การประเมินช่องโหว่ระบบบริหารจัดการทางการแพทย์ กรณีศึกษา โรงพยาบาลภูมิพลอดุลยเดช กรมแพทย์ทหารอากาศ

Vulnerability Assessment of Medical Management System: A Case Study of Bhumibol Adulyadej Hospital Royal Thai Air Force Medical Department

พัชรวัฒน์ โกสิตงามดีวงศ์ [1]
ดร.ชัยพร เขมะภาตะพันธ์ [2]

บทคัดย่อ

สารนิพนธ์ฉบับนี้ได้ทำการศึกษา ค้นคว้าเพื่อหาช่องโหว่ของระบบ Bhumibol Health information system (BHIS) กรณีศึกษาโรงพยาบาลภูมิพลอดุลยเดช กรมแพทย์ทหารอากาศ ว่าระบบดังกล่าวมีช่องโหว่หรือไม่ ช่องโหว่นั้นมีระดับความรุนแรงและมีผลกระทบต่อระบบอย่างไร โดยใช้โปรแกรมประยุกต์ เป็นเครื่องมือในการตรวจหาช่องโหว่ของเครื่องคอมพิวเตอร์แม่ข่าย และใช้วิธีการทดสอบเจาะระบบโดยใช้เทคนิค Information Disclosure ซึ่งได้แบ่งขั้นตอนในการหาช่องโหว่ของระบบเป็น 4 ขั้นตอน ประกอบด้วย

(1) Planning คือ การวางแผนก่อนการดำเนินงาน

(2) Discovery คือ กระบวนการค้นหาช่องโหว่ระบบ

(3) Attack คือ กระบวนการโจมตีเป้าหมายเมื่อมีการค้นพบช่องโหว่

(4) Report คือ ขั้นตอนการรายงานการประเมินผล

ผลลัพธ์จากการศึกษาค้นคว้าแสดงให้เห็นว่าสามารถตรวจพบช่องโหว่ของระบบบริหารจัดการทางการแพทย์ (Bhumibol Health information system) รวมทั้งสิ้นจำนวน 16 ช่องโหว่ ซึ่งเป็นช่องโหว่ที่มีความเสี่ยงสูงมาก 1 ช่องโหว่ ช่องโหว่ที่มีความเสี่ยงสูง 6 ช่องโหว่ ช่องโหว่ที่มีความเสี่ยงปานกลาง 6 ช่องโหว่ และช่องโหว่ที่มีความเสี่ยงต่ำ 3 ช่องโหว่ โดยหลังจากทำการรายงานผลและตรวจสอบแก้ไขแล้วยังคงเหลือเพียง 7 ช่องโหว่ คือ ช่องโหว่เสี่ยงปานกลาง 4 ช่องโหว่และช่องโหว่ความเสี่ยงต่ำ 3 ช่องโหว่

---

[1] นักศึกษาหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต สาขาวิศวกรรมคอมพิวเตอร์และโทรคมนาคม วิทยาลัยนวัตกรรมด้านเทคโนโลยีและวิศวกรรมศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิตย์

[2] อาจารย์ที่ปรึกษา

ABSTRACT

This thesis has been studied to explore the vulnerabilities of the Bhumibol Health Information System (BHIS) of Bhumibol Adulyadej Hospital, Medical Department of Royal Thai Air Force in order to examine the defects in the system, the severe level of the defects and how the defects affect the system. The Application Program has been employed to detect vulnerabilities in the server using Information Disclosure Technique for hanging method. Can be divided the steps to find system's vulnerabilities of into 4 steps as follows;

(1) Planning how to before the implementation.

(2) Discovery or finding the system's vulnerabilities.

(3) Attacking a target after vulnerabilities are discovered.

(4) Reporting or the process of the evaluation report.

The results of the study show that researchers can detect 16 vulnerabilities in the medical management system, Bhumibol Health information system. Vulnerabilities 6 high-risk vulnerabilities, 6 moderate-risk vulnerabilities and 3 low-risk vulnerabilities. After reporting the results and correcting the problems, there are only 7 vulnerabilities which are 4 medium vulnerabilities and 3 low-risk vulnerabilities.

1. บทนำ

การให้บริการทางการแพทย์นับเป็นปัจจัยที่มีความสำคัญต่อประเทศเป็นอย่างมาก โดยเฉพาะในแง่ของการยกระดับคุณภาพชีวิตของประชาชน ประเทศไทยได้ประกาศใช้นโยบาย Medical Hub ที่จะสนับสนุนและส่งเสริมประเทศไทยให้เป็นศูนย์กลางทางการแพทย์ในภูมิภาค[1] จึงทำให้มีการจัดเก็บข้อมูลส่วนบุคคลทางการแพทย์ในรูปแบบของข้อมูลอิเล็กทรอนิกส์กันอย่างแพร่หลาย และยังเป็นฐานสำคัญในการพัฒนาต่อยอดสู่การเป็น Smart Healthcare[2] ในอนาคต

ความก้าวหน้าทางเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว และมีแนวโน้มเกิดการละเมิดสิทธิในข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัวมีเพิ่มมากขึ้น ประเทศไทยได้เล็งเห็นและตระหนักถึงความสำคัญ จึงได้ตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 [3] และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562[4] ดังนั้น เพื่อให้สามารถป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที โรงพยาบาลภูมิพลอดุลยเดช กรมแพทย์ทหารอากาศ เป็นสถานพยาบาลระดับตติยภูมิชั้นสูง ที่ได้มีการพัฒนาระบบบริหารจัดการทางการแพทย์ขึ้นใช้งานเรียกว่า Bhumibol Adulyadej Hospital Information System (BHIS) ซึ่งถูกออกแบบและพัฒนาร่วมกับบริษัทเอกชน โดยมีมูลค่าการจัดทำระบบทั้งหมดกว่า 70 ล้านบาท มีการจัดเก็บและ

แลกเปลี่ยนข้อมูลส่วนบุคคลที่สำคัญของผู้ป่วยภายใต้ระบบ Client/Server Network ซึ่งปัจจุบันระบบดังกล่าว ได้ถูกนำไปประยุกต์ใช้ภายใต้แพลตฟอร์มที่คล้ายคลึงกันในสถานพยาบาลอื่น ๆ ทั้งในส่วนโรงพยาบาลของรัฐ และเอกชนหลายแห่ง

