เกมจำลองการโจมตีในระบบเครือข่าย

Cyber Security War Game

เสริมศักดิ์ ธรรมรัตนรังสี

อดิศร คำหว่าง

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2557

เกมจำลองการโจมตีในระบบเครือข่าย

Cyber Security War Game

เสริมศักดิ์ ธรรมรัตนรังสี

อดิศร คำหว่าง

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2557

ปริญญานิพนธ์ปีการศึกษา 2557

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง เกมจำลองการโจมตีในระบบเครือข่าย

CYBER SECURITY WAR GAME

ผู้จัดทำ

1. นายสริมศักดิ์	ธรรมรัตนรังสี	รหัสนักศึกษา	54011442
2. นายอดิศร	คำหว่าง	รหัสนักศึกษา	54011458

_____ อาจารย์ที่ปรึกษา

(ดร. อักฤทธิ์ สังข์เพ็ชร)

_____ อาจารย์ที่ปรึกษาร่วม

(ดร. อรทัย สังข์เพ็ชร)

เกมจำลองการโจมตีในระบบเครือข่าย

นาย เสริมศักดิ์ ธรรมรัตนรังสี 54011442
นายอดิศร คำหว่าง 54011458
ดร.อักฤทธิ์ สังข์เพ็ชร อาจารย์ที่ปรึกษา
ดร.อรทัย สังข์เพ็ชร อาจารย์ที่ปรึกษาร่วม
ปีการศึกษา 2557

บทคัดย่อ

ระบบเกมจำลองการโจมตีทางเครือข่ายคอมพิวเตอร์ เป็นระบบที่นำข้อมูลช่องโหว่ต่างๆภายในศูนย์ข้อมูลมาทำเป็นเกมเพื่อจำลองเส้นทางการโจมตีภายใต้เงื่อนไขต่างๆกัน โดยผู้ที่ทำการโจมตีไม่จำเป็นต้องมีความรู้ด้านการโจมตีเครือข่ายคอมพิวเตอร์ เนื่องจากในปัจจุบันระบบความปลอดภัยในเครือข่ายคอมพิวเตอร์เป็นเรื่องสำคัญมาก และการป้องกันการโจมตีทั้งหมดนั้นเป็นไปได้ยากเนื่องจากข้อจำกัดทั้งด้านทรัพยากรและบุคลากรผู้เชี่ยวชาญด้านการรักษาความปลอดภัยแต่ถ้าผู้ดูแลระบบสามารถวิเคราะห์ได้ว่าเส้นทางการโจมตีเส้นทางไหนมีโอกาสที่จะถูกโจมตีมาก ก็จะสามารถทำการป้องกันหรือเฝ้าระวังได้ดีขึ้น ความปลอดภัยของระบบก็จะ สูงขึ้น ดังนั้นโครงงานนี้จึงถูกพัฒนาขึ้นเพื่อใช้ศึกษาโอกาสที่เครือข่ายจะถูกโจมตีในแต่ละเส้นทาง โดยแบ่งการทำงานออกเป็นสามส่วนได้แก่ ส่วนเชื่อมต่อกับระบบภายนอก ทำหน้าที่รับข้อมูลต่างๆของเครือข่ายมาในรูปแบบที่กำหนด เช่น อุปกรณ์และช่องโหว่ของอุปกรณ์นั้นๆ เพื่อนำไปใช้แปลงเป็นวัตถุในเกมต่อไป ส่วนที่สองคือส่วนของเกมจำลองการโจมตีโดยนำข้อมูลเส้นทางการโจมตีมาแปลงเป็นวัตถุในเกมและกำหนดการปฏิสัมพันธ์กันของวัตถุแต่ละชนิด เพื่อพัฒนาให้เป็นเกมที่บุคคลทั่วไปสามารถเข้าใจได้ และเผยแพร่สู่สาธารณะเพื่อเก็บข้อมูลกลวิธีการโจมตีที่ใช้ ส่วนที่สามคือ ส่วนแสดงผล ซึ่งแปลงผลการเล่นเกมกลับมาเป็นข้อมูลเชิงสถิติให้ผู้ดูแลระบบ เช่น ลำดับเส้นทาง ชนิด ช่องโหว่ที่ใช้เป็นต้น

Cyber Security War Game

Mr. Sermsak Tummarattanarangsee 54011442
Mr. Adisorn Kumwang 54011458
Dr. Akkarit Sangpetch Advisor
Dr. Orathai Sangpetch Co-advisor

Academic Year 2014

Abstract

Cyber Security War game is a system that uses the vulnerabilities in a system for generating content in the game and then publish it to players. In this game, the players could be a person who don'thave network security background. Computer security has increasingly become an important issue. Protecting a computer system from all intrusion attempt is virtually impossible.The alternative is to identify components of the system with the highest probability of being hacked. The administrator can then closely monitor the most vulnerable components and decrease the risk of being compromised. This project consists of three parts -- the input, the game and the report. The input takes attack graphs from vulnerability assessment tools. The game then generates a scenario map for a turn-based strategy game from the attack graph. After the players playedthe game,the administrator can inspect the statistical report, such as path probability, sequence, attack type, etc. in order to identify the components that need to be monitored and protected.

กิตติกรรมประกาศ

ปริญญานิพนธ์ สำเร็จลงได้ด้วยความกรุณาอย่างยิ่งจาก ดร.อักฤทธิ์ สังข์เพ็ชร อาจารย์ที่ปรึกษา และ ดร. อรทัย สังข์เพ็ชร อาจารย์ที่ปรึกษาร่วม ที่ได้ให้คำแนะนำปรึกษา ตลอดจนตรวจแก้ไขข้อบกพร่องต่างๆ ด้วยความเอาใจใส่เป็นอย่างยิ่ง จนปริญญานิพนธ์สำเร็จได้ คณะผู้ศึกษาค้นคว้าขอกราบขอบพระคุณเป็นอย่างสูงไว้ ณ ที่นี้

โครงงานนี้ได้รับเงินทุนสนับสนุนและคำแนะนำบางส่วนจาก สวทช ผ่านการประกวด National Software Contest 2015 คณะผู้ศึกษาค้นคว้าขอขอบพระคุณเป็นอย่างยิ่ง

ขอขอบพระคุณบริษัท INET ที่อำนวยทรัพยากรให้ใช้ระหว่างพัฒนาโครงการและข้อมูลที่จำเป็นต่อการศึกษาค้นคว้าครั้งนี้ รวมไปถึงคำแนะนำที่พี่ๆทุกคนมอบให้ จึงทำให้โครงงานนี้สำเร็จลงได้ด้วยดี

ขอบคุณครอบครัว คุณพ่อ คุณแม่ ที่คอยให้กำลังใจมาและสนับสนุนในทุกๆเรื่องเสมอมา

นาย เสริมศักดิ์ ธรรมรัตนรังสี

นาย อดิศร คำหว่าง

สารบัญ

สารบัญภาพ

สารบัญตาราง

บทที่ 1 บทนำ

1.1 ความสำคัญและที่มาของโครงงาน

ในปัจจุบันความปลอดภัยของข้อมูลที่อยู่ในศูนย์ข้อมูล (Data Center)และองค์กรทางธุรกิจต่างๆ นับว่ามีความสำคัญอย่างยิ่งนักเจาะระบบพยายามคิดค้นวิธีการใหม่ๆ ในการเจาะระบบ โดยอาศัยช่องโหว่ทั้งทางด้านฮาร์ดแวร์, ซอฟต์แวร์และเครือข่ายแต่เดิมความรับผิดชอบในการป้องกันและทำให้ศูนย์ข้อมูลปลอดภัยจากการถูกเจาะระบบขึ้นอยู่กับผู้บริหารเครือข่าย ซึ่งแนวโน้มในปัจจุบันมีความพยายามในการเจาะระบบมากขึ้น เครื่องมือและซอฟต์แวร์ที่ใช้ในการโจรกรรมข้อมูลผ่านเครือข่ายสามารถหาได้ทางอินเตอร์เน็ตอย่างง่ายดายและไม่มีค่าใช้จ่าย อีกทั้งองค์ความรู้ต่างๆ ที่ใช้ในการเจาะระบบถูกรวบรวมและเผยแพร่อย่างแพร่หลายด้วยเหตุนี้ผู้บริหารเครือข่ายจำเป็นต้องมีองค์ความรู้เกี่ยวกับวิธีการที่นักเจาะระบบใช้ในการเจาะเข้าไปในระบบของตนเองซึ่งแต่เดิมกระบวนการประเมินความปลอดภัยของเครือข่ายในองค์กรขนาดใหญ่นั้นเป็นเรื่องที่เหนื่อยหน่ายและยาวนานรวมถึงอยู่ในความรับผิดชอบของกลุ่มคนเพียงไม่กี่คน ด้วยเหตุนี้เองผู้จัดทำโครงงานจึงมีแนวคิดที่จะผลักดันปัญหาของแต่ละองค์กรไปสู่สาธารณชน (Crowdsourcing) โดยเปลี่ยนแปลงปัญหาให้อยู่ในบริบทของเกม (Gamification)ที่คนจำนวนมากสามารถเข้าถึงและมีส่วนร่วมได้โดยง่าย

