การจัดการความรู้ของ ยศ.ทร.

ประจำปี ๒๕๖๐

วิธีปฏิบัติที่เป็นเลิศ Best Practice

หัวข้อ การป้องกันการรุกล้ำระบบเครือข่าย คอมพิวเตอร์และอินเตอร์เน็ต

หน่วย กบศ.ยศ.ทร.

คำนำ

การจัดการความรู้ของ กบศ.ยศ.ทร. เป็นหนึ่งในกระบวนการให้การสนับสนุน ยศ.ทร. เพื่อให้เป็นหน่วยงานแห่งการเรียนรู้ สามารถนำมาใช้เป็นแนวทางในการปฏิบัติ เพื่อให้เกิดความรวดเร็ว ถูกต้อง และสามารถนำไปใช้เป็นเครื่องมือในการพัฒนากำลังพลให้สามารถทำงานทดแทนกันได้

กบศ.ยศ.ทร. ได้ดำเนินการจัดทำองค์ความรู้ เรื่อง “การป้องกันการรุกล้ำระบบเครือข่ายคอมพิวเตอร์และอินเตอร์เน็ต” เป็น Best Practice(BP) โดยในการจัดทำองค์ความรู้นี้ ได้ดำเนินการตามสภาวการณ์ของเหตุการณ์ปัจจุบัน ที่ได้รับผลกระทบจากการพัฒนาทางเทคโนโลยีทางด้านคอมพิวเตอร์และอินเตอร์เน็ตที่มีการเชื่อมต่อกันอย่างที่เกือบจะเรียกได้ว่าไร้ขอบเขต ทำให้การเข้าถึง การใช้งาน และการลักลอบผ่านระบบอย่างไม่ถูกต้องเกิดมากขึ้นตามไปด้วย สิ่งต่าง ๆ เหล่านี้ จึงเป็นตัวผลักดันให้ กบศ.ยศ.ทร. โดยแผนกกรรมวิธีข้อมูล จำเป็นต้องค้นคว้าข้อมูลในเรื่องเหล่านี้ และดำเนินการจัดทำเป็นองค์ความรู้ เพื่อใช้เป็นแนวทางในการปฏิบัติและดำเนินการในเบื้องต้นได้ อย่างไรก็ตาม การจัดทำองค์ความรู้ครั้งนี้ ยังไม่ครอบคลุมไปถึงทุก ๆ สถานการณ์หรือโอกาสในการเกิดเหตุการณ์ต่าง ๆ ได้ทั้งหมด เพราะในทุก ๆ วัน จะมีวิธีการและเทคนิคในการรุกล้ำด้วยวิธีการใหม่ ๆ เกิดขึ้นตลอดเวลา องค์ความรู้นี้จึงยังเป็นเพียงแนวทางและเป็นจุดเริ่มต้นในการพัฒนาองค์ความรู้เพิ่มเติมในอนาคตต่อไป

แผนกกรรมวิธีข้อมูล หวังว่าแนวทาง “การป้องกันการรุกล้ำระบบเครือข่ายคอมพิวเตอร์และอินเตอร์เน็ต” ของแผนกจะสร้างประโยชน์ให้กับหน่วยงานและบุคลากรที่เกี่ยวข้องต่อไป

คณะทำงานการจัดการความรู้ของ กบศ.ยศ.ทร.

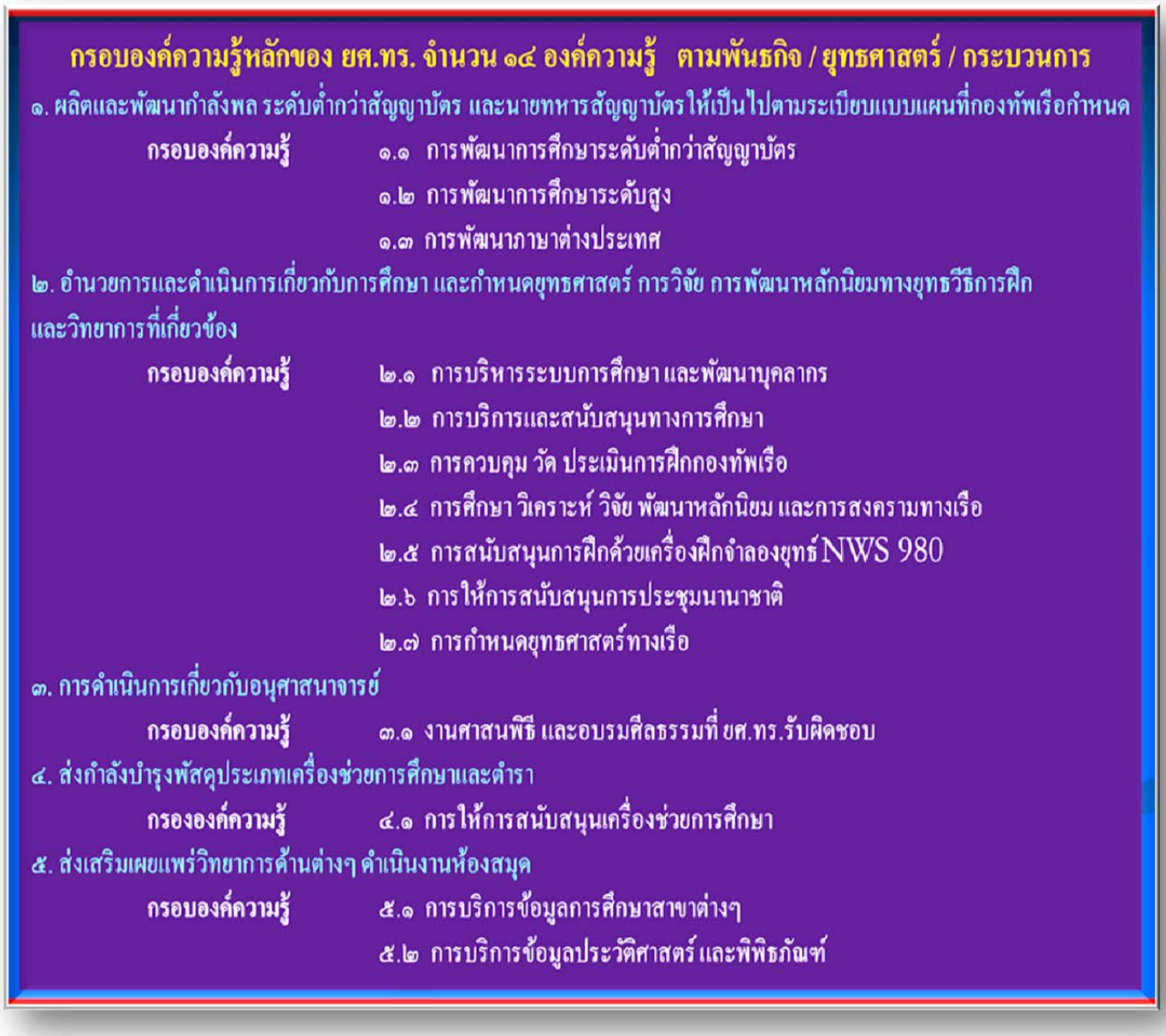
สารบัญ

หัวข้อ	๑
คำนำ	๒
สารบัญ	๓
ประวัติกรมยุทธศึกษาทหารเรือ บทเกริ่นนำสู่องค์ความรู้ ภารกิจและวิสัยทัศน์	๔
บทเกริ่นนำสู่องค์ความรู้	๔
กระบวนการการดำเนินการ หลักการและเหตุผล	๕
แบบการจัดเก็บองค์ความรู้	๖ – ๑๑
การโจมตีระบบเครือข่ายคอมพิวเตอร์แบบต่างๆ และการป้องกัน	๑๒ – ๒๑
ปัจจัยเกื้อหนุนการดำเนินการ และความสำเร็จ	๒๒
การถ่ายทอดและความยั่งยืน	๒๓

วิสัยทัศน์ : เป็นองค์กรแห่งการเรียนรู้ ก้าวทันเทคโนโลยี จัดการศึกษามีคุณภาพตามมาตรฐานสากล เป็นที่ปรึกษาทางวิชาการที่เชื่อถือได้ และเป็นเลิศในด้านกิจการทางทะเล เป็นต้นแบบในความเป็นมืออาชีพ จริยธรรมและคุณธรรม