ดังนั้น ผู้วิจัยจึงมีแนวความคิดที่จะทำการประเมินช่องโหว่ (Vulnerability assessment) ระบบบริหารจัดการทางการแพทย์ (BHIS) เพื่อค้นหาช่องโหว่ของระบบผ่านเครือข่าย Client/Server โดยงานวิจัยนี้ จะศึกษาระดับความรุนแรง และผลกระทบที่มีต่อระบบบริหารจัดการทางการแพทย์ Bhumibol Adulyadej Health information system (BHIS) ตลอดจนหาแนวทางป้องกัน เพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ และเป็นแนวทางในการพัฒนาระบบ ให้มีความมั่นคงปลอดภัย และยังเป็นประโยชน์ต่อสถานพยาบาลอื่นที่ได้นำระบบไปใช้งานภายใต้แพลตฟอร์มเดียวกันได้

โดยมีขอบเขตงานวิจัยดังนี้

1. ศึกษาช่องโหว่หรือจุดอ่อนของระบบโดยใช้โปรแกรมประยุกต์ เป็นเครื่องมือในการตรวจหาช่องโหว่หรือจุดอ่อนของบริหารจัดการทางการแพทย์ (BHIS)

2. ศึกษาช่องโหว่หรือจุดอ่อนของระบบบริหารจัดการทางการแพทย์ (BHIS) โดยวิธีการทดสอบเจาะระบบโดยผู้ทำการวิจัย

3. ศึกษาแนวทางในการป้องกันการเข้าถึงช่องโหว่หรือจุดอ่อนของระบบบริหารจัดการทางการแพทย์ (BHIS)

2. ทฤษฎีที่เกี่ยวข้อง

สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ(NIST) ของสหรัฐอเมริกา ได้เผยแพร่เอกสาร Technical Guide to Information Security Testing and Assessment[5] ซึ่งเป็นกระบวนการที่ใช้ในการตรวจสอบประเมินความปลอดภัยของระบบคอมพิวเตอร์ เพื่ออำนวยความสะดวกสบายในกระบวนการตัดสินใจทางเทคนิคที่เกี่ยวข้องกับการทดสอบความปลอดภัยและการประเมินผลที่จำเป็นโดยองค์กรมีส่วนร่วม ดังนี้

1) สามารถกำหนดระเบียบวิธีปฏิบัติ และบทบาทของผู้ประเมินชัดเจน

2) สามารถร่วมวางแผนการประเมิน และมีการลงนามรับรองทางกฎหมาย

3) สามารถเลือกวิธีการประเมินให้เหมาะสมกับองค์กร และมีความปลอดภัย

4) ร่วมจัดการข้อมูลได้อย่างเหมาะสมในการเก็บรวบรวมและทำลาย ตลอดจนการประเมินผล

5) ได้รับข้อมูลจากการวิเคราะห์และรายงานผล เพื่อปรับปรุงการรักษาความปลอดภัยของระบบภายในองค์กร

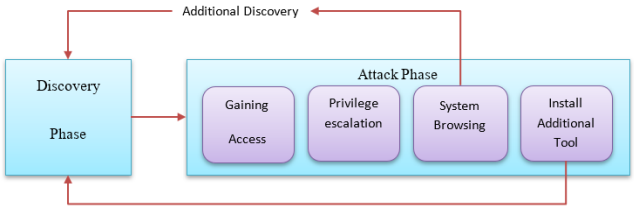
2.1 กระบวนการทำ Security Testing ประกอบไปด้วย 4 ขั้นตอน

รูปที่ 1 กระบวนการทำ Security Testing

1) Planning คือ กระบวนการวางแผนก่อนการทำงาน เป็นการรวบรวมข้อมูลที่จำเป็น การขออนุญาต ตรวจสอบสินทรัพย์ที่จะประเมิน การควบคุมความปลอดภัย เป็นต้น ซึ่งการวางแผนที่เหมาะสมเป็นสิ่งสำคัญสำหรับการประเมินความปลอดภัยที่ประสบผลสำเร็จ

2) Discovery คือ กระบวนการค้นหาช่องโหว่ระบบ และเป็นจุดเริ่มต้นของการทดสอบที่เกิดขึ้นจริงโดยครอบคลุมถึงการรวบรวมข้อมูล, การสแกนพอร์ตเครือข่ายและการระบุบริการต่าง ๆ บนเครือข่าย, พอร์ต, ช่องโหว่ ซึ่งอาจใช้ทักษะของทีมทดสอบหรือใช้เครื่องมือในการดำเนินการ

3) Attack คือ กระบวนการโจมตีเป้าหมายเมื่อมีการค้นพบ โดยแบ่งย่อยออกเป็น 4 ขั้นตอน คือ



รูปที่ 2 กระบวนการใน Attack phase

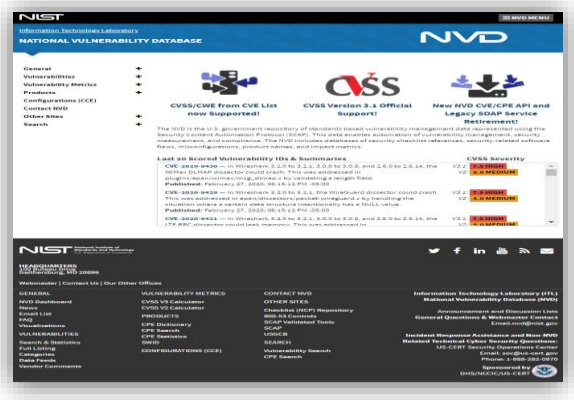
- Gaining Access เป็นการรวบรวมข้อมูลที่ให้เข้าถึงเป้าหมายได้อย่างเพียงพอ
- Escalating Privileges เป็นการเข้าถึงเป้าหมายและเลื่อนระดับสิทธิ์ผู้ดูแลหรือเป็นผู้ควบคุมได้
- System Browsing เป็นขั้นตอนกระบวนการรวบรวมข้อมูลขึ้นอีกครั้งเพื่อระบุกลไกในการเข้าถึงระบบเพิ่มเติม
- Install Additional Tools เป็นกระบวนการติดตั้งเครื่องมือที่จะให้เข้าถึงระบบได้อีกหนึ่งช่องทาง

2.1.2 Testing Viewpoints

ในกระบวนการทำ Security Testing นั้น เราสามารถทำได้หลายมุมมอง ทั้งมุมมองจากภายนอก(External) และภายใน(Internal) คำว่ามุมมองนี้หมายถึง ความรู้ที่ผู้ประเมินได้รับทราบ เช่น การทดสอบแบบภายนอกนี้จะดำเนินการเหนือความปลอดภัยขององค์กร ขณะที่การทดสอบภายในจะอยู่ในการดูแลขององค์กร โดยมุ่งเน้นการรักษาความปลอดภัยของระบบ(system-level security) การกำหนดค่าโปรแกรมประยุกต์(configuration including application) ตลอดจนการตรวจสอบความถูกต้องของสิทธิ์ในการเข้าถึง และการทำระบบให้มีความแข็งแรง (system hardening)

