were discovered during analysis will be discussed in the next section.

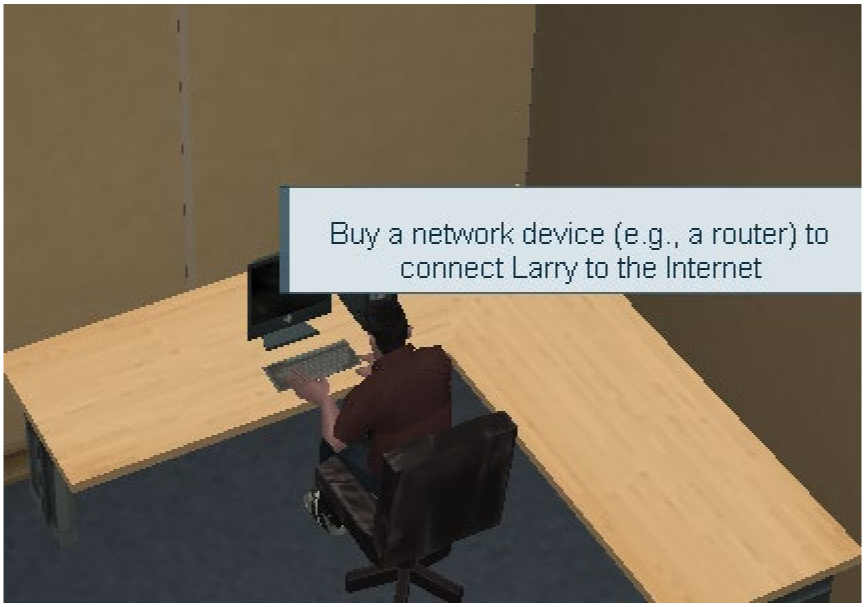
The learning objectives from this scenario are listed below.

By the end of the scenario the player will be able to:

- Understand the purpose of a router.
- Connect an enterprise network to the Internet.

- Configure a router or filter to block or permit access to different applications via specified networks.
- Protect assets on a network given their value to the company and the information security policy.
- Understand stateful routing.

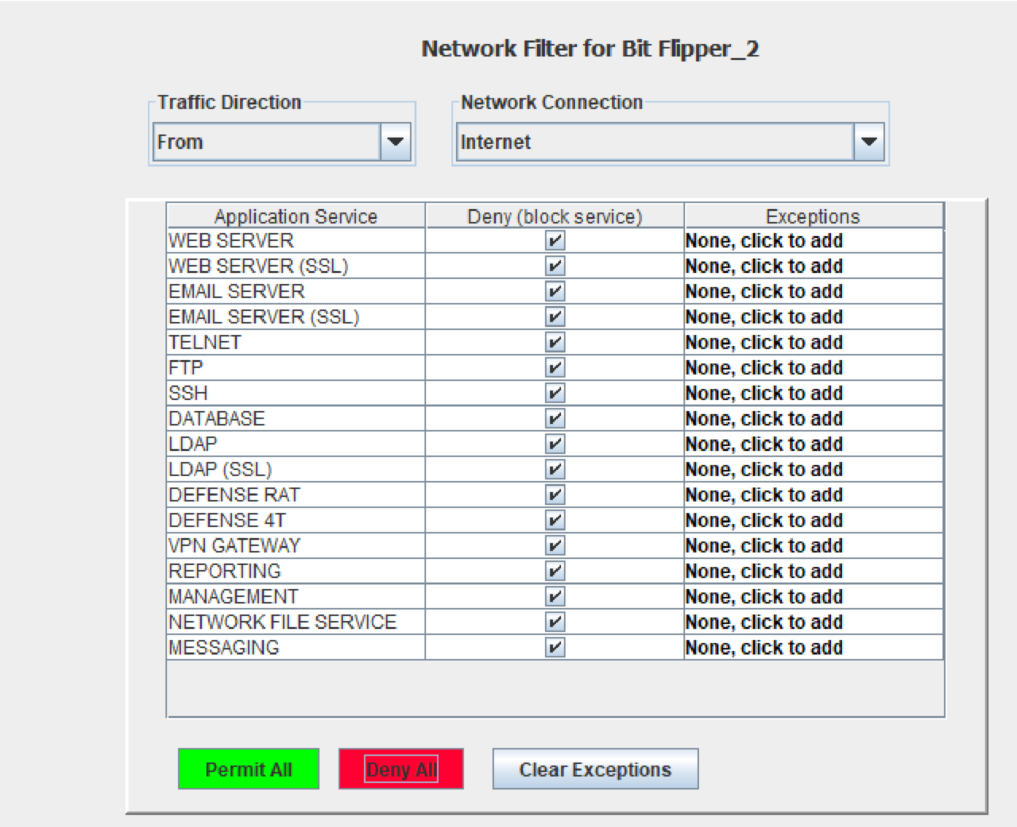
For Phase 1, the player is presented with the user Larry, who needs to perform research using the TirePly research database and resources on the web. The Network Filters lab manual identifies the following concept for this phase: “Internal networks of workstations and servers are typically connected to the Internet via a router or firewall” [14]. The player must purchase a router, as presented in Figure 14, and connect the router to both the Internet and the company’s Local Area Network (LAN). Once Larry is able to connect to the Internet and browses safely without incident for a while, the objective is marked as completed and the player moves on to the next phase.



Buy a network device (e.g., a router) to connect Larry to the Internet

Figure 14. The first phase in the network filters scenario introduces Larry and directs the player to purchase a router.

Phase 1A is technically a continuation of Phase 1 because it deals with the same user and problems associated with connecting a new router to the Internet. Thus, the game designer labeled this phase 1A. If the player connects the router to the Internet and does not configure the router to deny any outside traffic, then an attack is triggered and an outsider gains access to the research contained on the Local LAN. The learning objective associated with this phase is "Routers and firewalls typically can be configured to use filters to block or permit" traffic coming from specified networks or applications or going to specific applications within a network [14]. The player is directed to access the router network filter and configure it to deny traffic from the Internet. Figure 15 displays the router network filter configured to deny or block all traffic coming from the Internet into the local network. Successfully filtering outside traffic by denying all traffic as seen in Figure 15 will allow the player to move on to the next phase.



Network Filter for Bit Flipper_2

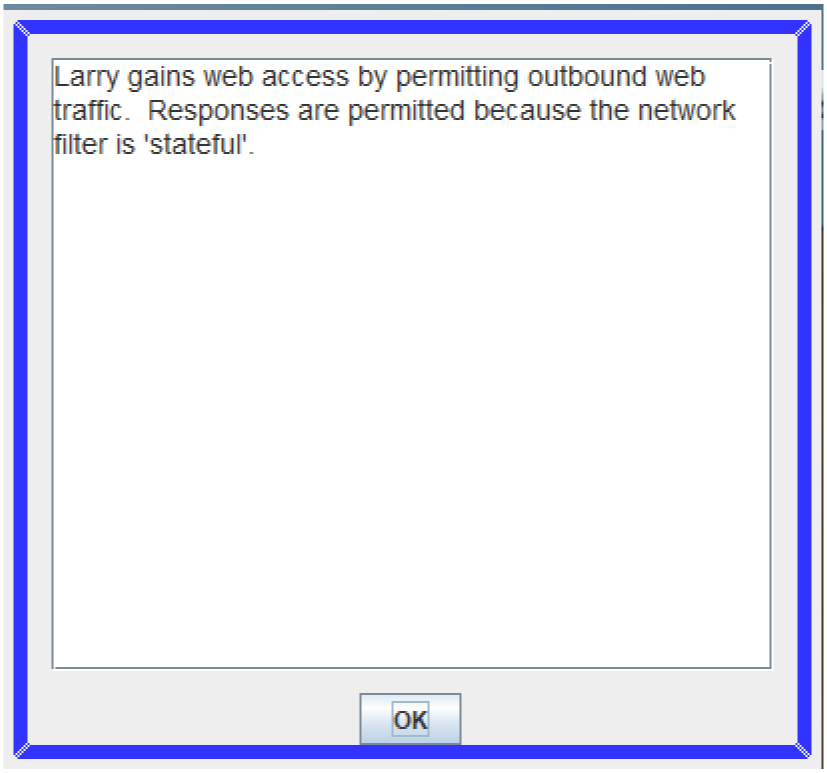
Traffic Direction: From

Network Connection: Internet

Application Service	Deny (block service)	Exceptions
WEB SERVER	☑	None, click to add
WEB SERVER (SSL)	☑	None, click to add
EMAIL SERVER	☑	None, click to add
EMAIL SERVER (SSL)	☑	None, click to add
TELNET	☑	None, click to add
FTP	☑	None, click to add
SSH	☑	None, click to add
DATABASE	☑	None, click to add
LDAP	☑	None, click to add
LDAP (SSL)	☑	None, click to add
DEFENSE RAT	☑	None, click to add
DEFENSE 4T	☑	None, click to add
VPN GATEWAY	☑	None, click to add
REPORTING	☑	None, click to add
MANAGEMENT	☑	None, click to add
NETWORK FILE SERVICE	☑	None, click to add
MESSAGING	☑	None, click to add

Figure 15. Router network filter screen for network filters scenario.

A secondary learning objective is the concept of stateful routing, meaning the router will remember the states of packets that come from the LAN and permit any received packets from the Internet in response to the original packets. This is not explicitly stated during the scenario, but review of the encyclopedia and a guide question as seen in Figure 16 imply this concept.



Larry gains web access by permitting outbound web traffic. Responses are permitted because the network filter is 'stateful'.

Figure 16. The response to a guide question at the end of Phase 1A introduces the concept of stateful routing.

Phase 2 introduces a new user, Mary, who is working on a new asset called "Steel Formula." The player is directed to learn the value of the asset and determine the best method for protecting that asset. Any attempts to configure the network filter to permit or deny traffic into the network are futile, as the value of the asset is so high that attackers always find access to the asset. If the player watches the encyclopedia tutorial movie on network filter limitations, they will learn that "sometimes the best way to protect a high value asset is to physically isolate it from other users and networks" [14]. The only acceptable resolution to this dilemma is to disconnect Mary's computer from the company LAN, and consequently, the Internet, as displayed in Figure 17. Successfully completing this will move the player to the next phase.

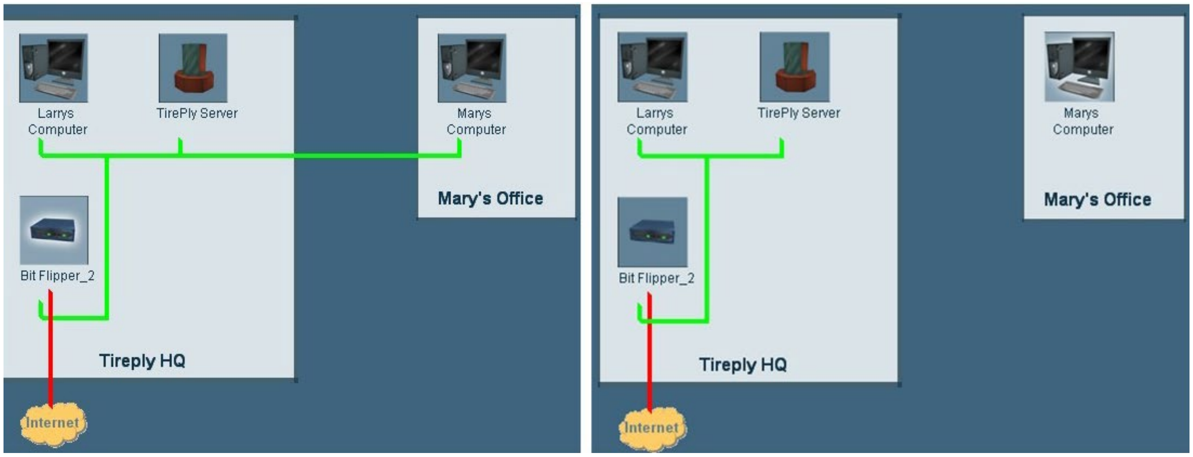
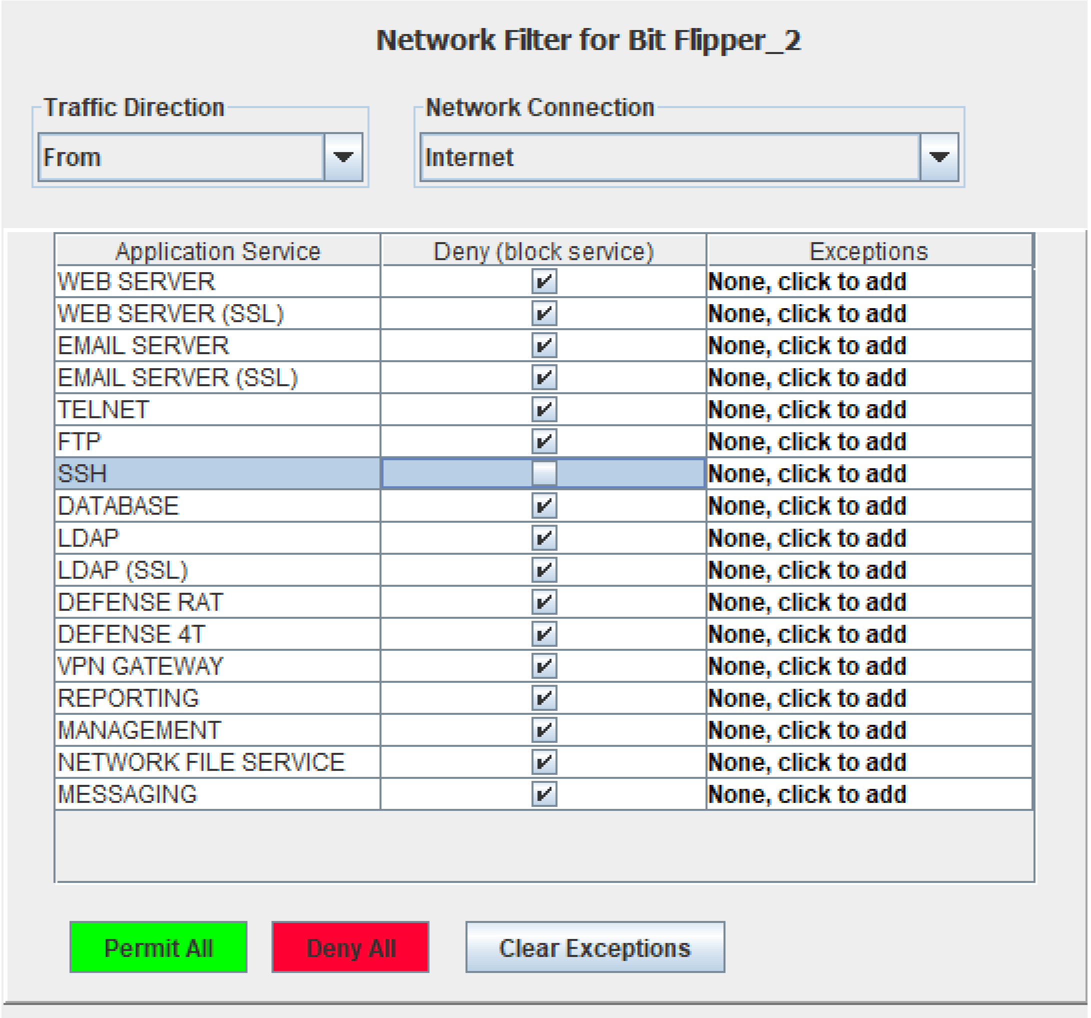


