รายงานการประเมินความเสี่ยง
ด้านสารสนเทศและการแก้ไขปัญหา

สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม

เล่มที่ 3 / 4
รายงานผลการดำเนินการศึกษา ตรวจสอบ วิเคราะห์
ประเมินความเสี่ยงของระบบเครือข่าย
และระบบความปลอดภัยสารสนเทศ

ACIS บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด

รายละเอียดของเอกสาร

ผู้ว่าจ้าง:	สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม
ประเภทของเอกสาร:	รายงานผลการดำเนินการศึกษา ตรวจสอบ วิเคราะห์ ประเมินความเสี่ยงของระบบเครือข่าย และระบบความปลอดภัยสารสนเทศ
โครงการ:	โครงการจัดจ้างที่ปรึกษาประเมินความเสี่ยงด้านสารสนเทศและการแก้ไขปัญหา
บริษัทผู้จัดทำ	บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด
ผู้จัดทำ:	นายสรวุฒิ ก้องกิติกุล
ผู้ตรวจสอบ:	นายณพพร ทองใบประสิทธิ์

รายละเอียดการแก้ไขเอกสาร

เวอร์ชั่น	วันที่แก้ไข	รายละเอียด
1.0	23 มีนาคม 2552	รายงานการประเมินความเสี่ยงด้านสารสนเทศและการแก้ไขปัญหา
1.1	31 กรกฎาคม 2552	รายงานการประเมินความเสี่ยงด้านสารสนเทศและการแก้ไขปัญหา (ฉบับสมบูรณ์)

สารบัญ

สารบัญ (ต่อ)

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญตาราง (ต่อ)

สารบัญตาราง (ต่อ)

สารบัญตาราง (ต่อ)

สารบัญตาราง (ต่อ)

สารบัญตาราง (ต่อ)

สารบัญตาราง (ต่อ)

สารบัญตาราง (ต่อ)

สารบัญตาราง (ต่อ)

สารบัญตาราง (ต่อ)

สารบัญตาราง (ต่อ)

สารบัญตาราง (ต่อ)

สารบัญภาพ

หน้า

สารบัญภาพ (ต่อ)

สารบัญภาพ (ต่อ)

สารบัญภาพ (ต่อ)

ส่วนที่ 2.1

รายงานการสำรวจสถานภาพด้านความปลอดภัยของระบบเครือข่าย

และระบบความปลอดภัยคอมพิวเตอร์

ความนำ

สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม มีความประสงค์ที่จะสำรวจสถานภาพด้านความปลอดภัย เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ซึ่งเป็นส่วนหนึ่งในโครงการพัฒนาระบบรักษาความปลอดภัยข้อมูลและระบบคอมพิวเตอร์ โดยเป้าหมายของการสำรวจสถานภาพด้านความปลอดภัยเครื่องคอมพิวเตอร์แม่ข่าย ในครั้งนี้ประกอบด้วย เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย รวมทั้งสิ้น 62 เครื่อง โดยได้ทำการสำรวจสถานภาพด้านความปลอดภัยเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย เมื่อวันที่ 15, 20 และ 21 มกราคม 2552 ชั้น 10 ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โดยใช้โปรแกรมในการตรวจสอบได้แก่ Internet Scanner (ISS), X-Scan และ Nessus โดยโปรแกรมดังกล่าวจะตรวจสอบ Port / Service ที่เกิดช่องโหว่ในแต่ละเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย โดยจะบ่งบอกบอกถึงผลกระทบของช่องโหว่และระดับความเสี่ยงที่เกิดขึ้น หากมีผู้บุกรุกทำการบุกรุกเข้ามายัง Port / Service ต่าง ๆ ที่เกิดช่องโหว่ ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย

ในการสำรวจสถานภาพด้านความปลอดภัย เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ครั้งนี้ บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด ได้ดำเนินการตามขอบเขตการดำเนินงานดังต่อไปนี้

- ขอบเขตการดำเนินงานข้อ 3.2.1.1: สำรวจ วิเคราะห์และประเมินจุดอ่อนของระบบหรือช่องโหว่ โดยทั่วไปของระบบคอมพิวเตอร์ การตั้งค่าของระบบคอมพิวเตอร์ (Configuration) เช่น ค่า Default ต่าง ๆ, Password Policy, Patch ด้วยรูปแบบการใช้ Utility Software หรือ ใช้เทคนิคต่าง ๆ ตามรายละเอียดดังนี้
    1) เร้าเตอร์ ไฟล์วอล์และสวิทส์ (Router, Firewall and Switch) ไม่น้อยกว่า 10 เครื่อง
    2) เครื่องคอมพิวเตอร์แม่ข่าย (Server) ไม่น้อยกว่า 40 เครื่อง
    3) เครื่องคอมพิวเตอร์ลูกข่าย (Client) ไม่น้อยกว่า 10 เครื่อง
- ขอบเขตการดำเนินงานข้อ 3.2.4: หลีกเลี่ยงแบบทดสอบที่อาจจะก่อให้เกิดการหยุดชะงักของระบบงาน เช่น การใช้แบบทดสอบ Denial of Service ตามความเห็นชอบของสำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อมที่จะกำหนดให้มีการทดสอบในเครื่องทดสอบแทน
- ขอบเขตการดำเนินงานข้อ 3.2.5: นำเสนอรายงานในรูปแบบแสดงระดับความเสี่ยงโดยเปรียบเทียบกับการควบคุม และวิธีปฏิบัติงานตามความเห็นชอบของสำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม พร้อมข้อเสนอแนะและแนวทางที่เหมาะสมในการปรับปรุง รวมทั้งออกแบบระบบความปลอดภัยของระบบเครือข่ายและความปลอดภัยคอมพิวเตอร์ของสำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม รองรับการขยายการบริการ และรองรับกฎ ระเบียบและข้อบังคับด้านความมั่นคงปลอดภัยระบบสารสนเทศและการสื่อสาร หรือมาตรฐานด้านความปลอดภัยระบบสารสนเทศที่เกี่ยวข้อง

- ขอบเขตการดำเนินงานข้อ 3.2.6: เมื่อค้นพบช่องโหว่ หรือข้อมูลสำคัญ ซึ่งอาจจะทำให้สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อมตกอยู่ในสถานะหรือสภาวะต่อการรั่วไหล หรือการหยุดชะงักของระบบคอมพิวเตอร์ ต้องมีการแจ้งเตือนเพื่อขออนุญาตดำเนินงานต่อไป
- ขอบเขตการดำเนินงานข้อ 3.2.7: หากเจ้าหน้าที่ดำเนินการค้นพบช่องโหว่ที่นอกเหนือจากรายการที่แจ้งไว้ จะต้องแจ้งให้สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อมให้ความเห็นชอบก่อนเข้าดำเนินการ ทั้งนี้ในระหว่างการดำเนินโครงการฯ ที่ปรึกษาจะต้องจัดเจ้าหน้าที่เพื่อให้คำแนะนำ ตอบคำถาม และให้การช่วยเหลือทางโทรศัพท์และพร้อมที่จะเข้าไปช่วยในกรณีเร่งด่วน โดยต้องอยู่ในขอบเขตการดำเนินโครงการฯ
- ขอบเขตการดำเนินงานข้อ 3.2.8: ดำเนินการวิเคราะห์และให้คำแนะนำ ในกรณีที่ระบบเครือข่ายของสำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม จำเป็นต้องได้รับการติดตั้งระบบ หรืออุปกรณ์เพิ่มเติม เพื่อเป็นการเพิ่มระดับการรักษาความปลอดภัยของระบบเครือข่ายและความปลอดภัยคอมพิวเตอร์ของสำนักงานปลัดกระทรวงทรัพย์ฯ สามารถเสนอเพื่อดำเนินการได้ทั้งนี้จะต้องไม่คิดค่าใช้จ่ายเพิ่มเติม

บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด ได้เสร็จสิ้นการสำรวจสถานภาพด้านความปลอดภัย เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อมแล้ว บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด ได้จัดทำเอกสารรายงานการสำรวจสถานภาพด้านความปลอดภัย เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย (Vulnerability Assessment Report) เพื่อนำเสนอผลการทดสอบต่อ สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม เพื่อให้ฝ่ายต่าง ๆ ที่เกี่ยวข้องได้รับทราบ และดำเนินการแก้ไขต่อไป

การสำรวจสถานภาพด้านความปลอดภัยนั้น เป็นผลที่ได้จากการสำรวจในช่วงเวลาหนึ่งเท่านั้น ซึ่งไม่ได้หมายความว่าหากมีการปรับปรุงทั้งหมดแล้ว ระบบสารสนเทศดังกล่าว จะไม่มีความเสี่ยงต่อภัยคุกคามใด ๆ อีกตลอดไป จึงเป็นการดีหาก สป.ทส. จะได้มีการสำรวจสถานภาพด้านความปลอดภัยอย่างต่อเนื่องเป็นประจำ เพื่อให้เกิดความมั่นใจว่าสถานภาพด้านความปลอดภัยในระบบของ สป.ทส. จะยังคงมีความปลอดภัยอย่างต่อเนื่อง การสำรวจสถานภาพด้านความปลอดภัยทั้งหมดในรายงานฉบับนี้ ไม่ได้มีเจตนาที่จะจับผิดการทำงานของแต่ละแผนกหรือแต่ละบุคคลที่เกี่ยวข้องกับระบบของ สป.ทส. แต่อย่างใด แต่ทั้งนี้เพื่อรายงานสถานะความปลอดภัยของระบบ ทุกฝ่ายควรใช้รายงานผลการสำรวจนี้ในการแก้ไขปัญหาร่วมกันเพื่อให้เกิดประโยชน์สูงสุด และความปลอดภัยสูงสุดในระบบสารสนเทศของ สป.ทส. ที่ปรึกษา มีความยินดีหากจะได้มีโอกาสสำรวจสถานภาพด้านความปลอดภัยระบบสารสนเทศให้กับ สป.ทส. ในครั้งต่อ ๆ ไป

เพื่อความสะดวกในการอ่านรายงานฉบับนี้ บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด จะเปลี่ยนการนำเสนอจากชื่อเต็มเป็นการใช้ชื่อย่อ ดังนี้

ชื่อเต็ม	ชื่อย่อที่ใช้
สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม	สป.ทส.
บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด	ที่ปรึกษา
โครงการจัดจ้างที่ปรึกษาประเมินความเสี่ยงด้านสารสนเทศและการแก้ไขปัญหา	โครงการฯ
การสำรวจสถานภาพด้านความปลอดภัย เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่าย	การสำรวจสถานภาพด้านความปลอดภัย

บทสรุปสำหรับผู้บริหาร

ที่ปรึกษา ดำเนินการสำรวจสถานภาพด้านความปลอดภัย โดยมีรายละเอียดของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ที่ดำเนินการตรวจสอบสถานภาพด้านความปลอดภัย ดังนี้

ตารางที่ 1 รายละเอียดจำนวนเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย

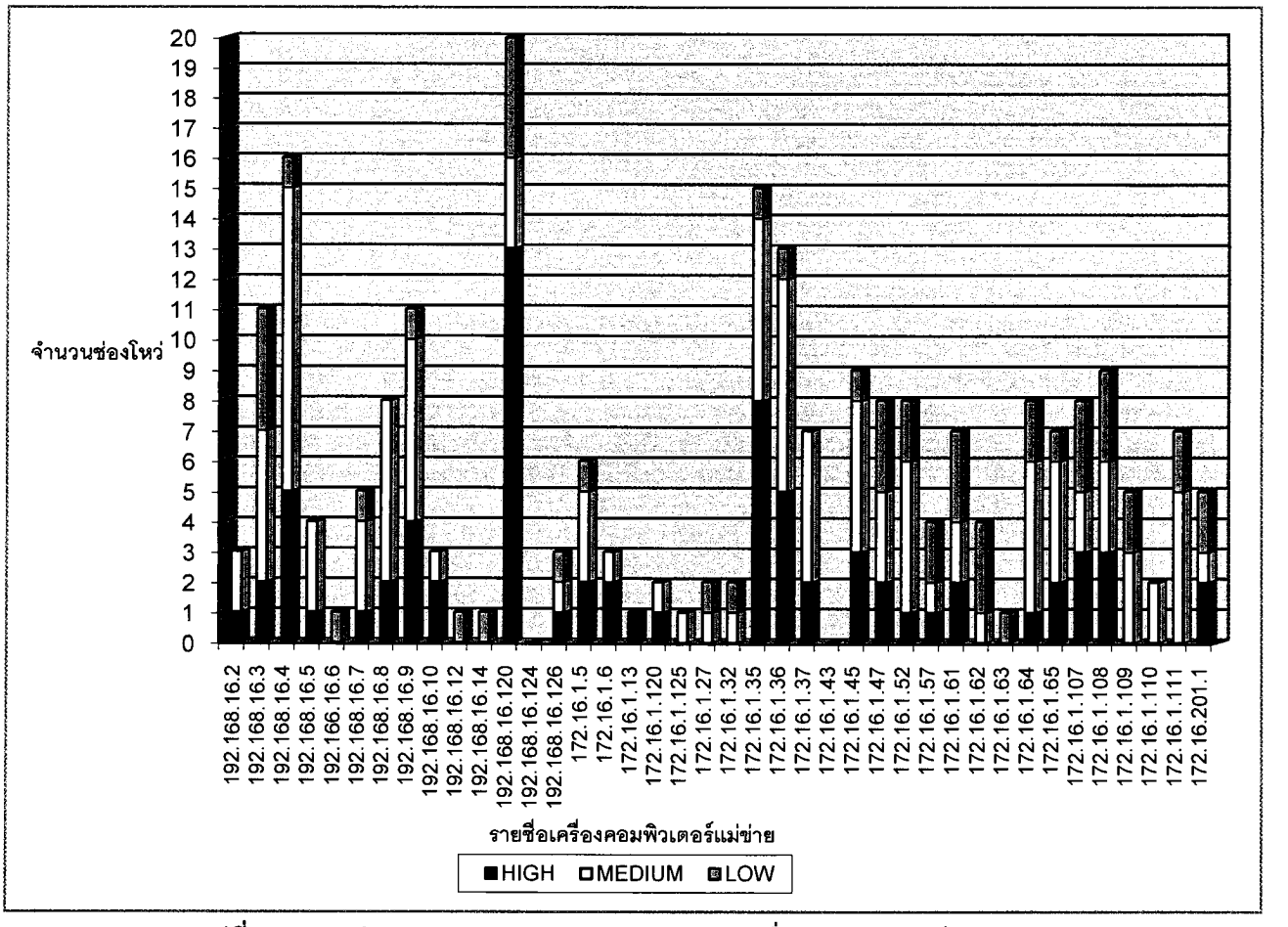
เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย	จำนวน
Servers Computer	40 เครื่อง
Network Devices	12 เครื่อง
Client Computer	10 เครื่อง
รวมทั้งสิ้น	**62 เครื่อง**

ผลลัพธ์จากการตรวจสอบสถานภาพด้านความปลอดภัย จะแสดงรายละเอียดของการเปิด Port / Service ที่เครื่องคอมพิวเตอร์แม่ข่าย นั้นเปิดอยู่ และแสดงช่องโหว่ที่พบใน Port / Service ที่เปิดอยู่ พร้อมทั้งแสดงระดับความเสี่ยงที่ตรวจพบ โดยในการประเมินระดับความเสี่ยงนั้น ที่ปรึกษา ได้จำแนกเป็น 3 ระดับได้แก่

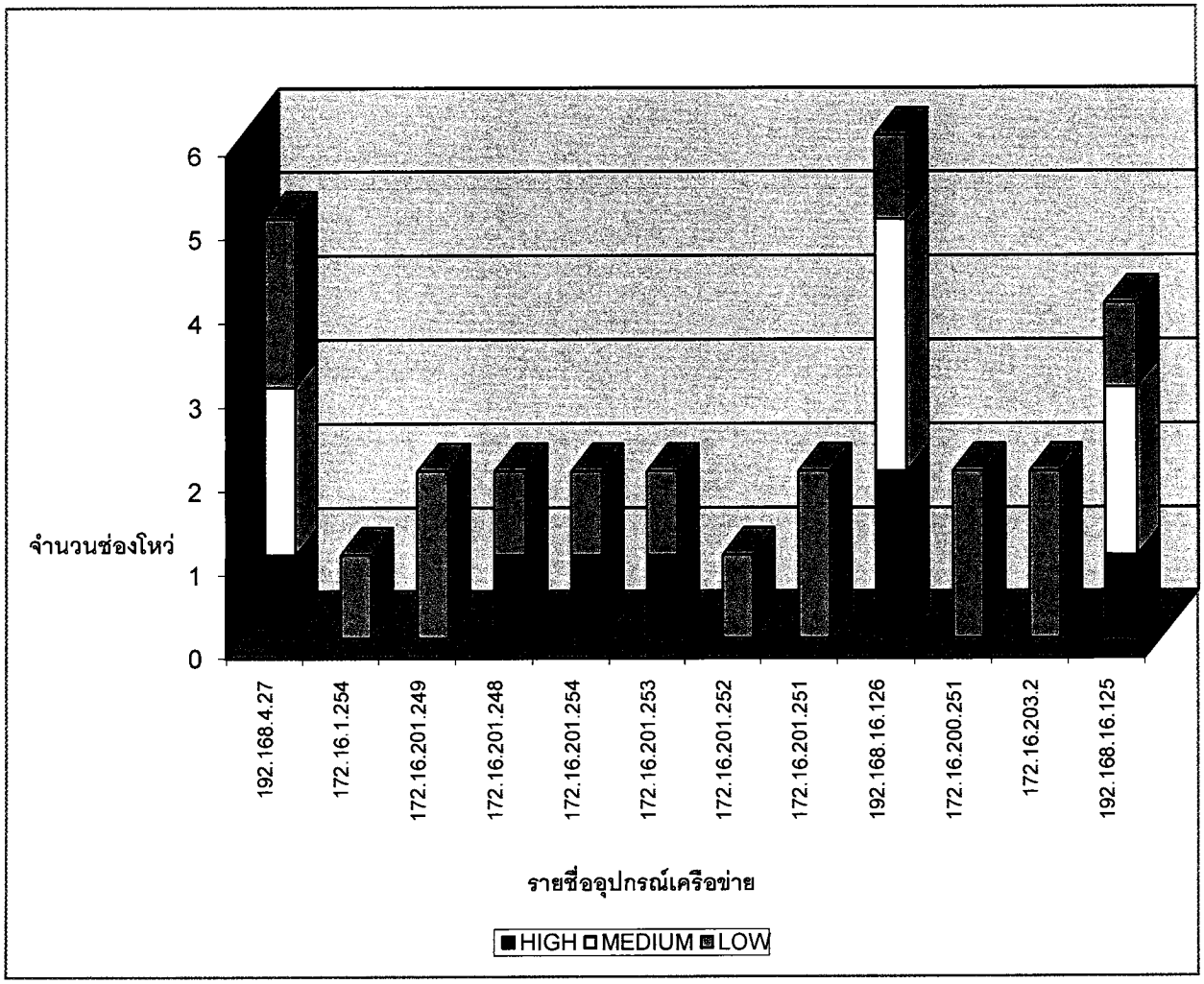
ตารางที่ 2 รายละเอียด เกี่ยวกับระดับความเสี่ยง

ระดับความเสี่ยง	รายละเอียด
สูง (HIGH)	เครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์เครือข่ายมีโอกาสที่จะถูกโจมตีจากผู้บุกรุก และสามารถควบคุมเครื่องคอมพิวเตอร์แม่ข่าย หรืออุปกรณ์เครือข่ายโดยสมบูรณ์ หากการประเมินจุดอ่อน หรือช่องโหว่นั้นไม่ได้ทำการแก้ไข
ปานกลาง (MEDIUM)	เครื่องคอมพิวเตอร์แม่ข่าย หรืออุปกรณ์เครือข่ายมีโอกาสที่ผู้บุกรุกจะสามารถเอาข้อมูลจากเครื่องเป้าหมายไปใช้ประโยชน์
ต่ำ (LOW)	เครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์เครือข่ายนั้นแสดงข้อมูลที่เป็นประโยชน์ต่อการโจมตีจากผู้บุกรุก