2.2 การประเมินช่องโหว่ (Vulnerability Assessment)

ช่องโหว่หรือจุดอ่อน (Vulnerability) หมายถึง ช่องทางที่อาจถูกใช้สำหรับการโจมตีได้ ซึ่งรวมถึงช่องโหว่ด้านกายภาพด้วย เช่น ประตูหน้าต่างที่ถูกเปิดทิ้งไว้ ซึ่งอาจเป็นสิ่งล่อให้ผู้ไม่หวังดีแอบเข้ามาขโมยทรัพย์สินในห้องหรืออาคารได้ ส่วนจุดอ่อนหรือช่องโหว่ของระบบคอมพิวเตอร์และเครือข่ายหมายถึงช่องทางที่เปิดให้ผู้ไม่ประสงค์ดีสามารถเจาะเข้าระบบหรือเครือข่ายได้ เช่น การเปิดพอร์ตทิ้งไว้โดยไม่จำเป็น ความอันตรายของช่องโหว่นั้นมีหลายระดับขึ้นอยู่กับความเสียหายหรือความรุนแรงที่อาจจะเกิดขึ้นกับระบบหากถูกโจมตีผ่านช่องทางนั้น



รูปที่ 3 แหล่งรวบรวมข้อมูลช่องโหว่(www.nvd.nist.gov)

จุดประสงค์ของการวิเคราะห์ช่องโหว่ (Vulnerability analysis) นั้นก็เพื่อเป็นการทดสอบสถานภาพขององค์กรในปัจจุบันว่าล่อแหลมต่อการถูกโจมตีหรือถูกทำลายมากน้อยแค่ไหน หรือเป็นการทดสอบการรักษาความลับ ความถูกต้อง และ ความพร้อมใช้งานของข้อมูลที่สำคัญขององค์กร และนอกจากนี้ยังเป็นการทดสอบว่าเครื่องมือหรือระบบที่ใช้สำหรับป้องกันและรักษาความปลอดภัย

นั้น มีประสิทธิภาพเพียงพอหรือไม่ ซึ่งปัจจุบันมีเครื่องมือหลายประเภทที่สามารถใช้สำหรับการวิเคราะห์ช่องโหว่หรือจุดอ่อนของระบบ เช่น

- Nmap (www.nmap.org)
- Nessus (www.nessus.org)
- Greenbone security (www.owasp.org)
- Wireshark (www.wireshark.org)

2.3 การประเมินโอกาสที่จะเกิด (Likelihood) [6]

โอกาสที่จะเกิดขึ้นนั้นสามารถกำหนดได้ 2 แบบ คือแบบเชิงปริมาณและแบบเชิงคุณภาพ เชิงปริมาณก็จะกำหนดเป็นตัวเลข หรือ ร้อยละ ส่วนการกำหนดโอกาสที่จะเกิดในเชิงคุณภาพนั้นนิยมกำหนดเป็น 5 ระดับ เช่น สูงมาก สูง ปานกลาง ต่ำ ต่ำมาก

ค่าเชิงคุณภาพ	ค่าเชิงปริมาณ	คำอธิบาย
สูงมาก (Very High)	5	เหตุการณ์ภัยคุกคามมีโอกาสที่จะเกิดเกือบจะแน่นอน
สูง (High)	4	เหตุการณ์ภัยคุกคามมีโอกาสที่จะเกิดสูง
ปานกลาง (Moderate)	3	เหตุการณ์ภัยคุกคามมีโอกาสที่จะเกิดปานกลาง
ต่ำ (Low)	2	เหตุการณ์ภัยคุกคามมีโอกาสที่จะเกิดน้อย
ต่ำมาก (Very Low)	1	เหตุการณ์ภัยคุกคามแทบจะไม่มีโอกาสที่จะเกิด

รูปที่4 เกณฑ์สำหรับประเมินโอกาสที่จะเกิดภัยคุกคาม

2.4 การประเมินผลกระทบ (Impact) [6]

โดยในท้ายที่สุดนั้นต้องทำการตรวจสอบธุรกิจ สอบถามพนักงานทั่วไปว่าความเสียหายจะเกิดแก่ธุรกิจขององค์กรมากน้อยแค่ไหน

ค่าเชิงคุณภาพ	ค่าเชิงปริมาณ	คำอธิบาย
สูงมาก (Very High)	5	เหตุการณ์ภัยคุกสามารถคามสร้างความเสียหายร้ายแรงมากหลายด้าน หรือสร้างความหายนะ ต่อการดำเนินธุรกิจขององค์กร ทรัพย์สิน พนักงาน องค์กรอื่น หรือประเทศชาติ จนทำให้องค์กรต้องหยุดดำเนินการ
สูง (High)	4	เหตุการณ์ภัยคุกคามสามารถสร้างความเสียหายร้ายแรงมากหรือสร้างความหายนะ ต่อการดำเนินธุรกิจขององค์กร ทรัพย์สิน พนักงาน องค์กรอื่น หรือประเทศชาติ มีผลกระทบต่อกระบวนการดำเนินธุรกิจอย่างรุนแรง
ปานกลาง (Moderate)	3	เหตุการณ์ภัยคุกคามสามารถสร้างความเสียหายร้ายแรง ต่อการดำเนินธุรกิจขององค์กร ทรัพย์สิน พนักงาน องค์กรอื่น หรือประเทศชาติ มีการหยุดชะงักงันอย่างมีนัยสำคัญในกระบวนการดำเนินธุรกิจขององค์กร
ต่ำ (Low)	2	เหตุการณ์ภัยคุกคามสามารถสร้างความเสียหายบางส่วน ต่อการดำเนินธุรกิจขององค์กร ทรัพย์สิน พนักงาน องค์กรอื่น หรือประเทศชาติ หรือมีผลกระทบเล็กน้อยต่อธุรกิจองค์กร
ต่ำมาก (Very Low)	1	เหตุการณ์ภัยคุกคามสร้างความเสียน้อยมากจนสามารถละเลยได้ ต่อการดำเนินธุรกิจขององค์กร ทรัพย์สิน พนักงาน องค์กรอื่น หรือประเทศชาติ การดำเนินกิจการขององค์กรยังคงดำเนินต่อไปได้

รูปที่5 เกณฑ์สำหรับประเมินโอกาสที่จะเกิดภัยคุกคาม

2.5 การคำนวณระดับความเสี่ยง (Risk Determination)