Figure 17. The green line on the left shows Mary's computer connected to the Tireply LAN, while the right side of the image shows her computer isolated from the network.

Phase 3 of the scenario moves the player to an offsite location where an individual working for a safety regulation agency who reviews tire safety data needs to access the data collected by Tireply. The learning objectives for this phase return to the Phase 1A learning objectives about configuring a router network filter. However, the player is asked to dive deeper into this subject and understand that a router can be configured to allow or deny specific protocols as well as source or destination ports. In this case, support of the external regulator requires that SSH packets from the Internet be allowed through the filter. Figure 18 demonstrates how the player can permit SSH packets from the Internet. This allows the regulator access to Tireply's research database and completes the scenario.



Network Filter for Bit Flipper_2

Traffic Direction: From

Network Connection: Internet

Application Service	Deny (block service)	Exceptions
WEB SERVER	☑	None, click to add
WEB SERVER (SSL)	☑	None, click to add
EMAIL SERVER	☑	None, click to add
EMAIL SERVER (SSL)	☑	None, click to add
TELNET	☑	None, click to add
FTP	☑	None, click to add
SSH	□	None, click to add
DATABASE	☑	None, click to add
LDAP	☑	None, click to add
LDAP (SSL)	☑	None, click to add
DEFENSE RAT	☑	None, click to add
DEFENSE 4T	☑	None, click to add
VPN GATEWAY	☑	None, click to add
REPORTING	☑	None, click to add
MANAGEMENT	☑	None, click to add
NETWORK FILE SERVICE	☑	None, click to add
MESSAGING	☑	None, click to add

Figure 18. Screenshot of the router network filter configuration page allowing SSH traffic from the Internet.

2. DMZ Scenario

The DMZ scenario builds on the lessons learned from the Network Filters scenario. The scenario takes place at the Professional Croquette Association (PCA) Headquarters. The users in the scenario maintain data for croquette standings and rankings around the world and collect sponsorships for hosting tournaments. This scenario has three phases:

Phase 1: Allow Dan to Surf the Web

Phase 2: Permit Ann to email back and forth with her daughter Bev, who is not in the PCA network

Phase 3: Provide Bobby Jack with offsite access to the PCA database.

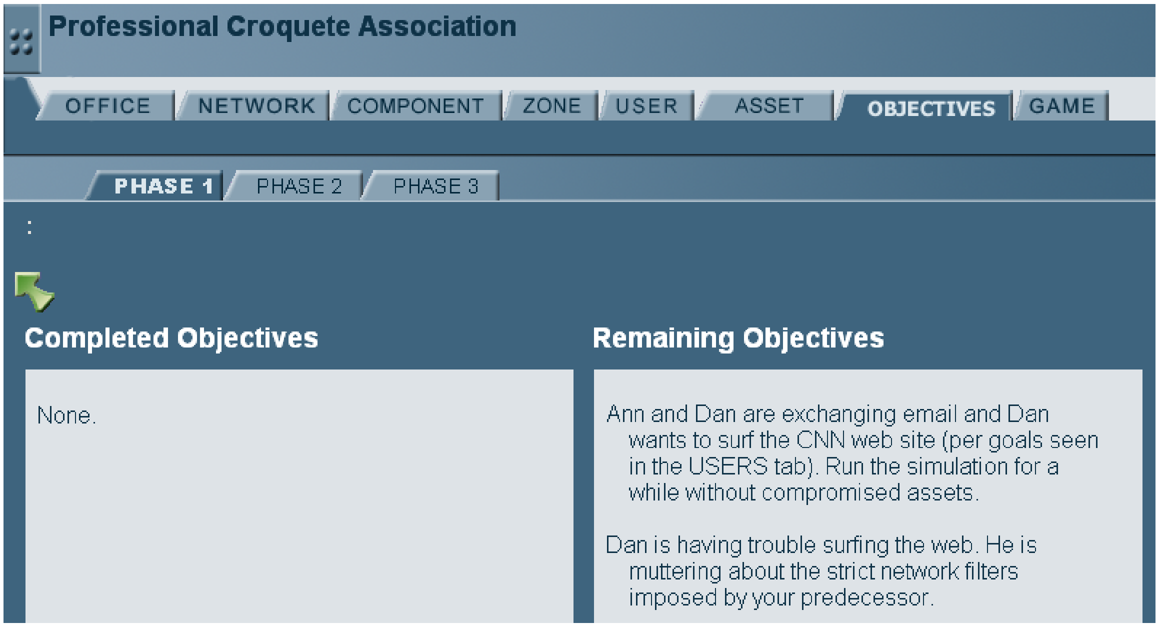
Of the game users just listed, Dan and Ann are internal to the PCA network, while Bev and Bobby Jack are external During each phase, an underlying objective is to protect the assets that reside on the PCA network, while still allowing users external to the network to communicate with users internal to the network.

The learning objectives from this scenario are listed below.

By the end of the scenario the player will be able to:

- Analyze a network configuration to identify points of entry.
- Establish patching requirements for a server.
- Understand that some server applications will always have flaws.
- Understand the purpose of a DMZ.
- Configure a DMZ.
- Understand the purpose of and be able to configure a mail proxy server.
- Understand and configure exceptions to filter configurations.
- Provide access to an asset from outside the network, while still protecting the network.

Phase 1 ties directly into the learning objectives of Phase 1A and Phase 3 of the Network Filters scenario, in that the player must configure the network filter on the router to allow the user Dan to surf the web and view the croquette standings on CNN.com. However, at this point, in game play, the player is no longer given as many hints or tips on how to achieve the objective as were provided in the Network Filters scenario. Players are required to discover the objectives on their own by selecting the appropriate tabs in the game screen, as displayed in Figure 19. Upon selecting the Objectives tab, the player will be directed to allow Dan to surf the CNN website. If the player configures the network filter to allow traffic to the Internet, then the phase will be marked as complete and the player will be moved to Phase 2.



None.

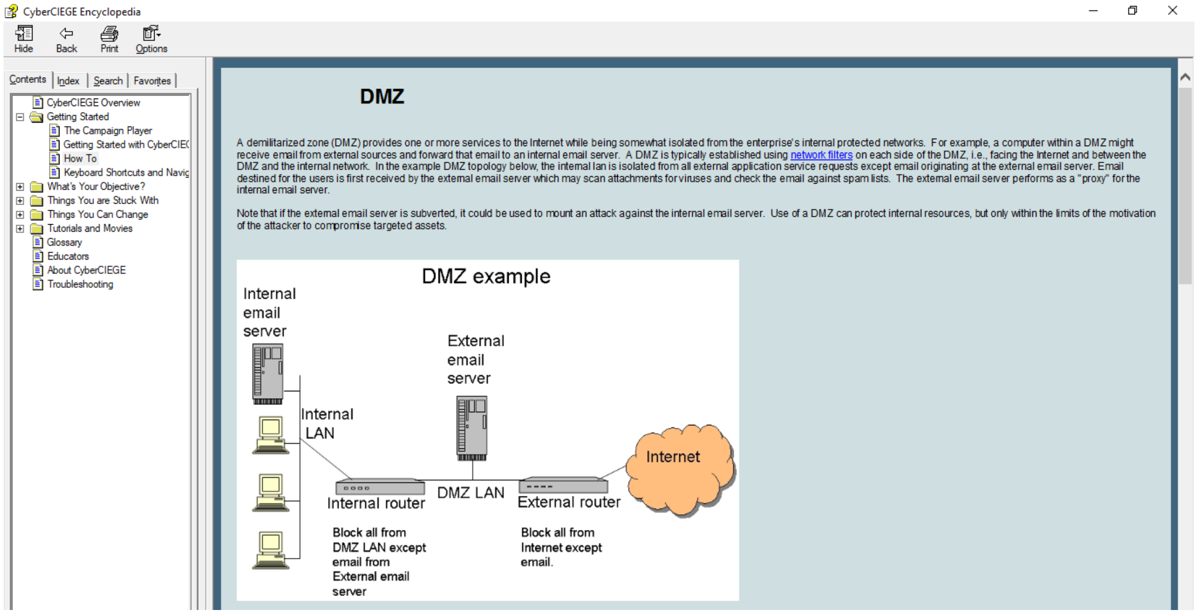
Ann and Dan are exchanging email and Dan wants to surf the CNN web site (per goals seen in the USERS tab). Run the simulation for a while without compromised assets.

Dan is having trouble surfing the web. He is muttering about the strict network filters imposed by your predecessor.

Figure 19. Screenshot of objectives tab in CyberCIEGE game.

Phase 2 of the DMZ scenario introduces a much more complex set of learning objectives. Bev is a new user who is not an employee of PCA but is trying to send an email to her mother Ann, who works for PCA and is a tournament director responsible for raising funds from sponsors. For Bev and Ann to be able to send emails back and forth and to still protect the assets located on PCA network the player is required to build a DMZ. The CyberCIEGE encyclopedia has a detailed entry on what a DMZ is and how to build one. A screenshot of the instructions is presented in Figure 20.

The instructor notes for the DMZ scenario [13] clarifies that the player must also learn that an email server that contains sensitive internal company emails can be hidden behind an internal network filter. “An external email ‘proxy’ can be configured to receive email from outside of the company and forward that email to the internal server” [13]. This requires the player to purchase the correct additional equipment and configure the routers and servers in a way that blocks malicious packets, but still allows safe packets in and out. After construction of the DMZ and activating the email proxy, Bev and Ann are able to exchange emails and the player is moved to the last phase in the scenario.



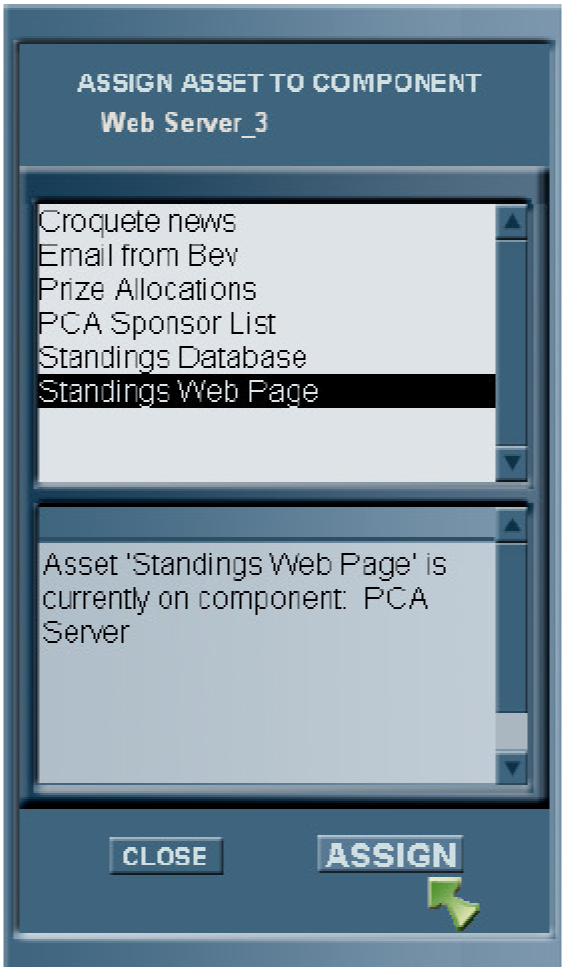
DMZ

A demilitarized zone (DMZ) provides one or more services to the Internet while being somewhat isolated from the enterprise's internal protected networks. For example, a computer within a DMZ might receive email from external sources and forward that email to an internal email server. A DMZ is typically established using network filters on each side of the DMZ, i.e., facing the Internet and between the DMZ and the internal network. In the example DMZ topology below, the internal lan is isolated from all external application service requests except email originating at the external email server. Email destined for the users is first received by the external email server which may scan attachments for viruses and check the email against spam lists. The external email server performs as a "proxy" for the internal email server.