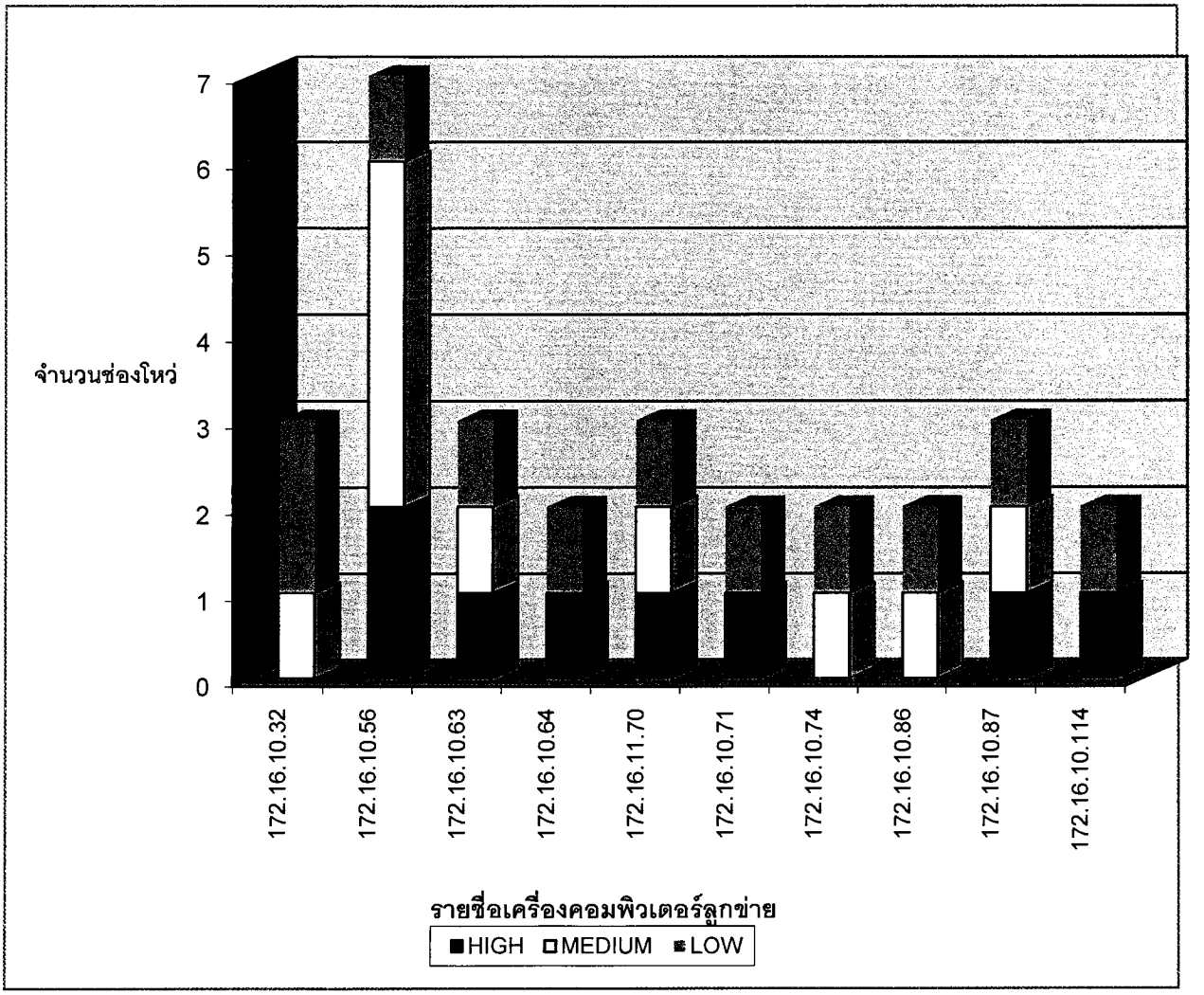
ในการสำรวจสถานภาพด้านความปลอดภัย ที่ปรึกษาได้จัดทำกราฟที่แสดงผลของการสำรวจสถานภาพความปลอดภัยของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย



รูปที่ 1 ผลการสำรวจสถานภาพความปลอดภัยของเครื่องคอมพิวเตอร์แม่ข่าย



รูปที่ 2 ผลการสำรวจสถานภาพความปลอดภัยของอุปกรณ์เครือข่าย



รูปที่ 3 ผลการสำรวจสถานภาพความปลอดภัยของเครื่องคอมพิวเตอร์ลูกข่าย

ผลการสำรวจสถานภาพด้านความปลอดภัย

ในการรายงานผลของการสำรวจสถานภาพด้านความปลอดภัยระบบเครือข่ายและระบบความปลอดภัยคอมพิวเตอร์ ที่ปรึกษาได้แบ่งการรายงานเป็น 3 ส่วนคือ

1. รายละเอียดของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ซึ่งเป็นการสรุปเป้าหมายทั้งหมดในการสำรวจสถานภาพครั้งนี้

2. ผลการสำรวจสถานภาพด้านความปลอดภัยเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ซึ่งแสดงรายละเอียดของการสำรวจ โดยจำแนกเป็นแต่ละหมายเลขไอพี

3. ผลการวิเคราะห์ช่องโหว่ในเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ซึ่งเป็นส่วนที่ชี้ให้เห็นสาเหตุของช่องโหว่ที่เกิดขึ้น นอกจากสาเหตุแล้วยังประกอบด้วยคำแนะนำเพื่อแก้ไขตามสาเหตุนั้น ๆ

1. รายละเอียดของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย

1.1 รายละเอียดของเครื่องคอมพิวเตอร์แม่ข่าย

ตารางที่ 3 รายละเอียดของเครื่องคอมพิวเตอร์แม่ข่าย

ลำดับที่	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	หมายเลขไอพี	หน้าที่	ระบบปฏิบัติการ
1	PXMNRE	192.168.16.2	Web กระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม	Windows Server 2003
2	EDOC	192.168.16.3	DCS / ระบบสารบรรณ	Windows Server 2003 SP2
3	ZINC	192.168.16.4	E-Mail / บริการเมล์	UNIX Sun Solaris 9
4	COPPER	192.168.16.5	E-Project Tracking / ระบบติดตามโครงการ	Windows Server 2003
5	MECURY	192.168.16.6	Database	Unix Sun Solaris 8
6	E-PETITION	192.168.16.7	E-Petition / รับเรื่องร้องเรียน	Linux Kernel 2.6
7	KNOWNLEDGE	192.168.16.8	KM Server	Linux Kernel 2.6
8	MISMNRE	192.168.16.9	MIS/ระบบสารสนเทศ	Windows Server 2003

ลำดับที่	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	หมายเลขไอพี	หน้าที่	ระบบปฏิบัติการ
			เพื่อการสื่อสาร	
9	EPROJECT	192.168.16.10	Web กลุ่มพัฒนาระบบบริหาร สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม	Windows Server 2000
10	IS~WALLBOARD	192.168.16.12	MMS Server	Unix Sun Solaris 8
11	NICNATURAL	192.168.16.14	โครงการ NIC	Unix Sun Solaris 8
12	CICTDB	192.168.16.120	Test Server	Windows XP SP2
13	EMERALD	192.168.16.124	DNS ภายนอก	Linux Kernel 2.6
14	FIREWALL	192.168.16.126	Firewall	Unix Sun Solaris 8
15	TEST1	172.16.1.5	Test Server	Windows Server 2003 SP1
16	TEST2	172.16.1.6	Test Server	Windows Server 2003 SP1
17	Ups1849	172.16.1.13	UPS Management	Windows Vista
18	TEST3	172.16.1.20	Test Server	Windows Server 2003 SP1
19	TOT	172.16.1.25	Test Server	Windows Server 2003
20	DOCFILESERV1	172.16.1.27	Web server	Windows Server 2003
21	DOCFILESERV2	172.16.1.32	File server	Windows Server 2003
22	DATATRAINING	172.16.1.35	ระบบข่าว / Database	Windows XP Pack 2
23	GISFILESERVER	172.16.1.36	File server	Windows Server 2003 SP2
24	INVENT	172.16.1.37	Web ระบบทะเบียนครุภัณฑ์	Linux 2.6 on Red Hat Enterprise Linux 5
25	GSERVER	172.16.1.43	Web ความหลากหลายทางชีวภาพ	Windows Server 2003 SP2
26	WAREHOUSE	172.16.1.45	Web Portal	Windows Server 2003 SP2
27	INTEL_SERVER	172.16.1.47	Web สำนักพัฒนาบริหารทรัพยากร	Windows Server 2003 SP2

ลำดับที่	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	หมายเลขไอพี	หน้าที่	ระบบปฏิบัติการ
			ธรรมชาติและสิ่งแวดล้อม	
28	GISWEB	172.16.1.52	Web ภูมิสารสนเทศ	Windows Server 2003 SP1
29	GOOGLEMNRE	172.16.1.57	ระบบสนับสนุนศูนย์ปฏิบัติการกระทรวงฯในรูปภูมิสารสนเทศบน Google Earth	Windows Server 2003 SP1
30	AVMNRE	172.16.1.61	Anti Virus	Windows Server 2003 SP2
31	MMNRE	172.16.1.62	Anti Spam	Windows Server 2003 SP2
32	OMESERV	172.16.1.63	Web Server	Windows Server 2003 SP2
33	LITHUIM	172.16.1.64	Tape Backup	Windows Server 2003 SP2
34	SERVER	172.16.1.65	Web สำนักความร่วมมือด้านทรัพยากรธรรมชาติและสิ่งแวดล้อมระหว่างประเทศ	Windows Server 2003 SP2
35	BACKUP-SERVER	172.16.1.107	Backup Server	Windows Server 2003 SP2
36	LOG-MANAGEMENT	172.16.1.108	Log Server	Windows Server 2003 SP2
37	DDMNRE	172.16.1.109	DHCP	Windows Server 2003 SP2
38	DNSMNRE	172.16.1.110	DNS	Linux Kernel 2.6
39	ADMNRE	172.16.1.111	Domain Active Directory	Windows Server 2003 SP2
40	NMS	172.16.201.1	Network Management Server	Windows Server 2003 SP1

1.2 รายละเอียดของ อุปกรณ์เครือข่าย

ตารางที่ 4 รายละเอียดของอุปกรณ์เครือข่าย

ลำดับที่	หมายเลขไอพี	หน้าที่	ระบบปฏิบัติการ
1	192.168.4.27	NetApp	NetApp Release 7.2.3
2	172.16.1.254	Switch	CISCO IOS 12.1
3	172.16.201.249	Switch	CISCO IOS 12.4
4	172.16.201.248	Router	Allied Telesyn AR320 Router
5	172.16.201.254	Router	Allied Telesyn AR320 Router
6	172.16.201.253	Router	Allied Telesyn AR320 Router
7	172.16.201.252	Switch	CISCO IOS 12.1
8	172.16.201.251	Switch	3Com SuperStack Switch
9	192.168.16.126	Firewall	Sun Solaris 8
10	172.16.200.251	Switch	3Com SuperStack Switch
11	172.16.203.2	Switch	CISCO IOS 12.1
12	192.168.16.125	Switch	Switch Alcatel

1.3 รายละเอียดของเครื่องคอมพิวเตอร์ลูกข่าย

ตารางที่ 5 รายละเอียดของเครื่องคอมพิวเตอร์ลูกข่าย

ลำดับที่	ชื่อเครื่องคอมพิวเตอร์ลูกข่าย	หมายเลขไอพี	หน้าที่	ระบบปฏิบัติการ
1	HOME-9481A27B35	172.16.10.32	Personal Computer	Microsoft Windows XP Professional
2	EDIT1	172.16.10.56	Personal Computer	Microsoft Windows XP Professional
3	AB10OUTXXMOC004	172.16.10.63	Personal Computer	Microsoft Windows XP Professional
4	AA11CICTK01	172.16.10.64	Personal Computer	Microsoft Windows XP Professional
5	MICROSOF-F44D0A	172.16.10.71	Personal Computer	Microsoft Windows XP Professional
6	TR14	172.16.10.74	Personal Computer	Microsoft Windows XP Professional
7	LENOVO-02AA5E49	172.16.10.86	Personal Computer	Microsoft Windows XP Professional
8	TR44	172.16.10.87	Personal Computer	Microsoft Windows XP Professional
9	IBMC1044	172.16.10.114	Personal Computer	Microsoft Windows XP Professional
10	IBM-D9FE7233D4	172.16.11.70	Personal Computer	Microsoft Windows XP Professional

2. ผลการสำรวจสถานภาพด้านความปลอดภัยเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย

ที่ปรึกษาได้สำรวจสถานภาพด้านความปลอดภัย เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย โดยมีรายละเอียดดังต่อไปนี้

2.1 ผลการสำรวจสถานภาพด้านความปลอดภัยของเครื่องคอมพิวเตอร์แม่ข่าย

2.1.1 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 1: PXMNRE

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	PXMNRE
หน้าที่	Web กระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม
ระบบปฏิบัติการ	Windows Server 2003
IP Address	192.168.16.2

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 6 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย PXMNRE