ผลที่ได้จากการประเมินความเสี่ยง คือ ระดับความเสี่ยงขององค์กร ซึ่งคำนวณจากระดับความเสียหายและโอกาสที่จะเกิดขึ้น ความเสี่ยงที่กล่าวถึงในที่นี้จะหมายถึง ความเสี่ยงรูปแบบต่าง ๆ ที่อาจก่อให้เกิดผลเสียหายต่อข้อมูลและระบบ อุปกรณ์ต่าง ๆ ที่สนับสนุนการทำงานให้กับข้อมูลนี้อยู่ โดยขั้นตอนนี้จะเป็นขั้นของการประเมินระดับของความเสี่ยง (Risk Level) ที่มีทั้งหมดต่อข้อมูลและทรัพย์สินต่าง ๆ ขององค์กร เพื่อนำความเสี่ยงที่เกินระดับที่องค์กรสามารถยอมรับได้ ไปดำเนินการควบคุมและแก้ไขความเสี่ยงในขั้นตอนต่อไป สามารถคำนวณได้ ดังนี้

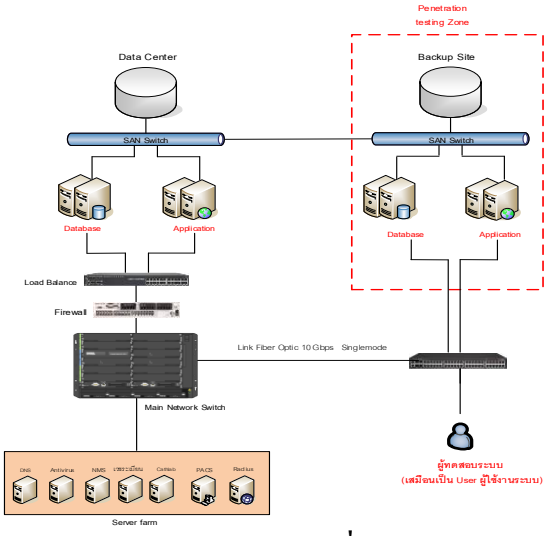
[ระดับความเสี่ยง = โอกาสที่จะเกิดขึ้น x ผลกระทบที่ตามมา]

3. วิธีการดำเนินการ

3.1 การวางแผนก่อนการดำเนินงาน (Planning)

ผู้วิจัยได้กำหนดขอบเขตของเป้าหมายในการทำ Security Testing ร่วมกับหน่วยงานเจ้าของระบบ BHIS นั่นคือ ศูนย์คอมพิวเตอร์ รพ.ภูมิพลอดุลยเดช พอ. และบริษัทที่ดูแล คือ Abstract Computer.Co.Ltd ตลอดจนรวบรวมข้อมูลที่จำเป็นพร้อมทั้งศึกษา Network Diagram ดังแสดงตามรูปที่ 6 โดยได้ทำหนังสือบันทึกข้อความเพื่อขออนุญาตเข้าทำการทำ Security Testing กับทาง หน.ศูนย์คอมพิวเตอร์ รพ.ภูมิพลอดุลยเดช พอ. ผ่านทางหนังสือราชการเพื่อทำการทดสอบเจาะระบบ ซึ่งกำหนดขอบเขตเวลาระหว่างวันที่ 1 มีนาคม พ.ศ.2559 โดยจะทดสอบในช่วงเวลา 17.30 น. ถึง 24.00 น. ซึ่งเป็นช่วงเวลาที่ไม่มีการเข้าใช้ข้อมูลในส่วนของ BackUp Site ซึ่งทางผู้จัดทำจะทำ

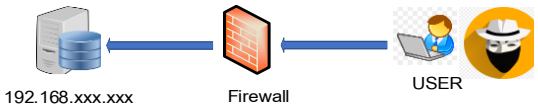
การเก็บข้อมูลที่ได้ระหว่างการทดสอบเป็นความลับ และส่งรายละเอียดที่ได้รับหลังจากการทดสอบกลับไปให้หน่วยงานต่อไป



รูปที่6 แสดง Network Diagram ในส่วนที่เลือกทำ Security Testing

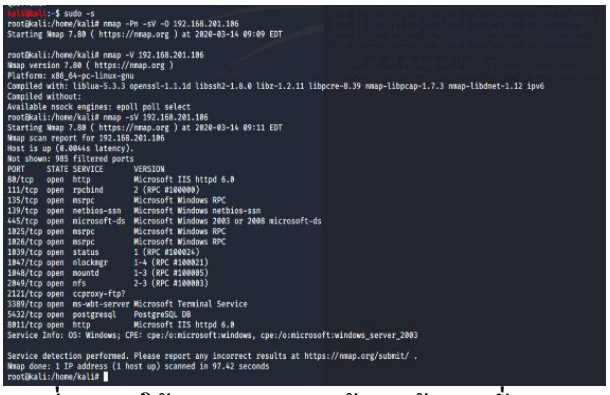
3.2 การค้นหาช่องโหว่ของระบบ (Discovery)

ในขั้นตอนการตรวจหาช่องโหว่นี้จะเลือกทำในส่วนที่ไม่ก่อให้เกิดความเสียหายใด ๆ ต่อระบบสารสนเทศและเซิร์ฟเวอร์ ของ รพ.ภูมิพลอดุลยเดช พอ.เนื่องจากเป็นการตรวจหาช่องโหว่กับระบบที่เปิดให้บริการอยู่โดยตลอด 24 ชั่วโมง และการทดสอบครั้งนี้จะทำเฉพาะภายในองค์กร(Internal) ซึ่งผู้วิจัยเปรียบเสมือนเป็นผู้ใช้งานระบบคนหนึ่ง ตามรูปที่ 7



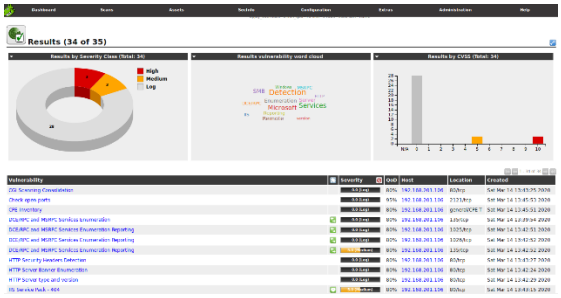
รูปที่7 รูปแบบในการเข้าถึงคอมพิวเตอร์แม่ข่ายระบบ BHIS

3.2.1 เริ่มต้นการทดสอบค้นหาช่องโหว่ของเครื่องคอมพิวเตอร์แม่ข่าย ด้วยการทดลองใช้คำสั่ง Nmap ผ่านระบบปฏิบัติการ Kali