Note that if the external email server is subverted, it could be used to mount an attack against the internal email server. Use of a DMZ can protect internal resources, but only within the limits of the motivation of the attacker to compromise targeted assets.

Figure 20. Screenshot of CyberCIEGE Encyclopedia entry on how to construct a DMZ.

Phase 3 of the DMZ scenario has a learning objective similar to that of Phase 2. The player is presented with Bobby Jack who is trying to access the PCA database from an offsite location. The initial thought may be to configure the router to allow access from the Internet to the database. The standings database and the web page are both hosted on the PCA Server If the player permits web traffic into the internal server, then flaws in its web server application will expose PCA assets to external users and attackers. The player must buy a web server for the DMZ, move the web page onto the new web server, and then permit database traffic from the DMZ into the internal server [13]. The player must then move the Web Page from the internal server to the DMZ server, as seen in Figure 21, so that outside parties can access it.



Croquete news
Email from Bev
Prize Allocations
PCA Sponsor List
Standings Database
Standings Web Page

Asset 'Standings Web Page' is currently on component: PCA Server

Figure 21. Screenshot of assigning Standings Web Page to the DMZ Web Server, listed as Web server_3.

B. DISCOVERED OBSTACLES

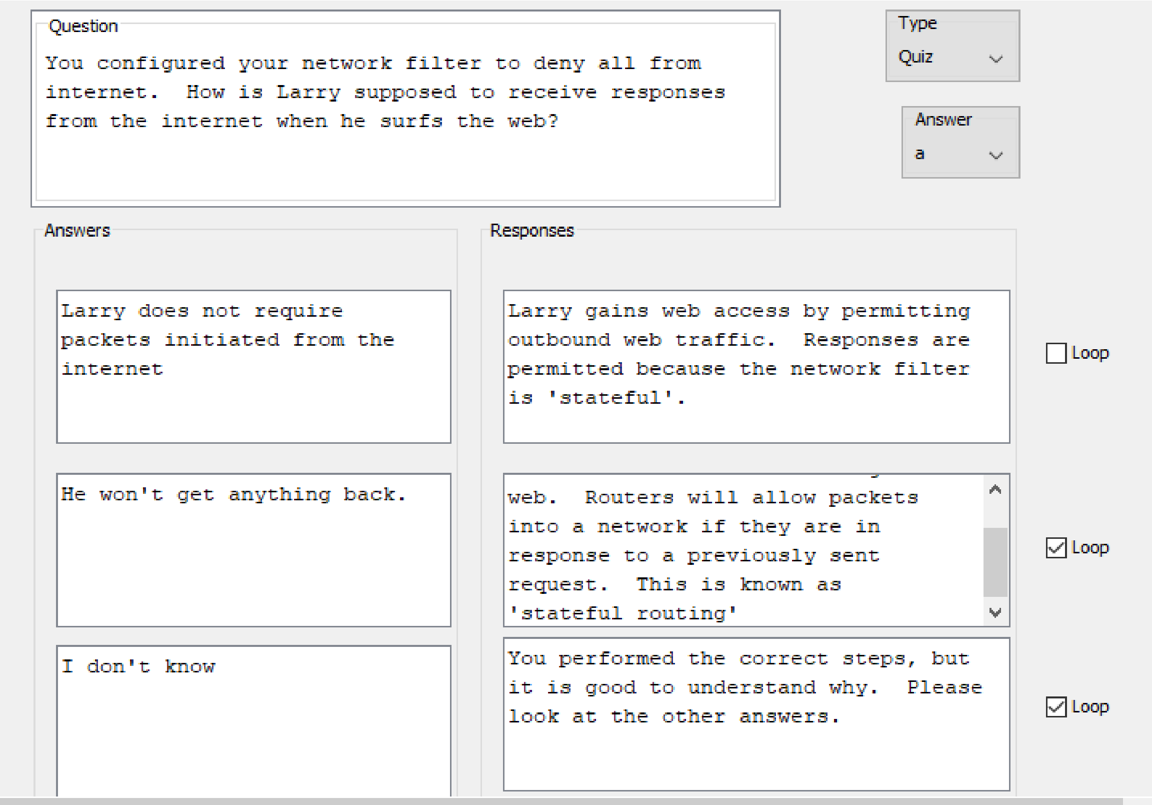
In this section, we will discuss the learning obstacles a player may encounter during game play. While creating our roadmap, we listed any point in the game that could be considered a learning obstacle or a game mechanics obstacle. These obstacles were determined by attempting to understand how an average game player may think. Many obstacle points already have sufficient help built into the game design to overcome the obstacle. In our work we only considered those points where additional help needed to be incorporated into the game to assist the player in surmounting the obstacles. As a result of our analysis, we were also able to provide comments about learning objectives that are not sufficiently met and how we made additions to the game play to remedy this.

1. Obstacles with Resolutions

Most of the obstacles we discovered during our analysis could be overcome by solutions that we implemented with guide questions and helptips. Those obstacles are discussed in this section.

a. Network Filters Scenario

Understanding the notion of stateful routing is one of the learning objectives that the game designers intended for the players to achieve. Players first encountered stateful routing in Phase 1A of the Network Filter Scenario. The phase contains a guide question that refers to stateful routing, but the question only pops up in the event that the player configures the network filter to allow Web Server traffic from the Internet but denies other types of traffic. Although this is a probable path the player may take, it is not possible to guarantee that every player will actually take that path. If the player chooses another solution, even the correct solution of denying Web Server traffic from the Internet, (s)he will not encounter a reference to stateful routing. To ensure that players were exposed to the notion of stateful routing, we created an additional quiz question at the completion of Phase 1A that asks the player to consider why they configured the router the way they did and how Larry can receive a response from the Internet. The question as programmed in the SDT can be seen in Figure 22.



Question

You configured your network filter to deny all from internet. How is Larry supposed to receive responses from the internet when he surfs the web?

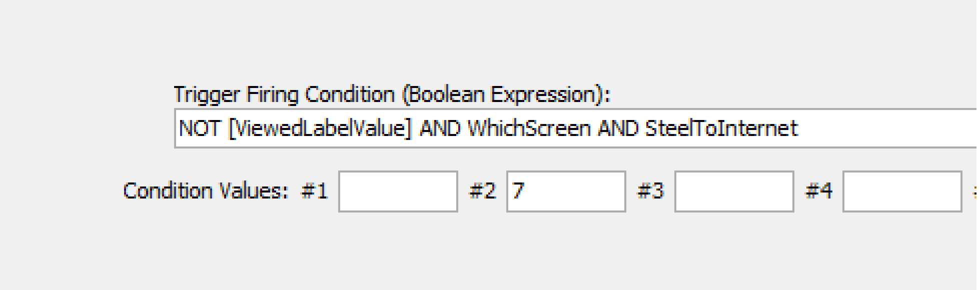
Type: Quiz

Answer: a

Answers	Responses	
Larry does not require packets initiated from the internet	Larry gains web access by permitting outbound web traffic. Responses are permitted because the network filter is 'stateful'.	□ Loop
He won't get anything back.	web. Routers will allow packets into a network if they are in response to a previously sent request. This is known as 'stateful routing'	☑ Loop
I don't know	You performed the correct steps, but it is good to understand why. Please look at the other answers.	☑ Loop

Figure 22. SDT entry for guide question that helps player to understand stateful routing.

In Phase 2, the player is required to disconnect Mary from the Local LAN. However, there are a number of concerns that were discovered in review of this phase. The game designer intends for the player to understand the value of an asset and why it is important to protect it. The phase contained a trigger that was designed to fire and help the player know where to click to learn about the asset's value, however, the trigger never fired. We discovered that the conditions for the helptip trigger to fire had to be met seven times. Waiting for a condition to be met seven times would exhaust a lot of game time and most players would not be on the asset screen long enough for the trigger to fire, so they would never know how to find the value of the asset. We deleted the requirement for seven iterations of the condition, at which point the helptip was visible the first time the conditions were met. Figure 23 shows that the parameters for the condition WhichScreen were set to 7, which indicates the player is viewing the asset screen. The SteelToInternet parameters were also set to 7, which is the faulty requirement that the condition be met 7 times.



Trigger Firing Condition (Boolean Expression):

NOT [ViewedLabelValue] AND WhichScreen AND SteelToInternet

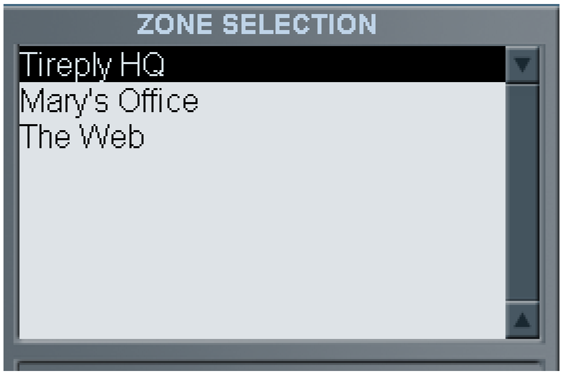
Condition Values: #1 #2 7 #3 #4

Figure 23. Trigger firing conditions for the prompt to view the steel formula value were fixed.

The scenario briefing tells the player they can largely ignore physical and procedural security in this scenario, and yet physical security is mentioned in the label description. If the player views the value of the asset, they will see that it is set to 600. The overall security of the building is 1000, which is sufficient physical security, but the current security level of Mary's Office is 497. Upon seeing this, the player may attempt to change the physical security of the Zone. To change the physical security, the player would select the tab for Zones and add security components to the appropriate zone. The zone in question is listed as Upper Right, but the player may not understand this is Mary's Office, so we changed the name of the Zone to Mary's Office as seen in Figure 24.

The physical security requirement for Mary's Office can also be misleading because no amount of physical security upgrades will affect the outcome of the scenario. In our analysis of the phase, we attempted to predict incorrect solutions that the player could attempt to implement and chose the three most likely. The most likely incorrect solutions were adding more secure locks, adding biometric requirements to enter the space, or attempting to add an additional filter. We reviewed the current triggers in the game that could help the player come to the correct solution and determined that there were triggers to help the player in two of the three likely incorrect solutions: the more secure locks and the biometric scanner.

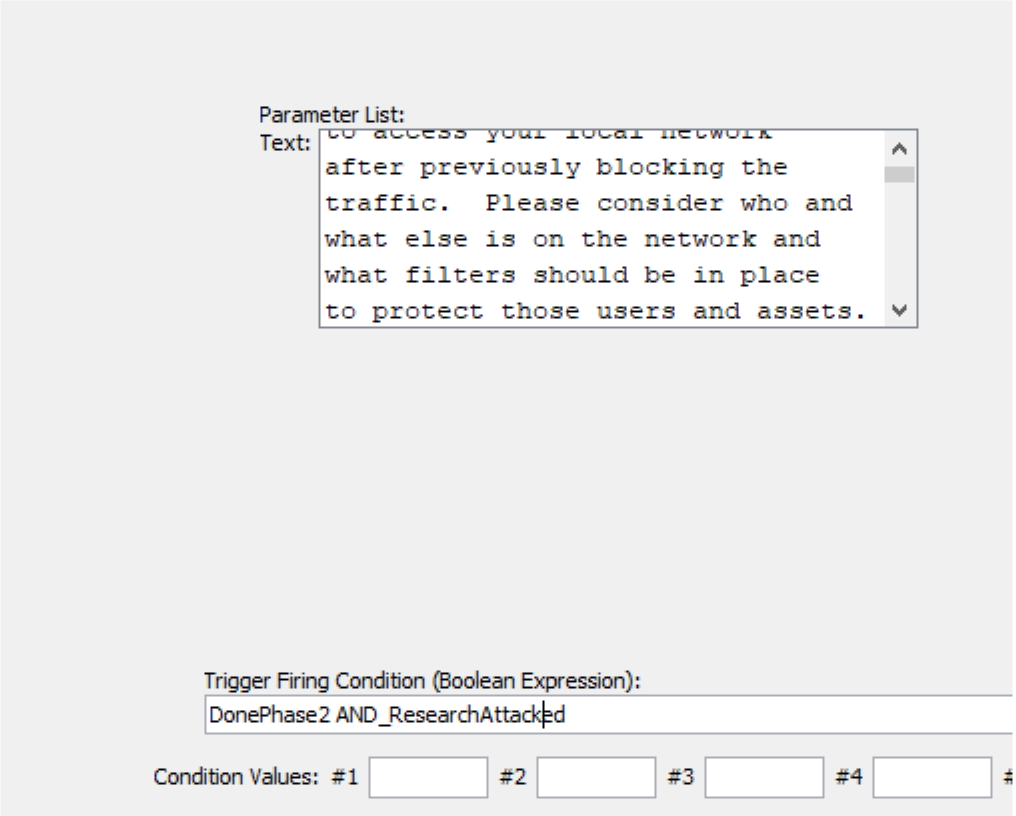
The third possible incorrect solution was for the player to add a second filter. To step the player past this incorrect choice, we developed a guide question to help the player understand that the value of the asset was so high that no number of filters would deter a determined hacker or prevent preexisting malware from sending the sensitive "Steel Formula" information to an external source.