1.2 วัตถุประสงค์

1) เพื่อออกแบบและพัฒนาแพลตฟอร์มที่สามารถแปลงวัตถุในชีวิตจริง (Real World Object) ในที่นี้หมายถึง Attack graph ที่แสดงถึงเส้นทางการโจมตีที่เกิดขึ้นได้ ให้เป็นวัตถุในเกม (Game Object)และสามารถกำหนดสถานะรูปแบบที่ใช้ในการแสดงผลและกฎต่างๆ ที่แต่ละวัตถุใช้ปฏิสัมพันธ์กันให้อยู่ในรูปแบบของเกมซึ่งจำลองเครือข่ายในศูนย์ข้อมูลให้อยู่ในบริบทอื่นๆ ที่ผู้เล่นทั่วไปสามารถเข้าใจได้ง่ายและรู้สึกสนุกเวลาเล่น ซึ่งผู้เล่นสามารถเล่นเกมนี้ผ่านทางเว็บบราวเซอร์และสามารถเข้าถึงได้เมื่อเชื่อมต่อกับอินเตอร์เน็ต
2) เพื่อออกแบบและพัฒนาระบบที่สามารถแปลข้อมูลการเล่นของผู้เล่นที่สามารถเอาชนะในแต่ละฉากเพื่อให้ได้มาซึ่งวิธีที่ผู้เล่นใช้ปฏิสัมพันธ์กับวัตถุในเกมและนำเสนอข้อมูลที่ได้ให้แก่องค์กรที่มอบข้อมูลให้เพื่อใช้ในการตัดสินใจในการเปลี่ยนแปลงองค์ประกอบต่างๆ ของเครือข่ายให้ปลอดภัยมากขึ้น
3) เพื่อศึกษาวิธีในการนำปัญหาของแต่ละองค์กรไปสู่สาธารณชนเพื่อให้เกิดแนวทางในการแก้ปัญหาร่วมกัน (Crowdsourcing) ผ่านทางสื่อกลางที่สาธารณะสามารถเข้าถึงได้

1.3. ขอบเขตของโครงงาน

ออกแบบและพัฒนาเกมโดยมีต้นแบบและมีวิธีการเล่นในรูปแบบของเกมวางแผน (Strategy)ซึ่งผู้เล่นต้องลักลอบส่งทหารเข้าไปในเมืองและสิ่งปลูกสร้าง เพื่อขโมยทรัพย์สินหรือทำลายเมืองต่างๆซึ่งแผนที่ของด่านนั้นๆได้มาจากกราฟการโจมตี (Attack graph)และให้ผู้เล่นทำการเลือกผู้บุกรุก (Threats or Intruder) และเส้นทางในการโจมตี(Attack Path)เพื่อยึดครองส่วนที่ลึกที่สุดเพื่อเข้าถึงสมบัติ(Data) ซึ่งผู้เล่นจะได้รับการตอบแทนเป็นคะแนนและเงินในเกมเมื่อพวกเขาเลือกผู้บุกรุกที่สามารถทะลุทะลวงการป้องกันเข้าไปได้(แม้เพียงเล็กน้อย) ทั้งนี้ช่องโหว่ในการเจาะขึ้นอยู่กับคุณสมบัติทางด้านความปลอดภัยของแต่ละอุปกรณ์และชนิดของผู้บุกรุก

โดยในโครงงานนี้แบ่งระบบออกเป็น 3 ส่วนด้วยกัน

1) ส่วนที่เชื่อมต่อระหว่างองค์กรภายนอกและระบบเกมซึ่งสามารถรับข้อมูลช่องโหว่ในระบบขององค์กรมาโดยจะต้องอยู่ในรูปแบบที่ระบบต้องการ
2) ส่วนที่เป็นเกมสามารถนำข้อมูลช่องโหว่ในระบบขององค์กรมาแสดงเป็นเนื้อหาภายในเกมโดยใช้คุณลักษณะต่างๆของเครื่องและช่องโหว่โดยระบบจะบันทึกกลวิธีที่ผู้เล่นใช้ในด่านนั้นๆ
3) ส่วนนำเสนอข้อมูลสามารถแสดงผลข้อมูลได้แก่ ชนิด, ลำดับ, เส้นทางการโจมตีและความถี่ของวิธีที่ผู้เล่นใช้ทำการโจมตี

1.4 วิธีการดำเนินงาน

1) ศึกษาการทำงานของโปรโตคอล HTTPรวมทั้งวิธีเบื้องต้น (e.g. GET,POST,PUT,DELETE) ที่ใช้ในการส่งข้อมูลผ่านเครือข่าย
2) ศึกษาเกี่ยวกับ Data Center Topology และความปลอดภัยของคอมพิวเตอร์และเครือข่าย (Computer & Network Security)
3) ศึกษาเกี่ยวกับการพัฒนา Web Application (ในที่นี้คือ CreateJS และ Javascript)โดยใช้ Google App Engine รวมถึง Web Technology อื่นๆ ที่จำเป็น
4) ออกแบบรูปแบบในการจัดเก็บข้อมูลลงในฐานข้อมูล
5) ศึกษาเกี่ยวกับ RESTful APIและวิธีในการออกแบบ API ที่ใช้การติดต่อระหว่างระบบ
6) ศึกษาเกี่ยวกับการออกแบบเกมและออกแบบส่วนติดต่อผู้ใช้งาน
7) พัฒนาส่วนเชื่อมต่อโปรแกรม
8) พัฒนาส่วนที่เป็นตัวโครงหลักของเกม
9) พัฒนาส่วนที่ใช้นำเสนอข้อมูลที่ผู้เล่นเลือกเล่น
10) ทดสอบกับ attack graph หลายๆแบบเพื่อตรวจสอบความถูกต้องของการออกแบบ

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1) ผู้ใช้ที่เป็นผู้ดูแลระบบสามารถทำการจำลองการโจมตีได้ในราคาถูกและผู้ที่เข้าร่วมทำการทดลองก็ไม่จำเป็นต้องมีความรู้ด้านการโจมตีเครือข่ายคอมพิวเตอร์อีกด้วย
2) ผู้ใช้ที่เป็นผู้ดูแลระบบสามารถจัดอันดับได้ว่าเส้นทางใดมีโอกาสถูกโจมตีมากที่สุด และสามารถนำข้อมูลที่ได้ไปใช้ในการปรับปรุงการป้องกันได้

บทที่ 2 ทฤษฎีที่เกี่ยวข้อง

ในโครงงานนี้จำเป็นต้องใช้ทฤษฎีเกี่ยวกับการพัฒนาเว็ปไซต์ การพัฒนาเกม และความปลอดภัยในระบบเครือข่ายคอมพิวเตอร์ โดยใช้ทฤษฎีในการพัฒนาเว็ปไซต์ในการทำส่วนที่ใช้ติดต่อกับผู้ดูแลระบบคือรับข้อมูลช่องโหว่ในระบบและแสดงสถิติการเล่นของผู้เล่น ข้อมูลช่องโหว่ที่ได้จะนำมาแปลงเป็นเนื้อหาภายในเกมโดยการใช้ทฤษฎีเกี่ยวกับความปลอดภัยในระบบเครือข่าย

2.1. ทฤษฎีและเทคโนโลยีที่เกี่ยวข้องกับการพัฒนาเว็ปไซต์

2.1.1. JSON (Java Script Object Notation)

JSON[2]คือรูปแบบที่ใช้ในการจัดเก็บและแลกเปลี่ยนข้อมูลเนื่องจากJSON ใช้ไวยากรณ์ของภาษา Javascript แต่จัดเก็บให้อยู่ในรูปแบบ Text เท่านั้นจึงสามารถนำไปใช้เป็นรูปแบบข้อมูล (data format) โดยภาษาที่ใช้ในการเขียนโปรแกรมอื่นได้

2.1.2. AJAX (Asynchronous JavaScript and XML)

AJAX[6]เป็นวิธีในการแลกเปลี่ยนข้อมูลไปยังเครื่อง Server เพื่อปรับปรุงบางส่วนของหน้าเว็บไซต์โดยไม่ต้องดึงข้อมูลหน้าเว็บไซต์ทั้งหมดใหม่อีกครั้ง(Asynchronous update)AJAX เป็นการนำมาตรฐานเดิมที่มีอยู่มาใช้ ซึ่งเป็นการผสมผสานระหว่าง XMLHttpRequest Object, Javascript DOM, CSS, XML ซึ่งสามารถทำงานได้โดยเป็นอิสระไม่ยึดติดกับBrowser และ Platformซึ่ง AJAX ถูกนำมาใช้ประมวลผลข้อมูลที่อยู่ในรูปแบบ JSON เพื่อสร้าง Dynamic Web Application

2.1.3. jQuery

jQuery[7]เป็น Javascript Library ที่ถูกนำมาใช้เพื่อให้สามารถสร้าง Web Application เป็นไปได้ง่าย รวดเร็ว และลดความซับซ้อนในการเขียนโปรแกรมด้วยภาษา Javascript โดย jQuery ช่วยให้สามารถเขียนโปรแกรมเพื่อควบคุมการทำงานบางอย่างของ Web Browser เช่น HTML/DOM Manipulator, CSS Manipulator, HTMLEvent, AJAX เป็นไปได้ง่ายขึ้น

2.1.4. REST (Representation State transfer)

REST[8]เป็นรูปแบบของสถาปัตยกรรมที่ใช้ในการออกแบบซอฟท์แวร์ที่ให้บริการผ่านเครือข่าย โดยจัดเตรียมวิธีที่ทำให้ผู้ให้บริการสามารถแลกเปลี่ยนข้อมูลกับผู้ใช้บริการโดยการร้องของผ่าน URL ที่กำหนดไว้

2.1.5. RESTful API

RESTful API[9] เป็น API ที่ทำงานบนหลักการของ REST ซึ่งทำให้ client สามารถเข้าถึงทรัพยากรบน Server ผ่าน HTTP verb (ตัวอย่างเช่น GET,POST,PUT,UPDATE,DELETE ฯลฯ) ผ่านการเขียนโปรแกรม (programmatic access)ได้โดยที่ Client ไม่จำเป็นต้องมีความรู้เกี่ยวกับโครงสร้างของ API ของ Server

2.1.6.Google App Engine

Google App Engine[10]คือ แพลตฟอร์มการให้บริการ (Platform as a service)ที่ให้บริการสร้างและเปิดใช้งานแอปพลิเคชัน(application)ผ่านโครงสร้างพื้นฐานของบริษัทGoogle โดยแอปพลิเคชันที่Google App Engine รองรับสามารถพัฒนาด้วยภาษา 4 ภาษา ได้แก่ Java, PHP, Python และ Go