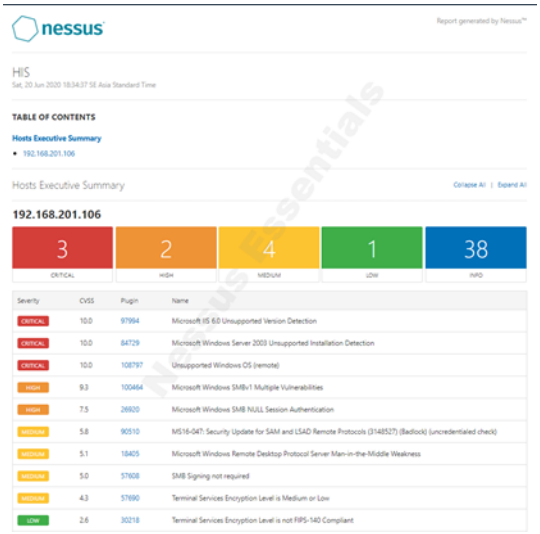
รูปที่ 8 การใช้ Kali สแกนหาข้อมูลด้วยคำสั่ง Nmap

หลังจากทราบถึงข้อมูลบางส่วนของระบบแล้ว ลำดับถัดมาจึงทำการตรวจหาช่องโหว่คอมพิวเตอร์เป้าหมาย ผ่านโปรแกรม Greenbone Security Assistant ซึ่งผลการสแกนช่องโหว่ผ่านโปรแกรมดังกล่าวทำให้ทราบว่า เครื่องคอมพิวเตอร์แม่ข่ายมีช่องโหว่อยู่หลายช่องโหว่ และมีช่องโหว่ที่ร้ายแรงสำคัญที่ต้องได้รับการแก้ไขทันทีถึง 3 ช่องโหว่ ตามรูปที่ 9



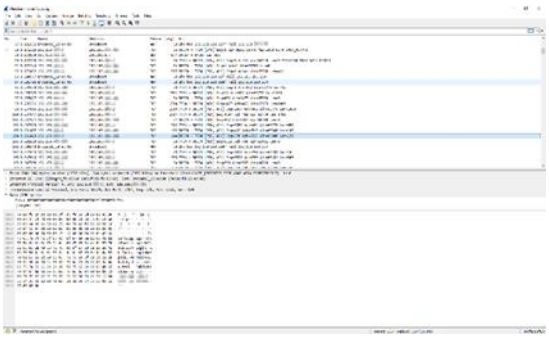
รูปที่ 9 ผลการสแกนช่องโหว่ด้วยโปรแกรม Greenbone Security Assistant

3.2.2 เพื่อให้เกิดความมั่นใจและคาดหวังว่าจะได้ผลลัพธ์ที่แตกต่างออกไปในการตรวจสอบช่องโหว่ จึงได้เลือกโปรแกรม Nessus มาเป็นอีกเครื่องมือหนึ่งเพื่อตรวจสอบหาช่องโหว่ตามรูปที่ 10



รูปที่ 10 ผลการสแกนช่องโหว่(เพิ่มเติม) ด้วยโปรแกรม Nessus

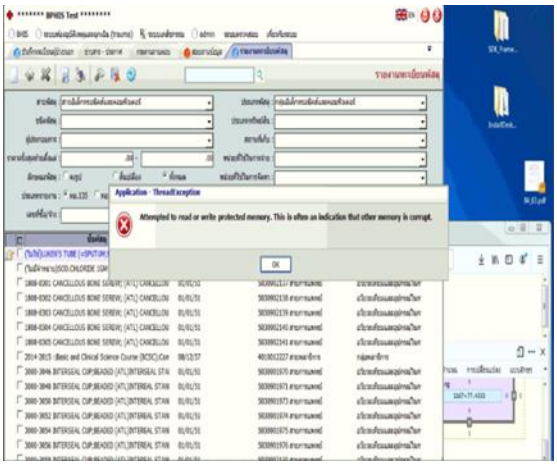
3.2.3 จากข้อมูลที่ได้ทราบว่าระบบได้มีการเข้าถึงโปรแกรมผ่านเครือข่าย Client-Server จึงนำโปรแกรม Wireshark มาตรวจสอบอีกเครื่องมือหนึ่ง และทำให้ผู้วิจัยตรวจพบว่าโปรแกรมมีการส่งข้อมูล Username และ Password เข้าไปถึงเครื่องคอมพิวเตอร์แม่ข่ายโดยปราศจากการ Encryption ข้อมูลตามรูปที่ 11



รูปที่ 11 ทดสอบใช้ Wireshark มาวิเคราะห์ช่องโหว่ของระบบ

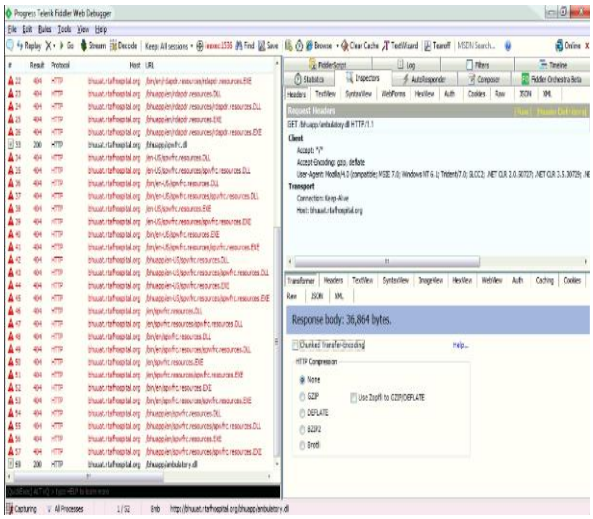
3.2.4 หลังจากได้ตรวจสอบเพื่อค้นหาช่องโหว่ของระบบแล้ว ลำดับถัดไป ผู้วิจัยจึงได้ทำการค้นหาข้อมูล (Discovery) เพิ่มเติมอีก พร้อม ๆกันกับการหาช่องโหว่เพื่อให้ได้มาซึ่งการเข้าถึงฐานข้อมูล ดังนี้

(1) เริ่มการค้นหาช่องโหว่ของระบบผ่านหน้าจอโปรแกรม ด้วยการทดลองใส่อักขระพิเศษเมื่อล็อกอินเข้าสู่หน้าจอของโปรแกรมสารสนเทศ BHIS ตามรูปที่ 12