ZONE SELECTION

Tireply HQ
Mary's Office
The Web

Figure 24. The upper right zone was renamed to Mary's Office.

In the third phase of this scenario, the player is, for a second time, presented with a situation that requires configuring the network filter. If the player undoes the configurations from previous phases and allows other traffic from the Internet to access the company LAN, the assets on the local network will be attacked again. To help the player avoid this mistake, we introduced a help tip that reminds the player to think of who else needs access to the Internet and what assets reside on the network to determine how the filter should be configured for the other users and assets on the network to stay safe from malware and attacks. The SDT entry for this trigger can be seen in Figure 25.



Parameter List:

Text:

```
to access your local network
after previously blocking the
traffic.  Please consider who and
what else is on the network and
what filters should be in place
to protect those users and assets.
```

Trigger Firing Condition (Boolean Expression):

DonePhase2 AND_ResearchAttacked

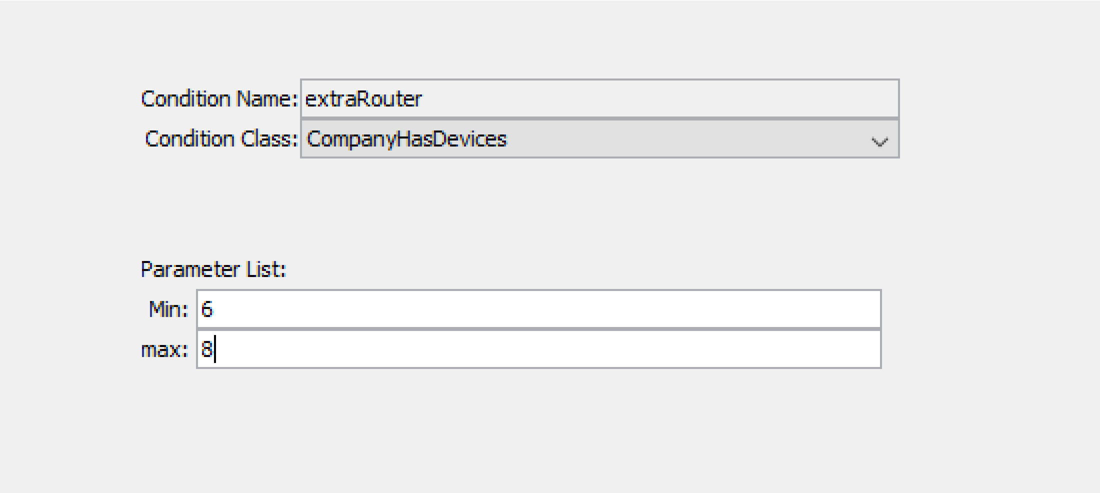
Figure 25. SDT entry for filterundone trigger.

b. DMZ Scenario

In Phase 2 of the DMZ scenario, the average player will not know how to construct a DMZ, nor even understand the need for one. All phases of the Network Filters scenario and the Phase 1 of the DMZ scenario were solved by configuring a network filter. Well configured networks, though, are insufficient for DMZ Phase 2. The optimal way for a player to learn about a DMZ and how to construct one is to reference the DMZ section in the Encyclopedia. However, if the player does not even know enough to ask about a DMZ, then they will never come to the correct solution.

This phase of the scenario was designed with one MessageTrigger that should have fired instructing the player to press F1 and read the Encyclopedia entry on DMZs. Experimentation showed that this trigger was not firing. Upon further analysis, we discovered that one of the conditions for the trigger was a total count of company devices. The game engine keeps a count of all components in a scenario, including components purchased by the player. When the count meets the parameters specified by the game designer, then the condition is met. The problem with this is that the game engine cannot differentiate between devices owned by the company and devices in other locations, such as the hotel room. The original condition was set to count only the company devices. Once we changed the parameters of the condition to include the total number of network components in the scenario, as seen in Figure 26, the trigger fired. This solution was sufficient for the one preexisting trigger to fire, but we determined that more references to the Encyclopedia were needed.

Up to this point, the player could have completed all phases without ever referring to the Encyclopedia, so it is possible that the player may not be familiar with the CyberCIEGE Encyclopedia. In the event that the player did not execute the game in a way that met the conditions discussed in the previous paragraph, additional message triggers and references to the Encyclopedia were added at different points to give proper support to the player.



Condition Name: extraRouter
Condition Class: CompanyHasDevices

Parameter List:
Min: 6
max: 8

Figure 26. Revised condition parameters for the MessageTrigger to fire including an increased number of devices counted.

While analyzing the instructions for the DMZ, we again attempted to predict likely mistakes a player may make while building the DMZ. The four most probable errors were: (1) the direction of the filter configuration, (2) connecting the internal router to the Internet,

(3) forgetting to configure the proxy server and (4) forgetting to select regular or automatic patching for the server.

In the first case, the player is required to allow email traffic from the Internet into the DMZ. However, when the player opens the network filter configuration window, there are drop downs to select which network to configure and in which direction the filtered traffic is flowing – whether into or out of the router. For example, Figure 18 displays the network configuration window. At the top of the screen, the player can select the direction To or From as well as the network in reference, meaning the traffic is flowing to the specified network or from the network. Once the DMZ LAN is established, then the player can choose from either the Internet, the DMZ LAN or the PCA LAN. This could be confusing, and it would be easy to misconfigure the filters. If a player does this, (s)he will continue to fail to achieve the Send Email goals. Although there is a way to determine if the filters are configured for an asset to be accessible from one direction and not the other, we instead recommended a time condition that refers the player back to the Encyclopedia entry to review the proper configuration of the DMZ. A time condition keeps track of the amount of time that has passed in the game, and a trigger with a time condition fires after the specified amount of time.

The last three hypothesized errors already have sufficient support, or we determined that, at this point in the game, the player should be able to find the solution on their own. Each is described below.

If a player makes the second likely error of connecting the internal router to the Internet, then they will be continuously attacked.

The third probable error deals with configuring the email proxy. Once the email server is purchased and connected to the DMZ, the player must still enable the proxy server by checking a box in the email server configuration page. We could create helptips that references the Encyclopedia DMZ entry if a certain number of attacks occurs or if the email server is purchased but not working, but at this point, we want the player to be able to recognize attacks and identify a way to prevent attacks.

The fourth likely error is forgetting to establish a patching policy as in Phase 1 of the scenario. There are already Message Triggers installed in the game to remind the player to do so.

One of the learning objectives for Phase 2 is the need for proper patching. Helptip triggers guide the player to ensure patches are either regularly or automatically updated. Although this is a requirement for successfully completing Phase 3, it does not meet the conditions necessary to complete Phase 2. As already discussed, the player is required to construct a DMZ. Once the DMZ is constructed, the player may be confused as to why patching was required, even though it did not completely solve the problem. To alleviate this confusion, we created a guide question to discuss why patching is inadequate, but still necessary. This will help the player to remember to patch additional equipment purchased for Phase 3.

In Phase 3, the player is asked to provide a way for an outside entity to gain access to an internal asset. This is very similar to the final phase in the Network Filters scenario. Unfortunately, the solution used in the Network Filters scenario will not work for the DMZ scenario. If a player tries to configure the network filter as they did in the previous scenario, it is possible the player does not recognize the differences in the two situations, that SSH access requires use of an application service (and thus a different TCP port) than does viewing a web page hosted on a server. Our solution was to add a guide question that helped the player identify the differences in the two scenarios and lead them to installing a web server within the DMZ as the solution.

2. Obstacles without resolutions

Two points in game play stands out as unfixable at our level and must be referred to the game designer for further consideration. The first point is in Phase 2 of the Network Filters scenario. As discussed already, there are references to the value of the asset and the physical security of the zone where the asset is located. In attempting to adjust the physical security level of the entire office and Mary’s Office, we identified a bug. In theory, if the physical security level of the zone were lower than the value of the asset, the asset would be vulnerable to physical attacks, such as someone walking into the space and stealing the asset. Inspection shows that those attack triggers are firing, but the game does not present any successful physical attacks. There is a bug in the game design that allows physical security vulnerabilities to exist but not be exploited. However, in this scenario physical security is a distraction, and not a solution. Consequently, we presented two possible solutions to this issue. The first is the simplest solution: to remove all references to physical security and the value description of the asset. That would be consistent with the initial scenario design, which was intended to avoid having the player worry about physical security. The second is to create a feature that prevents players from adjusting the physical security of a zone in those scenarios where physical security is not the primary concern.

The second point that requires designer attention is in Phase 1 of the DMZ scenario where the player is asked to allow Dan to surf the web, specifically giving him access to the CNN website. The solution is to configure the router to allow Web Server messages from the PCA LAN to the Internet. If a player already has previous knowledge of network filters, (s)he may create a filter exception as a viable solution to permit Dan to surf cnn.com. However, the game design requires the exception to provide the full host name "CNN Web Server" or the domain and a wildcard such as CNN.*. If a player attempts to add an exception but lists the server as anything other than the two permitted forms of the host name, then the exception will not work. The encyclopedia does not provide help on this topic to guide the player. Additionally, there is no current way to determine that the player has defined an incorrect network filter exception. We can track conditions to determine if a filter has been configured, but additional analysis would be needed to determine the correctness of the filter exception. Even though an understanding of filter exceptions is not necessary to complete the phase, it is still applicable to this scenario and could help those players who have a more advanced understanding of network filter configuration and are familiar with exceptions to policy.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION AND FUTURE WORK

This chapter provides a summary of our research and a discussion of possible future work.

A. CONCLUSION

With the concepts and processes developed by this thesis research, it is now possible to evaluate current and future CyberCIEGE scenarios for effectiveness in achieving learning objectives, identifying learning or game mechanics obstacles a player may encounter during game play, and helping players overcome those obstacles. By creating a process that can be repeated, educators and scenario designers can systematically apply it to ensure that students and players are learning in accordance with the intended learning objectives.

Our research focused on two scenarios from the CyberCIEGE game: Network Filters and DMZ. We selected these scenarios since the Network Filters scenario is considered a beginner scenario, i.e., one that can be played without any previous experience, and the DMZ scenario builds on lessons learned in the Network Filters scenario. It was important to evaluate scenarios that build on each other, as our research was focused on how learning objectives are met and utilized as students advance from rudimentary to more advanced scenarios during game play.

During our analysis, we identified two types of barriers the player may encounter during game play. The first type of obstacle we defined as a learning obstacle. These are the points in the game where a player is required to take a certain action to complete the phase, but in which a lack of requisite knowledge prevents the player from completing the action.

The second type of obstacle is a game mechanics obstacle. When the task presented to the player is unlike any previous tasks, the play may not know what to do to complete the task. An example of this is the very beginning of the Network Filters scenario. The player is told to purchase a router and connect it to the Tireply network. If this is the first scenario played by the player, they may not be familiar with where to purchase a router, and on which screen (s)he can connect it to the network. This is not a barrier to understanding the concept, but of how to accomplish the task.

The scenario designers were able to identify most of the obstacles a player may encounter and used a combination of helptip triggers and guide questions. The helptips are bubbles that pop up telling the player where to click or what to do to take the correct action to complete the phase. The guide questions fire at specific times when the game state meets specified conditions indicating the player has made a mistake in trying to complete the phase. The questions were designed by first analyzing the logic that led to the mistake and then by providing prompts within the game that help the player make correct actions.

The assessment and guide questions and helptips that we designed as a result of our analysis of the two scenarios serve as examples of in-game support that can help players overcome these two types of barrier. If the assessment and feedback can help the player overcome these two barriers, then they can progress to more scenarios and concepts. Ultimately, this provides the player with a deeper understanding of cybersecurity.

We conclude that the revised scenarios meet the learning objectives intended by the scenario designer and there are sufficient guides and helptips to ensure a player at any level of previous experience can overcome obstacles that they may be encountered in the game.

B. FUTURE WORK

Our primary goal was to determine if learning objectives were being met and if there were obstacles players might encounter that the scenario designer had not accounted for. A second goal was to develop a method for similar evaluations of additional game scenarios. While we do not anticipate that this process can be automated yet, we believe that the approach presented in Chapter III can be applied to additional scenarios. This would be the next logical step.