No.	Port / Service	Port Number
1	ftp	21/tcp
2	http	80/tcp
3	MySql	3306/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 7 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย PXMNRE

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
ftp (21/tcp)	1	FTP-Password: "anonymous/[Blank password]"	HIGH
http (80/tcp)	2	HTTP TRACE / TRACK Methods	MEDIUM
	3	Apache < 2.2.9 Multiple Vulnerabilities (DoS, XSS)	MEDIUM

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ทำการ Disable user anonymous

ลำดับที่ 2-3 : ทำการ Upgrade Apache ให้มีเวอร์ชั่นที่สูงกว่า 2.2.9

2.1.2 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 2: EDOC

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	EDOC
หน้าที่	DCS/ ระบบสารบรรณ
ระบบปฏิบัติการ	Windows Server 2003 SP2
IP Address	192.168.16.3

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 8 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย EDOC

No.	Port / Service	Port Number
1	Domain	53/udp
2	Ldaps	636/tcp
3	Ms-sql-s	1433/tcp
4	Domain	53/tcp
5	Netbios-ns	137/udp
6	Ms-sql-m	1434/udp
7	Microsoft-ds	445/tcp
8	Ntp	123/udp
9	ftp	21/tcp
10	Netbios-ssn	139/tcp
11	http	80/tcp
12	Smtp	25/tcp
13	Epmap	135/tcp
14	Ldap	389/tcp
15	Windows Terminal Services	3389/tcp
16	https	443/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 9 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย EDOC

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
ftp (21/tcp)	1	FTP-Password: "anonymous/[Blank password]"	HIGH
	2	FTP-Password: "ftp/[Blank password]"	HIGH
Domain (53/udp)	3	The remote DNS Server is vulnerable to cache snooping attacks.	MEDIUM
	4	DNS Server Recursive Query Enabled	MEDIUM
Ldap (389/tcp)	5	LDAP allows anonymous binds	MEDIUM
	6	LDAP allows null bases	MEDIUM
	7	Use LDAP search request to retrieve information from NT Directory Services	MEDIUM
Windows Terminal Services (3389/tcp)	8	Windows Terminal Service Enabled	LOW
Netbios-ns (137/udp)	9	Using NetBIOS to retrieve information from a Windows host	LOW
Microsoft-ds (445/tcp)	10	SMB LanMan Pipe Server browse listing	LOW
http (80/tcp)	11	Find if IIS Server allows BASIC and/or NTLM authentication	LOW

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1-2 : ทำการ Disable user anonymous และทำการ เปลี่ยนรหัสผ่าน ftp ให้มีความซับซ้อนมากยิ่งขึ้น

ลำดับที่ 3-4 : กำหนดสิทธิ์ในการเรียกใช้ nameserver เฉพาะเครื่องคอมพิวเตอร์แม่ข่ายที่จำเป็นต้องใช้บริการ nameserver จากเครื่องนี้

ลำดับที่ 5-7 : - ทำการ กำหนดค่า LDAP Server so that it does not allow NULL BINDs

- ทำการ Disable NULL BASE queries on your LDAP Server

ลำดับที่ 8 : - หากไม่มีการใช้งาน Windows Terminal Services ควรทำการ Disable

- หากจำเป็นต้องใช้งาน ไม่ควรมีการเปิดสิทธิ์แบบ allow ควรมีการตรวจสอบสิทธิ์การใช้งาน

ลำดับที่ 9 : ผู้บุกรุกสามารถเข้าถึงข้อมูลที่สำคัญเช่นคอมพิวเตอร์ชื่อเวิร์กกรุ๊ป, ชื่อปัจจุบันล็อกอินชื่อผู้ใช้ เป็นต้น แต่ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์แม่ข่าย

ลำดับที่ 10 : เป็นไปได้ที่ผู้บุกรุกจะสามารถได้รับข้อมูลเกี่ยวกับเครื่องคอมพิวเตอร์ในเครือข่าย แต่ไม่มีผลกระทบกกับเครื่องคอมพิวเตอร์

ลำดับที่ 11 : หากมีการใช้งาน IIS ที่ Allows หรือมีการตั้งค่ารหัสผ่านที่ไม่ซับซ้อนก็อาจทำให้ผู้บุกรุกสามารถเข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย ดังนั้นควรมีการตรวจสอบการตั้งค่ารหัสผ่าน แต่ก็ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์

2.1.3 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 3: ZINC

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	ZINC
หน้าที่	E-mail/ บริการเมล์
ระบบปฏิบัติการ	Unix Sun Solaris 9
IP Address	192.168.16.4

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 10 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย ZINC

No.	Port / Service	Port Number
1	Smtp	25/tcp
2	ftp	21/tcp
3	Mysql	3306/tcp
4	Ssh	22/tcp
5	https	443/tcp
6	Imaps	993/tcp
7	http	80/tcp
8	Ntp	123/udp
9	Domain	53/tcp
10	Domain	53/udp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 11 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย ZINC

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Mysql (3306/tcp)	1	MySQL User-Defined Function Buffer Overflow Vulnerability	MEDIUM
	2	MySQL Remote Insecure Default Password Vulnerability	HIGH
	3	MySQL mysqlhotcopy script insecure temporary file	MEDIUM
	4	MySQL multiple flaws (2)	MEDIUM

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
	5	MySQL buffer overflow	MEDIUM
	6	MySQL Anonymous Login Handshake Remote Information Disclosure	MEDIUM
https (443/tcp) http (80/tcp)	7	HTTP TRACE / TRACK Methods	MEDIUM
	8	WebDAV enabled	LOW
	9	Apache < 2.0.59	HIGH
	10	Apache < 2.0.63 Multiple XSS Vulnerabilities	MEDIUM
	11	PHP < 4.4.5 Multiple Vulnerabilities	HIGH
	12	PHP < 4.4.1 / 5.0.6 Multiple Vulnerabilities	HIGH
	13	Apache mod_proxy_ftp Directory Component Wildcard Character Globbing XSS	MEDIUM
Domain (53/udp)	14	DNS Cache Snooping	MEDIUM
	15	DNS Server Recursive Query Enabled	MEDIUM
	16	Remote DNS Resolver Uses Non-Random Ports	HIGH

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1-6 : - ทำการตั้งค่ารหัสผ่านให้มีความซับซ้อน

- ทำการ Upgrade MySql ให้มีเวอร์ชั่นที่สูงกว่า 4.0.25 เป็นอย่างน้อย

- ควรมีการกำหนดสิทธิ์ IP บนเครื่องคอมพิวเตอร์แม่ข่ายที่จะเข้าถึง Database

ลำดับที่ 7-13 :-ติดตั้ง Patch: http://www.microsoft.com/technet/security/bulletin/ms03-039.mspx

-หากไม่มีการใช้งาน WebDEV ควรทำการ Disable

-ทำการอัพเกรด PHP ให้มี version สูงกว่า 4.4.1

-ทำการอัพเกรด Apache ให้มี version สูงกว่า 2.0.59

ลำดับที่ 14-16 : -กำหนดสิทธิ์ในการเรียกใช้ nameserver เฉพาะเครื่องคอมพิวเตอร์แม่ข่ายที่จำเป็นต้องใช้บริการ nameserver จากเครื่องนี้

2.1.4 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 4: COPPER

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	COPPER
หน้าที่	E-Project Tracking/ ระบบติดตามโครงการ
ระบบปฏิบัติการ	Windows Server 2003
IP Address	192.168.16.5

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 12 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย COPPER

No.	Port / Service	Port Number
1	Windows Terminal Services	3389/tcp
2	ftp	21/tcp
3	Mysql	3306/tcp
4	http	80/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 13 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย COPPER

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
http (80/tcp)	1	Web Server Uses Plain Text Authentication Forms	MEDIUM
	2	HTTP TRACE / TRACK Methods	MEDIUM
	3	Apache < 2.2.9 Multiple Vulnerabilities (DoS, XSS)	MEDIUM
	4	PHP 5 < 5.2.7 Multiple Vulnerabilities	HIGH

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1-4 : - ทำการอัพเกรด PHP ให้มี version สูงกว่า 5.2.7

- ทำการอัพเกรด Apache ให้มี version สูงกว่า 2.2.9

2.1.5 เครื่องคอมพิวเดอร์แม่ข่ายลำดับที่ 5: MECURY

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	MECURY
หน้าที่	Database
ระบบปฏิบัติการ	Unix Sun Solaris 8
IP Address	192.168.16.6

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 14 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเดอร์แม่ข่าย MECURY

No.	Port / Service	Port Number
1	ftp	21/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 15 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย MECURY

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
ftp (21/tcp)	1	FTP Clear Text Authentication	LOW

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : หากไม่มีการใช้งาน ควรทำการ Disable หากใช้งานควรเปลี่ยนไปใช้ SSH แทน

2.1.6 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 6: E-PETITION

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	E-PETITION
หน้าที่	E-Petition/ ระบบรับเรื่องร้องเรียน
ระบบปฏิบัติการ	Linux Kernel 2.6
IP Address	192.168.16.7

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 16 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย E-PETITION

No.	Port / Service	Port Number
1	ftp	21/tcp
2	Ssh	22/tcp
3	http	80/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 17 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย E-PETITION

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
http (80/tcp)	1	Web Server hosting copyrighted material	MEDIUM
	2	JBoss Enterprise Application Platform (EAP) Status Servlet Request Remote Information Disclosure	MEDIUM
	3	Web Server Cross Site Scripting	MEDIUM
	4	Test HTTP dangerous methods	HIGH
	5	Apache UserDir Sensitive Information Disclosure	LOW

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1-5 : - ทำการ Delete files ที่ไม่จำเป็นออก

- ทำการ Upgrade to JBoss EAP version 4.2.0.CP03 / 4.3.0.CP01.
- ทำการ Disable Test HTTP dangerous method

- ทำการ Disable โดยวิธการเปลี่ยน 'UserDir public_html' (or whatever) to 'UserDir disabled'.
- ทำการใช้ RedirectMatch โดยการแก้ไขที่ Apache

2.1.7 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 7: KNOWNLEDGE

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	KNOWNLEDGE
หน้าที่	KM Server
ระบบปฏิบัติการ	Linux Kernel 2.6
IP Address	192.168.16.8

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 18 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย KNOWNLEDGE

No.	Port / Service	Port Number
1	ftp	21/tcp
2	Mysql	3306/tcp
3	Ssh	22/tcp
4	http	80/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 19 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย KNOWNLEDGE

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Mysql (3306/tcp)	1	MySQL User-Defined Function Buffer Overflow Vulnerability	MEDIUM
	2	MySQL multiple flaws (2)	MEDIUM
	3	MySQL Anonymous Login Handshake Remote Information Disclosure	MEDIUM
http (80/tcp)	4	Web Server hosting copyrighted material	MEDIUM
	5	Web Server Uses Plain Text Authentication Forms	MEDIUM
	6	HTTP TRACE / TRACK Methods	MEDIUM
	7	PHP < 4.4.5 Multiple Vulnerabilities	HIGH
	8	PHP < 4.4.1 / 5.0.6 Multiple Vulnerabilities	HIGH

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1-3 :- ทำการ Upgrade MySql ให้มีเวอร์ชั่นที่สูงกว่า 4.0.25 เป็นอย่างน้อย