2.1.7. Python Programming Language

Python เป็นภาษาที่ใช้พัฒนาโปรแกรมแบบInterpreted, Object-oriented ซึ่งได้รับความนิยมเนื่องจากมีไวยากรณ์ที่อ่านและทำความเข้าใจได้ง่าย รองรับโครงสร้างข้อมูลระดับสูงเช่นลิสต์และดิกชันนารีและจัดเตรียมวิธีการในการเข้าถึงโครงสร้างข้อมูลระดับสูงเหล่านี้ไว้ให้แล้ว ทำให้สามารถพัฒนา Application อย่างรวดเร็ว (Rapid Development)

2.1.8. Jinja2 (Template Language)

Jinja2 เป็น Python Library ที่ใช้สำหรับ Generate Markup ที่ใช้ในการแสดงผลบนเอกสาร HTML

2.1.9. LESS

LESS เป็น dynamic stylesheet language ที่สามารถ compile ให้เป็น CSS ซึ่งการสร้าง Stylesheet ด้วย LESS ทำให้สามารถจัดการ CSS ได้ง่ายขึ้นเมื่อ Application มีขนาดใหญ่เนื่องจาก LESS ยอมให้มีการกำหนดตัวแปร,Mix-in, Nestingรวมถึงสามารถใช้ฟังก์ชันและมีการคำนวณต่างๆ บน CSS ได้

2.2 ทฤษฎีและเทคโนโลยีที่เกี่ยวข้องกับการพัฒนาเกม

2.2.1 Gamification

Gamification[3]คือการใช้เทคนิคการออกแบบเกมและกลไกของเกมมาปรับใช้กับเนื้อหาที่ไม่เกี่ยวกับเกมเพื่อปรับเปลี่ยนพฤติกรรมของผู้ใช้เช่น เพิ่มระยะเวลา ความถี่ ในการปฏิสัมพันธ์กับระบบให้มากยิ่งขึ้น

ใน Gamification ผู้เล่นเป็นปัจจัยหลักในการทำให้ผลลัพธ์ออกมา เนื่องจากเกมเป็นตัวกระตุ้นให้ผู้เล่นสามารถทำเรื่องต่างๆในทิศทางที่กำหนดได้อย่างเต็มใจ โดยเจาะจงไปที่ปัจจัยสามอย่างคือ ความเพลิดเพลิน รางวัล และเวลาซึ่งนำมาใช้เป็นแนวทางในการพัฒนาเกมโดยใช้ภาพเคลื่อนไหวและเสียงประกอบเพื่อสร้างความเพลิดเพลิน มีการให้คะนนเป็นผลตอบแทนทุกครั้งที่โจมตีสำเร็จ และมีหลายระดับให้ผู้เล่นเลือกเล่นได้ต่อไปเรื่อยๆ

2.2.2 Crowdsourcing

Crowdsourcing[4]คือกระบวนการที่ใช้กลุ่มบุคคลภายนอกโดยเฉพาะชุมชนออนไลน์มาสร้างเนื้อหา แนวคิด หรือบริการ แทนที่จะเป็นกลุ่มคนในองค์กรหรือผู้จัดทำระบบ เพื่อให้ได้ข้อมูลที่แตกต่างหลากหลาย โดยให้ผู้ใช้ส่งเนื้อหาเข้ามายังระบบและทำการตรวจสอบเพื่อเป็นองค์ความรู้ในระบบต่อไป เช่น Wikipedia อนุญาตให้ผู้ใช้ทั่วไปสามารถแก้ไขเนื้อหาภายในเว็ปไซต์ได้

ซึ่งในโครงงานนี้ได้นำ Crowdsourcing มาใช้ในการหาความน่าจะเป็นในการเลือกเส้นทางที่ผู้โจมตีเลือกใช้ โดยอ้างอิงจากสถิติของการเลือกเส้นทางโจมตีจากที่ผู้เล่นเลือกใช้

2.2.3 CreateJS

CreateJS คือชุดของ library ที่ทำหน้าที่ร่วมกันเพื่อใช้สำหรับพัฒนา interactive content ผ่าน HTML5 โดย library ทั้งชุดนี้ออกแบบมาให้สามารถทำงานแบบแยกกันหรือร่วมกันได้โดยสมบูรณ์แบบ ใน Createjs ประกอบด้วย EaseUS สำหรับการแสดงผลภาพและการโต้ตอบ TweenJS สำหรับทำการเคลื่อนที่ของวัตถุแบบ tween SoundJS สำหรับบริหารจัดการเสียง และ PreloadJS สำหรับทำ preloader ซึ่งในจะนำมาใช้ในการพัฒนาเกมวางแผนการรบในโครงงานนี้

2.3 Computer & Network Security

ในการแปลงเนื้อหาจากระบบจริงเป็นเนื้อหายภายในเกม จะใช้ทฤษฎีของความปลอดภัยในเครือข่ายคอมพิวเตอร์ โดยการใช้ Attack graph คือตัวที่ระบุว่าในระบบมีช่องโหว่อะไรบ้าง ซึ่งในแต่ละช่องโหว่จะระบุชื่อด้วย CVE และอธิบายคุณลักษณะด้วยค่า CVSS เช่นความยากง่ายในการใช้ช่องโหว่ หรือผลกระทบที่เกิดขึ้น เป็นต้น

2.3.1. CVE

CVE[11]คือฐานข้อมูลที่ใช้ระบุชื่อช่องโหว่ต่างๆในเครือข่ายคอมพิวเตอร์ที่ค้นพบแล้วและเห็นว่าสำคัญโดยมีรายละเอียดว่าเป็นอุปกรณ์/software อะไร ช่องโหว่คืออะไร มีผลอย่างไรบ้าง ซึ่งข้อมูลเหล่านี้ได้มาจากเจ้าของผลิตภัณฑ์ และฐานข้อมูลช่องโหว่อื่นๆ เป้าหมายคือการรวบรวมและกำหนดชื่อให้กับช่องโหว่ที่ค้นพบ

2.3.2. CVSS

CVSS[1]คือเกณฑ์การให้คะแนนของ CVE ว่ามีความร้ายแรงขนาดไหน ซึ่งประกอบด้วย Metrics 3 กลุ่ม ได้แก่ Base –แสดงคุณลักษณะพื้นฐานของช่องโหว่นั้นๆที่ไม่ขึ้นกับเวลาและสิ่งแวดล้อม, Temporal – คือคุณลักษณะที่เปลี่ยนไปตามเวลาแต่ไม่ขึ้นกับสิ่งแวดล้อมและ Environmental – คือคุณลักษณะของช่องโหว่ที่แตกต่างกันไปตามสภาพแวดล้อมของผู้ใช้โดยคะแนนนั้นจะสามารถคำนวณได้จำเป็นต้องมี base metrics 6 ตัว แบ่งเป็นAccess ที่แสดงถึงความยากง่ายในการอาศัยช่องโหว่ในการโจมตี 3 ตัว และ Impact ที่แสดงถึงผลกระทบหลังจากถูกโจมตี 3 ตัว ได้แก่

- AV(Access vector) บอกว่าสามารถใช้ช่องโหว่นี้ได้จากการเชื่อมต่อระดับไหนRemote – เข้าจากเครือข่ายภายนอกได้, Adjacent – เข้าจากในเครือข่ายเดียวกัน(Subnet เดียวกัน), Local – เข้าได้จากเครื่องนั้นๆเท่านั้น
- AC(Access Complexity) ในการเจาะเครือข่ายด้วยช่องโหว่นี้มีความซับซ้อนมากน้อยอย่างไร Low, Medium, High
- AU(Access Authentication) ช่องโหว่นี้ต้องผ่านการยืนยันตนมากี่รอบก่อนที่จะทำการโจมตีได้ 0, 1, 2 ขึ้นไป
- C(Confidential Impact) ความสามารถในการอ่านข้อมูลในระบบเมื่อเจาะสำเร็จ none, partial, full
- I(Integrity Impact) ความสามารถในการเปลี่ยนแปลงระบบเมื่อเจาะสำเร็จ none, partial, full
- A(Availability Impact) ความสามารถในการหยุดการทำงานของระบบเมื่อทำการโจมตีได้สำเร็จ none, partial, full

ซึ่งคะแนนของ CVSS นั้นสามารถคำนวณได้จากสูตร ดังนี้

BaseScore = (.6*Impact +.4*Exploitability-1.5)*f(Impact)

Impact = 10.41 * (1 - (1 - ConfImpact) * (1 - IntegImpact) * (1 - AvailImpact))

Exploitability = 20 * AccessComplexity * Authentication * AccessVector

f(Impact) = 0 if Impact=0 หรือ 1.176 เมื่อเป็นค่าอื่น

2.3.3. Attack graph

Attack graph[14] คือกราฟที่ใช้ในการแสดงสถานะความปลอดภัยของระบบ การใช้ช่องโหว่ต่างๆ ในระบบประกอบกันเป็นการโจมตีแต่ละรูปแบบ แสดงเส้นทางที่ใช้ในการโจมตีแต่ละจุดในเครือข่าย โดยใช้ Verticesแสดงสถานะก่อนและหลังโจมตี และ Edges แสดงวิธีการที่ใช้โจมตีในเครือข่าย

2.4 งานวิจัยที่เกี่ยวข้อง

Jared Cechanowicz[5] ได้ทำการวิจัยว่า gamify มีผลต่อการเข้าร่วมของผู้ใช้หรือไม่ โดยทำการสร้างแบบสอบถามขึ้นมาสามแบบคือ แบบสอบถามธรรมดา แบบสอบถามที่มีลักษณะกึ่งเกม และแบบสอบถามที่มีลักษณะเป็นเกม โดยวัดจากจำนวนข้อที่ทำแบบสอบถามเสร็จ โดยผลที่ได้คือ gamification มีผลต่อพฤติกรรมการใช้งานของผู้ใช้ ในด้านเวลาสามารถอยู่ในระบบได้นานขึ้น ในด้านกิจกรรมมีปฏิสัมพันธ์กับระบบมากขึ้น และในด้านความพึงพอใจก็มีความพึงพอใจมากขึ้นเช่นกันจากงานวิจัยชิ้นนี้ทางผู้พัฒนาคาดว่าระบบจะสามารถดึงดูดผู้เล่นได้มากกว่าการทำเป็นการจำลองการเจาะระบบธรรมดา