บทเกริ่นนำสู่องค์ความรู้

จากผังการจัดหน่วยของ ยศ.ทร.ที่มีขนาดใหญ่หลากหลายภารกิจ ได้กำหนดกรอบองค์ความรู้หลักตามภารกิจ ได้ ๕ กรอบ ๑๔ องค์ความรู้ และทุกองค์ความรู้ล้วนเปรียบเสมือนเส้นเลือดใหญ่ที่หล่อเลี้ยงหัวใจ ยศ.ทร.ทั้งสิ้น ซึ่งมีการปฏิบัติงานมาตั้งแต่อดีตกว่าร้อยปี ดังนั้น การจัดทำองค์ความรู้ที่เป็น Best Practice ทุกภารกิจสามารถกระทำได้เพราะมีการปฏิบัติและพัฒนางานให้ทันสมัยตามเทคโนโลยีมาตลอด



วิธีปฏิบัติที่เป็นเลิศ (Best Practice : BP)

ภารกิจ : มีหน้าที่พิจารณากำหนดอัตราและความต้องการ การผลิต เก็บรักษา จัดหา ควบคุม ซ่อมบำรุง จำหน่าย และบริการพัสดุประเภทเครื่องช่วยการศึกษาและตำรา ให้แก่หน่วยต่างๆในกองทัพเรือ การบันทึกภาพต่างๆตามที่กองทัพเรือมอบหมาย การดำเนินการด้านสารสนเทศ การผลิตสื่อต่างๆ การเขียนประกาศนียบัตรและปริญญาบัตรให้แก่สถานศึกษาในบังคับบัญชา

วิสัยทัศน์ : กองบริการการศึกษา กรมยุทธศึกษาทหารเรือ ให้บริการเครื่องช่วยการศึกษา และด้าสารสนเทศให้กับหน่วยต่าง ๆ ในกรมยุทธศึกษาทหารเรือ และหน่วยขึ้นตรงกองทัพเรือ

แผนกกรรมวิธีข้อมูล “มีหน้าที่ดำเนินการด้านกรรมวิธีข้อมูลและสารสนเทศ ตลอดจนการให้บริการด้านต่าง ๆ กับกำลังพลของกรมยุทธศึกษาทหารเรือ และนักเรียน นายทหารนักเรียน นักศึกษาในหลักสูตรต่าง ๆ”

แบบการจัดเก็บองค์ความรู้ในการปฏิบัติงานของผู้ปฏิบัติงาน

ความรู้ในการปฏิบัติงาน เรื่อง การรุกล้ำระบบเครือข่ายคอมพิวเตอร์และอินเตอร์เน็ต

เจ้าของความรู้ชื่อ น.ท.นิรันดร์ วงศ์บุญรอด ตำแหน่ง หน.กรรมวิธีข้อมูล กบศ. สังกัด ยศ.ทร.

.....

วันที่บันทึกความรู้ ๘/พ.ค./๖๐.

วัตถุประสงค์ของความรู้

กระบวนการ/ขั้นตอน/วิธีปฏิบัติ	ข้อแนะนำ/ข้อพึงระวัง
๑. ตรวจสอบระบบเครือข่าย ๒. จัดเจ้าหน้าที่ดูแลระบบเครือข่าย ๓. การประสานงานระหว่างหน่วยที่เกี่ยวข้อง (ยศ.ทร. → ← สสท.ทร.) ๔. เตรียมความพร้อมในการแก้ไขปัญหาที่อาจเกิดขึ้นได้ ผู้บันทึก น.ท.นิรันดร์ วงศ์บุญรอด หน.กรรมวิธีข้อมูล สังกัด กบศ.ยศ.ทร. ติดต่อได้ที่ โทร. ๕๓๖๕๑ หรือ ๐๘๙ ๗๘๗ ๐๗๘๒	

(ลงชื่อ) น.อ.เพิ่มพงษ์ จันทพิมพะ

(เพิ่มพงษ์ จันทพิมพะ)

ผอ.กบศ.ยศ.ทร.

วิสัยทัศน์ : กองบริการการศึกษา กรมยุทธศึกษาทหารเรือ ให้บริการเครื่องช่วยการศึกษา และด้านสารสนเทศให้กับหน่วยต่าง ๆ ในกรมยุทธศึกษาทหารเรือ และหน่วยขึ้นตรงกองทัพเรือ

ภารกิจ : มีหน้าที่พิจารณากำหนดอัตราและความต้องการ การผลิต เก็บรักษา จัดหา ควบคุม ซ่อมบำรุง จำหน่าย และบริการพัสดุประเภทเครื่องช่วยการศึกษาและตำรา ให้แก่หน่วยต่างๆในกองทัพเรือ การบันทึกภาพต่างๆ ตามที่กองทัพเรือมอบหมาย การดำเนินการด้านสารสนเทศ การผลิตสื่อต่างๆ การเขียนประกาศนียบัตรและปริญญาบัตรให้แก่สถานศึกษาในบังคับบัญชา ตามภารกิจของ ยศ.ทร.จะต้องจัดทำองค์ความรู้หลักให้ตอบสนองประเด็นยุทธศาสตร์ ทร. ประเด็นที่ ๓ “พัฒนาระบบงานและการบริหารจัดการให้มีความทันสมัยและมีคุณภาพ”

กลุ่มความรู้ KM1	**หัวข้อความรู้** KM2	**หัวข้อความรู้ย่อ** KM3
<u>กองบริการการศึกษา</u> มีหน้าที่พิจารณากำหนดอัตราและความต้องการ การผลิต เก็บรักษา จัดหา ควบคุม ซ่อมบำรุง จำหน่าย และบริการพัสดุประเภทเครื่องช่วยการศึกษาและตำรา ให้แก่หน่วยต่างๆในกองทัพเรือ การบันทึกภาพต่างๆตามที่กองทัพเรือมอบหมาย การดำเนินการด้านสารสนเทศ การผลิตสื่อต่างๆ การเขียนประกาศนียบัตรและปริญญาบัตรให้แก่สถานศึกษาในบังคับบัญชา	<u>แผนกกรรมวิธีข้อมูลฯ</u> มีหน้าที่ดำเนินการด้านกรรมวิธีข้อมูลและสารสนเทศ ตลอดจนการให้บริการด้านต่าง ๆ กับกำลังพลของกรมยุทธศึกษาทหารเรือและนักเรียน นายทหารนักเรียน นักศึกษา ในหลักสูตรต่าง ๆ	- จัดทำระบบประเมินผลการศึกษาของหลักสูตรต่างๆ และฐานข้อมูลการรับสมัครบุคคลพลเรือนเข้าเป็นนักเรียนจ่า เพื่อเก็บไว้เป็นหลักฐาน - จัดทำบัตรแสดงตนของข้าราชการทหาร และลูกจ้างของ ยศ.ทร. และงานด้านคอมพิวเตอร์กราฟิก - ดูแล ตรวจสอบระบบสารสนเทศ ยศ.ทร. และระบบสารสนเทศของ ทร. ให้บริการอินเตอร์เน็ทใช้งานได้ตลอดเวลา - ซ่อมคอมพิวเตอร์ และปริ๊นเตอร์ในเบื้องต้น - ประชาสัมพันธ์ข้อมูลข่าวสารของ ยศ.ทร. ลงในเว็บไซต์ และจอ LED

น.ท.<u>นิรันดร์ วงศ์บุญรอด</u>

หน.กรรมวิธีข้อมูล กบศ.ยศ.ทร.

ตามภารกิจของ ยศ.ทร.จะต้องจัดทำองค์ความรู้หลักให้ตอบสนองประเด็นยุทธศาสตร์ ทร. ประเด็นที่ ๓ “พัฒนาระบบงานและการบริหารจัดการให้มีความทันสมัยและมีคุณภาพ”

การจัดการความรู้ของ แผนกกรรมวิธีข้อมูล กบศ.ยศ.ทร.