- ควรมีการกำหนดสิทธิ์ IP บนเครื่องคอมพิวเตอร์แม่ข่ายที่จะเข้าถึง Database

ลำดับที่ 4-8 : - ทำการ Delete files ที่ไม่จำเป็นออก

- ทำการ Disable HTTP TRACE / TRACK Methods

- ทำการ Upgrade PHP ให้มีเวอร์ชั่นที่สูงกว่า 4.4.1

2.1.8 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 8: MISMNRE

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	MISMNRE
หน้าที่	MIS/ ระบบสารสนเทศเพื่อการบริหาร
ระบบปฏิบัติการ	Windows Server 2003
IP Address	192.168.16.9

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 20 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย MISMNRE

No.	Port / Service	Port Number
1	ftp	21/tcp
2	Mysql	3306/tcp
3	http	80/tcp
4	Windows Terminal Services	3389/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 21 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย MISMNRE

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Windows Terminal Services (3389/tcp)	1	Windows Terminal Service Enabled	LOW
	2	Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure Vulnerability	MEDIUM
ftp (21/tcp)	3	FTP-Password: "ftp/[Password is same as username]"	HIGH
	4	FTP-Password: "anonymous/[Blank password]"	HIGH
Mysql (3306/tcp)	5	Unpassworded MySQL	HIGH
	6	MySQL Authentication bypass through a zero-length password	HIGH
	7	MySQL password handler overflaw	MEDIUM
	8	MySQL multiple flaws (2)	MEDIUM

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
	9	MySQL buffer overflow	MEDIUM
	10	MySQL Anonymous Login Handshake Remote Information Disclosure	MEDIUM
http (80/tcp)	11	Web Server Uses Plain Text Authentication Forms	MEDIUM

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1-2 : - หากไม่มีการใช้งาน Windows Terminal Services ควรทำการ Disable

- หากจำเป็นต้องใช้งาน ไม่ควรมีการเปิดสิทธิ์แบบ allow ควรมีการตรวจสอบสิทธิ์การใช้งาน

ลำดับที่ 3-4 : - ทำการ Disable user anonymous และทำการ เปลี่ยนรหัสผ่าน ftp ให้มีความซับซ้อนมากยิ่งขึ้น

ลำดับที่ 5-10 : - ทำการตั้งค่ารหัสผ่านให้มีความซับซ้อน

- ทำการ Upgrade MySql ให้มีเวอร์ชั่นที่สูงกว่า 4.0.25 เป็นอย่างน้อย

- ควรมีการกำหนดสิทธิ์ IP บนเครื่องคอมพิวเตอร์แม่ข่ายที่จะเข้าถึง Database

ลำดับที่ 11 : ทำการตัวสอบผลของการ transmits over HTTPS

2.1.9 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 9: EPROJECT

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	EPROJECT
หน้าที่	Web กลุ่มพัฒนาระบบบริหารสำนักปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม
ระบบปฏิบัติการ	Windows Server 2000
IP Address	192.168.16.10

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 22 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย EPROJECT

No.	Port / Service	Port Number
1	ftp	21/tcp
2	Mysql	3306/tcp
3	http	80/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 23 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย EPROJECT

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
ftp (21/tcp)	1	FTP Clear Text Authentication	LOW
http (80/tcp)	2	PHP < 5.2 Multiple Vulnerabilities	HIGH
	3	PHP < 4.4.1 / 5.0.6 Multiple Vulnerabilities	HIGH

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : หากไม่มีการใช้งาน FTP ควร Disable หรือหากใช้งาน ควรเปลี่ยนไปใช้ SSH แทน

ลำดับที่ 2-3 : ทำการ Upgrade PHP ให้มีเวอร์ชั่นที่สูงกว่า 4.4.1

2.1.10 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 10: IS~WALLBOARD

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	IS~WALLBOARD
หน้าที่	MMS Server
ระบบปฏิบัติการ	Unix Sun Solaris 8
IP Address	192.168.16.12

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 24 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย IS~WALLBOARD

No.	Port / Service	Port Number
1	ftp	21/tcp
2	http	80/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 25 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย IS~WALLBOARD

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
ftp (21/tcp)	1	FTP Clear Text Authentication	LOW

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : หากไม่มีการใช้งาน FTP ควร Disable หรือหากใช้งาน ควรเปลี่ยนไปใช้ SSH แทน

2.1.11 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 11: NICNATURAL

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	NICNATURAL
หน้าที่	โครงการ NIC
ระบบปฏิบัติการ	Unix Sun Solaris 8
IP Address	192.168.16.14

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 26 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย NICNATURAL

No.	Port / Service	Port Number
1	ftp	21/tcp
2	http	80/tcp
3	HTTP proxy Server	8080/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 27 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย NICNATURAL

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
ftp (21/tcp)	1	FTP Clear Text Authentication	

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : หากไม่มีการใช้งาน FTP ควร Disable หรือหากใช้งาน ควรเปลี่ยนไปใช้ SSH แทน

2.1.12 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 12: CICTDB

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	CICTDB
หน้าที่	Test Server
ระบบปฏิบัติการ	Windows XP SP2
IP Address	192.168.16.120

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 28 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเดอร์แม่ข่าย CICTDB

No.	Port / Service	Port Number
1	Domain	53/tcp
2	Veritas Netbackup	13717/tcp
3	Ntp	123/udp
4	http	80/tcp
5	telnet	23/tcp
6	X11	6000/tcp
7	Epmap	135/tcp
8	Netbios-ssn	139/tcp
9	Microsoft-ds	445/tcp
10	Pcanywhere	65301/tcp
11	VNC	5900/tcp
12	Windows Terimanl Services	3389/tcp
13	MySql	3306/tcp
14	Oracle Database	1521/tcp
15	Radmin	4899/tcp
16	https	443/tcp
17	Network blackjack	1025/tcp
18	Netbios-ns	137/udp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 29 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย CICTDB

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Microsoft-ds (445/tcp)	1	SMB LanMan Pipe Server browse listing	LOW
http (80/tcp) https (443/tcp)	2	OpenSSL password interception	MEDIUM
	3	OpenSSL overflow via invalid certificate passing	HIGH
	4	mod_ssl overflow	HIGH
	5	mod_ssl off by one	HIGH
	6	mod_ssl SSL_Util_UUEncode_Binary Overflow	HIGH
	7	mod_ssl hook functions format string vulnerability	HIGH
	8	Apache < 1.3.28	HIGH
	9	mod_ssl wildcard DNS cross site scripting vulnerability	LOW
	10	Apache mod_include priviledge escalation	MEDIUM
	11	Apache Error Log Escape Sequence Injection	LOW
	12	http TRACE XSS attack	MEDIUM
Epmap (135/tcp)	13	Microsoft RPC Interface Buffer Overrun (KB824146)	HIGH
Netbios-ns (137/udp)	14	Using NetBIOS to retrieve information from a Windows host	LOW
Oracle Database (1521/tcp)	15	Oracle tnslsnr security	HIGH
	16	Oracle timezone overflow	HIGH
	17	Oracle SOAP denial	HIGH
	18	Oracle LINK overflow	HIGH
	19	Oracle Database 8i/9i Multiple Remote Directory Traversal Vulnerabilities	HIGH
	20	Oracle DBS_SCHEDULER vulnerability	HIGH

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : เป็นไปได้ที่ผู้บุกรุกจะสามารถได้รับข้อมูลเกี่ยวกับเครื่องคอมพิวเตอร์ในเครือข่าย แต่ไม่มีผลกระทบกกับเครื่องคอมพิวเตอร์

ลำดับที่ 2-12 : - ทำการ Upgrade OpenSSL เป็นเวอร์ชั่น 0.9.6k หรือที่สูงกว่า

- ทำการ Upgrade Apache เป็นเวอร์ชั่น ที่สูงกว่า 1.3.28

ลำดับที่ 13 : ติดตั้ง Patch: http://www.microsoft.com/technet/security/bulletin/ms03-039.mspx

ลำดับที่ 14 : ผู้บุกรุกสามารถเข้าถึงข้อมูลที่สำคัญเช่นคอมพิวเตอร์ชื่อเวิร์กกรุ๊ป, ชื่อปัจจุบันล็อกอินชื่อผู้ใช้ เป็นต้น แต่ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์แม่ข่าย

ลำดับที่ 15-20 : - ทำการกำหนดสิทธิ์ การเข้าถึง Database โดยทำการแก้ไข ที่ file httpd.conf /oprocmgr-status/dms0

- ทำการ Upgarde Oracle ให้มีเวอร์ชั่น สูงกว่า 9.0.2.3

2.1.13 เครื่องคอมพิวเดอร์แม่ข่ายลำดับที่ 13: EMERALD

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	EMERALD
หน้าที่	DNS ภายนอก
ระบบปฏิบัติการ	Linux Kernel 2.6
IP Address	192.168.16.124

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 30 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย EMERALD

No.	Port / Service	Port Number
1	Domain	53/tcp
2	X11	6000/tcp
3	Domain	53/udp
4	Ssh	22/tcp
5	Pop3	110/tcp
6	http	80/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 31 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย EMERALD

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Not Found			

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

-

2.1.14 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 14: FIREWALL

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	FIREWALL
หน้าที่	Firewall
ระบบปฏิบัติการ	UNIX Sun Solaris 8
IP Address	192.168.16.126

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 32 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย FIREWALL

No.	Port / Service	Port Number
1	ftp	21/tcp
2	Ssh	22/tcp
3	Check Point Firewall-1	18264/tcp
4	Domain	53/tcp
5	Domain	53/udp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 33 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย FIREWALL

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
ftp (21/tcp)	1	FTP Clear Text Authentication	LOW
Ssh (22/tcp)	2	OpenSSH < 3.7.1	HIGH
	3	OpenSSH X11 Session Hijacking Vulnerability	MEDIUM

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : หากไม่มีการใช้งาน FTP ควร Disable หรือหากใช้งาน ควรเปลี่ยนไปใช้ SSH แทน

ลำดับที่ 2-3 : ควรทำการ Upgrade SSH ให้มีเวอร์ชั่นที่สูงกว่า 3.7.1

2.1.15 ผลการสำรวจสถานภาพด้านความปลอดภัยลำดับที่ 15: TEST1

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	TEST1
หน้าที่	Test Server
ระบบปฏิบัติการ	Windows Server 2003 SP1
IP Address	172.16.1.5

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 34 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย TEST1

No.	Port / Service	Port Number
1	Netbios-ns	137/udp
2	Windows Terminal Services	3389/tcp
3	Mysql	3306/tcp
4	Microsoft-ds	445/tcp
5	Epmap	135/tcp
6	http-alt	8080/tcp
7	http	80/tcp
8	Network blackjack	1025/tcp
9	Radmin	4899/tcp
10	Netbios-ssn	139/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 35 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย TEST1

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Mysql (3306/tcp)	1	MySQL Anonymous Login Handshake Information Leakage Vulnerability	MEDIUM
http (80/tcp)	2	PHP < 5.2 Multiple Vulnerabilities	HIGH
	3	PHP < 4.4.1 / 5.0.6 Multiple Vulnerabilities	HIGH
	4	HTTP TRACE / TRACK Methods	MEDIUM
Windows Terminal Services (3389/tcp)	5	Windows Terminal Service Enabled	LOW
	6	Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure Vulnerability	MEDIUM