One future improvement is to the visual representations of the game flow, or the roadmaps which were created and are represented in Appendix A and Appendix C. It is important to note that these roadmaps are a personal attempt at a visual rendering of the choices a player can make in the game to identify points where obstacles can occur but may be difficult for others to follow. A standard modeling system, e.g., UML or Monterey Phoenix, could be applied to the scenarios, thus creating game flow aids in a more structured format.

Another area of future works is in the automation of portions of the scenario analysis, such as identifying all triggers and conditions and parsing the log files. Again, automation was beyond the scope of this research, but the method developed in this research might be encoded to automate the identification of obstacles. This would simplify review of all the scenarios in the CyberCIEGE game. Such automation could be applied to future scenarios as designers try to identify the best ways to help players through a given scenario.

A third area for future work involves the guide questions. The guide questions we created were at points where we determined the learning objectives were not being met. The triggers for these questions are intended to fire at points when it appears that the player needs assistance in completing the phase. The intent is for the questions to be more selective: given a determination of the player’s current barrier, the appropriate question will be chosen. For example, if the player displays sufficient understanding of the scenario through the actions already chosen, the guide question could be skipped or could present a topic that requires deeper analysis. On the other hand, if the player is struggling to complete a phase, then the guide question that fires will be more focused on helping the player learn the correct information to complete the phase. The second example of questions firing when a player is struggling is along the lines of what we developed in our research.

Finally, the ultimate extension of this research would be to conduct a study of players attempting these and other scenarios. This work would identify additional obstacles that players may encounter. With a large enough population of subjects, statistical analysis could be used to identify trends in game play and particular points at which players may encounter barriers to scenario completion. Live tests and postgame feedback forms and log file reviews could all be used in this study.

Our intent was not to conduct a comprehensive analysis of all CyberCIEGE scenarios. Rather, we provide an initial study of how to improve CyberCIEGE so future players have the information necessary to complete phases and scenarios, and that obstacles encountered during game play are overcome.

.

APPENDIX A. NETWORK FILTERS SCENARIO GAME FLOW ROADMAP TO DETERMINE OBSTACLES

The purpose of this appendix is to show the game flow roadmap that we created to determine points where the player may experience obstacles to achieving the scenario objectives in the Network Filters scenario.

A. METHODOLOGY

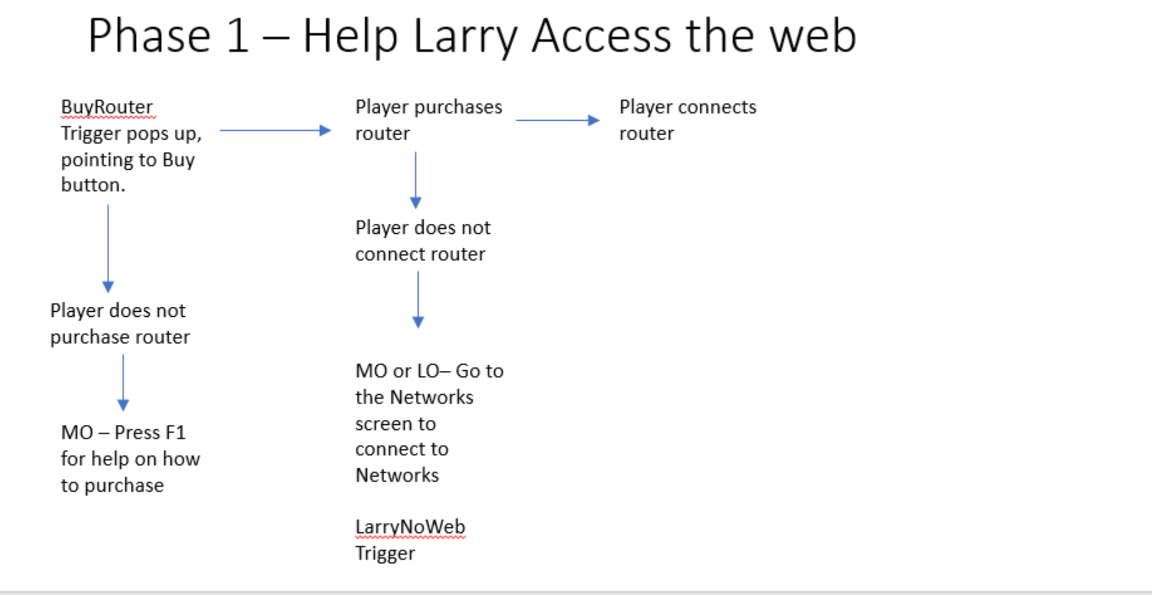
As discussed in Chapter III, we started the game flow at the completion of the last phase and ended the flow with the task necessary to complete the phase. From there, we created a road map that included possible options a player might take based on the given information and the communicated objectives. If there was an option to take an action that did not accomplish the tasks assigned, then we labeled that point an obstacle. If the required action was new to the game play, then we determined the obstacle to be game mechanics. If the required action was one that had been completed already in a previous phase, then we determined that the obstacle was in the understanding of the material and required more instruction to overcome.

The red circles indicate points in the game we determined could use additional help in overcoming the obstacle.

B. LEGEND

Game mechanics obstacles are labeled MO.

Learning obstacles are labeled LO.



Phase 1 – Help Larry Access the web

BuyRouter Trigger pops up, pointing to Buy button.

Player does not purchase router

MO – Press F1 for help on how to purchase

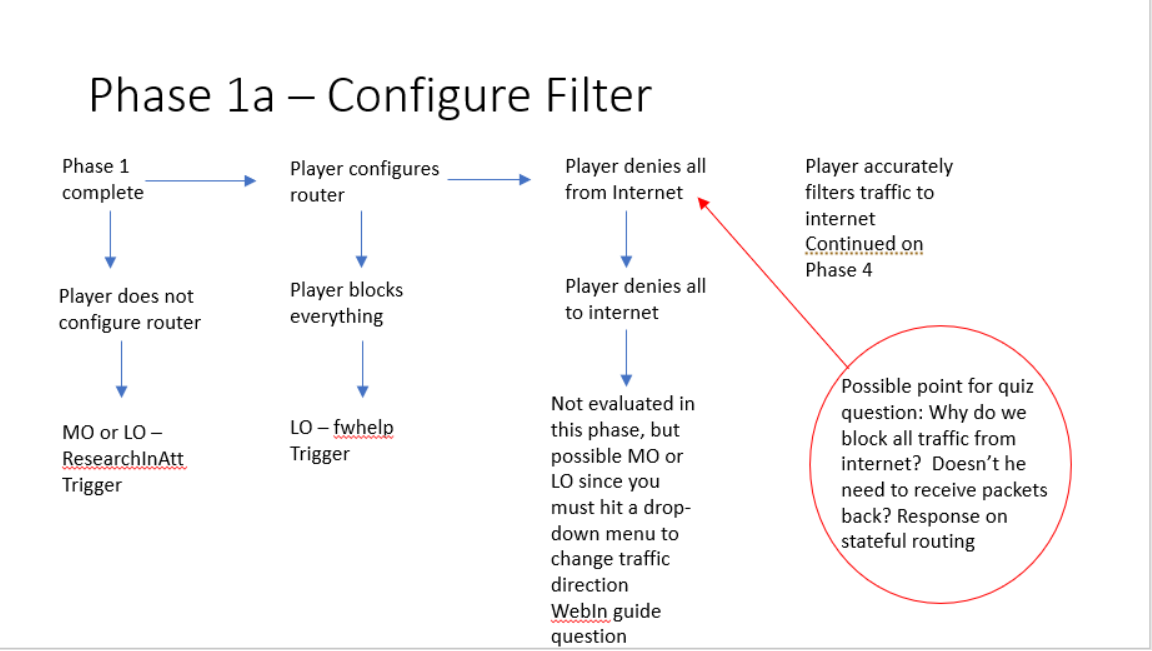
Player purchases router

Player does not connect router

MO or LO– Go to the Networks screen to connect to Networks

LarryNoWeb Trigger

Player connects router



Phase 1a – Configure Filter

Phase 1 complete

Player does not configure router

MO or LO – ResearchInAtt Trigger

Player configures router

Player blocks everything

LO – fwhelp Trigger

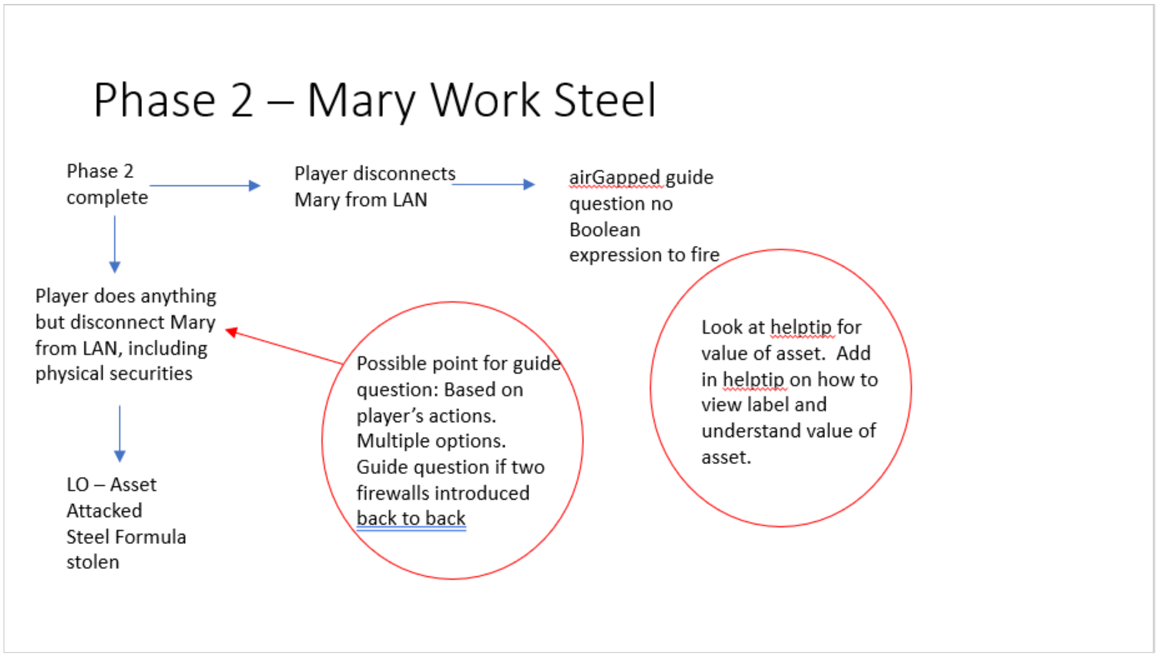
Player denies all from Internet

Player denies all to internet

Not evaluated in this phase, but possible MO or LO since you must hit a drop-down menu to change traffic direction WebIn guide question

Player accurately filters traffic to internet Continued on Phase 4

Possible point for quiz question: Why do we block all traffic from internet? Doesn't he need to receive packets back? Response on stateful routing



Phase 2 – Mary Work Steel

Phase 2 complete

Player disconnects Mary from LAN

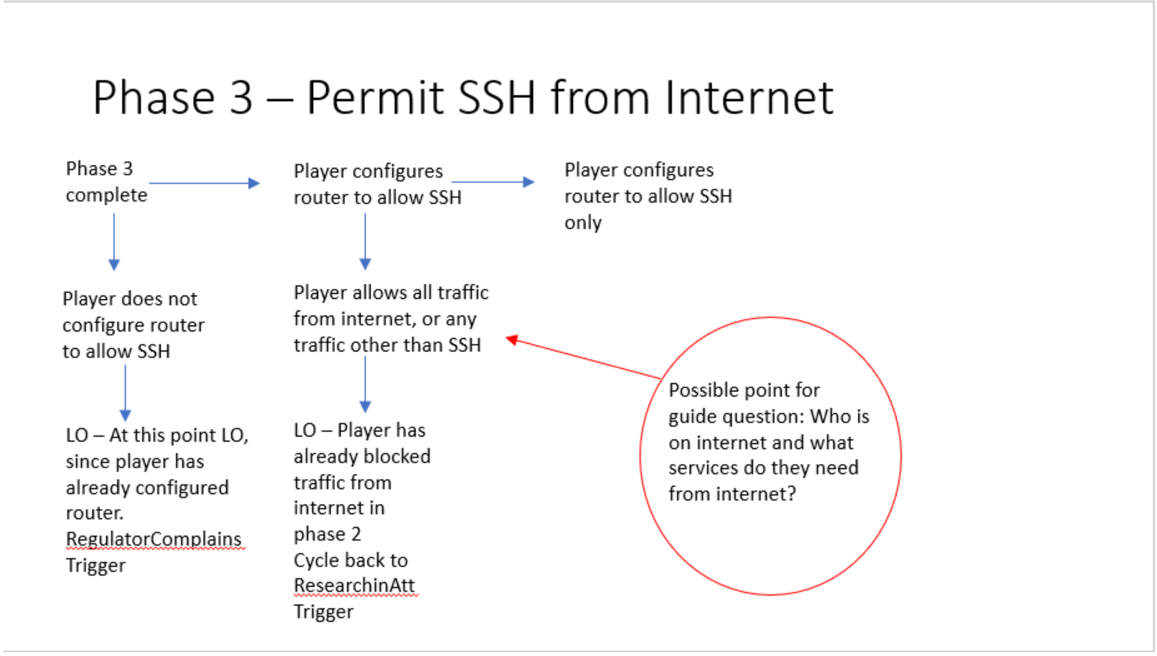
airGapped guide question no Boolean expression to fire

Player does anything but disconnect Mary from LAN, including physical securities

Possible point for guide question: Based on player's actions. Multiple options. Guide question if two firewalls introduced back to back

Look at helptip for value of asset. Add in helptip on how to view label and understand value of asset.