ภารกิจ

มีหน้าที่ดำเนินการด้านกรรมวิธีข้อมูลและสารสนเทศ ตลอดจนการให้บริการด้านต่าง ๆ กับกำลังพลของกรมยุทธศึกษาทหารเรือ และนักเรียน นายทหารนักเรียน นักศึกษา ในหลักสูตรต่าง ๆ

ลำดับ	ชื่อองค์ความรู้	อยู่ในกรอบองค์ความรู้ ๑ ใน ๑๔ กรอบ	รูปแบบการถ่ายทอด /เครื่องมือ	วัตถุประสงค์ /ผลสัมฤทธิ์	จัดทำองค์ความรู้ สำเร็จเมื่อ ปีงป.	หน่วยรับผิดชอบ /โทรศัพท์
๑.	ผ.กรรมวิธีข้อมูลฯ – จัดทำฐานข้อมูลประเมินผลการศึกษา และระบบการรับสมัครบุคคลพลเรือนเข้าเป็นนักเรียนจ่า – ให้บริการด้านอินเตอร์เน็ต ซ่อมบำรุงคอมพิวเตอร์ - จัดทำบัตรแสดงตนและงานคอมพิวเตอร์กราฟิก – ประชาสัมพันธ์ข้อมูลข่าวสารของ ยศ.ทร. ลงในเว็บไซต์ และจอ LED	การบริการด้านกรรมวิธีข้อมูลและสารสนเทศ	ปฏิบัติตามตำแหน่งหน้าที่รับผิดชอบ และตามคำสั่ง ยศ.ทร. และที่ผู้บังคับบัญชามอบหมาย	- การประเมินผลการศึกษาหลักสูตรต่างๆ ดำเนินการอย่างมีประสิทธิภาพ - เพื่อเป็นหลักฐานในการสอบคัดเลือกของผู้สมัคร - ดำเนินการตามหน้าที่ความรับผิดชอบเพื่อให้ใช้งานระบบได้ - ข้าราชการ ทหาร และลูกจ้างของ ยศ.ทร. มีบัตรแสดงตนใช้อย่างถูกต้องตามระเบียบ รปภ. - เพื่อเผยแพร่ระชาสัมพันธ์ข้อมูลข่าวสารของ ยศ.ทร. ลงในเว็บไซต์ และจอ LED ให้บุคคล และประชาชนทราบ	งป.๖๐	ผ.กรรมวิธีข้อมูลฯ

น.ท.นิรันดร์ วงศ์บุญรอด

หน.กรรมวิธีข้อมูล กบศ.ยศ.ทร.

แนวทางการจัดการความรู้ของ แผนกกรรมวิธีข้อมูล กบศ.ยศ.ทร. ตามนโยบายการจัดการความรู้ของ ทร.

วิสัยทัศน์ : กองบริการการศึกษา กรมยุทธศึกษาทหารเรือ ให้บริการเครื่องช่วยการศึกษา และด้านสารสนเทศให้กับหน่วยต่าง ๆ ในกรมยุทธศึกษาทหารเรือ และหน่วยขึ้นตรงกองทัพเรือ

ภารกิจ : มีหน้าที่พิจารณากำหนดอัตราและความต้องการ การผลิต เก็บรักษา จัดหา ควบคุม ซ่อมบำรุง จำหน่าย และบริการพัสดุประเภทเครื่องช่วยการศึกษาและตำรา ให้แก่หน่วยต่างๆในกองทัพเรือ การบันทึกภาพต่างๆตามที่กองทัพเรือมอบหมาย การดำเนินการด้านสารสนเทศ การผลิตสื่อต่างๆ การเขียนประกาศนียบัตรและปริญญาบัตรให้แก่สถานศึกษาในบังคับบัญชาและในกำกับ และในกำกับ ตามภารกิจของ ยศ.ทร.จะต้องจัดทำองค์ความรู้หลักให้ตอบสนองประเด็นยุทธศาสตร์ ทร. ประเด็นที่ ๓ “พัฒนาระบบงานและการบริหารจัดการให้มีความทันสมัยและมีคุณภาพ”

กระบวนการสนับสนุน SP5 กระบวนการพัฒนาโปรแกรมฐานข้อมูล และงานบริการด้านกรรมวิธีข้อมูล

แบบรายละเอียดกระบวนการสนับสนุน (Support Process) ของ แผนกกรรมวิธีข้อมูล กบศ.ยศ.ทร.

SP5 ชื่อกระบวนการพัฒนาระบบสารสนเทศและกรรมวิธีข้อมูล

กระบวนการสนับสนุน SP5.1 กระบวนการพัฒนาโปรแกรมฐานข้อมูล และงานบริการด้านกรรมวิธีข้อมูล

ภารกิจ มีหน้าที่ดำเนินการด้านกรรมวิธีข้อมูลและสารสนเทศ ตลอดจนการให้บริการด้านต่าง ๆ กับกำลังพลของกรมยุทธศึกษาทหารเรือ และนักเรียน นายทหารนักเรียน นักศึกษา ในหลักสูตรต่าง ๆ

ลำดับ	กิจกรรม	ขั้นตอนและแนวทางการปฏิบัติ	มาตรฐานที่กำหนด	KM/เอกสารที่เกี่ยวข้อง	ผู้รับผิดชอบ	ข้อแนะนำที่สำคัญ
๑.	จัดทำฐานข้อมูลระบบประเมินผลการศึกษาของหลักสูตรต่างๆ และฐานข้อมูลของผู้สมัครสอบคัดเลือกบุคคลพลเรือนเข้าเป็นนักเรียนจ่า รวมทั้งให้บริการด้านสารสนเทศ จัดทำบัตรแสดงตนข้าราชการ ทหาร และลูกจ้างของประชาสัมพันธ์ข้อมูลข่าวสารของ ยศ.ทร.	ดำเนินการตามวงรอบการปฏิบัติงานและที่ นขต.ยศ.ทร.ขอรับการสนับสนุน และตามคำสั่ง ยศ.ทร.	- หลักสูตรต่างๆ สามารถประเมินผลการศึกษาอย่างมีประสิทธิภาพ - เพื่อเป็นหลักฐานและสามารถตรวจสอบข้อมูลของผู้สมัคร - ข้าราชการ ทหาร และลูกจ้างของ ยศ.ทร. มีบัตรแสดงตนใช้อย่างถูกต้องตามระเบียบ รปภ. - เพื่อเผยแพร่ประชาสัมพันธ์ข้อมูลข่าวสารของ ยศ.ทร. ลงในเว็บไซต์ และจอ LED ให้บุคคล และประชาชนทราบ	คู่มือการพัฒนาระบบงาน ระเบียบ ทร.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ. ๒๕๕๐	หน.กรรมวิธีข้อมูล และเจ้าหน้าที่แผนกกรรมวิธีข้อมูลฯ	

น.ท.นิรันดร์ วงศ์บุญรอด.....

หน.กรรมวิธีข้อมูล กบศ.ยศ.ทร.

แบบรายละเอียดกระบวนการสนับสนุน (Support Process) ของ แผนกกรรมวิธีข้อมูล กบศ.ยศ.ทร.

SP5 ชื่อกระบวนการพัฒนาระบบสารสนเทศและกรรมวิธีข้อมูล

กระบวนการสนับสนุน SP5.2 กระบวนการซ่อมบำรุงระบบคอมพิวเตอร์และระบบเครือข่าย

ภารกิจ มีหน้าที่ดำเนินการด้านกรรมวิธีข้อมูลและสารสนเทศ ตลอดจนการให้บริการด้านต่าง ๆ กับกำลังพล ของกรมยุทธศึกษาทหารเรือ และนักเรียน นายทหารนักเรียน นักศึกษา ในหลักสูตรต่าง ๆ

ลำดับ	กิจกรรม	ขั้นตอนและแนวทางการปฏิบัติ	มาตรฐานที่กำหนด	KM/เอกสารที่เกี่ยวข้อง	ผู้รับผิดชอบ	ข้อแนะนำที่สำคัญ
๑.	ดูแล ตรวจสอบ ซ่อมบำรุงระบบคอมพิวเตอร์และระบบเครือข่ายสารสนเทศ	ดำเนินการตามหน้าที่การปฏิบัติงานและที่ นขต.ยศ.ทร.ขอรับการ	- ให้ระบบงานสารสนเทศของ ยศ.ทร.และที่เชื่อโยงระบบสารสนเทศของ ทร. ใช้งานได้ตลอดเวลา	คู่มือการพัฒนาระบบงาน ระเบียบ ทร.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ. ๒๕๕๐	หน.กรรมวิธีข้อมูล และเจ้าหน้าที่ ผนกกรรมวิธีข้อมูลฯ	

น.ท.นิรันดร์ วงศ์บุญรอด.....

หน.กรรมวิธีข้อมูล กบศ.ยศ.ทร.