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : - ทำการ Upgrade MySql ให้มีเวอร์ชั่นที่สูงกว่า 4.0.25 เป็นอย่างน้อย

- ควรมีการกำหนดสิทธิ์ IP บนเครื่องคอมพิวเตอร์แม่ข่ายที่จะเข้าถึง Database

ลำดับที่ 2-4 : - ทำการ Delete files ที่ไม่จำเป็นออก

- ทำการ Disable HTTP TRACE / TRACK Methods

- ทำการ Upgrade PHP ให้มีเวอร์ชั่นที่สูงกว่า 4.4.1

ลำดับที่ 5-6 : - หากไม่มีการใช้งาน Windows Terminal Services ควรทำการ Disable

- หากจำเป็นต้องใช้งาน ไม่ควรมีการเปิดสิทธิ์แบบ allow ควรมีการตรวจสอบสิทธิ์การใช้งาน

2.1.16 ผลการสำรวจสถานภาพด้านความปลอดภัยลำดับที่ 16: TEST2

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	TEST2
หน้าที่	Test Server
ระบบปฏิบัติการ	Windows Server 2003 SP1
IP Address	172.16.1.6

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 36 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย TEST2

No.	Port / Service	Port Number
1	Windows Terminal Services	3389/tcp
2	Microsoft-ds	445/tcp
3	Epmap	135/tcp
4	http	80/tcp
5	Mysql	3306/tcp
6	Network blackjack	1025/tcp
7	Radmin	4899/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 37 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย TEST2

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
http (80/tcp)	1	PHP < 5.2 Multiple Vulnerabilities	HIGH
	2	PHP < 4.4.1 / 5.0.6 Multiple Vulnerabilities	HIGH
	3	HTTP TRACE / TRACK Methods	MEDIUM

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1-3 : - ทำการ Delete files ที่ไม่มีการใช้งาน

- ทำการ Disable HTTP TRACE / TRACK Methods

- ทำการ Upgrade PHP ให้มีเวอร์ชั่นที่สูงกว่า 4.4.1

2.1.17 ผลการสำรวจสถานภาพด้านความปลอดภัยลำดับที่ 17: UPS1849

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	UPS1849
หน้าที่	UPS Management
ระบบปฏิบัติการ	Windows Vista
IP Address	172.16.1.13

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 38 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย UPS1849

No.	Port / Service	Port Number
1	Smtp	25/tcp
2	Windows XP UPNP	5000/tcp
3	telnet	23/tcp
4	http	80/tcp
5	Snmp	161/udp
6	Netbios-ns	137/udp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 39 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย UPS1849

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Snmp (161/udp)	1	Snmp-Password: "public"	HIGH

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ทำการเปลี่ยนรหัสผ่านให้มีความซับซ้อนมากขึ้น หรือหากไม่มีการใช้งาน ควรทำการ Disable

2.1.18 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 18: TEST3

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	TEST3
หน้าที่	Test Server
ระบบปฏิบัติการ	Windows Server 2003 SP2
IP Address	172.16.1.20

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 40 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย TSET3

No.	Port / Service	Port Number
1	Ssh	22/tcp
2	Checkpoint	18264/tcp
3	http	80/tcp
4	Pop3	110/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 41 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย TEST3

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
http (80/tcp)	1	Proxy accepts CONNECT requests	HIGH
	2	Proxy accepts gopher:// requests	MEDIUM

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1-2 : - ทำการตรวจสอบและ reconfigure สำหรับ CONNECT proxy

2.1.19 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 19: TOT

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	TOT
หน้าที่	Test Server
ระบบปฏิบัติการ	Windows Server 2003
IP Address	172.16.1.25

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 42 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย TOT

No.	Port / Service	Port Number
1	Netbios-ns	137/udp
2	Microsoft-ds	445/tcp
3	Windows Terminal Services	3389/tcp
4	Oracle Database	1521/tcp
5	Epmap	135/tcp
6	Netwokl blackjack	1025/tcp
7	Netbios-ssn	139/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 43 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย TOT

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Windows Terminal Services (3389/tcp)	1	Windows Terminal Service Enabled	LOW
	2	Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure Vulnerability	MEDIUM

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1-2 : - หากไม่มีการใช้งาน Windows Terminal Services ควรทำการ Disable

- หากจำเป็นต้องใช้งาน ไม่ควรมีการเปิดสิทธิ์แบบ allow ควรมีการตรวจสอบสิทธิ์การใช้งาน

2.1.20 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 20: DOCFILESERV1

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	DOCFILESERV1
หน้าที่	Web Server
ระบบปฏิบัติการ	Windows Server 2003
IP Address	172.16.1.27

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 44 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย DOCFILESERV1

No.	Port / Service	Port Number
1	Windows Terminal Services	3389/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 45 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย DOCFILESERV1

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Windows Terminal Services (3389/tcp)	1	Windows Terminal Service Enabled	MEDIUM
	2	Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure Vulnerability	

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1-2 : - หากไม่มีการใช้งาน Windows Terminal Services ควรทำการ Disable

- หากจำเป็นต้องใช้งาน ไม่ควรมีการเปิดสิทธิ์แบบ allow ควรมีการตรวจสอบสิทธิ์การใช้งาน

2.1.21 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 20: DOCFILESERV2

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	DOCFILESERV2
หน้าที่	File Server
ระบบปฏิบัติการ	Windows Server 2003
IP Address	172.16.1.32

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 46 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย DOCFILESERV2

No.	Port / Service	Port Number
1	Windows Terminal Services	3389/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 47 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย DOCFILESERV2

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Windows Terminal Services (3389/tcp)	1	Windows Terminal Service Enabled	LOW
	2	Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure Vulnerability	MEDIUM

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1-2 : - หากไม่มีการใช้งาน Windows Terminal Services ควรทำการ Disable

- หากจำเป็นต้องใช้งาน ไม่ควรมีการเปิดสิทธิ์แบบ allow ควรมีการตรวจสอบสิทธิ์การใช้งาน

2.1.22 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 22: DATATRAINNG

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	DATATRAINING
หน้าที่	ระบบข่าว/ Database
ระบบปฏิบัติการ	Windows XP SP2
IP Address	172.16.1.35

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 48 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย DOCTRAINING

No.	Port / Service	Port Number
1	Netbios-ns	137/udp
2	Oracle Database	1521/tcp
3	Microsoft-ds	445/tcp
4	Ntp	123/udp
5	Netbios-ssn	139/tcp
6	http	80/tcp
7	Epmap	135/tcp
8	Windows Terminal Services	3389/tcp
9	Radmin	4899/tcp
10	http-alt	8080/tcp
11	ftp	21/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 49 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย DOCTRAINING

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Windows Terminal Services (3389/tcp)	1	Windows Terminal Service Enabled	LOW
Oracle Database (1521/tcp)	2	Oracle SET TIME_ZONE Query Overflow	HIGH
	3	Oracle DBS_SCHEDULER Remote Command Execution	HIGH
	4	Oracle CREATE DATABASE LINK Query Overflow	HIGH
	5	Oracle Database 8i/9i Multiple Directory Traversal Vulnerabilities	MEDIUM
	6	Oracle SOAP / XML Remote Denial of Service	HIGH
	7	Unpassworded Oracle Listener Program (tnslsnr) Service	MEDIUM
Microsoft-ds (445/tcp)	8	SMB shares access	HIGH
http (80/tcp)	9	Apache /Server-status accessible	MEDIUM
	10	HTTP TRACE / TRACK Methods	MEDIUM
	11	Apache < 1.3.37	HIGH
	12	Apache < 1.3.41 Multiple Vulnerabilities (DoS, XSS)	MEDIUM
	13	PHP < 4.4.3 / 5.1.4 Multiple Vulnerabilities	HIGH
	14	PHP < 4.4.1 / 5.0.6 Multiple Vulnerabilities	HIGH
	15	AppServ appserv/main.php appserv_root Variable Remote File Inclusion	MEDIUM

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : - หากไม่มีการใช้งาน Windows Terminal Services ควรทำการ Disable

- หากจำเป็นต้องใช้งานไม่ควรมีการเปิดสิทธิ์แบบ Allow ควรมีการตรวจสอบสิทธิ์การใช้งาน

ลำดับที่ 2-7 : - Upgrade to Oracle 9.2.0.3 - http://metalink.oracle.com

- ทำการ ใช้ CHANGE_PASSWORD command เพื่อทำการกำหนดค่ารหัสผ่าน

ลำดับที่ 8 : - ติดตั้ง Patch: http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่

- ติดตั้ง Patch: http://www.microsoft.com/technet/security/bulletin/ms06-035.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่

- ติดตั้ง Patch: http://www.microsoft.com/technet/security/bulletin/ms06-040.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่

ลำดับที่ 9 -15 : - ทำการอัพเกรด Apache's configuration file(s) โดยการdisablezmod_status หรือทำการกำหนดสิทธิ์ในการ access เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย

- ทำการอัพเกรด PHP ให้มี version สูงกว่า 4.4.1

- ทำการอัพเกรด Apache ให้มี version สูงกว่า 1.3.37

- ทำการ Disable HTTP TRACE / TRACK Methods

2.1.23 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 23: GISFILESERVER

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	GISFILESERVER
หน้าที่	File Server
ระบบปฏิบัติการ	Windows Server 2003 SP2
IP Address	172.16.1.36

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 50 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย GISFILESERVER

No.	Port / Service	Port Number
1	Gds_db	3050/tcp
2	Mysql	3306/tcp
3	Netbios-ns	137/udp
4	Microsoft-ds	445/tcp
5	Netbios-ssn	139/tcp
6	http	80/tcp
7	Epmap	135/tcp
8	Windows Terminal Services	3389/tcp
9	Radmin	4899/tcp
10	http-alt	8080/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 51 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย GISFILESERVER

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Windows Terminal Services (3389/tcp)	1	Windows Terminal Service Enabled	
	2	Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure Vulnerability	MEDIUM
Gds_db (3050/tcp)	3	Firebird DataBase Server Buffer Overflow	HIGH
Mysql (3306/tcp)	4	MySQL Remote Insecure Default Password Vulnerability	HIGH
	5	MySQL multiple flaws (4)	MEDIUM
http (80/tcp)	6	Apache /Server-status accessible	MEDIUM
	7	HTTP TRACE / TRACK Methods	MEDIUM
	8	Apache < 1.3.37	HIGH
	9	Apache < 1.3.41 Multiple Vulnerabilities (DoS, XSS)	MEDIUM
	10	phpinfo.php	MEDIUM
	11	PHP < 4.4.3 / 5.1.4 Multiple Vulnerabilities	HIGH
	12	PHP < 4.4.1 / 5.0.6 Multiple Vulnerabilities	HIGH
	13	AppServ appserv/main.php appserv_root Variable Remote File Inclusion	MEDIUM

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1-2 : - หากไม่มีการใช้งาน Windows Terminal Services ควรทำการ Disable

- หากจำเป็นต้องใช้งาน ไม่ควรเปิดสิทธิ์แบบ allow ควรมีการตรวจสอบสิทธิ์การใช้งาน

ลำดับที่ 3 : - ทำการ Upgrade to Firebird 2.0.1 or later.