Seth Cooper[12]และคณะได้ทำการพัฒนาเกมFoldit สำหรับแก้ปัญหาทางวิทยาศาสตร์ โดยใช้ความสามารถในการแก้ปัญหาของผู้เล่นเข้ามาช่วย วิธีที่ใช้คือนำให้ผู้เล่นหาโครงสร้างที่ดีที่สุดของโปรตีน โดยคะแนนสามารถคำนวณได้จากคุณลักษณะทางวิทยาศาสตร์ เช่น ระดับพลังงาน พันธะไฮโดรเจน เป็นต้น ผลที่ได้คือผู้เล่นช่วยกันพับงอโครงสร้างของโปรตีนจนค้นพบเอนไซม์ Retroviral Proteases ซึ่งมีความสำคัญอย่างมากในการพัฒนายารักษาโรคเอดส์ทำให้ผู้พัฒนาได้แนวคิดเดี่ยวกับการคิดคะแนนในการแก้ปัญหาแต่ละวิธี และการแสดงปัญหาให้ออกมาในรูปแบบที่เป็นเกมและเข้าใจได้ง่าย

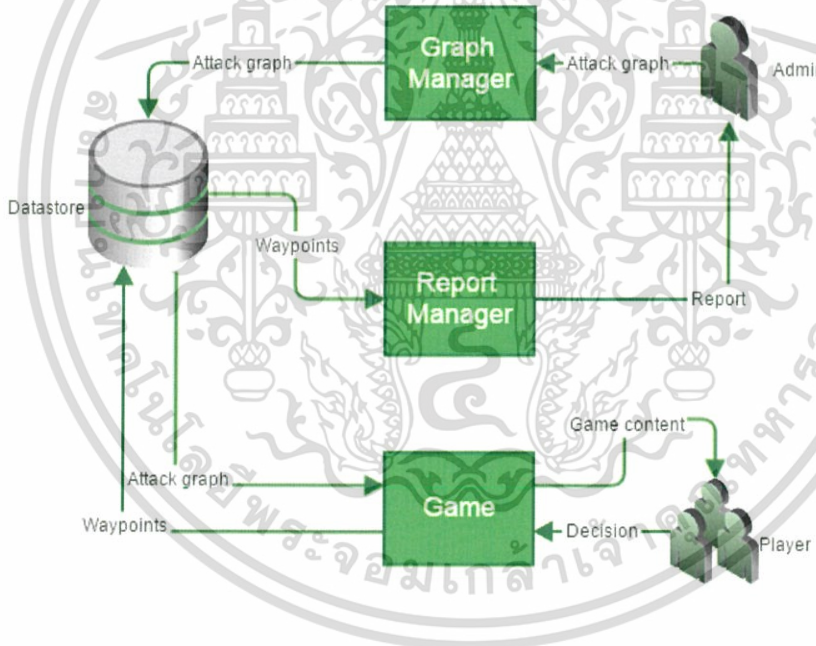
McNab[13]และคณะ ได้ทำการพัฒนาเกมThe great brain experiments เพื่อใช้เก็บข้อมูลเกี่ยวกับการทำงานของสมอง เช่น ความจำ การตอบสนอง การจดจ่อ และการตัดสินใจ โดยการทำเป็นเกมย่อยเพื่อทดสอบในแต่ละส่วน สิ่งที่ค้นพบจากข้อมูลที่ได้จากเกมเหล่านี้คือ สมองจะกำจัดสิ่งรบกวนที่ออกมาในขณะพักได้ดีกว่าในขณะที่กำลังทำงาน ซึ่งจากงานวิจัยชิ้นนี้ทางผู้พัฒนาได้ใช้แนวคิดเกี่ยวกับการทำใช้เกมเพื่อเป็นเครื่องมือในการเก็บสถิติเพื่อนำมาใช้ในการวิเคราะห์แก้ปัญหาต่อไป

บทที่ 3 การออกแบบและพัฒนา

การวิเคราะห์และออกแบบระบบเกมจำลองการโจมตีในระบบเครือข่ายนั้นได้นำทฤษฎีที่ศึกษาค้นคว้าจากบทที่ 2 มาใช้ในการออกแบบและพัฒนาระบบ โดยในบทนี้จะกล่าวถึงภาพรวมทั้งหมดของระบบและอธิบายรายละเอียดของส่วนประกอบในระบบ พร้อมทั้งอธิบายถึงเทคโนโลยีและภาษาที่ใช้ในการพัฒนาระบบ

โครงงานนี้ได้เลือกใช้ Google App Engine และ wepapp2 เป็นเฟรมเวิร์คภาษาไพทอนในการพัฒนาแอปพลิเคชัน รับข้อมูลช่องโหว่ของเครือข่ายในรูปแบบ JSON นำมาเก็บใน Datastore ซึ่งเป็นบริการฐานข้อมูลของ Googleและใช้ CreateJS ในการพัฒนาเกมที่แปลงจากข้อมูลช่องโหว่ในเครือข่าย เมื่อได้ข้อมูลการเลือกเส้นทางของผู้เล่นแล้ว จะนำไปแสดงผลให้กับผู้ดูแลระบบทั้งในรูปแบบตารางเพื่อให้เห็นรายละเอียด และแบบแผนภาพเพื่อให้เห็นภาพรวม

3.1 ภาพรวมของระบบ



ภาพที่ 3.1. ภาพรวมของระบบ

Datastore คือส่วนที่ใช้เก็บข้อมูล Attack graph คือข้อมูลช่องโหว่ในเครือข่ายที่ผู้ดูแลระบบส่งเข้ามาและ Waypointsคือข้อมูลการตัดสินใจเลือกใช้เส้นทางต่างๆที่ผู้เล่นเลือกใช้

Graph manager คือส่วนที่บริหารจัดการ Attack graph ของผู้ดูแลระบบของแต่ละองค์กร ได้แก่เพิ่ม/แก้ไข/ลบ Attack graph

Report manager คือส่วนที่สร้างรายงานผลจากข้อมูล Waypoints ที่มี เพื่อให้ผู้ดูแลระบบดูว่าเครื่อง, เซอร์วิสและเส้นทางใด เป็นที่นิยม และผลกระทบในแต่ละจุดเป็นอย่างไร

Game คือส่วนที่จะแปลง Attack graph มาเป็นแผนที่ในเกมแนววางแผนการรบที่ผู้เล่นจะต้องเลือกโจมตีในแต่ละจุดด้วยทหารที่มีคุณสมบัติแตกต่างกัน

3.2. Graph manager

รับข้อมูล Attack Graph ซึ่งประกอบด้วย ชื่อCVE คะแนนCVSS และช่องโหว่ของเซอร์วิสในแต่ละเครื่องมาเก็บไว้ใน Datastoreโดยจะต้องส่งข้อมูลของ Attack graph มายังระบบด้วยการกรอก HTML form หรือส่ง HTTP POST ในรูปแบบ JSON ซึ่งมีข้อมูลดังนี้

ตารางที่ 3.1. รูปแบบข้อมูลนำเข้า

ชื่อ	ประภท	ความหมาย
API key	String	API key สำหรับการบริหารจัดการกราฟ
name	String	ชื่อกราฟ
machines	List	ลิสของเครื่องในกราฟ
services	List	ลิสของเซอร์วิสของทุกๆเครื่อง
paths	List	ลิสของเส้นทางการโจมตีในกราฟ

ตารางที่ 3.2. ข้อมูลของเครื่องในกราฟ

ชื่อ	ประภท	ความหมาย
name	String	ชื่อเครื่อง
machineID	Integer	รหัสของเครื่อง
status	String	สถานะของเครื่อง มีค่าเป็น {Hidden | Found}

ตารางที่ 3.3. ข้อมูลของเซอร์วิสในเครื่อง

ชื่อ	ประภท	ความหมาย
name	String	ชื่อเซอร์วิส
Service id	Integer	รหัสของเซอร์วิส

machine	Integer	เครื่องที่เป็นเจ้าของเซอร์วิสนั้นๆ
Status	String	สถานะของเซอร์วิสมีค่าเป็น {Hidden | Found}

ตารางที่ 3.4. ข้อมูลของเส้นทางการโจมตี

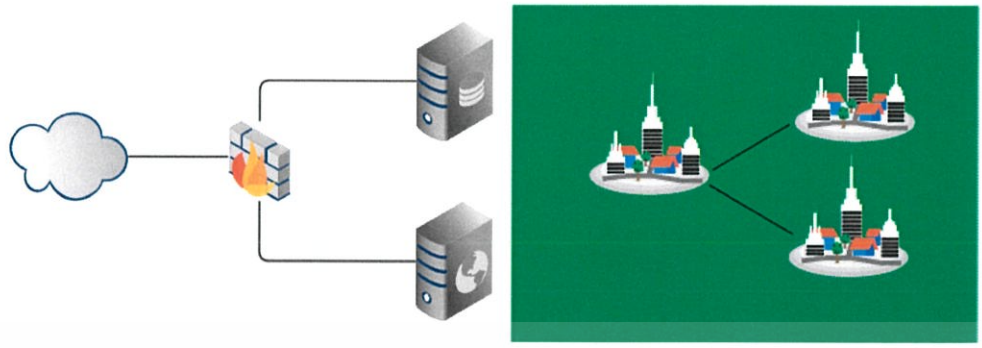
ชื่อ	ประภท	ความหมาย
name	String	ชื่อเส้นทาง คือประเภทของการโจมตี ซึ่งตรงกับ CWE
Id	Integer	รหัสของเส้นทาง
Source	Integer	รหัสของเซอร์วิสที่เป็นต้นทางในการโจมตี
Destination	Integer	รหัสของเซอร์วิสที่เป็นปลายทางในการโจมตี
CVE	String	ชื่อ CVE
AV	Integer	Access Vector
AC	Integer	Access Complex
AU	Integer	Authentication
CI	Integer	Confidential Impact
AI	Integer	Availability Impact
II	Integer	Integrity Impact