การโจมตีระบบเครือข่ายคอมพิวเตอร์

แม้ว่าระบบเครือข่ายคอมพิวเตอร์ จะเป็นเทคโนโลยีที่น่าอัศจรรย์ แต่ก็ยังมีความเสี่ยงอยู่มากถ้าไม่มีการควบคุมหรือป้องกันที่ดี การโจมตีหรือการบุกรุกเครือข่าย หมายถึง ความพยายามที่จะเข้าใช้ระบบ (Access Attack) การแก้ไขข้อมูลหรือระบบ (Modification Attack) การทำให้ระบบไม่สามารถใช้การได้ (Deny of Service Attack) และการทำให้ข้อมูลเป็นเท็จ (Repudiation Attack) ซึ่งจะกระทำโดยผู้ประสงค์ร้าย ผู้ที่ไม่มีสิทธิ์ หรืออาจเกิดจากความไม่ได้ตั้งใจของผู้ใช้เองต่อไปนี้เป็นรูปแบบต่าง ๆ ที่ผู้ไม่ประสงค์ดีพยายามที่จะบุกรุกเครือข่ายเพื่อลักลอบข้อมูลที่สำคัญหรือเข้าใช้ระบบโดยไม่ได้รับอนุญาต

แพ็กเก็ตสนิฟเฟอร์

ข้อมูลที่คอมพิวเตอร์ส่งผ่านเครือข่ายนั้นจะถูกแบ่งย่อยเป็นก้อนเล็ก ๆ ที่เรียกว่า “แพ็กเก็ต (Packet)” แอพพลิเคชันหลายชนิดจะส่งข้อมูลโดยไม่เข้ารหัส (Encryption) หรือในรูปแบบเคลียร์เท็กซ์ (Clear Text) ดังนั้นข้อมูลอาจจะถูกคัดลอกและโพรเซสโดยแอพพลิเคชันอื่นก็ได้

การป้องกันการถูกดักอ่านข้อมูลโดย sniffer

1. อย่างแรก เปลี่ยนจาก Hub มาใช้ Switch

2. หลีกเลี่ยงการส่งข้อมูลที่ไม่มีการเข้ารหัส

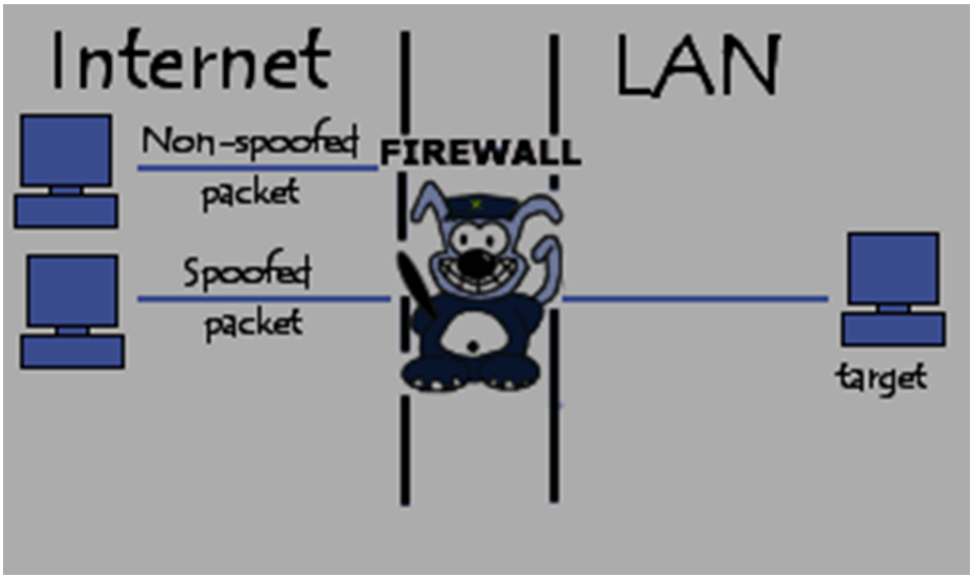
3. ให้ตระหนักว่า ใน network นั้นสามารถถูกดักอ่านได้เสมอ เพราะฉะนั้นการส่งข้อมูลแต่ละครั้ง ต้องประเมินว่า หากโดนดักอ่านแล้วจะคุ้มกันมั้ย หากมีความสำคัญมากควรหาวิธีอื่นในการส่งข้อมูล

4. หากมีการใช้บริการเกี่ยวกับด้านการเงิน หรือข้อมูลรหัสผ่าน ให้เลือกใช้ผู้บริการที่เข้ารหัสข้อมูลด้วย SSL

5. หากสามารถเพิ่มความปลอดภัยของการส่งข้อมูลด้วยการเข้ารหัส ก็จะเป็นวิธีที่ดี แม้การส่งแบบนี้จะโดนดักได้ แต่ข้อมูลมีการเข้ารหัสไว้ ทำให้คนที่ดักไป ต้องไปนั่งปวดหัวถอดกันอีก โดยใช้โปรแกรมเข้ารหัสไฟล์

6. หากมีการสื่อสารข้อมูลภายในองค์กรโดยผ่านอินเทอร์เน็ต การนำเทคโนโลยีของ VPN (Vitual Private Network) มาใช้จะช่วยเพิ่มความปลอดภัยได้

การโจมตีรหัสผ่าน



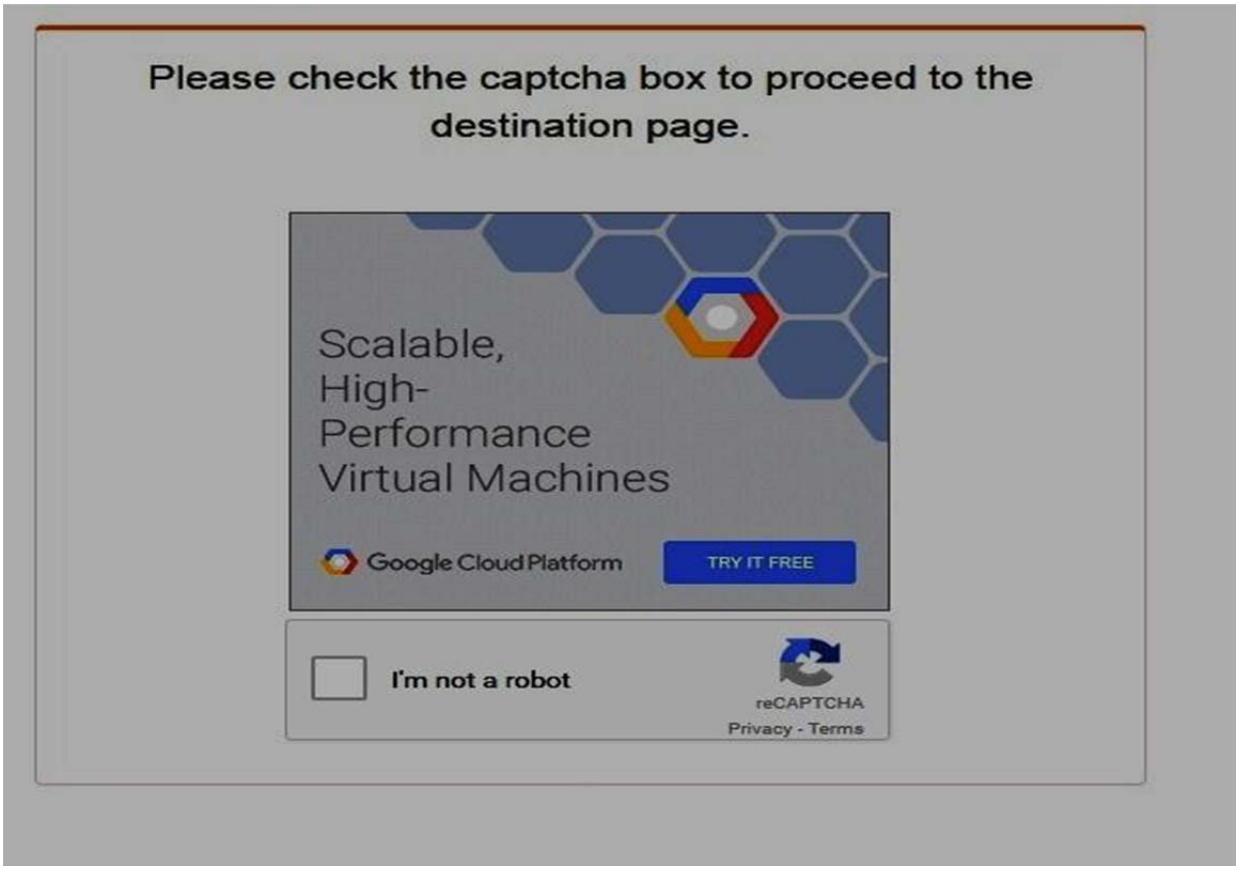
การโจมตีรหัสผ่าน (Password Attacks) หมายถึงการโจมตีที่ผู้บุกรุกพยายามเดารหัสผ่านของผู้ใช้คนใดคนหนึ่ง ซึ่งวิธีการเดานั้นก็มีหลายวิธี เช่น บรู๊ทฟอร์ช (Brute-Force) ,โทรจันฮอร์ส (Trojan Horse) , ไอพีสปูฟิง , แพ็กเก็ตสนิฟเฟอร์ เป็นต้น การเดาแบบบรู๊ทฟอร์ช หมายถึง การลองผิดลองถูกรหัสผ่านเรื่อย ๆ จนกว่าจะถูก บ่อยครั้งที่การโจมตีแบบบรู๊ทฟอร์ชใช้การพยายามล็อกอินเข้าใช้รีซอร์สของเครือข่าย โดยถ้าทำสำเร็จผู้บุกรุกก็จะมีสิทธิ์เหมือนกับเจ้าของแอ็คเคาท์นั้น ๆ ถ้าหากแอ็คเคาท์นี้มีสิทธิ์เพียงพอผู้บุกรุกอาจสร้างแอ็คเคาท์ใหม่เพื่อเป็นประตูหลัง (Back Door) และใช้สำหรับการเข้าระบบในอนาคต