LO – Asset Attacked Steel Formula stolen



Phase 3 – Permit SSH from Internet

Phase 3 complete

Player configures router to allow SSH

Player configures router to allow SSH only

Player does not configure router to allow SSH

Player allows all traffic from internet, or any traffic other than SSH

Possible point for guide question: Who is on internet and what services do they need from internet?

LO – At this point LO, since player has already configured router. RegulatorComplains Trigger

LO – Player has already blocked traffic from internet in phase 2 Cycle back to ResearchinAtt Trigger

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. DMZ SCENARIO GAME FLOW ROADMAP TO DETERMINE OBSTACLES

The purpose of this appendix is to show the game flow roadmap that we created to determine points where the player may experience obstacles to achieving the scenario objectives in the DMZ scenario.

A. METHODOLOGY

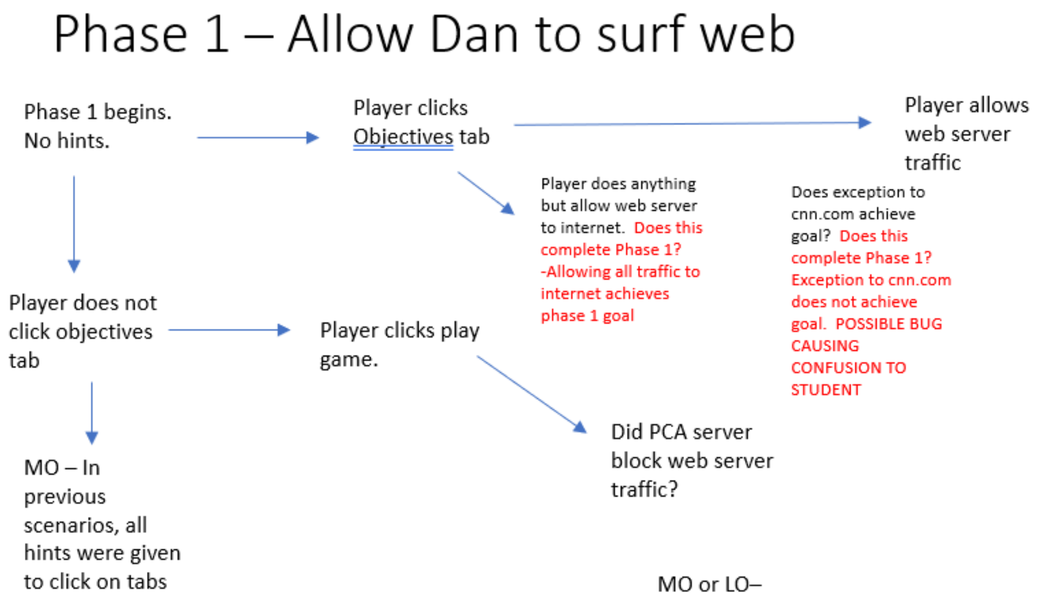
As discussed in Chapter III, we started the game flow at the completion of the last phase and ended the flow with the task necessary to complete the phase. From there, we created a road map that included possible options a player might take based on the given information and the communicated objectives. If there was an option to take an action that did not accomplish the tasks assigned, then we labeled that point an obstacle. If the required action was new to the game play, then we determined the obstacle to be game mechanics. If the required action was one that had been completed already in a previous phase, then we determined that the obstacle was in the understanding of the material and required more instruction to overcome.

The red circles indicate points in the game we determined could use additional help in overcoming the obstacle.

B. LEGEND

Game mechanics obstacles are labeled MO.

Learning obstacles are labeled LO.



Phase 1 – Allow Dan to surf web

Phase 1 begins. No hints.

Player clicks Objectives tab

Player allows web server traffic

Player does anything but allow web server to internet. Does this complete Phase 1? -Allowing all traffic to internet achieves phase 1 goal

Does exception to cnn.com achieve goal? Does this complete Phase 1? Exception to cnn.com does not achieve goal. POSSIBLE BUG CAUSING CONFUSION TO STUDENT

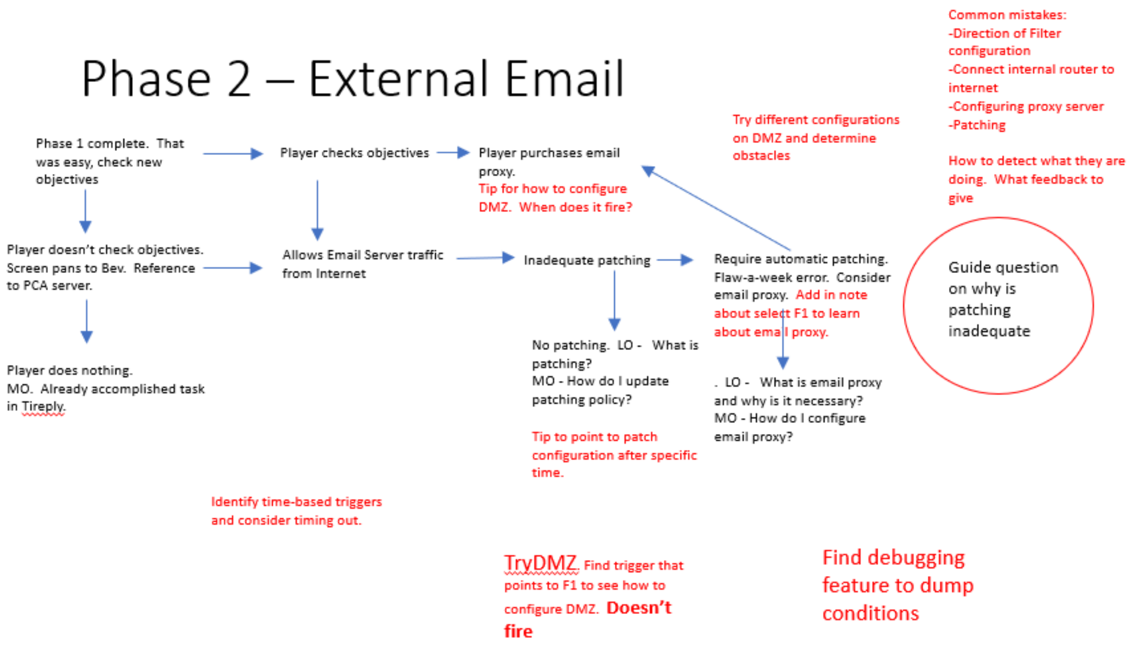
Player does not click objectives tab

Player clicks play game.

MO – In previous scenarios, all hints were given to click on tabs

Did PCA server block web server traffic?

MO or LO–



Phase 2 – External Email

Common mistakes:
-Direction of Filter configuration
-Connect internal router to internet
-Configuring proxy server
-Patching

How to detect what they are doing. What feedback to give

Try different configurations on DMZ and determine obstacles

Phase 1 complete. That was easy, check new objectives

Player checks objectives

Player purchases email proxy. Tip for how to configure DMZ. When does it fire?

Player doesn't check objectives. Screen pans to Bev. Reference to PCA server.

Allows Email Server traffic from Internet

Inadequate patching

Require automatic patching. Flaw-a-week error. Consider email proxy. Add in note about select F1 to learn about email proxy.

Guide question on why is patching inadequate

Player does nothing. MO. Already accomplished task in Tireply.

No patching. LO - What is patching? MO - How do I update patching policy?

Tip to point to patch configuration after specific time.

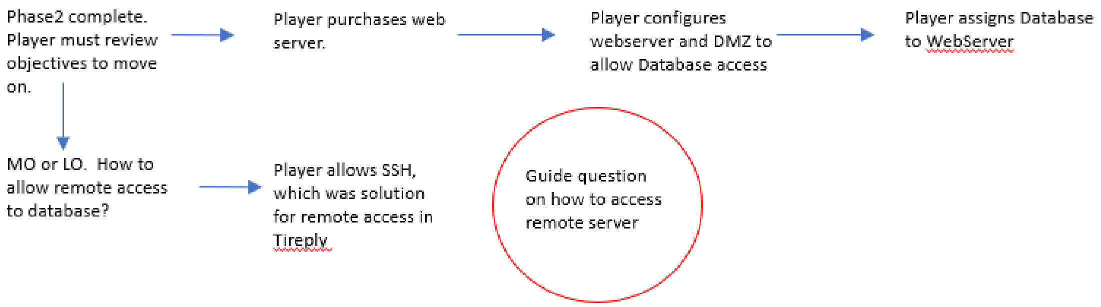
. LO - What is email proxy and why is it necessary? MO - How do I configure email proxy?

Identify time-based triggers and consider timing out.

TryDMZ. Find trigger that points to F1 to see how to configure DMZ. **Doesn't fire**

Find debugging feature to dump conditions

Phase 3 – Bobby Jack Access to Database



Phase2 complete. Player must review objectives to move on.

Player purchases web server.

Player configures webserver and DMZ to allow Database access

Player assigns Database to WebServer

MO or LO. How to allow remote access to database?

Player allows SSH, which was solution for remote access in Tireply

Guide question on how to access remote server

Identify three most likely rat holes and we can help with those.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. NETWORK FILTERS SCENARIO LOG FILES ADAPTED TO IDENTIFY TRIGGERS, CONDITIONS, ASSETS, AND GOALS

This appendix documents the triggers, conditions, assets and goals that were encountered during game play in the Network Filters scenario in a chronological order. All descriptions of the item come directly from the particular scenario's SDF and can be viewed in the SDT itself. Please see Chapter 3 for a detailed explanation on the process used to complete these tables.

A. LOG FILE AND TRIGGERS

Event	Name	Conditions	Sub-event	Details
gameEvent	loadFile			
gameEvent	loadFile			
goalFailure	Web and Basic Research	Requires ability to reach Web Servers via the Internet.		Web Page: WEB SERVER, WEB BROWSER
gameEvent	start			
trigger	HideRegulator	time1day OR_NOT time1day	HIDE_SITE	
trigger	BuyRouter	(WhichScreen AND_NOT DonePhase1) AND_NOT Has2Devices	HELPTIP_TRIGGER	WhichScreen set to 2 (looking at office)
trigger	buyScreen2NetworkDevice	(WhichScreen AND_NOT DonePhase1) AND_NOT Has2Devices		WhichScreen set to 9(looking at Buy)
componentEvent	Bit Flipper_2			
trigger	GoNetworkScreen	(WhichScreen AND_NOT DonePhase1) AND Has2Devices AND_NOT LarryConnectedToWebServer	HELPTIP_TRIGGER	WhichScreen set to 2(looking at office)
trigger	NetScreenHelp	WhichScreen AND has2Devices	HELPTIP_TRIGGER	WhichScreen set to 3(looking at Network)
trigger	Larry No Web	LarryNoWeb AND time1hour	ECONTEXT_TRIGGER	
trigger	Larry No Web Message	LarryNoWeb AND time1hour AND_NOT WebObjective	MESSAGE_TRIGGER	
trigger	LarryGetsWebSpeak	WhichScreen AND_NOT LarryNoWeb	SPEAK_TRIGGER	WhichScreen set to 2 (looking at office)
trigger	WebObjectiveMet	NOT LarryNoWeb	SET_OBJECTIVE_STATUS	
trigger	LarryOnWeb	NOT LarryNoWeb	SET_OBJECTIVE_STATUS	
trigger	goPhase1A	WebObjective	SET_PHASE	NewPhase FirstA
trigger	savePhase1	WebObjective	SAVEGAME_TRIGGER	FilterPhase1.sdf
trigger	LarrysDate	NOT LarryNoWeb	TICKER_TRIGGER	
triggerErase	LarryGetsWebSpeak	WhichScreen AND_NOT LarryNoWeb	SPEAK_TRIGGER	WhichScreen set to 2 (looking at office)
trigger	LarryGetsWebTicker	NOT LarryNoWeb	TICKER_TRIGGER	
assetAttacked	Basic Research		ATTACK_OUTSIDER_INTERNET	