ลำดับที่ 4-5 : - ทำการ Upgrade MySql ให้มีเวอร์ชั่นที่สูงกว่า 4.0.25 เป็นอย่างน้อย

- ควรมีการกำหนดสิทธิ์ IP บนเครื่องคอมพิวเตอร์แม่ข่ายที่จะเข้าถึง Database

ลำดับที่ 6-13 : - ทำการ Update Apache's configuration file(s) to either disable mod_status หรือ มีการกำหนดสิทธิ์ การเข้า access เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย

- ทำการ Upgrade PHP ให้มี version สูงกว่า 4.4.1
- ทำการ Upgrade Apache ให้มี version สูงกว่า 1.3.37
- ทำการ Disable HTTP TRACE / TRACK Methods
- ทำการ Delete file phpinfo.php

2.1.24 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 24: INVENT

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	INVENT
หน้าที่	Web ระบบทะเบียนครุภัณฑ์
ระบบปฏิบัติการ	Linux 2.6 on Red Hat Enterprise Linux 6
IP Address	172.16.1.37

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 52 รายละเอียต Port / Service ที่เปิต ของเครื่องคอมพิวเตอร์แม่ข่าย INVENT

No.	Port / Service	Port Number
1	ftp	21/tcp
2	Mysql	3306/tcp
3	Ssh	22/tcp
4	https	443/tcp
5	http	80/tcp
6	Sunrpc	111/udp
7	Sunrpc	111/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 53 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย INVENT

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
ftp (21/tcp)	1	FTP-Password: "ftp/[Blank password]"	HIGH
	2	FTP-Password: "anonymous/[Blank password]"	HIGH
https (443/tcp)	3	phpMyAdmin XSS	MEDIUM
http (80/tcp)	4	PHPMyAdmin < 2.6.4 Cross-Site Scripting Vulnerabilities	MEDIUM
	5	HTTP TRACE / TRACK Methods	MEDIUM
	6	Web Server Uses Plain Text Authentication Forms	MEDIUM
	7	phpinfo.php	MEDIUM

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1-2 : ทำการ Disable user anonymous และทำการ เปลี่ยนรหัสผ่าน ftp ให้มีความซับซ้อนมากยิ่งขึ้น

ลำดับที่ 3-7 : - ทำการอัพเกรด PHPMyAdmin ให้มี version สูงกว่า 2.6.4

- ทำการ Disable HTTP TRACE / TRACK Methods

- ทำการ Delete file phpinfo.php

2.1.25 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 25: GSERVER

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	GSERVER
หน้าที่	Web ความหลากหลายทางชีวภาพ
ระบบปฏิบัติการ	Windows Server 2003 SP2
IP Address	172.16.1.43

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 54 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย GSERVER

No.	Port / Service	Port Number
1	Microsoft-ds	445/tcp
2	Epmap	135/tcp
3	Network blackjack	1025/tcp
4	Radmin	4899/tcp
5	Netbios-ssn	139/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 55 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย GSERVER

Port / Service	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Not Found		

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

-

2.1.26 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 26: WAREHOUSE

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	WAREHOUSE
หน้าที่	Web Portal
ระบบปฏิบัติการ	Windows Server 2003 SP2
IP Address	172.16.1.45

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 56 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย WAREHOUSE

No.	Port / Service	Port Number
1	Ms-sql-s	1433/tcp
2	Mysql	3306/tcp
3	Netbios-ns	137/udp
4	Ms-sql-m	1434/udp
5	Microsoft-ds	445/tcp
6	ftp	21/tcp
7	Netbios-ssn	139/tcp
8	http	80/tcp
9	Epmap	135/tcp
10	Network blackjack	1025/tcp
11	Windows Terminal Services	3389/tcp
12	Radmin	4899/tcp
13	http-alt	8080/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 57 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย WAREHOUSE

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
ftp (21/tcp)	1	FTP-Password: "ftp/[Blank password]"	HIGH
	2	FTP-Password: "anonymous/[Blank password]"	HIGH
Ms-sql-s (1433/tcp)	3	Vulnerabilities in Microsoft SQL Server Could Allow Elevation of Privilege (941203)	HIGH
http (80/tcp)	4	phpinfo.php	MEDIUM
Windows Terminal Services (3389/tcp)	5	Windows Terminal Service Enabled	
	6	Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure Vulnerability	MEDIUM
http-alt (8080/tcp)	7	Tomcat Hello World Sample App Cross-Site Scripting Vulnerability	MEDIUM
	8	Tomcat cal2.jsp Sample App Cross-Site Scripting Vulnerability	MEDIUM
	9	Tomcat snoop.jsp Cross-Site Scripting Vulnerability	MEDIUM

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1-2 : ทำการ Disable user anonymous และทำการ เปลี่ยนรหัสผ่าน ftp ให้มีความซับซ้อนมากยิ่งขึ้น

ลำดับที่ 3 : ทำการ Upgrade Ms-Sql http://www.microsoft.com/technet/security/bulletin/ms08-040.mspx

ลำดับที่ 4 : ทำการ Disable file phpinfo.php

ลำดับที่ 5-6 : - หากไม่มีการใช้งาน Windows Terminal Services ควรทำการ Disable

- หากจำเป็นต้องใช้งาน ไม่ควรมีการเปิดสิทธิ์แบบ allow ควรมีการตรวจสอบสิทธิ์การใช้งาน

ลำดับที่ 7-9 : - ทำการปิดพอร์ต 8080 บนเครื่องคอมพิวเตอร์แม่ข่าย หากไม่มีการใช้งานดังกล่าว

- ทำการตรวจสอบค่า remote proxy ที่เข้ามาภายในเครือข่ายเพื่อป้องกันการถูกบุกรุก

- ไม่ทำการ Deploy the Tomcat ทั้งในส่วนของตัวอย่าง หรือเอกสารต่าง ๆ ที่เกี่ยวกับ Web application ของเครื่องคอมพิวเตอร์แม่ข่าย

2.1.27 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 27: INTEL_SERVER

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	INTEL_SERVER
หน้าที่	Web สำนักพัฒนาบริหารทรัพยากรธรรมชาติและสิ่งแวดล้อม
ระบบปฏิบัติการ	Windows Server 2003 SP2
IP Address	172.16.1.47

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 58 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย INTEL_SERVER

No.	Port / Service	Port Number
1	Netbbios-ssn	139/tcp
2	http	80/tcp
3	ftp	21/tcp
4	Windows TerminalServices	3389/tcp
5	Network blackjack	1025/tcp
6	Epmap	135/tcp
7	Mysql	3306/tcp
8	Microsoft-ds	445/tcp
9	Netbios-ns	137/udp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 59 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย INTEL_SERVER

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
http (80/tcp)	1	HTTP TRACE / TRACK Methods	MEDIUM
	2	Apache < 2.0.59	HIGH
	3	Apache < 2.0.63 Multiple Vulnerabilities	
	4	PHP < 4.4.9 Multiple Vulnerabilities	HIGH
	5	phpinfo.php	MEDIUM

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Windows Terminal Services (3389/tcp)	6	Windows Terminal Service Enabled	LOW
	7	Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure Vulnerability	MEDIUM
Netbios-ns (137/udp)	8	Using NetBIOS to retrieve information from a Windows host	LOW

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1-5 : - ทำการอัพเกรด PHP ให้มี version สูงกว่า 4.4.9

- ทำการอัพเกรด Apache ให้มี version สูงกว่า 2.0.59

- ทำการ Disable HTTP TRACE / TRACK Methods

- ทำการ Disable file phpinfo.php

ลำดับที่ 6-7 : - หากไม่มีการใช้งาน Windows Terminal Services ควรทำการ Disable

- หากจำเป็นต้องใช้งาน ไม่ควรมีการเปิดสิทธิ์แบบ allow ควรมีการตรวจสอบสิทธิ์การใช้งาน

ลำดับที่ 8 : ผู้บุกรุกสามารถเข้าถึงข้อมูลที่สำคัญเช่นคอมพิวเตอร์ชื่อเวิร์กกรุ๊ป, ชื่อปัจจุบันล็อกอินชื่อผู้ใช้ เป็นต้น แต่ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์แม่ข่าย

2.1.28 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 28: GISWEB

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	GISWEB
หน้าที่	Web ภูมิสารสนเทศ
ระบบปฏิบัติการ	Windows Server 2003 SP1
IP Address	172.16.1.52

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 60 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย GISWEB

No.	Port / Service	Port Number
1	Pop3	110/tcp
2	Imap	143/tcp
3	Mysql	3306/tcp
4	Oracle Database	1521/tcp
5	Netbios-ns	137/udp
6	Microsoft-ds	445/tcp
7	Netbios-ssn	139/tcp
8	http	80/tcp
9	Smtp	25/tcp
10	Epmap	135/tcp
11	Network blackjack	1025/tcp
12	Windows Terminal Services	3389/tcp
13	Radmin	4899/tcp
14	https	443/tcp
15	http-alt	8080/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 61 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย GISWEB

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
http (80/tcp)	1	Apache Tomcat servlet/JSP container default files	MEDIUM
Windows Terminal Services (3389/tcp)	2	Windows Terminal Service Enabled	LOW
	3	Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure Vulnerability	MEDIUM
Netbios-ns (137/udp)	4	Using NetBIOS to retrieve information from a Windows host	LOW
Pop3 (110/tcp)	5	ArGoSoft Mail Server _DUMP Command System Information Disclosure	MEDIUM
Oracle Database (1521/tcp)	6	Unpassworded Oracle Listener Program (tnslsnr) Service	MEDIUM
Microsoft-ds (445/tcp)	7	SMB shares access	HIGH
Smtp (25/tcp)	8	EXPN and VRFY commands	MEDIUM

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : Review the files and delete those that are not needed.

ลำดับที่ 2-3 : - หากไม่มีการใช้งาน Windows Terminal Services ควรทำการ Disable

- หากจำเป็นต้องใช้งาน ไม่ควรเปิดสิทธิ์แบบ allow ควรมีการตรวจสอบสิทธิ์การใช้งาน

ลำดับที่ 4 : ผู้บุกรุกสามารถเข้าถึงข้อมูลที่สำคัญเช่นคอมพิวเตอร์ชื่อเวิร์กกรุ๊ป, ชื่อปัจจุบันล็อกอินชื่อผู้ใช้ เป็นต้น แต่ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์แม่ข่าย

ลำดับที่ 5 : ทำการ Upgrade to ArGoSoft Mail Server 1.8.8.6 or later.

ลำดับที่ 6 : ทำการ ใช้ CHANGE_PASSWORD command เพื่อทำการกำหนดค่ารหัสผ่าน

ลำดับที่ 7 : ควรมีการกำหนดสิทธิ์ในการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย โดยวิธีการเปิด explorer, do a right click on each shares, go to the 'sharing' tab, and click on 'permissions'

ลำดับที่ 8 : หากมีการใช้ Sendmail, ควรมีการเพิ่มเงื่อนไข ดังต่อไปนี้

PrivacyOptions=goawayin /etc/sendmail.cf.