Brute force attack เป็นการโจมตีแบบเดารหัสผ่านโดยการสุ่มไปเรื่อยๆ ซึ่งการทำจะใช้โปรแกรมทำให้การโจมตีทำได้เร็ว นอกจากเว็บเราจะมีความเสี่ยงแล้วในการที่จะถูกแฮ็กแล้ว ยังทำให้โหลดบนเว็บเราเพิ่มขึ้นอีกด้วย ทางเดียวที่เราจะป้องกันคือการตรวจสอบว่าทรานแซ็คชั่นใดคือการทำ Brute Forace และทำการบล็อกไอพีเหล่านั้นทันที

ในการที่จะเดารหัสผ่านโดยใช้หลักการ Brute Force Attack นั้นผู้โจมตีจะต้องเดาข้อมูลสองตัวคือชื่อผู้ใช้และรหัสผ่าน ดังนั้นข้อแนะนำแรกที่จะต้องทำเพื่อความปลอดภัยสำหรับเว็บไซต์ที่ติดตั้งจูมล่าคือการเปลี่ยนชื่อผู้ใช้จาก admin เป็นชื่ออื่น เพราะหากคุณไม่เปลี่ยนเท่ากับว่าคุณได้ช่วยแฮ็กเกอร์ไปแล้วครึ่งหนึ่งการโจมตีของเขาก็ทำได้ง่ายขึ้น

การป้องกันการโจมตีแบบ Brute Force ป้องกันโดยการใช้ Recaptcha

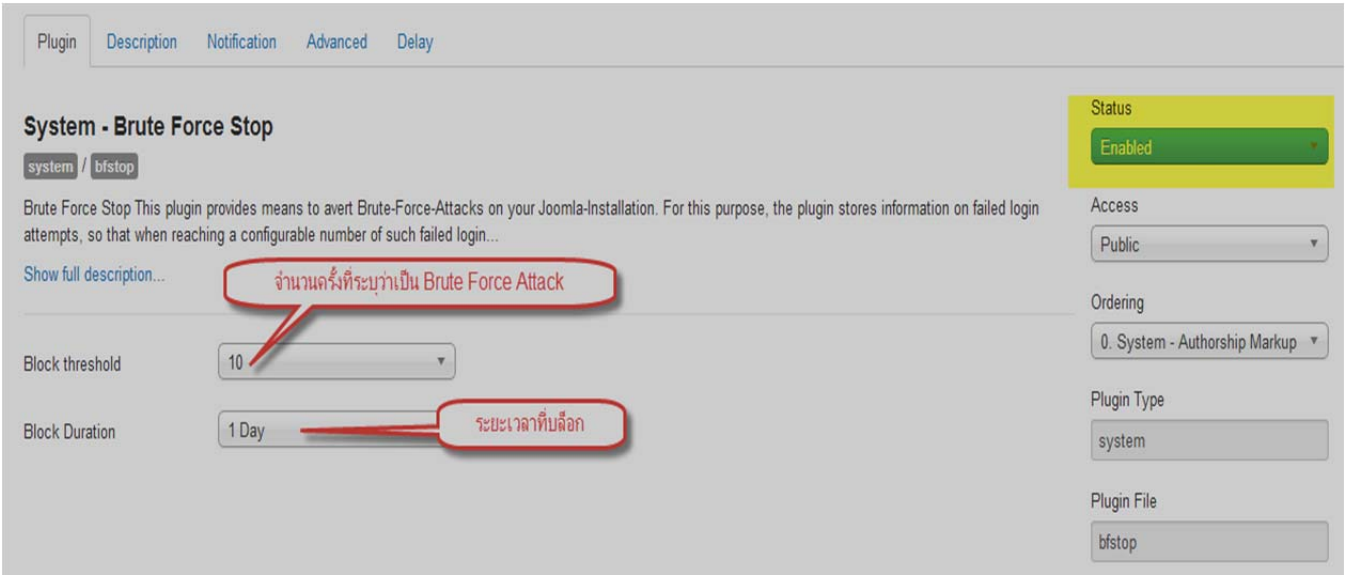
อย่างที่บอกว่าการโจมตีด้วยเทคนิก Brute Force Attack จะทำโดยการใช้โปรแกรมซึ่งจะเรียงชื่อผู้ใช้และรหัสผ่านแล้วก็ทดลองล็อกอินเข้าเว็บของเรา ดังนั้นทางหนึ่งที่จะป้องกันก็คือการป้องกันไม่ให้ทำการล็อกอินโดยใช้เทคนิกประเภท recaptCha เมื่อเทียบกับการใช้งานผ่านโปรแกรม