trigger	filterEncy	(WebObjective AND LarryNoWeb) OR ResearchAttacked	ECONTEXT_TRIGGER	
trigger	ResearchInAtt	ResearchAttacked	MESSAGE_TRIGGER	
trigger	tonetfiltertest	DonePhase1 AND ResearchToInternetFTP	MESSAGE_TRIGGER	
trigger	Filler1	DonePhase1	TICKER_TRIGGER	
trigger	filterProblem	WebObjective AND LarryNoWeb	MESSAGE_TRIGGER	
trigger	Filler2	DonePhase1 AND_NOT DonePhase1a	TICKER_TRIGGER	
trigger	SafelyOnWeb	NOT ResearchAttacked AND_NOT LarryNoWeb	SET_OBJECTIVE_STATUS	
trigger	researchProtected	Slaved to SafelyOnWeb - RegC of protectedResearch question	QuestionMult	
trigger	savePhase1A	SafeOnNetObjective	SAVEGAME_TRIGGER	
trigger	goPhase2	SafeOnNetObjective AND [researchProtected]	SET_PHASE	
trigger	Steel Goal	DonePhase1a - Mary Goal - Modify Steel Formula	CHANGE_ASSET_USAGE_TRIGGER	
assetEvent	Steel Formula		Add Mary's Computer	
trigger	Steel Goal Mary Description	DonePhase1a - Mary will now start work on the steel formula	CHANGE_USER_DESC_TRIGGER	
trigger	Camera to Mary	SteelGoalChanged	CAMERA_TO_USER	
trigger	Message	SteelGoalChanged	SPEAK_TRIGGER	
trigger	PromptViewAsset	NOT [ViewedLabelValue] AND WhichScreen AND SteelToInternet - Not WhichScreen15 (Label)	HELPTIP_TRIGGER	WhichScreen set to 2 (looking at office)
trigger	ViewedLabelValue	WhichScreen	LOG_TRIGGER	WhichScreen set to 15 (looking at Label Screen)
assetAttacked	Steel Formula		ATTACK_OUTSIDER_INTERNET	
trigger	Steel Stolen Ency	SteelAttacked	ECONTEXT_TRIGGER	
trigger	WarnExfilt	SteelAttacked AND_NOT SteelToInternet AND_NOT SteelToInternet AND SteelToInternet	TICKER_TRIGGER	
trigger	PromptSelectSteelFormula	NOT [ViewedLabelValue] AND WhichScreen AND SteelToInternet	HELPTIP_TRIGGER	WhichScreen set to 7 (looking at Asset Screen)
trigger	Steel Stolen	[WarnExfilt] x2 or [WarnAsGW] x2 (SteelAttacked AND_NOT SteelToInternet AND SteelToInternet)	LOSE_TRIGGER	
reset to line 37				
componentEvent	Mary's Computer		network Disconnect: Internal LAN 1	

trigger	MaryWorkedSteel	NOT MaryNoSteel AND DonePhase1a AND_NOT SteelAttacked AND SteelGoalChanged1 AND_NOT LarryNoWeb	SET_OBJECTIVE_STATUS	
trigger	SavePhase2	MaryWorksSteel	SAVEGAME_TRIGGER	
trigger	MaryNoInternet	SteelGoalChanged AND_NOT SteelToInternet AND_NOT LarryNoWeb AND_NOT MaryNoSteel AND_NOT SteelToLarrys	MESSAGE_TRIGGER	
trigger	airGapped	Slaved to MaryNoInternet RegD	QUESTION_MULT	
trigger	goPhase3	MaryWorksSteel	SET_PHASE	
trigger	Regulator Tire Safety Description	DonePhase2	CHANGE_USER_DESC_TRIGGER	
trigger	Regulator Tire Safety Message	DonePhase2	TICKER_TRIGGER	
trigger	showRegulator	DonePhase2 - slaves TireSafetyInspectorGoal	HIDE_SITE	
trigger	TireSafetyInspectorGoal	Slaved to showRegulator	CHANGE_ASSET_USER_TRIGGER	
componentEvent	Regulator Workstation		accountAdd: Regulator	
componentEvent	Regulator Workstation		accountRemove: Public	
goalFailure	TireSafety			
trigger	RegulatorSpeaks	DonePhase2	SPEAK_TRIGGER	
trigger	regulatorDone	DonePhase2 AND_NOT MaryNoSteel AND_NOT regulatorNoSafety AND_NOT larryNoWeb AND NOT ResearchAttacked	SET_OBJECTIVE_STATUS	
trigger	Fw4win	RegulatorDone	WIN_TRIGGER	
Unused triggers in log				
	addDB	NOT LarryNoWeb AND_NOT ResearchToInternetWeb AND_NOT ResearchToInternetFTP AND ResearchToInternetDB	ADD_SOFTWARE	From Larry's Computer
	addFTP	NOT LarryNoWeb AND_NOT ResearchToInternetWeb AND ResearchToInternetFTP	ADD_SOFTWARE	From Larry's Computer
	BuyRouterRunning	(WhichScreen AND_NOT DonePhase1) AND_NOT Has2Devices	HELPTIP_TRIGGER	WhichScreen set to 2 (looking at office)
	GoBackAndBuy	WhichScreen AND_NOT has2Devices	HELPTIP_TRIGGER	WhichScreen set to 3(looking at Network)

	InspectorSafetyHint	RegulatorNoSafety and DonePhase2	TICKER_TRIGGER	
	RegulatorComplains	RegulatorNoSafety and DonePhase2	TICKER_TRIGGER	
	Research5lose	[ResearchInAtt] - 3 times	LOSE_TRIGGER	
	NoInternetLose	LarryNoWeb	LOSE_TRIGGER	
	PromptViewCarTire	NOT [ViewedLabelValue] AND WhichScreen AND SteelToInternet	HELPTIP_TRIGGER	WhichScreen set to 7(looking at Asset screen)
	Inattack	donePhase1 and time1hourPhase AND (DonePhase2 OR_NOT DonePhase1a)	ATTACK_TRIGGER	attack on asset from internet
	outBlock	NOT allowedOut AND_NOT LarryNoWeb	QUESTION_MULT	
	WebInAttack	ResearchToInternetWeb AND_NOT ResearchToInternetFTP AND_NOT LarryNoWeb	QUESTION_MULT	
	ResearchRetinaMessage	ResearchRetinaScan	TICKER_TRIGGER	
	ResearchRetinaLose3000	ResearchRetinaScan	CASH_TRIGGER	
	MaryCipherLock	MaryCipherLock	TICKER_TRIGGER	
	lose1M	Slaved to SteelStolen, SteelFilterSubverted, SteelStolenOther	CASH_TRIGGER	
	SteelFilterSubverted	[WarnSubvert] x2	LOSE_TRIGGER	
	WarnAsGW	SteelAttacked AND_NOT SteelToInternet AND SteelToInternet	TICKER_TRIGGER	
	WarnSubvert	SteelAttacked AND SteelToInternet	TICKER_TRIGGER	
	SteelStolenOther	SteelAttacked AND_NOT [WarnExfilt] x0 AND_NOT [WarnSubvert] x0	LOSE_TRIGGER	
	Internet Attack	SteelGoalChanged	ATTACK_TRIGGER	attack on asset from internet
	SteelAttackMalware	SteelGoalChanged	ATTACK_TRIGGER	Malware Attack
	Physical Attack	SteelGoalChanged	ATTACK_TRIGGER	Physical Attack

B. CONDITIONS

Condition	**Class**	**Parameters**	
Has2Devices	CompanyHasDevices	3 - 99	
LarryConnectedtoWebServer	ComputersAreConnected	Larry to Web Page	
LarryNoWeb	UserFailsGoal	Larry did not complete Web and Basic Research	

WhichScreen	OnScreen parameter defines window		
WebObjective	ObjectiveCompleted	LarryonWeb (Not LarryNoWeb)	
ResearchAttacked	AssetAttacked	Basic Research	Any attack type
DonePhase1	PhaseCompleted	First Phase	
ResearchToInternetFTP	AssetToNetworkByFilterType	Determine if filters are blocking access to Basic Research from Internet through FTP	
DonePhase1a	PhaseCompleted	FirstA Phase	
SafeOnNetObjective	ObjectiveCompleted	SafelyOnWeb	
SteelGoalChanged	TriggerGoneOff	Min - 1, Max - 1	
SteelToInternet	AssetToNetwork	Steel Formula Read over Internet	
SteelAttacked	AssetAttacked	SteelFormula	Any attack type
MaryNoSteel	UserFailsGoal	Mary - Modify Steel Formula	
SteelGoalChanged1	TriggerGoneOff	Steel Goal 1 time	
MaryWorksSteel	ObjectiveCompleted	MaryWorksSteel	
SteelToLarrys	ComputersAreConnected	Steel Formula to Larry	
allowedOut	AssetToNetworkFilterCount	Basic Research to Internet, 4 assets	
DonePhase2	PhaseCompleted	Second Phase	
regulatorNoSafety	UserFailsGoal	Regulator - Tire Safety	
regulatorDone	ObjectiveCompleted	TireSafety	
Unused conditions			
ResearchToInternetWeb	AssetToNetworkByFilterType	Determine if filters are blocking access to Basic Research from Internet through WEB SERVER	
ResearchToInternetDB	AssetToNetworkByFilterType	Determine if filters are blocking access to Basic Research from Internet through DATABASE	
ResearchRetinaScan	AssetZoneHasPolicy	ModerateIrisScanner in Basic Research Zone	
MaryCipherLock	AssignedComputerZoneHasPolicy	CipherLockOnDoor for Mary	
cash3000	MaxCashOnHand	2910	
SteelSomeAllowed	AssetToNetworkFilterCount	Steel Formula to Internet	

C. ASSETS

Asset	Description	State	ACL
Web Page	TirePly's vast research database of publicly available publications.	Instantiated	Intended ACL: Public can Read, Write, Cntrl and Ex
Basic Research	Though not of great value, if this data is not available, research progress is severely hampered.	Instantiated	Intended ACL: Larry Can Read, Write, Cntrl and Ex
Steel Formula	Tireply training manual	CreateWhilePaused	Intended ACL: Engineering can Read, Write, Cntrol, and Ex
Tire Safety	Tire safety test data that by law must be made available to external regulators.	Instantiated	Intended ACL: Admin group can Read

D. GOALS

Goal	**Description**	**Software**	**Asset**
Web and Basic Research	Requires ability to reach Web Servers via the Internet.	WEB SERVER/WEB BROWSER	Web Page WEB SERVER
Modify Steel Formula	Access the Steel Formula design material to keep it up to date and revise it.	Spreadsheet	Steel Formula
TireSafety	Read tire safety data over the Internet using SSH and a database application. This access has been authorized by management.	DATABASE/DATABASE CLIENT	TireSafety DATABASE

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D. DMZ SCENARIO LOG FILES ADAPTED TO IDENTIFY TRIGGERS, CONDITIONS, ASSETS, AND GOALS

This appendix documents the triggers, conditions, assets and goals that were encountered during game play in the DMZ scenario in a chronological order. All descriptions of the item come directly from the particular scenario's SDF and can be viewed in the SDT itself. Please see Chapter III for a detailed explanation on the process used to complete these tables.

A. LOG FILE AND TRIGGERS

Event	Name	Conditions	Sub-event	Details
trigger	HideBev	Not PhaseOneDone	HIDE_SITE	Zone: Bev's House
trigger	HideBobbyJack	Not PhaseOneDone	HIDE_SITE	Zone: Bobby Jack's Hotel
goalFailure	View Croquet Network			
assetEvent	Prize Allocations	Add: PCA Server	Add: PCA Server	
trigger	NoWeb	(PhaseOneDone AND_NOT BevFailsSend AND DanFailsWeb) OR (DanFailsWeb AND_NOT PhaseOneDone)	UserWhineTrigger	
trigger	dmzEncy	PrizeAllocationCompromised OR SponsorListCompromised	ChangeEncyloTrigger	DMZ.html
trigger	DanSurfed	NOT DanFailsWeb AND_NOT DanSurfing	SetObjectiveStatus	
trigger	RanSecure	NOT PrizeAllocationCompromised AND AllGoalsMet	SetObjectiveStatus	
trigger	PhaseOneDone	RanSecure	SetPhase	
trigger	SavePhaseOne	Slaved to PhaseOneDone	SaveGameTrigger	
trigger	ShowBev	PhaseOneDone	HIDE_SITE	Zone: Bev's House
trigger	EmailFromBev	Slaved to ShowBev	CHANGE_ASSET_USAGE_TRIGGER	
trigger	EmailToAnn	Slaved to EmailFromBev	CHANGE_ASSET_USAGE_TRIGGER	
componentEvent	Bev's Workstation		accountAdd: Bev	
trigger	BevCannotSend	PhaseOneDone AND BevFailsSend	USER_WHINE_TRIGGER	
trigger	BevFailsNoAttacks	BevFailsSend AND_NOT PrizeAllocationCount AND BevConnected AND_NOT extraRouter	QuestionMult	
trigger	BevFailsAttacks	BevFailsSend AND PrizeAllocationCount AND_NOT extraRouter AND BevConnected	QuestionMult	
trigger	dmzEncyFailGoal	BevFailsSend	ChangeEncyloTrigger	DMZ.html
componentEvent	PCA Router		appFilter	
assetEvent	Email from Bev		Add:PCA Server	