3.3.เกมวางแผนการรบ

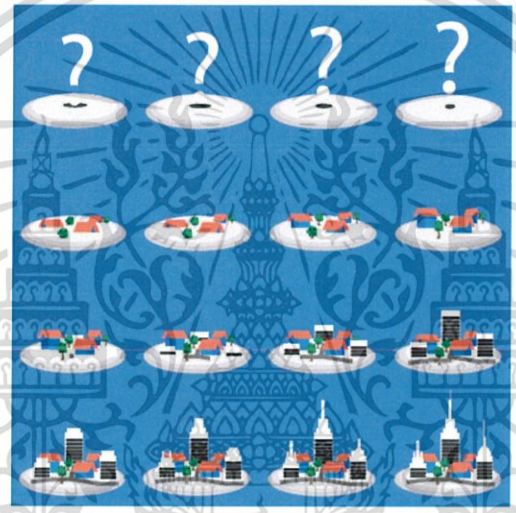
ในส่วนเกม พัฒนาเป็นเกมแนววางแผนเล่นผ่านเว็บบราวเซอร์ ซึ่งพัฒนาด้วย HTML5, Javascript และ CreateJS และบันทึกข้อมูลการเล่นของผู้เล่นกลับไปยังระบบ

3.3.1. การแปลง Attack graph เป็นเนื้อหาภายในเกม

การแปลงข้อมูล attack graph เป็นแผนที่ในเกม จะใช้เมืองแทน logical machine ในเมืองจะมีสิ่งปลูกสร้างต่างๆแทน service ที่มีในเครื่องนั้นๆ (ภาพที่ 3.2) ใช้ทหารส่งเข้าไปโจมตีสิ่งปลูกสร้างไปในเมือง แทนการโจมตีตามช่องโหว่ในระบบ โดยในตัวละครแต่ละตัวที่ใช้ส่งไปโจมตีจะถูกแทนค่าคุณสมบัติด้วย CVSS base metrics (ตารางที่ 3.5)โดยชื่อเครื่องและเซอร์วิสทั้งหมดจะถูกซ่อนไว้ ใช้เป็นชื่อเมืองและสิ่งปลูกสร้างแทน ซึ่งขนาดของเมืองจะขึ้นอยู่กับจำนวนของสิ่งปลูกสร้างในเมืองนั้นๆ (ภาพที่ 3.3) และสิ่งปลูกสร้างเองก็จะต้องสื่อถึงคุณลักษณะของเซอร์วิสนั้นๆด้วยเช่นกัน (ภาพที่ 3.4)



ภาพที่ 3.2. ตัวอย่างการแปลงจากเครื่องเป็นเมือง



ภาพที่ 3.3. เมืองในขนาดต่างๆ แถวแรก – เมืองที่ยังไม่ถูกสำรวจ, แถวที่2 – เมืองขนาดเล็ก, แถวที่3 – เมืองขนาดกลาง, แถวที่4 – เมืองขนาดใหญ่

ในการแปลงสิ่งปลูกสร้าง และคุณลักษณะของช่องโหว่ มีแนวคิดคือเมื่อปัจจัยที่มีผลต่อการตัดสินใจของผู้เล่นใกล้เคียงกับระบบจริงแล้วผลการตัดสินใจของผู้เล่นจะใกล้เคียงกับการตัดสินใจของผู้โจมตีระบบเช่นกันซึ่งปัจจัยที่คาดว่ามีผลต่อการตัดสินใจของผู้โจมตี ได้แก่ เซอร์วิสเป้าหมาย และคุณสมบัติของเส้นทางที่เลือกใช้ ในส่วนของเซอร์วิสนั้นจะให้ความสำคัญกับหน้าที่ของเซอร์วิส ซึ่งเลือกใช้สิ่งปลูกสร้างในเกมแทนเซอร์วิสดังนี้

Headquarter เป็นศูนย์กลางการออกคำสั่งทั้งหมดในเมืองนั้นๆ ใช้แทน OS

Barracks แทนเซอร์วิสประเภทออกคำสั่งทางไกล เช่น SSH

Trade port แทนเซอร์วิสประเภทที่เป็นที่รองรับคำขอจากบุคคลภายนอก เช่น Web application

Turret แทนเซอร์วิสประเภทที่เป็นการรักษาความปลอดภัย เช่น Firewall

Warehouse แทนเซอร์วิสประเภทที่เป็นส่วนเก็บไฟล์ข้อมูล เช่น Database, FTP

Lab เซอร์วิสประเภทอื่นๆที่ระบบไม่รู้จัก

ส่วนของการแปลงคุณลักษณะของช่องโหว่เป็นคุณลักษณะของทหารตามตาราง ดังนี้

ตารางที่ 3.5. การแปลค่าต่างๆจาก CVSS เป็นคุณลักษณะของตัวละครในเกม

CVSS Base metrics	Unit attributes
Access Vector	ความสามารถในการเข้าถึงสิ่งปลูกสร้างของทหาร
Access Complexity	จำนวนเทิร์นที่ใช้ในการทำการโจมตี
Access Authentication	จำนวนกุญแจที่มี/ต้องการ
Integrity Impact	ความสามารถในการเข้ายึดครอง
Confident Impact	จำนวนของที่ขโมยได้
Availability Impact	ความเสียหายที่ทำได้

Access Vector คือค่าที่แสดงว่าในการโจมตีช่องโหว่นั้นจะโจมตีได้จากระยะไกลแค่ไหน จะแปลงเป็นความสามารถในการเข้าโจมตีของตัวละคร Remote – สามารถโจมตีจากที่ไหนก็ได้, Network – สามารถโจมตีได้จากเมืองที่อยู่ติดกันเท่านั้น, Local – สามารถโจมตีได้จากในเมืองนั้นเท่านั้น

Access Complexityคือค่าที่แสดงว่าช่องโหว่นั้น มีความซับซ้อนในการเจาะมากน้อยเพียงใด จะแปลงเป็นจำนวนเทิร์นที่ต้องใช้ในการทำภารกิจ Low – 1 เทิร์น, Med –2 เทิร์น, High –3 เทิร์น

Access Authenticationคือค่าที่แสดงว่าช่องโหว่นั้น ต้องผ่านการยืนยันตัวตนมากี่รอบ จึงจะทำการโจมตีได้ จะแปลงเป็นว่า เส้นทางนั้น ต้องการบัตรผ่านกี่ใบ ซึ่งถ้าต้องการจะทำการโจมตีผ่านเส้นทางนี้ จะต้องเอาบัตรผ่านมาให้ได้ครบจำนวนก่อน

Integrity Impactคือค่าที่แสดงว่าเมื่อโจมตีแล้ว ผู้โจมตีจะสามารถเปลี่ยนแปลงระบบได้มากน้อยเพียงใด จะแปลงเป็นความหมายว่า ทหารคนนั้นๆมีความสามารถในการยึดครองมากน้อยเพียงใด none – ไม่สามารถยึดครองได้, partial – สามารถยึดครองสิ่งปลูกสร้างนั้นได้, full – สามารถยึดเมืองนั้นได้ทั้งเมือง และเมื่อยึดสิ่งปลูกสร้างใดๆได้แล้วสามารถใช้เป็นฐานในการทำการโจมตีต่อไปได้

Confidential Impactคือค่าที่แสดงว่าเมื่อโดนโจมตีแล้ว ผู้โจมตีจะสามารถอ่านค่าต่างๆจากระบบได้มากน้อยเพียงใด จะแปลงเป็นความหมายว่า สามารถขโมยเงินไปได้มากน้อยเท่าไร

Availability Impactคือค่าที่แสดงว่าเมื่อโดนโจมตีแล้ว เซอร์วิสนั้นๆจะยังคงให้บริการได้อยู่หรือไม่ แปลงมาเป็นค่าความเสียหายที่สามารถทำได้

นอกจากการแปลงเนื้อหาในด้านวัตถุแล้ว ในด้านกระบวนการก็ต้องแปลมาให้สอดคล้องกับตัวเกมเช่นกัน ซึ่งกระบวนการในเกมนี้จะอ้างอิงจากกระบวนการโจมตีระบบจริง

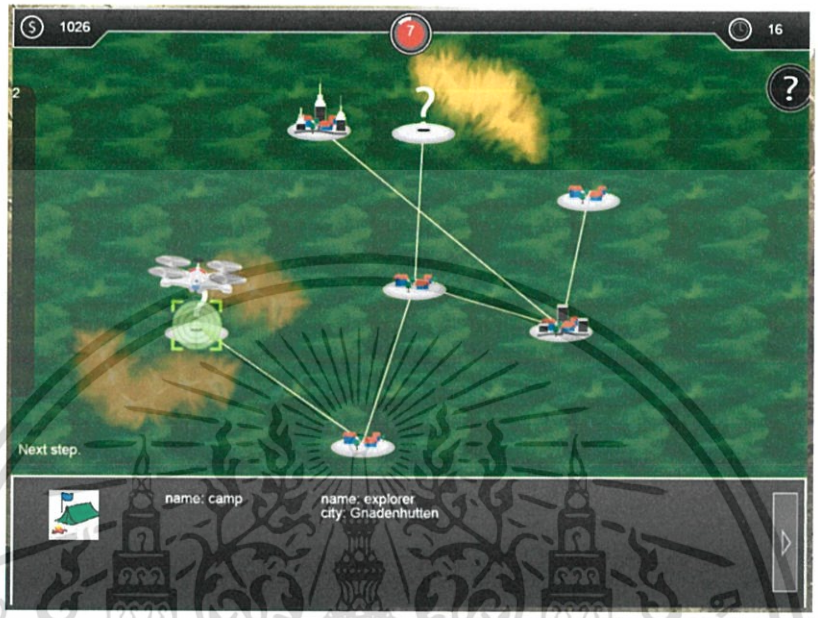
ในการโจมตีระบบจริงแบ่งขั้นตอนคร่าวๆออกได้เป็น 5 ขั้นตอนได้แก่ Reconnaissanceหาเป้าหมายที่ต้องการ – สแกนเป้าหมายเช่นซอฟท์แวร์ที่ใช้ เวอร์ชั่น ช่องโหว่ เป็นต้น –Exploit โจมตีโดยอาศัยช่องโหว่ที่พบในขั้นตอนที่แล้ว เพื่อให้ได้มาซึ่งสิทธิ์การเข้าถึงระบบ –Maintain สร้างช่องทางลับในการเข้าถึงระบบใหม่ในภายภาคหน้า –Clear trackทำลายหลักฐานที่ผู้ดูแลระบบจะสามารถสืบได้ว่ามีเราเข้ามาในระบบหรือเข้ามาจากที่ไหนเป็นแบบนี้วนไปเรื่อยๆ