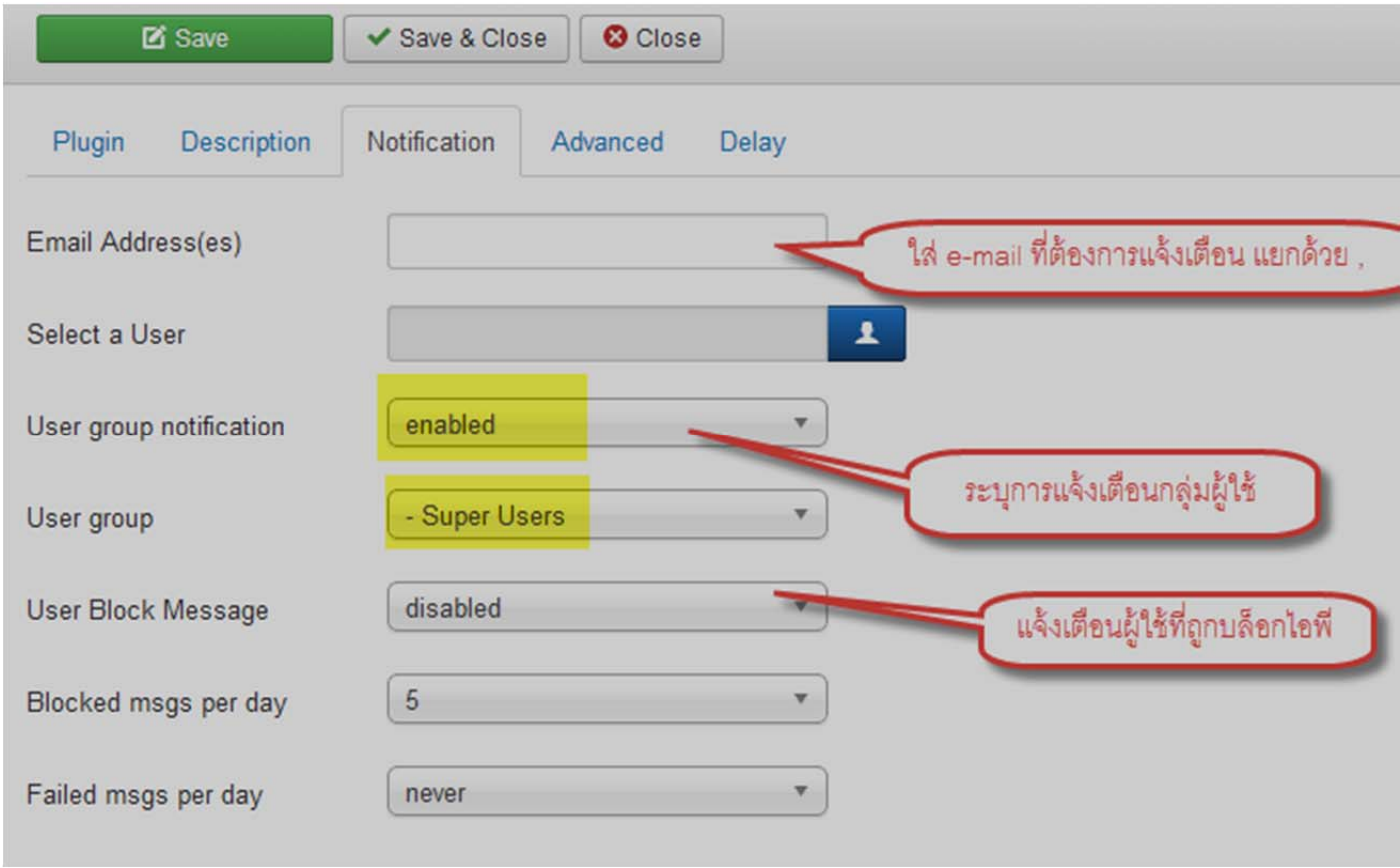
ป้องกันโดยการบล็อกไอพี

หลังจากที่เราป้องกันการโจมตีโดยใช้โปรแกรมคอมพิวเตอร์ในการเดารหัสผ่านแล้ว เรายังสามารถเพิ่มความปลอดภัยขึ้นอีกระดับโดยทำการบล็อกไอพีของผู้ที่พยายามจะทำการล็อกอินโดยการเดารหัสผ่าน หลักการทำงานก็คือเราจะถือว่าผู้ใช้ที่พยายามล็อกอินโดยไม่สำเร็จหลายๆ ครั้งติดต่อกัน เช่น 10 ครั้งน่าจะเข้าข่ายเป็นการโจมตีแบบ Brute Force เราจะทำการบล็อกไอพีนั้นๆ เป็นระยะเวลาเช่น 1 วัน โดยหลังจากผ่านไปหนึ่งวันแล้วก็จะยกเลิกการบล็อกสำหรับตัว Brute Force Stop ใช้งานค่อนข้างง่าย เป็นตัวปลั๊กอินหนึ่งตัวที่ทำหน้าที่ในการตรวจสอบและบล็อกไอพี ส่วนคอมโพเนนท์จะทำหน้าที่ในการแสดงรายงาน ยกเลิกการบล็อก และกำหนดไวท์ลิสท์ (White List) หรือไอพี หรือกลุ่มไอพีที่เราไม่มีการบล็อกในทุกกรณี

การติดตั้งจะเป็นการติดตั้ง package ประกอบด้วยคอมโพเนนท์และปลั๊กอินภายในการติดตั้งครั้งเดียว หลังจากนั้นให้เข้าไปที่ Plugin Manager เลือกประเภทเป็น System จะเจอ Brute Force Stop ก็เข้าไปแก้ไขค่าต่างๆ ที่ลืมไม่ได้คือการ Enable ตัวปลั๊กอิน



หลังจากการ Enable ตัวปลั๊กอินแล้ว สิ่งสำคัญที่ต้องกำหนดคือ จำนวนครั้งของการล็อกอินผิดพลาดที่เราจะทำการบล็อก (Block threshold) และระยะเวลาในการปล็อก (Block Duration) ส่วนที่สองที่เราควรจะทำการตั้งค่าคือการแจ้งเตือน ก็คลิกเลือกที่แท็บ Notification จะมีหน้าจอแสดงดังรูปถัดไป

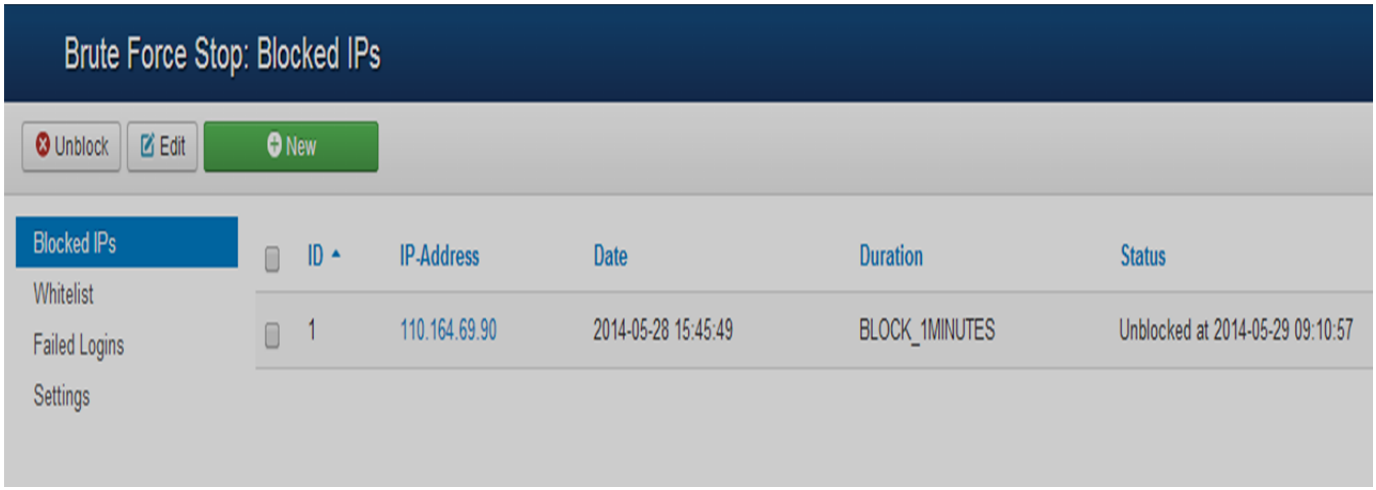


จากรูปเราจะสามารถตั้งค่าตัวเลือกในการแจ้งเตือนได้หลายรูปแบบเช่นในส่วนของ E-mail Address(es) เราสามารถใส่ e-mail address ที่ต้องการจะส่ง e-mail ไปแจ้งเตือนได้โดยถ้ามีมากกว่าหนึ่งตัวก็ให้ใช้คอมม่าเป็นตัวคั่นระหว่าง e-mail หรือเราต้องการจะส่ง e-mail แจ้งผู้ใช้งานที่เราเลือกก็ได้ หรือจะเลือกกลุ่มผู้ใช้อย่างกรณีรูปด้านบนก็ได้เช่นกัน

คอมโพเนนท์ Brute Force Stop Administration

เมื่อเข้าไปในส่วนของคอมโพเนนท์เราจะเห็นส่วนต่างๆ ดังนี้

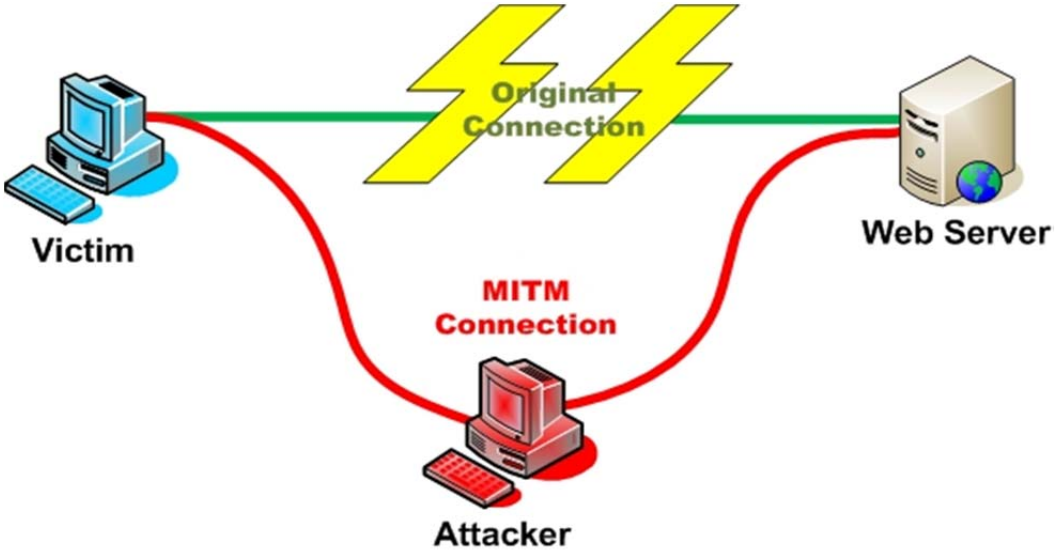
- Blocked IPs แสดงรายการไอพีที่ถูกปล็อกโดยตัวปลั๊กอิน เราสามารถยกเลิกการบล็อกได้ในส่วนนี้
- Whitelist กำหนดค่าไอพีที่ต้องการให้ไม่ต้องตรวจสอบ ไม่มีการบล็อกในทุกกรณี
- Failed Logins แสดงรายการล็อกอินที่ไม่สำเร็จพร้อมทั้งข้อความแสดงเหตุผลที่ทำการล็อกอินไม่สำเร็จ
- Settings จะมีตัวเลือกในการทดสอบการแจ้งเตือนให้เราทดลอง



สำหรับในส่วนของ Whitelist เราสามารถใส่ไอพีที่เราไม่ต้องการให้บล็อกซึ่งอาจจะเป็นไอพีของเราเอง กรณีที่เราใช้ Fixed IP ก็ได้

จากข้อมูลทั้งหมดที่กล่าวมาเราก็จะสามารถทำการป้องกันการโจมตีโดยการเดาชื่อผู้ใช้และรหัสผ่านหรือ Brute Force Attack ได้โดยใช้ reCaptcha และ Brute Force Stop ซึ่งจะช่วยลดปัญหาให้เราได้พอสมควร อย่างน้อยก็จะทำให้เราไม่เป็นตัวเลือกแรกๆ ในการโจมตีจากแฮกเกอร์