Event	Name	Conditions	Sub-event	Details
trigger	EmailFromBevOK	PhaseOneDone AND AllGoalsMet	SetObjectiveStatus	
assetAttacked	Prize Allocations	read Prize Allocations via some zombie computer on the Internet. Remote access to PCA Server was gained because the Email Server service was compromised. Looks like an unpatched flaw. Email was unprotected.		
trigger	dmzEncy	PrizeAllocationCompromised OR SponsorListCompromised	ECONTEXT_TRIGGER	DMZ.html
trigger	patchDiagnostics	PrizeAllocationCompromised	COMPUTER_DIAGNOSTICS	PCA Server
trigger	CameraTo0	Slaved to patchDiagnostics	SET_CAMERA_TO_INDEX	Index 0
trigger	Patches	NOT NotPatched AND PrizeAllocationCompromised	MessageTrigger	
trigger	TwoRouterOpen	PrizeAllocationCount AND extraRouter and BevConnected AND AllGoalsMet AND PrizeAllocationCompromised AND PrizeGoalToInternet	QuestionMult	
trigger	TryDMZ	[patchDiagnostics] AND_NOT extraRouter AND PrizeAllocationCompromised	MessageTrigger	patchDiagnosticsc twice
componentEvent	Email Server_2		buy	
componentEvent	Email Server_3		buy	
componentEvent	Email Server_3		networkConnect:PCA LAN	
trigger	RanPhase2Secure	PhaseOneDone AND AllGoalsMet AND_NOT PrizeAllocationCompromised	SetObjectiveStatus	
trigger	PhaseTwoDone	EmailFromBev and RanSecurePhase2 AND PhaseOneDone	SetPhase	
trigger	SavePhaseTwo	Slaved to PhaseTwoDone	SaveGameTrigger	
trigger	ShowBobby	PhaseTwoDone	HIDE_SITE	Bobby Jack's Hotel
trigger	StandingsBobby	Slaved To ShowBobby	CHANGE_ASSET_USAGE_TRIGGER	AssetGoal ReportStandings
componentEvent	Bobby Jack's PC		AccountAdd: Bobby Jack	
componentEvent	Bobby Jack's PC		AccountRemove: Public	
goalFailure	Report Standings			

Event	Name	Conditions	Sub-event	Details
trigger	StandingsAnn	Slaved To ShowBobby	CHANGE_ASSET_USAGE_TRIGGER	
trigger	BobbyJackNoStandings	PhaseTwoDone AND BobbyFailsStandings	USER_WHINE_TRIGGER	
Other triggers				
trigger	DanNotSurfed	DanFailsWeb AND DanSurfing	SetObjectiveStatus	
trigger	FinalQuizDone	NOT regD	SetObjectiveStatus	
trigger	BobbyWebDone	NOT BobbyWebDone AND_NOT BobbyFailsStandings AND PhaseTwoDone	SetObjectiveStatus	
trigger	BobbyWebNotDone	BobbyWebDone AND BobbyFailsStandings	SetObjectiveStatus	
trigger	Win	PhaseTwoDone AND AllGoalsMet AND_NOT StandingsCompromised AND_NOT PrizeAllocationCompromised AND_NOT SponsorListCompromised	WinTrigger	
trigger	losePickyFilter	PhaseOneDone AND AllGoalsMet AND_NOT PrizeAllocationCompromised AND namesThemMail	LoseTrigger	
trigger	ChangeSMTPName	PhaseOneDone AND AllGoalsMet AND_NOT PrizeAllocationCompromised AND namesMeMail	ChangeComponentName	
trigger	ChangeSMTPthem	PhaseOneDone AND AllGoalsMet AND_NOT PrizeAllocationCompromised AND namesUsMail	ChangeComponentName	
trigger	NameChangeMessage	Slaved To ChangeSMTPName	MessageTrigger	
trigger	NameChangeMessage2	Slaved To ChangeSMTPthem	MessageTrigger	
trigger	FinalQuiz	EmailFromBev AND RanSecurePhase2 AND BobbyWebDone	Question	
trigger	finalA, finalB, finalC, finalD	regD conditions:a, b, c, d	MessageTrigger	
trigger	P3CutListFromWeb	SponsorListCount AND SponsorListCompromised AND custListToInternet AND PhaseTwoDone	QuestionMult	Count of 1

Event	Name	Conditions	Sub-event	Details
trigger	StandingsFromWeb	StandingsCount AND StandingsCompromised AND standingsToInternet AND PhaseTwoDone	QuestionMult	
trigger	DMZWebNoStanding	StandingsOnSameServer AND twoServersInDMZ AND PhaseTwoDone AND BobbyFailsStandings	SpeakTrigger	
trigger	DMZWebNoStandingThought	StandingsOnSameServer AND twoServersInDMZ AND PhaseTwoDone AND BobbyFailsStandings	SetUserThought	Bobby Jack
trigger	Internet	OneHour	AttackTrigger	Attack Type 19: Attack on assets from the internet
trigger	Breakin-Hacking	OneHour	AttackTrigger	Attack Type 18: Attacker enters zone and accesses computer
trigger	Bad Policies	OneHour	AttackTrigger	Attack Type 7: Bad Policy resulting in malware
trigger	DOS	OneHour	AttackTrigger	Attack Type 15: Denial of Service

B. CONDITIONS

Condition	Class	Parameters	
PhaseOneDone	PhaseCompleted	PhaseOne	
BevFailsSend	UserFailsGoal	Bev : Send email to Ann	
DanFailsWeb	UserFailsGoal	Dan fails View Croquet Network News	
DanSurfing	ObjectiveCompleted	Dan surf	
PrizeAllocationCompromised	AssetAttacked	Asset name: Prize Allocations	
AllGoalsMet	AllAssetGoalsMeet		
RanSecure	ObjectiveCompleted	Objective: Run Secure	
SponsorListCompromised	AssetAttacked	Asset name: PCA Sponsor List	
NotPatched	AssetComputerHasPolicy	Asset name: Prize Allocations	UpdatePatches: None
extraRouter	CompanyHasDevices	Parameter 4–6	
BevFailsSend	UserFailsGoal	Bev fails Send email to Ann	

Condition	Class	Parameters	
BevConnected	ComputersAreConnected	Bev has access to Prize Allocations	
PrizeGoalToInternet	AssetToNetworkByFilterType	From Internet to PrizeAllocations. Goal set to 1 to determine if filters are blocking an asset goal	EMAIL SERVER
EmailFromBev	ObjectiveCompleted	EmailFromBev	
RanSecurePhase2	ObjectiveCompleted	runSecurePhase2	
PhaseTwoDone	PhaseCompleted	PhaseTwo	
BobbyFailsStandings	UserFailsGoal	Bobby Jack fails Report Standings	
BobbyWebDone	ObjectiveCompleted	Web Service	
StandingsCompromised	AssetAttacked	Asset name: Standings Database	
namesThemMail	FilterNamesComponent	ThemMail Mail Server	
namesMeMail	FilterNamesComponent	MeMail Mail Server	
namesUsMail	FilterNamesComponent	UsMail Mail Server	
SponsorListCount	AassetAttackCount	SponsorListCompromised	
CustListToInternet	AssetToNetworkByFilterType	From Internet to PCA Sponsor List	WEB SERVER
StandingsOnSameServer	AssetsOnSameComputer	Asset name: Standings Database and Standings Web Page	
twoServersInDMZ	NumComputersOnNetwork	Network: DMZ Lan	3-Feb
PrizeAllocationCount	AssetAttackCount	PrizeAllocationCompromised	
StandingsCount	AssetAttackCount	StandingsCompromised	
PrizeToInternet	AssetToNetworkByFilterType	From Internet to PrizeAllocations	EMAIL SERVER
StandingsToInternet	AssetToNetworkByFilterType	From Internet to Standings Database	WEB SERVER
FinalQuizDone	ObjectiveCompleted	FinalQuiz	

C. ASSETS

Asset	Description	Intended ACL	Actual ACL
Prize Allocations	Details of how much prize money will be awarded at each upcoming PCA tournament. This asset is maintained as a series of emails from Ann to Dan.	Intended ACL: PCA can read	Actual ACL: None
Standings Database	Individual and group player ranking database.	Intended ACL: PCA can read and write	Actual ACL: None
Croquete news	A conglomeration of tweets, blogs and observations about the international croquet circuit.	Intended Access List: Public has read privilege	Actual ACL: None
Email from Bev	Messages from Bev to Ann who is her mother.	Intended ACL: Ann has read, write privilege	Actual ACL: None
Sponsor List	List of cash sponsors for PCA tournaments	Intended ACL: PCA can read and write	Actual ACL: None

D. GOALS

Goal	Description	Software	Asset	
View Croquet Network News	Surf all the latest croquet news from around the world at CNN's website	WEB BROWSER/ WEB SERVER	Croquete News	Filtered WEB SERVER
Send email to Ann		EMAIL CLIENT/EMAIL SERVER	Email from Bev	Filtered EMAIL SERVER
Get email From Bev		EMAIL CLIENT/EMAIL SERVER	Email from Bev	Filtered EMAIL SERVER
Report Standings	Use a web interface to adjust the individual and group rankings. The Standings Web Page is hosted on a web server. That web server must be able to access the Standings Database, which should remain on the PCA server.	WEB BROWSER	Standings Database and Standings Web Page	Filtered: DATABASE and WEB SERVER

Goal	Description	Software	Asset	
Manage Standings	Manage the standings database using a suite of database access forms.	DATABASE CLIENT	Standings Database	Filtered: DATABASE
Maintain Sponsor List	Update the list of sponsors		PCA Sponsor List	
Send Prize Values to Dan	Email Dan the prize plans	EMAIL CLIENT/EMAIL SERVER	Prize Allocations	Filtered: EMAIL SERVER
Receive prize values from Ann	Receive prize plans from Ann	EMAIL CLIENT/EMAIL SERVER	Prize Allocations	Filtered: EMAIL SERVER

E. OBJECTIVES

Objective	Objective not complete text
Run Secure	Ann and Dan are exchanging email and Dan wants to surf the CNN website (per goals seen in the USERS tab). Run the simulation for a while without compromised assets.
Dan Surf	Dan is having trouble surfing the web. He is muttering about the strict network filters imposed by your predecessor.
EmailFromBev	Ann would like to be able to receive email from her daughter, Bev.
runSecurePhase2	Run for a while without compromises.
FinalQuiz	Take a brief quiz.
Web Service	Bobby Jack is a stringer who travels the circuit and provides the PCA with player ranking scouting information. Make sure he can remotely access the Standings database via a web interface.
runWebSecure	Run for a while without any major problems.

LIST OF REFERENCES

[1] S.-R. Sabillon, "An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness Training Model (CATRAM). A case study in Canada," J*ournal of Cases on Information Technolog*y (JCIT), vol. 21, no. 3 , pp. 26–39, Jul. 2019. [Online]. doi: 10.4018/JCIT.2019070102.

[2] Prensky, M., *Digital Game-Based Learning*, New York: McGraw-Hill, 2001.

[3] Cone, B. D., Thompson, M. F., Irvine, C. E., & Nguyen, T. D. "Cyber security training and awareness through game play," Monterey, CA: Naval Postgraduate School, 2006.

[4] Thompson, M.F., Irvine, C.E., "CyberCIEGE scenario design and implementation," Monterey, CA: Naval Postgraduate School, 2011.

[5] Irvine, C.E., Thompson, M.F. and Allen, K., "CyberCIEGE: An information assurance teaching tool for training and awareness," presented at Federal Information Systems Security Educators' Association Conference, North Bethesda, MD, March 2005.

[6] Cone, I. "A video game for cyber security training and awareness," *Computers & Securit*y, vol. 26, no. 1, pp. 63–72, 2007, doi: 10.1016/j.cose.2006.10.005.

[7] "CyberCIEGE Scenario Development Tool User's Guide," Jun. 2013. [Online]. Availableble: https://nps.edu/documents/107523844/117287768/SDT.pdf/2b555b1a-56bb-4f37-9e1b-4c52afbffff3?t=1541174271000

[8] Cross, K.P., "Feedback in the classroom: making assessment matter," Washington, D.C.: American Association for Higher Education, 1988.

[9] Thompson, M., and Irvine, C., "Active learning with the CyberCIEGE video game," 2011. https://www.researchgate.net/publication/228837831_Active_learning_with_the_CyberCIEGE_video_game

[10] M. Butler, *A Teacher's Guide to Classroom Assessment: Understanding and Using Assessment to Improve Student Learnin*g, 1st ed. San Francisco, CA, USA: Jossey-Bass, 2006.

[11] **"**Incorporating CyberCIEGE into an Introductory Cyber Security Course," March 2017. [Online]. Available: https://nps.edu/web/c3o/syllabus.

[12] "CyberCIEGE Instructor Notes," [Online]. Available: https://nps.box.com/shared/static/pc3f6vzoe3ob0vbqraqhsvzw0r6e8j8a.zip.

[13] "Instructor Notes for the DMZ Scenario," May 2013.

[14] "Lab 9 CyberCIEGE Network Filters Lab Manual," Nov 2009. [Online]. Available: https://nps.edu/documents/107523844/117288929/filters.pdf/f0ef01a6-95dc-4c7b-8cec-94de05033ee9?t=1490388220000

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California