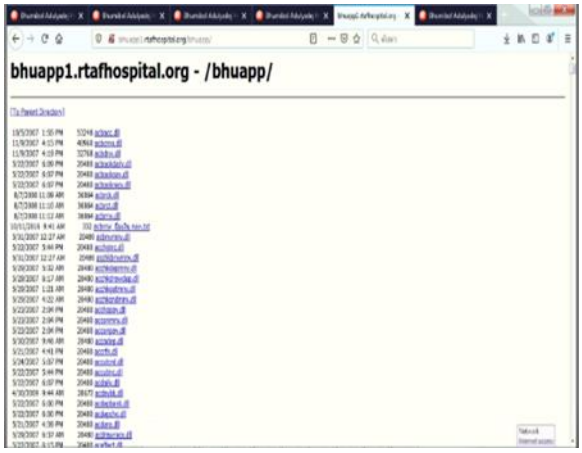
รูปที่ 12 แสดงข้อความ error เมื่อทดลองใส่อักขระพิเศษในโปรแกรม BHIS

(2) ใช้โปรแกรม Fiddler Web Debugger ซึ่งเป็นเครื่องมือที่ใช้ในการดู Traffic ของเป้าหมายที่มีการใช้งานโปรโตคอล HTTP / HTTPS และทำให้ผู้วิจัยเห็นว่าโปรแกรม BHIS เรียกใช้งาน path และ file อะไรบ้าง โดยข้อมูลที่พบ คือ มีการเข้าถึงไฟล์ที่ Result = 200 โดยมีการตอบสนองที่ Url : bhuapp1.rtafhospital.org/bhuapp/ ตามรูปที่ 13



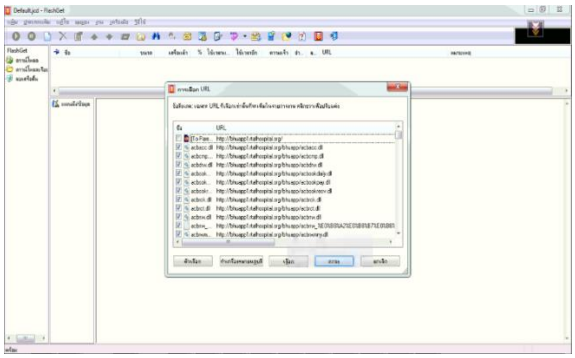
รูปที่ 13 แสดงการตรวจสอบ Traffic ด้วย Fiddler Web Debugger

(3) จากข้อมูลที่ได้มาข้างต้น ยังถือว่าไม่เพียงพอต่อนักต่อการโจมตีเข้าระบบ ผู้วิจัยจึงทำการค้นหาไฟล์อื่นๆ โดยใช้เบราว์เซอร์ ของ Firefox เพื่อดูว่ามีไฟล์อะไรบ้าง ในระบบในเว็บเซฟเวอร์ แต่ไม่พบข้อผิดปกติใดๆ จากนั้นจึงทดลองนำข้อมูล URL ที่ได้ คือ bhuapp1.rtafhospital.org/bhuapp/ ไปพิมพ์ใส่ Browser ผลคือทำให้สามารถเห็นข้อมูลไฟล์ต่างๆ ตามรูปที่ 14



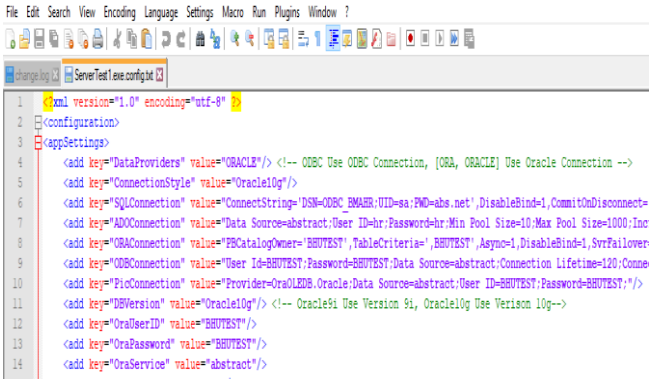
รูปที่ 14 แสดงการเปิดเข้าถึงไฟล์สำคัญต่างๆ ได้ผ่าน URL

(4) จากนั้นจึงได้ทำการติดตั้งโปรแกรมช่วยดาวน์โหลด และได้ทำการดาวโหลดไฟล์ลงมาที่เครื่อง ตามรูปที่ 15 พบว่าส่วนใหญ่เป็นไฟล์ระบบที่สำคัญๆ



รูปที่ 15 แสดงการดาวน์โหลดไฟล์ข้อมูลด้วยโปรแกรมช่วยดาวน์โหลด

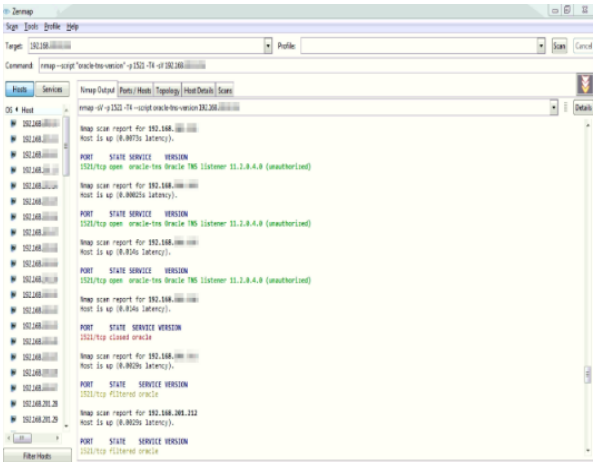
(5) ผู้วิจัยตรวจสอบพบไฟล์ที่มีชื่อน่าสนใจ คือ Server.Test.exe.config จึงทำการเปิดดูเนื้อหาภายใน ตามรูปที่ 16



รูปที่ 16 แสดงการพบเนื้อหาที่น่าสงสัยจากไฟล์ที่ได้จากการดาวโหลด

(6) หลังจากดาวโหลดไฟล์ต่าง ๆ และค้นหาไฟล์ที่มีข้อมูล จึงทำให้พบไฟล์ที่มีข้อมูลน่าสงสัยซึ่งปรากฏข้อความต่าง ๆ ซึ่งเมื่อพิจารณาข้อมูลดังกล่าวแล้ว จึงทำให้ผู้วิจัยเริ่มให้ความสนใจในเรื่องของฐานข้อมูลที่ใช้งานกับระบบสารบริหารจัดการทางการแพทย์ว่าอาจจะเป็น Oracle

(7) ทดลองทำการสแกนเน็ตเวิร์กอีกครั้ง โดยใช้โปรแกรม Zenmap เพื่อสแกนที่วงเครือข่ายที่คาดว่าเป็นเซฟเวอร์โซน ซึ่งพบว่ามีเครื่องเซฟเวอร์จำนวน 3 เครื่อง ทำหน้าที่ เป็น Database Server ที่ใช้งานและอาจพบฐานข้อมูลของ Oracle ตามรูปที่ 17