การโจมตีแบบ Man-in-the-Middle



Man In The Middle (MITM) คือ เทคนิคการโจมตีของแฮคเกอร์ที่จะปลอมเป็นคนกลางเข้ามาแทรกสัญญาณการรับส่งข้อมูลระหว่างผู้ใช้ (เบราว์เซอร์) และเซิร์ฟเวอร์ โดยใช้โปรแกรมดักฟังข้อมูลของเหยื่อ แล้วแฮกเกอร์ก็เป็นตัวกลางส่งผ่านข้อมูลให้ระหว่างเบราว์เซอร์กับเซิร์ฟเวอร์ วิธีการทำอย่างหนึ่งคือการส่งข้อมูล MAC Address ของเครื่องของแฮกเกอร์ไปให้กับเครื่องของผู้ใช้โดยแจ้งว่าเป็น MAC Address ของ Gateway ของระบบเครือข่าย หลังจากนั้นเมื่อเครื่องเหยื่อรับ MAC Address ดังกล่าวไปใส่ไว้ใน ARP Table cached แล้ว กระบวนการส่งข้อมูลจากเบราว์เซอร์ของเครื่องเหยื่อจะถูกส่งผ่านไปยังเครื่องแฮกเกอร์ก่อนที่จะส่งไปยังเครื่องเซิร์ฟเวอร์ ดังนั้นเมื่อเครื่องเหยื่อเข้าไปยังหน้าเว็บเพจที่ต้อง login ด้วย Username และ Password โปรแกรมดักฟังข้อมูลก็จะทำการส่งหน้าเว็บเพจที่ไม่ได้ป้องกัน (หน้าเว็บเพจปลอม) ไปให้เครื่องเหยื่อ

ผู้ใช้ทั่วไปจะสังเกตไม่ออก (หรือไม่มีความรู้) ก็จะคลิกผ่านคำเตือนใดๆที่เบราว์เซอร์แจ้งเตือนไปแล้ว สุดท้ายผู้ใช้งานก็จะใส่ Username และ Password ในหน้า login ซึ่งแฮกเกอร์ก็จะได้ข้อมูลดังกล่าว

การป้องกัน Man In The Middle(MITM) ดักบัญชีผู้ใช้และรหัสผ่าน

การป้องกันที่ดีที่สุดคือ

1) การให้ความรู้วิธีการใช้งานเบราว์เซอร์ทั้ง IE, Google Chrome, Firefox หรือ Safari เป็นต้น ความรู้ที่ว่าก็คือ ผู้ใช้ต้องสังเกตว่า เว็บเพจที่เข้าใช้งานประจำนั้นปรกติหน้า login จะต้องมีอักษร https แสดงอยู่ที่มุมซ้ายบรรทัดที่อยู่ของเว็บเพจ และจะต้องไม่มีการเตือนว่า “ไม่ปลอดภัย” และถามว่า “จะดำเนินการต่อหรือไม่”

แต่หากวันใดที่เราถูกแฮกเกอร์ทำ MITM กับเครื่องของเราแล้ว เราจะเห็นหน้าเว็บเพจแปลกไปจากเดิม เราจะต้องไม่คลิกปุ่มเพื่อดำเนินการต่อไป

เราสามารถตรวจสอบด้วยวิธีอย่างง่ายๆด้วยคำสั่ง arp -a ทั้งบนวินโดวส์และลินุกซ์ เพื่อดูว่ามีเลข MAC Address ของ IP คู่ใดบ้างที่ซ้ำกัน มักจะเป็นคู่ระหว่าง IP ของ Gateway กับ IP ของเครื่องแฮกเกอร์ ถ้าพบว่ามีคู่ที่ซ้ำกันจริง ๆ แสดงว่าเครื่องนั้น ๆ โดน HACKAER เล่นงานเข้าแล้ว ทางแก้ไขทางเดียวคือปิดเครื่องและแจ้งผู้ดูแลระบบประจำหน่วยงานของท่าน

2) การป้องกันตัวเองไม่ต้องรอพึ่งระบบเครือข่าย(เพราะอาจไม่มีระบบป้องกัน) ในทุกครั้งที่เปิดเครื่องและก่อนใช้งานใดๆ ให้ใช้คำสั่ง arp -s เพื่อทำ static ค่า IP กับ MAC ของ Gateway ลงในตาราง ARP ของเครื่องคอมพิวเตอร์ฯ

คำสั่ง คือ **arp -s [IP ของ Gateway] [MAC Address ของ Gateway]**
เราจะรู้ค่า IP และ MAC Address ของ Gateway ก็ด้วยคำสั่งดังนี้

1. ดูว่า IP ของ Gateway (default) คือเบอร์ใด

ลินุกซ์ ip route show

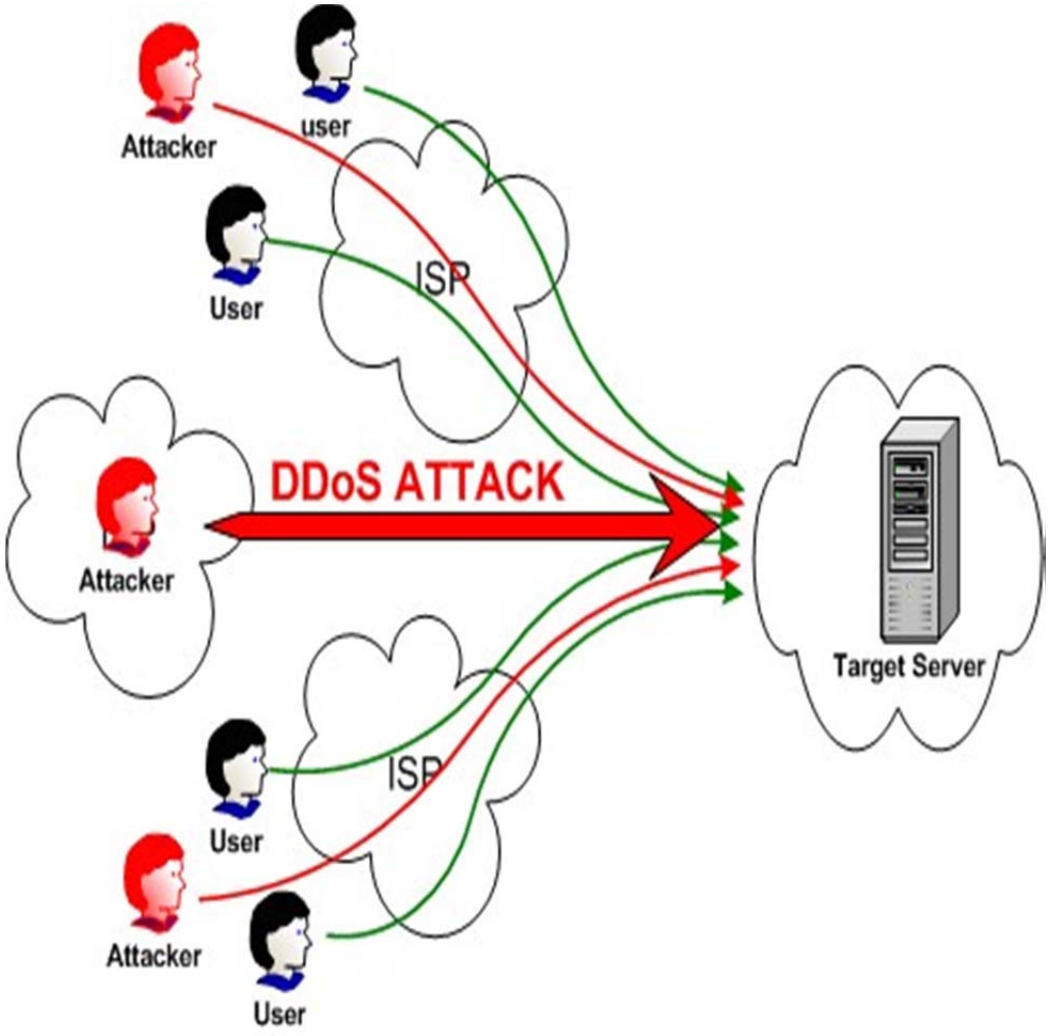
วินโดวส์ route -4 print

2. arp -a เพื่อดูค่า IP กับ MAC คู่ที่ต้องการ เช่น IP ของ Gateway คือ 192.168.10.1 และ MAC Address ของ Gateway คือ 00-13-64-2b-3d-a1 ก็ใช้คำสั่งว่า arp -s 192.168.10.1 00-13-64-2b-3d-a1