กระบวนการโจมตีภายในเกมวางแผนการรบจะมีขั้นตอนดังนี้ 1.) สำรวจเมืองเพื่อให้ทราบว่าภายในเมืองนั้นมีสิ่งปลูกสร้างอะไรบ้าง และในสิ่งปลูกสร้างมีช่องโหว่อะไรให้โจมตีได้บ้าง 2.) โจมตีสิ่งปลูกสร้างต่างๆเข้ายึดครองเพื่อค้นหาเส้นทางเข้าไปโจมตีเมืองข้างๆ 3.) ทำลายหลักฐานเพื่อไม่ให้ถูกจับได้

ตารางที่ 3.6. กระบวนการในระบบจริงและในเกม

ระบบจริง	**เกมวางแผนการรบ**
Reconnaissance	ค้นหาเมืองใกล้เคียง
Scanning	ค้นหาสิ่งปลูกสร้างในเมือง
Exploit	ส่งทหารเข้าไปปฏิบัติภารกิจ
Maintaining	เข้ายึดเมือง
Clear tracks	หยุดภารกิจเพื่อลดระดับการตรวจพบ

3.2.2. รูปแบบการเล่น



ภาพที่ 3.4. ตัวอย่างภาพในเกม

ในหน้าเล่นเกมจะแบ่งออกเป็นสามส่วนคือ

1. ข้อมูลผู้เล่นด้านบน ไล่จากซ้ายไปขวาคือ คะแนน ระดับการถูกตรวจจับ และเทิร์นโดยคะแนนคำนวณได้จากการกระทำของผู้เล่นแต่ละขั้นตอน โดยใช้วิธีคำนวณแบบเดียวกับ CVSS , ระดับการถูกตรวจจับจะเพิ่มขึ้นเมื่อทำการโจมตีในแต่ละขั้นตอน โดยค่าที่สูงขึ้นจะทำให้มีโอกาสถูกจับได้มากขึ้น และถ้าหากถูกจับได้จะเสียเมืองที่ทำการควบคุมได้ไป ส่วนสุดท้ายคือจำนวนเทิร์นแสดงจำนวนเทิร์นที่ใช้ไปในการโจมตีทั้งหมด

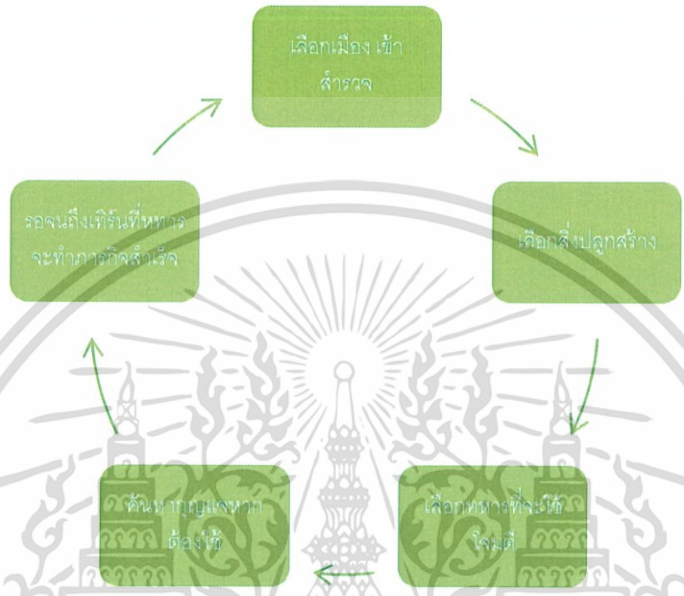
2. แผนที่ แสดงเมืองและสิ่งปลูกสร้างใดๆและสามารถเข้าถึงกันได้ด้วยเส้นทางใด มีสองแบบคือแผนที่ด่านจะแสดงเมืองทั้งหมด และเมื่อกดเข้าไปในแต่ละเมืองก็จะแสดงสิ่งปลูกสร้างทั้งหมดที่มีในเมืองนั้น

3. แผงควบคุม แสดงรายละเอียดวัตถุที่เลือก และตัวละครที่สามารถส่งไปโจมตีได้

รูปแบบการเล่น มีลักษณะการเล่นเป็นเทิร์น จุดมุ่งหมายคือผู้เล่นจะต้องทำการโจมตีให้ได้คะแนนมากที่สุดในจำนวนเทิร์นที่น้อยที่สุด โดยตอนเริ่มต้นฐานหลักของผู้เล่นจะอยู่ด้านนอกเมือง ผู้เล่นจะต้องทำการสำรวจเมืองก่อนว่าในเมืองนั้นๆมีสิ่งปลูกสร้างใดและมีเส้นทางถึงเมืองใดบ้าง เมื่อสำรวจเมืองได้แล้วจึงส่งทหารออกไปตามสิ่งปลูกสร้างต่างๆ เพื่อทำการโจมตีซึ่งผลตอบแทนในแต่ละภารกิจคือคะแนน หรือในบางครั้งตัวละครเองก็สามารถยึดเมืองได้ด้วย ยิ่งโจมตีได้มาก คะแนนก็จะได้มากไปด้วย โดยผู้เล่นจะต้องโจมตีและยึดเมืองเพื่อใช้โจมตีส่วนที่ลึกเข้า

ไปเรื่อยๆ โดยมีเงื่อนไขในการจบเกม 3 แบบคือ 1.) Detected หมายความว่าผู้เล่นทำการโจมตีถี่เกินไปจนถูกจับได้ 2.) Retire หมายความว่าผู้เล่นยอมแพ้3.) Win หมายความว่าผู้เล่นสามารถเข้ายึดเมืองได้ทุกเมืองแล้ว

ในการแปลงกลับ จะใช้ข้อมูลการกระทำของผู้เล่นในแต่ละเทิร์นมาแปลเป็นเหตุการณ์ที่อาจเกิดขึ้นได้ในโลกแห่งความจริง รวมทุกๆขั้นตอนเป็นกลวิธี(Waypoint) เพื่อใช้สรุปให้กับผู้ดูแลระบบต่อไป



ภาพที่ 3.5. การกระทำที่ผู้เล่นต้องทำในแต่ละเทิร์น

3.3. ส่วนนำเสนอ

แสดงข้อมูลเชิงสถิติให้ผู้ดูแลระบบดู โดยใช้ข้อมูลจาก Waypoint(กลวิธีที่ผู้เล่นใช้ในการผ่านด่านแต่ละด่าน)ซึ่งประกอบด้วย Stepคือรายละเอียดที่แสดงว่าในการโจมตีของผู้เล่นแต่ละครั้ง ผู้เล่นเลือกโจมตีเครื่องใดมาจากเครื่องใดใช้ช่องโหว่ใดมาสรุปให้ผู้ดูแลระบบนั้นๆดู เพื่อนำไปใช้พัฒนาระบบของตนต่อไป โดยจะแสดงข้อมูลดังต่อไปนี้ แสดงข้อมูลตามลำดับคะแนนผู้เล่น แสดงข้อมูลตามความนิยมของเส้นทาง แสดงข้อมูลตามความนิยมของเครื่อง

ตารางที่ 3.7. ข้อมูลที่เก็บ Waypoints

ชื่อ	**ประภท**	**ความหมาย**
Id	Integer	**รหัสของ** Waypoint
Play by	String	**รหัสของผู้เล่น**
Map Id	Integer	**รหัสของกราฟที่ใช้ในการทำด่านนั้นๆ**

Status	String	สถานะของการเล่นมีค่าที่เป็นไปได้คือ { Win | Retire | Detected }
Score	Integer	คะแนนคำนวณแบบเดียวกับ CVSS base score
Steps	Collections	ขั้นตอนในการเล่นแต่ละขั้นตอน
Saved turn	Integer	จำนวนเทิร์นที่ใช้

ตารางที่ 3.8. ข้อมูลที่เป็นขั้นตอนการเล่น (Steps)

ชื่อ	**ประภท**	**ความหมาย**
name	String	ชื่อเส้นทาง คือประเภทของการโจมตี ซึ่งตรงกับ CWE
Id	Integer	รหัสของเส้นทาง
From city	Integer	รหัสของเครื่องที่เป็นต้นทางในการโจมตี
To city	Integer	รหัสของเครื่องที่เป็นปลายทางในการโจมตี
Path	Integer	รหัสของเส้นทางที่ใช้ในการโจมตี
Operation	String	รูปแบบการโจมตี มีค่าที่เป็นไปได้คือ {Scan | Exploit | Key}

3.3.1.การนำเสนอในรูปแบบตาราง

ในการแสดงผลในรูปแบบตารางจะมีรายละเอียดของเส้นทางที่ถูกใช้และสรุปกลวิธีที่ผู้เล่นใช้ ในแต่ละเส้นทางจะมีบอกค่า CVSS base scoreจำนวนครั้งที่ถูกใช้ จำนวนครั้งที่ถูกใช้โดยเฉลี่ยมีค่าระหว่าง 0-1 และส่วนที่รายงานผล waypoint จะแสดงให้เห็นถึงการเล่นในแต่ละครั้ง ประกอบด้วยคะแนน ผู้เล่น จำนวนเทิร์น และสถานะว่าแพ้ชนะหรือยังเล่นไม่จบ

Path Summary

ID	Name	Hits	Avg. Hits	AV	AC	AU	AI	II	CI
1	Scan	6	0.3	Remote	Med	1	None	Partial	Partial
2	CSRF	7	0.35	Remote	High	2+	Complete	Partial	Partial
3	SQL Injection	7	0.35	Remote	Med	1+	Partial	Complete	Partial