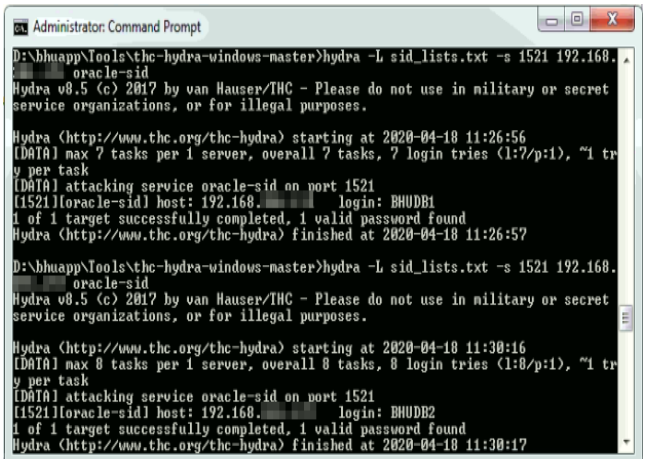


รูปที่ 17 แสดงการจากการสแกนระบบเครือข่ายด้วยโปรแกรม Zenmap

.

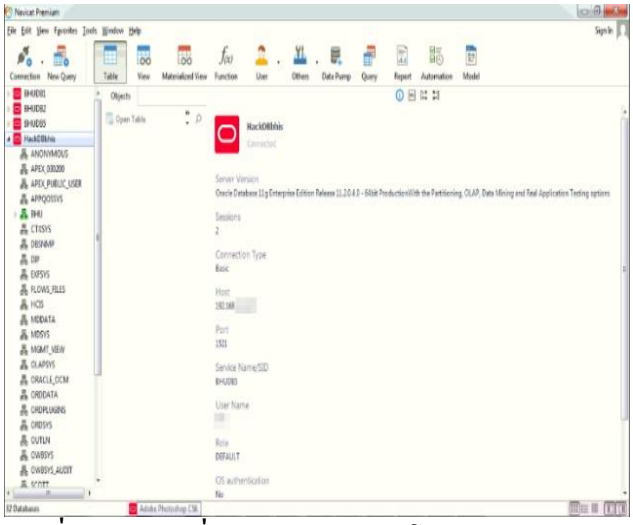
3.3 การโจมตีเป้าหมายเมื่อมีการค้นพบช่องโหว่ (Attack)

(1) ในกระบวนการโจมตีเป้าหมายนั้น ผู้วิจัยได้เริ่มดำเนินการเมื่อ ทราบว่าเป้าหมายมีการระบุถึง Database จำนวน 3 เครื่อง โดยได้มาจากข้อมูลสำคัญ ที่ได้มาจากการดาวโหลดด้วยโปรแกรมช่วยดาวโหลด แล้วมาทำการหาข้อมูลที่น่าสนใจ ซึ่งจุดนี้ทำให้ผู้วิจัยได้ข้อมูล Login และ SID จากการใช้โปรแกรม Hydra brute force [7] ซึ่งเป็นโปรแกรมสำหรับการสุ่มเดาพาสเวิร์ด และทำให้ได้ผลลัพธ์เป็น “SIDที่ถูกต้อง” จึงค่อนข้างมั่นใจว่าเครื่องที่ลงท้ายด้วย IP ที่พบเจอนั้น เป็นเครื่องเป้าหมายที่มีการเก็บข้อมูล Database อยู่ โดยปรากฏ SID ตามรูปที่ 18



รูปที่ 18 วิเคราะห์ Username และ Password ด้วยโปรแกรม Hydra brute force

(2) หลังจากที่ผู้วิจัยทราบ SID ว่ามี SID ชื่ออะไร สามารถใช้งานได้ที่ SERVER ไหน ผู้วิจัย จึงทำการทดลองเพื่อเข้าถึงข้อมูลโดยใช้โปรแกรมเชื่อมฐานข้อมูล โดยใช้โปรแกรมที่มีชื่อว่า Navicat [8] ซึ่งเป็นโปรแกรมบริหารจัดการฐานข้อมูล เพื่อทดสอบการเชื่อมต่อเครื่องเซฟเวอร์กับโปรแกรมจัดการฐานข้อมูล และทำให้สามารถเข้าถึงเครื่องเซฟเวอร์ฐานข้อมูล Oracle ได้สำเร็จทั้งหมด ทุกฐานข้อมูลที่ทำการเชื่อมต่อ ตามรูปที่ 19



รูปที่ 19 แสดงเชื่อมฐานข้อมูลด้วยโปรแกรม Navicat

3.4 การวิเคราะห์ความรุนแรงของช่องโหว่และการประเมินความเสี่ยง (Vulnerability and Risk Analysis) [6]

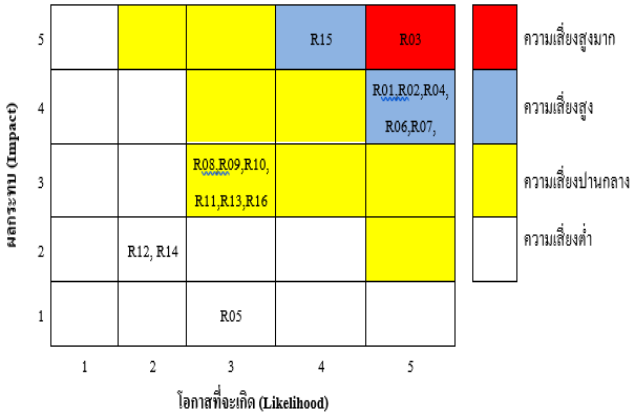
จากผลการทำ Security Testing ด้วยการสแกนช่องโหว่และทำการทดสอบเจาะระบบบริหารจัดการทางการแพทย์ (BHIS) นั้น นอกจากได้ตรวจสอบค้นหาช่องโหว่ที่ได้จากการใช้โปรแกรมประยุกต์ตรวจสอบแล้ว ผู้วิจัยยังสามารถทำการเจาะระบบจนเข้าถึงข้อมูลสำคัญได้