โดยที่เครื่องวินโดวส์รุ่นใหม่ๆ (8 ขึ้นไป) ให้คลิกขวาที่ปุ่ม Start เลือก “Command Prompt (Admin)” เพื่อเปิดหน้าต่าง Cmd แล้วทำการพิมพ์คำสั่งตามที่ได้กล่าวไป

ส่วนเครื่องลินุกซ์ ให้เปิด Terminal แล้วใส่คำว่า sudo นำหน้าคำสั่งนั้นด้วย

การโจมตีแบบ DOS



การโจมตีแบบดีไนล์ออฟเซอร์วิส หรือ DOS (Denial-of Service) หมายถึง การโจมตีเซิร์ฟเวอร์โดยการทำให้เซิร์ฟเวอร์นั้นไม่สามารถให้บริการได้ ซึ่งปกติจะทำโดยการใช้รีซอร์สของเซิร์ฟเวอร์จนหมด หรือถึงขีดจำกัดของเซิร์ฟเวอร์ ตัวอย่างเช่น เว็บเซิร์ฟเวอร์ และเอฟทีพีเซิร์ฟเวอร์ การโจมตีจะทำได้โดยการเปิดการเชื่อมต่อ (Connection) กับเซิร์ฟเวอร์จนถึงขีดจำกัดของเซิร์ฟเวอร์ ทำให้ผู้ใช้คนอื่น ๆ ไม่สามารถเข้ามาใช้บริการได้

โทรจันฮอร์ส เวิร์ม และไวรัส

คำว่า “โทรจันฮอร์ส (Trojan Horse)” นี้เป็นคำที่มาจากสงครามโทรจัน ระหว่างทรอย (Troy) และกรีก (Greek) ซึ่งเปรียบถึงม้าโครงไม้ที่ชาวกรีกสร้างทิ้งไว้แล้วซ่อนทหารไว้ข้างในแล้วถอนทัพกลับ พอชาวโทรจันออกมาดูเห็นม้าโครงไม้ทิ้งไว้ และคิดว่าเป็นของขวัญที่กรีซทิ้งไว้ให้ จึงนำกลับเข้าเมืองไปด้วย พอตกดึกทหารกรีกที่ซ่อนอยู่ในม้าโครงไม้ก็ออกมาและเปิดประตูให้กับทหารกรีกเข้าไปทำลายเมืองทรอย สำหรับในความหมายของคอมพิวเตอร์แล้ว โทรจันฮอร์ส หมายถึงโปรแกรมที่ทำลายระบบคอมพิวเตอร์โดยแฝงมากับโปรแกรมอื่น ๆ เช่น เกม สกรีนเวฟเวอร์ เป็นต้น

การป้องกัน

- การนำสื่อเก็บข้อมูลจากแหล่งอื่น มาใช้ภายในหน่วยงาน อาจมีไวรัสติดแอบแฝงเข้ามาด้วยซึ่งกรณีนี้พบได้บ่อยมาก หากมีความจำเป็น ก็จะต้องมีการตรวจสอบไวรัสก่อนการใช้งานทุกครั้ง
- การใช้ Firewall เพื่อป้องกันการโจมตีจากแฮกเกอร์
- ติดตั้งโปรแกรมแอนตี้ไวรัสให้กับเครื่องคอมพิวเตอร์ทุกเครื่อง และต้องมีการอัพเดทข้อมูลแอนตี้ไวรัสนั้น ๆ อย่างสม่ำเสมอด้วย
- สำรองข้อมูลที่จำเป็นอย่างสม่ำเสมอ

ปัจจัยเกื้อหนุนการดำเนินการ

การหาข้อมูลความรู้ที่เกี่ยวข้อง ปัจจุบันสามารถสืบค้นได้จากแหล่งความรู้ต่าง ๆ โดยเฉพาะที่สำคัญก็คือ ระบบอินเตอร์เน็ต นั่นเอง ประกอบกับความพร้อมของระบบเครือข่ายที่มีอยู่นั้น สามารถให้บริการได้อย่างต่อเนื่องและทั่วถึง อีกทั้งยังมีหน่วยงานที่ดูแลรับผิดชอบที่มีความสามารถหลัก ๆ ก็คือ สสท.ทร. และ นขต.ทร. ประสานการทำงานร่วมกัน จัดฝึกอบรมให้ความรู้แก่เจ้าหน้าที่ที่มีหน้าที่ในทุก ๆหน่วยที่เกี่ยวข้อง ทำให้ระบบที่มีอยู่สามารถให้บริการได้อย่างมีประสิทธิภาพ

แหล่งข้อมูล

- บุคลากรที่มีประสบการณ์
- ศึกษาจาก WebSite ที่มีข้อมูลเกี่ยวข้องกับการใช้งานและการป้องกันระบบเครือข่าย

ความสำเร็จของการดำเนินการ

การรุกล้ำระบบเครือข่ายคอมพิวเตอร์และอินเตอร์เน็ตในหน่วยงานของส่วนราชการ โดยทั่วไปไม่ได้พบเห็นกันบ่อยนัก อาจจะเรียกได้ว่าเป็นเรื่องใหม่เลยก็ว่าได้ อย่างไรก็ตาม กรมสื่อสารและเทคโนโลยีสารสนเทศกองทัพเรือ (สสท.ทร.) ก็ได้เฝ้าระวัง ตรวจจับ ทดสอบ และฝึกอบรมให้แก่เจ้าหน้าที่ของตนเองและเจ้าหน้าที่ของหน่วยขึ้นตรงกองทัพเรือ เป็นประจำทุกปี ในห้วงเวลาหลายปีที่ผ่านมา เป็นการเพิ่มพูนทักษะ สร้างองค์ความรู้และเพิ่มประสบการณ์ในการป้องกันระบบเครือข่ายของหน่วยงานที่ตนเองรับผิดชอบ เมื่อเกิดเหตุการณ์วิกฤติที่ส่งผลกระทบในระดับภาพรวมขององค์กรหรือในระดับกองทัพ สสท.ทร. ก็สามารถดำเนินการตรวจสอบและป้องกันได้ทันท่วงที พร้อมทั้งได้ดำเนินการประสานและให้คำแนะนำแก่ จนท. หน่วยต่าง ๆ ในทันที ทั้งยังได้ให้คำแนะนำเกี่ยวกับเทคนิค วิธีการต่าง ๆ ในการป้องกันระบบเครือข่ายของหน่วยนั้น ๆ เพื่อไม่ให้ระบบเครือข่ายทั้งหมดเกิดการ “สะดุด” และต้องสามารถดำเนินการต่อไปได้อย่างต่อเนื่อง

กระบวนการต่าง ๆ อันเป็นปัจจัยทำให้เกิด

๑. การวางแผนงานที่ดี
๒. การปฏิบัติตามหน้าที่ที่รับผิดชอบ
๓. การประสานงานระหว่างหน่วยที่เกี่ยวข้อง (ยศ.ทร. ⇄ สสท.ทร.)
๔. ความพร้อมในการแก้ไขปัญหาที่อาจเกิดขึ้นได้

การถ่ายทอดและความยั่งยืน

หน่วยงานของ สสท.ทร. เป็นหน่วยงานที่มีหน้าที่รับผิดชอบโดยตรงในเรื่องที่เกี่ยวกับการใช้งานระบบเครือข่ายคอมพิวเตอร์และอินเตอร์เน็ตของกองทัพเรือ อีกทั้งยังมีหน้าที่ดำเนินการฝึกอบรมเกี่ยวกับเรื่องของการป้องกันการรุกล้ำระบบเครือข่ายคอมพิวเตอร์ ให้แก่ จนท. กรรมวิธีข้อมูลและสารสนเทศของ นขต. เป็นประจำทุกปี ในรอบ ๒-๓ ปีที่ผ่านมา สสท.ทร.ได้ดำเนินการอย่างต่อเนื่องและเป็นรูปธรรม ทำให้ จนท. หน่วยได้รับความรู้และประสบการณ์ต่าง ๆ เป็นอย่างดี สิ่งต่าง ๆ เหล่านี้ ถูกจัดเก็บด้วยเครื่องมือและวิธีการดังต่อไปนี้

๑. จัดเก็บความรู้ ด้วยเครื่องมือ KM ตามแบบการจัดเก็บความรู้ของ ยศ.ทร.
๒. จัดเก็บรวบรวมข้อมูลของการปฏิบัติงานของแผนกกรรมวิธีข้อมูล ไว้ที่เครื่องคอมพิวเตอร์ข้อมูลกลางของแผนกกรรมวิธีข้อมูล
๓. จัดเก็บข้อมูลไว้ในเว็บ KM Blog ในเว็บ KM ของ ยศ.ทร.
๔. จัดทำรูปเล่มเอกสาร KM วิธีปฏิบัติที่เป็นเลิศ“Best Practice.ทร.ของ ยศ ”