Waypoint Summary

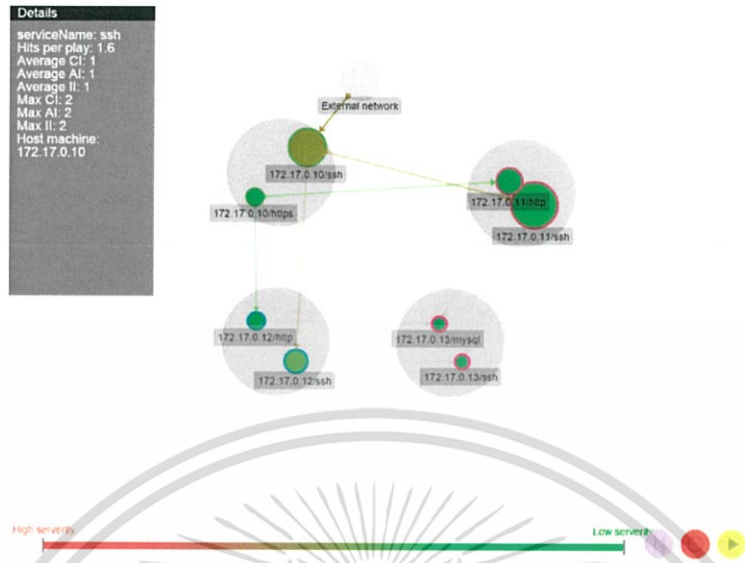
Waypoint ID	Play by	Turn	Score	Status
1	iyochan32	35	7850	Win
1	vincerio	40	7350	Win
1	HANAHANA	17	2550	Playing
1	miyuki69	8	1200	Retired

ภาพที่ 3.6. การรายงานผลในรูปแบบตาราง

3.3.2. การนำเสนอในรูปแบบแผนภาพ

ในการแสดงผลภาพรวมด้วยแผนภาพ เลือกใช้ Ajax และ EaseUS มาใช้ในการแสดงผล 3 ส่วน

1) ส่วนหน้าต่างรายละเอียด จะแสดงรายละเอียดของสิ่งที่เม้าส์ชี้อยู่ ได้แก่ชื่อ ค่าเฉลี่ย ค่าสูงสุด ของผลกระทบที่เกิดขึ้นในแต่ละเครื่องแต่ละเซอร์วิส
2) ส่วนแผนภาพแสดงผลในรูปแบบของกราฟโดยมีโหนดเล็กที่แสดงถึงเซอร์วิสภายในเครื่องที่แสดงด้วยโหนดใหญ่สีเทาที่คลุมอยู่ ซึ่งสีในเซอร์วิสหมายถึงระดับผลกระทบเฉลี่ยที่เกิดขึ้นในการเล่นแต่ละเทิร์น สีเขียวคืออันตรายน้อยไล่ไปถึงสีแดงคืออันตรายมาก ขนาดของโหนดหมายถึงความถี่ของการตกเป็นเป้าหมายการโจมตี คือโหนดที่มีขนาดใหญ่ถูกโจมตีบ่อยกว่าโหนดที่มีขนาดเล็ก สีขอบของโหนดคือสีที่ใช้แสดงว่าเป็นเครื่องเดียวกันหรือไม่ เครื่องเดียวกันจะถูกแทนด้วยสีขอบเดียวกัน ส่วนเส้นทางแทนด้วยเส้นลูกศรระดับความอันตรายไล่จากสีเขียวไปแดงเช่นเดียวกับโหนด ส่วนความถี่ของเส้นทางจะแสดงด้วยความโปร่งใสของเส้น เส้นที่เข้มมากคือเส้นทางที่ถูกใช้ในการเล่นบ่อยๆ
3) แถบควบคุมด้านล่างจะมีแถบสีใช้เทียบระดับความอันตราย ปุ่ม N คือ ซ่อน/แสดงชื่อโหนด ปุ่ม O คือให้จัดเรียงใหม่ ในบางกรณีที่มีเส้นหรือโหนดซ้อนกัน ปุ่ม Play/Pause คือให้หยุดจัดตำแหน่งเมื่อสามารถมองส่วนที่ต้องการออกแล้ว



ภาพที่ 3.7. การรายงานผลในรูปแบบแผนภาพ

3.4 การพัฒนา

3.4.1. เซิร์ฟเวอร์

ใช้Google App Engine และพัฒนาAPI ในการทำคำสั่งที่เรียกมาจากภายนอก ซึ่งพัฒนาด้วยภาษา Python มีฟังก์ชันการทำงานดังนี้

ตารางที่ 3.9 API **ฟังก์ชันของเซิร์ฟเวอร์**

ชื่อฟังก์ชัน	**ประเภท**	**รายละเอียด**
Maplist	GET	แสดงรายชื่อ Attack graph ทั้งหมดในระบบ
Get-graph	GET	แสดงรายละเอียดของ Attack graph ที่ต้องการ
Create-waypoints	POST	สร้าง Waypoint สำหรับเก็บรายละเอียดการเล่น
Postgraph	POST	ส่ง Attack graph ขึ้นไปในระบบ
Add-step	POST	ส่งรายละเอียดการโจมตีในแต่ละครั้ง
Map-report	GET	แสดงผลสรุปการเล่นของ Attack graph
Host-report	GET	แสดงผลสรุปการเล่น โดยจำแนกตามเครื่องที่ถูกโจมตี
Node-report	GET	แสดงผลสรุปการเล่น โดยจำแนกตามเซอร์วิสที่ถูกโจมตี
Path-report	GET	แสดงผลสรุปการเล่น โดยจำแนกตามเส้นทางที่ถูกเลือกใช้
Update-score	POST	บันทึกสถานะการเล่น เพื่อใช้เล่นต่อในภายหลัง

End-game	POST	หยุดบันทึกขั้นตอนการเล่นของผู้เล่น และสรุปว่าผู้เล่นเล่นจบแล้ว
Get-highscore	GET	แสดงคะแนนผลการเล่นสูงสุด 10 อันดับแรกของ Attack graph

3.4.2 ส่วนติดต่อกับผู้ดูแลระบบ

ผู้พัฒนาใช้ Google App Engine ในการพัฒนาส่วนติดต่อกับผู้ดูแลระบบ โดยที่ผู้ดูแลระบบต้องลงทะเบียนสมัครเป็นสมาชิกและใช้ข้อมูลในการลงทะเบียนได้แก่ชื่อผู้ใช้และรหัสผ่านในการเข้าสู่ระบบ ระบบจะทำการสร้าง API Key สำหรับบัญชีผู้ใช้ของผู้ดูแลระบบแต่ละคนเพื่อให้ใช้ API Key ในการยืนยันตนเมื่อต้องการแลกเปลี่ยนข้อมูลด้วยรูปแบบข้อมูลแบบ JSON กับเครื่องแม่ข่ายผ่านบริการ RESTful API

ส่วนติดต่อกับผู้ดูแลระบบบนเว็บแอปพลิเคชันถูกพัฒนาด้วยภาษา Python ร่วมกับ Jinja2 ในการสร้างแม่พิมพ์ HTML เพื่อใช้แสดงผลแบบกราฟฟิคและใช้ LESS CSS ในการจัดการ Style Sheet

3.4.3 เกม

ในส่วนเกมจะแบ่งการทำงานออกเป็น Scene โดยแต่ละ Scene คือกลุ่มของวัตถุที่จะใช้วาดในแต่ละฉาก ได้แก่ Preload, Level, Play และ End ซึ่งในการเปลี่ยน Scene จะกระทำผ่าน Scene Manager

Preload scene มีหน้าที่ preload ภาพและเสียงที่ใช้ในเกมมาเก็บไว้ก่อน เพื่อลดปัญหาภาพและเสียงไม่แสดงผลระหว่างเล่นเกมเนื่องจากยังโหลดไม่เสร็จ

Level scene มีหน้าที่แสดงรายชื่อ Attack graph ทั้งหมดในระบบ โดยเรียก API graph-listของฝั่งเซิร์ฟเวอร์ ผ่านทาง Ajax

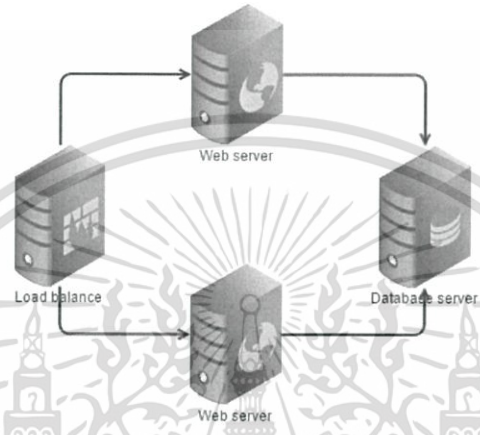
Play scene ทำการดึงรายละเอียดของ Attack graph ที่ผู้เล่นเลือกในหน้า Levelโดยเรียก API /get-graph ขอฝั่งเซิร์ฟเวอร์ด้วย Ajax จากนั้นนำ Attack graph ที่ได้มาทำการวาดเป็นแผนที่ในเกม โดยใช้สิ่งปลูกสร้างในเมืองแทนเซอร์วิสในเครื่อง และใช้ทหารแทนช่องโหว่ในแต่ละจุด ซึ่งในการวาด Scene นี้จะมีความซับซ้อนมากกว่า Scene อื่นๆ จึงต้องทำการแบ่งการวาดออกเป็น 3 ระดับ เพื่อให้ภาพไม่เกิดการซ้อนกันผิดกันแหน่ง ได้แก่ world map สำหรับวาดเมืองในแผนที่ city map สำหรับวาดสิ่งปลูกสร้างในเมือง และ gui สำหรับวาดแผนผังควบคุมและแสดงรายละเอียดของวัตถุภายในเกม

ในการเล่นทุกครั้งที่ทำการโจมตีระบบจะบันทึกรายละเอียดของแต่ละขั้นตอนด้วยการเรียก API /add-step เพื่อระบุว่าผู้เล่นโจมตีอย่างไรในแต่ละขั้นตอน

End scene เมื่อเล่นจบจะไปที่หน้า End scene สรุปผลการเล่นว่าผู้เล่นได้คะแนนเท่าไร และคะแนนสูงสุด 10 อันดับแรกของด่านนั้นเป็นเท่าไร

บทที่ 4 การทดลองและผลการทดลอง

ในการทดลองวัฏจักรของระบบเกมจำลองการโจมตีในระบบเครือข่าย ทำการทดลองเพื่อยืนยันว่าระบบสามารถทำงานได้ตามที่ออกแบบไว้ คือสามารถรับข้อมูล Attack graph มาแปลงเป็นเนื้อหาภายในเกม บันทึกผลการตัดสินใจของผู้เล่นในแต่ละขั้นตอน และแสดงผลออกมาในเชิงสถิติ ซึ่งในการทดลองจะใช้ระบบจำลองประกอบด้วย Load balancer, 2 Web server และ Database serverดังภาพที่ 4.1.และมีช่องโหว่ดังตาราง 4.1.