3.4.1 สรุปข้อมูลของช่องโหว่ที่ตรวจพบจากการสแกนและเจาะระบบ

ระดับความเสี่ยง	สูงมาก	สูง	ปานกลาง	ต่ำ
จำนวนช่องโหว่	1	6	6	3

รูปที่20 แสดงจำนวนของช่องโหว่ที่ตรวจพบและระดับความเสี่ยง

จากข้อมูลในรูปที่ 20 สามารถวิเคราะห์ความรุนแรงของช่องโหว่ได้ ตามรูปที่ 21



รูปที่ 21 แสดงผลการวิเคราะห์ความรุนแรงของช่องโหว่

4. ผลลัพธ์จากการดำเนินการ

จากผลการทดสอบการประเมินช่องโหว่ของระบบบริหารจัดการทางการแพทย์ รพ.ภูมิพลอดุลยเดช พอ. นั้น ผู้วิจัยบรรลุวัตถุประสงค์ที่ตั้งไว้ดังนี้

1) เพื่อศึกษาการทดสอบเจาะระบบและประเมินค่าช่องโหว่ของระบบบริหารจัดการทางการแพทย์ (BHIS)

2) เพื่อกำหนดวิธีในการแก้ไขและหาแนวทางป้องกันช่องโหว่หรือจุดอ่อนของระบบบริหารจัดการทางการแพทย์ (BHIS) ให้มีความมั่นคง ปลอดภัย

4.1 การรายงานและการประเมินผล (Report)

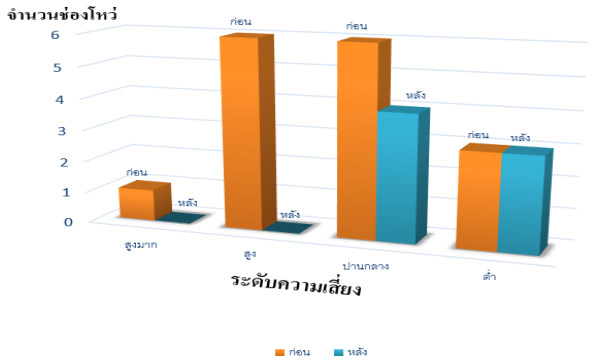
ผู้วิจัยได้จัดทำรายงานและแนวทางการแก้ไขและการป้องกันช่องโหว่ให้กับผู้เกี่ยวข้องได้นำไปแก้ไข ซึ่งในรายละเอียดของรายงานดังกล่าวสามารถให้คำแนะนำเกี่ยวกับวิธีการแก้ไขช่องโหว่และแนวทางการป้องกันสำหรับระบบบริหารจัดการทางการแพทย์ (BHIS) ได้

4.2 การแก้ไขช่องโหว่

ในการดำเนินการแก้ไขช่องโหว่นั้น ได้ทำหนังสือรายงานความเสี่ยงให้ศูนย์คอมพิวเตอร์ รพ.ภูมิพลอดุลยเดช พอ. เพื่อนำเรียนผู้บริหาร ให้รับทราบถึงช่องโหว่และความเสี่ยงที่เกิดขึ้น ซึ่งทางผู้บริหารสามารถนำข้อมูลไปประกอบการตัดสินใจในการหาแนวทางป้องกันร่วมกับทางบริษัท Abstract Computer Co.Ltd. ซึ่งเป็นบริษัทที่รับผิดชอบหลักในการดูแล และพัฒนาระบบบริหารจัดการทางการแพทย์ (BHIS) ตามคำแนะนำที่ให้ไว้

4.3 ผลลัพธ์จากการแก้ไขช่องโหว่

หลังจากผู้วิจัยได้ทำการสรุปแนวทางการแก้ไข รายงานศูนย์คอมพิวเตอร์ รพ.ภูมิพลอดุลยเดช พอ. เป็นที่เรียบร้อยแล้ว บริษัทผู้ดูแลระบบได้ดำเนินการแก้ไขในหัวข้อปัญหาต่าง ๆ ตามแนวทางที่ให้ไว้ โดยเริ่มจากหัวข้อที่มีความเสี่ยงสูงมากและสูงก่อนเป็นอันดับแรก ซึ่งสามารถสรุปการแก้ไขช่องโหว่ได้ดังแสดงตามรูปที่ 22



รูปที่ 22 แผนภูมิก่อนและหลังการแก้ไขปัญหาช่องโหว่

5 สรุปผลการวิจัย

จากการที่ผู้วิจัยทำการประเมินช่องโหว่ (Vulnerability assessment) ของระบบระบบบริหารจัดการทางการแพทย์(BHIS) ผลลัพธ์สามารถทำได้ตามขอบเขตงานวิจัยที่กำหนดไว้ ดังนี้

1) ศึกษาช่องโหว่หรือจุดอ่อนของระบบโดยใช้โปรแกรมประยุกต์ เป็นเครื่องมือในการตรวจหาช่องโหว่หรือจุดอ่อนของบริหารจัดการทางการแพทย์ (BHIS)

2) ศึกษาช่องโหว่หรือจุดอ่อนของระบบบริหารจัดการทางการแพทย์ (BHIS) โดยวิธีการทดสอบเจาะระบบโดยผู้ทำการวิจัย

3) ศึกษาแนวทางในการป้องกันการเข้าถึงช่องโหว่หรือจุดอ่อนของระบบบริหารจัดการทางการแพทย์ (BHIS)

5.2 แนวทางการพัฒนาต่อในอนาคต

5.2.1 ตรวจหาช่องโหว่หรือจุดอ่อนของระบบอื่น ๆ ที่เข้ามาเชื่อมต่อกับระบบบริหารจัดการทางการแพทย์ (BHIS) เพื่อเป็นการรักษาความมั่นคงปลอดภัยของระบบโดยภาพรวม

บรรณานุกรม

[1] กองสุขภาพระหว่างประเทศ กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข, ยุทธศาสตร์การพัฒนาประเทศไทยให้เป็นศูนย์กลางสุขภาพนานาชาติ (MEDICAL HUB) (พ.ศ. ๒๕๖๐-๒๕๖๙), 2560

[2] ดร.พชรพจน์ นันทรามาศ และ ณัฐพร ศรีทอง จาก 5G สู่อนาคตของ Smart Healthcare March 2020, 2563

[3] ราชกิจจานุเบกษา, พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒

[4] ราชกิจจานุเบกษา, พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒

[5] Technical Guide to Information Security Testing and Assessment of Nation Institute of Standard and Technology U.S.Department Commerce, 2008

[6] กองสงครามอิเล็กทรอนิกส์และสารสนเทศ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ , คู่มือจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารหน่วยงานขึ้นตรงกองทัพอากาศ, 2559: ออนไลน์

[7] “Hydra brute force” [ออนไลน์]: เข้าถึงเมื่อ 18 เม.ย. 2563 จาก: https://redteamtutorials.com/2018/10/25/hydra-brute-force-https/

[8] “Navicat” [ออนไลน์]: เข้าถึงเมื่อ 18 เม.ย. 2563 จาก: https://www.navicat.com/en/