ภาพที่ 4.1 ระบบเป้าหมายที่จะใช้ในการทดลอง

ตารางที่ 4.1 ช่องโหว่ของระบบเป้าหมาย

เครื่อง	**เซอร์วิส**	**ประเภทช่องโหว่**
Load balance	SSH	OS Command Injection
		Authentication issue
		Code
Web server	HTTP	Information Leak
	SSH	OS Command Injection
		Authentication issue
		Code
Database server	MySql	Unknown
	SSH	OS Command Injection
		Authentication issue
		Code

ทดลองนำเข้าข้อมูลระบบดังกล่าวในรูปแบบ JSON (ภาพ 4.2) ส่งเข้าไปในระบบผ่าน POST method โดยใช้ API Key ที่ผู้ดูแลระบบในระบบทุกคนจะได้รับ สามารถนำขึ้นระบบได้อย่างถูกต้อง(ภาพ 4.3)

```
api_key=vXKCzDOZZfVtCxFSHFDY
graphName=MyCompany

machines={"machines":[
    {
      "machineID":1,
      "name":"172.17.0.10",
      "status":"found"
    },{
      "machineID":2,
      "name":"172.17.0.11",
      "status":"hidden"
    },{
      "machineID":3,
      "name":"172.17.0.12",
      "status":"hidden"
    },{
      "machineID":4,
```

ภาพที่ 4.2. ตัวอย่างข้อมูลนำเข้าบางส่วนในรูปแบบ JSON

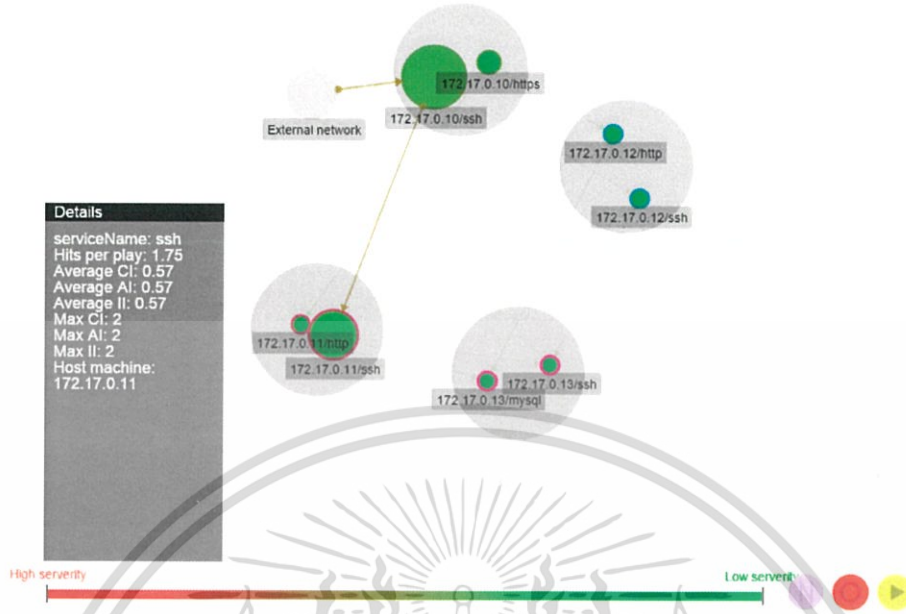
STATUS 200 OK TIME 7093 ms

ภาพที่ 4.3. การตอบรับจากเซิฟเวอร์เมื่อส่งเข้าระบบได้สำเร็จ

ทดสอบการแสดงผลของเกม เมื่อเมืองยังไม่ถูกสำรวจจะไม่สามารถเข้าเมืองได้ (ภาพที่ 4.4 ซ้ายบน) จะต้องทำการสำรวจก่อน เมื่อสำรวจแล้วจึงจะสามารถเข้าเมืองได้ (ภาพที่ 4.4 ขวาบน) ในเมืองมีการแสดงสิ่งปลูกสร้างและช่องโหว่ในระบบได้ถูกต้องตามระบบจริง (ภาพที่ 4.4 ซ้ายล่าง) เมื่อทำการโจมตีผลลัพธ์ที่เกิดขึ้นตรงกับความสามารถของทหารที่ส่งไป และเมื่อจบเกมแล้วมีการแสดงคะแนนที่ผู้เล่นทำได้และคะแนนสูงสุดของผู้เล่นคนอื่น (ภาพที่ 4.4 ล่างขวา)

ภาพที่ 4.4. ทดสอบการแสดงผลในเกม

ทดสอบการรายงานสรุปผลการเล่น (ภาพที่ 4.5) แผนภาพจะสอดคล้องกับข้อมูลการเล่นที่ผู้เล่นเล่นที่มีสามารถแสดงชื่อ สี ขนาด ได้สอดคล้องกันกับ Waypoints ทั้งหมด ในรายงานนี้ผู้ดูแลระบบเห็นได้ชัดว่าเซอร์วิสที่ถูกโจมตีบ่อยที่สุดคือเซอร์วิสใด และผลกระทบเฉลี่ยที่อาจเกิดขึ้น การแก้ไขในสถานการณ์นี้คือ จัดการกับช่องโหว่เส้นทางแรกที่ทำให้เข้ามาในระบบได้ โดยทำการชี้เมาส์ไปที่เส้นดังกล่าว จะมีรายละเอียด ของ CVE ซึ่งผู้ดูแลระบบสามารถนำไปค้นหาแนวทางป้องกันต่อได้



ภาพที่ 4.5. รายงานผลการเล่น

บทที่ 5 สรุปผลการทดลอง ข้อเสนอแนะ

โครงงานนี้ได้พัฒนาเครื่องมือสำหรับเก็บสถิติการเลือกใช้เส้นทางในการโจมตีเครือข่ายคอมพิวเตอร์โดยใช้หลักการของ Crowdsourcing และ Gamification คือทำการแปลงข้อมูลช่องโหว่ในเครือข่ายให้เป็นเกมและเก็บพฤติกรรมการตัดสินใจโจมตีในแต่ละจุดของผู้เล่น

การทดสอบว่าสามารถใช้สถิติการเล่นเป็นตัวแทนความน่าจะเป็นในการโจมตีแต่ละจุดได้ จำเป็นจะต้องมีข้อมูลประวัติการถูกโจมตีในระบบ เพื่อนำมาเปรียบเทียบว่าสถิติการเล่นที่ได้รับจากผู้เล่นมีความสอดคล้องกับสถิติการถูกโจมตีมากน้อยเพียงใด

ระบบนี้สามารถรองรับการเปลี่ยนแปลงเป็นเกมในรูปแบบอื่นได้อีก โดยใช้รูปแบบการรับส่งข้อมูลให้อยู่ในรูปแบบที่กำหนด

โครงงานนี้ได้พัฒนาเครื่องมือเก็บสถิติการเลือกใช้เส้นทางในการโจมตีเครือข่ายคอมพิวเตอร์ เพื่อนำสถิติการเล่นมาใช้แทนความน่าจะเป็นในการโจมตีแต่ละจุด เพื่อใช้เป็นข้อมูลในการตัดสินใจปรับปรุงระบบ ว่าผู้ดูแลระบบควรจะป้องกันช่องโหว่ที่เซอร์วิสใดก่อน

บรรณานุกรม

[1] P. Mell, K. Scarfone, and S. Romanosky. (2014, Oct).*A Complete Guide to the Common Vulnerability Scoring System Version 2.0* [Online]. Available: http://www.first.org/cvss/cvss-guide.html

[2] ECMA International. "The JSON data interchange format". In Standard ECMA-404.

[3] Gabe Zinchermann and Christopher Cunnningham. "Gamification" in Gamification By Design.1st Edition. CA.

[4] Willet, W., Heer, J., and Agrawala, M,. "Strategies for crowdsourcing social data analysis" in Human Factor in Computing System Conf. ACM, New York. 2012. 227-236.

[5] Jared Cechanowicz et al. "Effects of Gamification on Participation and Data Quality in a Real-World Market Research Domain"

[6] W3.org. (2014, Dec). Javascript Web APIs [Online]. Available: http://www.w3.org/standards/webdesign/script

[7] jQuery. (2014, Dec). What is jQuery [Online]. Available: http://jquery.com/

[8] restapitutorial.com. (2014, Dec). What is REST? [Online]. Available: http://www.restapitutorial.com/lessons/whatisrest.html

[9] restapitutorial.com. (2014, Dec). Learn REST: A RESTful tutorial [Online]. Available: http://www.restapitutorial.com/

[10] Google. (2014, Dec). Google App Engine: Platform as a Service [Online]. Available: https://cloud.google.com/appengine/docs

[11] MITRE. (2014, Oct). Frequently Asked Questions [Online]. Available: http://cve.mitre.org/about/faqs.html

[12] Seth Cooper et al., (2011). Crystal structure of a monomeric retroviral protease solved by protein folding game players. Nature Structural and Molecular Biology 18, 1175-1177, 2011.

[13] McNab et al., May 2015. Proceedings of the National Academy of Sciences USA

[14] Oleg Mikhali Sheyner. Scenario Graphs and Attack Graphs. PhD thesis. School of Computer Science, Carnegie Melon University, April 2004.