2.1.29 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 29: GOOGLEMNRE

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	GOOGLEMNRE
หน้าที่	ระบบสนับสนุนศูนย์ปฏิบัติการกระทรวงฯ ในรูปแบบภูมิสารสนเทศบน Google Earth
ระบบปฏิบัติการ	Windows Server 2003 SP1
IP Address	172.16.1.57

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 62 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเดอร์แม่ข่าย GOOGLEMNRE

No.	Port / Service	Port Number
1	Netbios-ns	137/udp
2	VERITAS Backup	10000/tcp
3	Windows Terminal Services	3389/tcp
4	Microsoft-ds	445/tcp
5	Epmap	135/tcp
6	http-alt	8080/tcp
7	Ms-sql-m	1434/udp
8	http	80/tcp
9	Netbios-ssn	139/tcp
10	Ms-sql-s	1433/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 63 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย GOOGLEMNRE

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Ms-sql-s (1433/tcp)	1	Microsoft SQL Server Multiple Privilege Escalation (941203) - Network Check	HIGH
Windows Terminal Services (3389/tcp)	2	Windows Terminal Service Enabled	LOW
	3	Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure Vulnerability	MEDIUM
Netbios-ns (137/udp)	4	Using NetBIOS to retrieve information from a Windows host	LOW

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ทำการ Upgrade Patch

http://www.microsoft.com/technet/security/bulletin/ms08-040.mspx

ลำดับที่ 2-3 : - หากไม่มีการใช้งาน Windows Terminal Services ควรทำการ Disable

- หากจำเป็นต้องใช้งาน ไม่ควรมีการเปิดสิทธิ์แบบ allow ควรมีการตรวจสอบสิทธิ์การใช้งาน

ลำดับที่ 4 : ผู้บุกรุกสามารถเข้าถึงข้อมูลที่สำคัญเช่นคอมพิวเตอร์ชื่อเวิร์กกรุ๊ป, ชื่อปัจจุบันล็อกอินด้วยชื่อผู้ใช้ (Username) เป็นต้น แต่ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์แม่ข่าย

2.1.30 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 30: AVMNRE

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	AVMNRE
หน้าที่	Anti virus
ระบบปฏิบัติการ	Windows Server 2003 SP2
IP Address	172.16.1.61

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 64 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย AVMNRE

No.	Port / Service	Port Number
1	nntp	119/tcp
2	Netbios-ns	17/udp
3	Microsoft-ds	445/tcp
4	ftp	21/tcp
5	Netbios-ssn	139/tcp
6	http	80/tcp
7	Smtp	25/tcp
8	Epmap	135/tcp
9	Windows Terminal Services	3389/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 65 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย AVMNRE

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
ftp (21/tcp)	1	FTP-Password: "ftp/[Blank password]"	HIGH
	2	FTP-Password: "anonymous/[Blank password]"	HIGH
Netbios-ns (137/udp)	3	Using NetBIOS to retrieve information from a Windows host	
http (80/tcp)	4	WebDAV enabled	MEDIUM
	5	Private IP address leaked in HTTP headers	

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Windows Terminal Services (3389/tcp)	6	Windows Terminal Service Enabled	LOW
	7	Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure Vulnerability	MEDIUM

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1-2 : ทำการ Disable user anonymous และทำการ เปลี่ยนรหัสผ่าน ftp ให้มีความซับซ้อนมากยิ่งขึ้น

ลำดับที่ 3 : ผู้บุกรุกสามารถเข้าถึงข้อมูลที่สำคัญเช่นคอมพิวเตอร์ชื่อเวิร์กกรุ๊ป, ชื่อปัจจุบันล็อกอินชื่อผู้ใช้ เป็นต้น แต่ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์แม่ข่าย

ลำดับที่ 4-5 : ทำการ Disable WebDev

ลำดับที่ 6-7 :- หากไม่มีการใช้งาน Windows Terminal Services ควรทำการ Disable

- หากจำเป็นต้องใช้งาน ไม่ควรมีการเปิดสิทธิ์แบบ Allow ควรมีการตรวจสอบสิทธิ์การใช้งาน

2.1.31 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 31: MMNRE

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	MMNRE
หน้าที่	Anti Spam
ระบบปฏิบัติการ	Windows Server 2003 SP2
IP Address	172.16.1.62

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 66 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย MMNRE

No.	Port / Service	Port Number
1	Smtp	25/tcp
2	Windows Termainl Services	3389/tcp
3	Microsoft-ds	445/tcp
4	Epmap	135/tcp
5	Netbios-ssn	139/tcp
6	http	80/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 67 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย MMNRE

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Microsoft-ds (445/tcp)	1	SMB LanMan Pipe Server browse listing	
Windows Terminal Services (3389/tcp)	2	Windows Terminal Service Enabled	
	3	Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure Vulnerability	MEDIUM
Netbios-ns (137/udp)	4	Using NetBIOS to retrieve information from a Windows host	

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : เป็นไปได้ที่ผู้บุกรุกจะสามารถได้รับข้อมูลเกี่ยวกับเครื่องคอมพิวเตอร์ในเครือข่าย แต่ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์

ลำดับที่ 2-3 : - หากไม่มีการใช้งาน Windows Terminal Services ควรทำการ Disable

- หากจำเป็นต้องใช้งาน ไม่ควรมีการเปิดสิทธิ์แบบ allow ควรมีการตรวจสอบสิทธิ์การใช้งาน

ลำดับที่ 4 : ผู้บุกรุกสามารถเข้าถึงข้อมูลที่สำคัญเช่นคอมพิวเตอร์ชื่อเวิร์กกรุ๊ป, ชื่อปัจจุบันล็อกอินชื่อผู้ใช้ เป็นต้น แต่ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์แม่ข่าย

2.1.32 เครื่องคอมพิวเดอร์แม่ข่ายลำดับที่ 32: OMESERV

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	OMESREV
หน้าที่	Web Server
ระบบปฏิบัติการ	Windows Server 2003 SP2
IP Address	172.16.1.63

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 68 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเดอร์แม่ข่าย OMESERV

No.	Port / Service	Port Number
1	ftp	21/tcp
2	Netbios-ns	137/udp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 69 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเดอร์แม่ข่าย OMSERV

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Netbios-ns (137/udp)	1	Using NetBIOS to retrieve information from a Windows host	[redacted]

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ผู้บุกรุกสามารถเข้าถึงข้อมูลที่สำคัญเช่นคอมพิวเตอร์ชื่อเวิร์กกรุ๊ป, ชื่อปัจจุบันล็อกอินชื่อผู้ใช้ เป็นต้น แต่ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์แม่ข่าย

2.1.33 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 33: LITHUIM

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	LITHUIM
หน้าที่	Tape Backup
ระบบปฏิบัติการ	Windows Server 2003 SP2
IP Address	172.16.1.64

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 70 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย LITHUIM

No.	Port / Service	Port Number
1	Netbios-ns	137/udp
2	Microsoft-ds	445/tcp
3	Epmap	135/tcp
4	http	80/tcp
5	Network blackjack	1025/tcp
6	Radmin	4899/tcp
7	Netbios-ssn	139/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 71 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย LITHUIM

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Netbios-ns (137/udp)	1	Using NetBIOS to retrieve information from a Windows host	LOW
http (80/tcp)	2	Web Server Uses Plain Text Authentication Forms	MEDIUM
	3	Apache < 1.3.41 Multiple Vulnerabilities	MEDIUM
	4	Backup CGIs download	MEDIUM
	5	HTTP TRACE / TRACK Methods	MEDIUM
	6	PHP < 4.4.9 Multiple Vulnerabilities	HIGH
Windows Terminal	7	Windows Terminal Service Enabled	LOW

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Services (3389/tcp)	8	Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure Vulnerability	MEDIUM

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ผู้บุกรุกสามารถเข้าถึงข้อมูลที่สำคัญเช่นคอมพิวเตอร์ชื่อเวิร์กกรุ๊ป, ชื่อปัจจุบันล็อกอินชื่อผู้ใช้ เป็นต้น แต่ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์แม่ข่าย

ลำดับที่ 2-6 : - ทำการอัพเกรด PHP ให้มี version สูงกว่า 4.4.9

- ทำการอัพเกรด Apache ให้มี version สูงกว่า 1.3.41

- ทำการ Disable HTTP TRACE / TRACK Methods

- ทำการ Delete file Backup

ลำดับที่ 7-8 : - หากไม่มีการใช้งาน Windows Terminal Services ควรทำการ Disable

- หากจำเป็นต้องใช้งาน ไม่ควรมีการเปิดสิทธิ์แบบ Allow ควรมีการตรวจสอบสิทธิ์การใช้งาน

2.1.34 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 34: SERVER

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	SERVER
หน้าที่	Web สำนักความร่วมมือด้านทรัพยากรธรรมชาติและสิ่งแวดล้อมระหว่างประเทศ
ระบบปฏิบัติการ	Windows Server 2003 SP2
IP Address	172.16.1.65

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 72 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย SERVER

No.	Port / Service	Port Number
1	Microsoft-ds	445/tcp
2	Netbios-ssn	139/tcp
3	Mysql	3306/tcp
4	http	80/tcp
5	Ms-sql-s	1433/tcp
6	Network blackjack	1025/tcp
7	Epmap	135/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 73 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย SERVER

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Netbios-ns (137/udp)	1	Using NetBIOS to retrieve information from a Windows host	LOW
http (80/tcp)	2	Apache /Server-status accessible	MEDIUM
	3	HTTP TRACE / TRACK Methods	MEDIUM
	4	Apache < 1.3.37	HIGH
	5	Apache < 1.3.41 Multiple Vulnerabilities	MEDIUM
	6	AppServ appserv_root Parameter Remote File Include	MEDIUM

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
		Vulnerability	
	7	PHP < 4.4.9 Multiple Vulnerabilities	HIGH

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ผู้บุกรุกสามารถเข้าถึงข้อมูลที่สำคัญเช่นคอมพิวเตอร์ชื่อเวิร์กกรุ๊ป, ชื่อปัจจุบันล็อกอินชื่อผู้ใช้ เป็นต้น แต่ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์แม่ข่าย

ลำดับที่ 2-7 : - ทำการอัพเกรด PHP ให้มี version สูงกว่า 4.4.9

- ทำการอัพเกรด Apache ให้มี version สูงกว่า 1.3.37

- ทำการ Disable HTTP TRACE / TRACK Methods

2.1.35 เครื่องคอมพิวเดอร์แม่ข่ายลำดับที่ 35: BACKUP-SERVER

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	BACKUP-SERVER
หน้าที่	Backup Server
ระบบปฏิบัติการ	Windows Server 2003 SP2
IP Address	172.16.1.107

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 74 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเดอร์แม่ข่าย BACKUP-SERVER

No.	Port / Service	Port Number
1	nntp	119/tcp
2	VERITAS Backup	10000/tcp
3	Netbios-ns	137/udp
4	Ms-sql-m	1434/udp
5	Microsoft-ds	445/tcp
6	ftp	21/tcp
7	Netbios-ssn	139/tcp
8	http	80/tcp
9	Smtp	25/tcp
10	Epmap	135/tcp
11	Windows Terminal Services	3389/tcp
12	Radmin	4899/tcp
13	http-alt	8080/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 75 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย BACKUP-SERVER

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
ftp (21/tcp)	1	FTP-Password: "ftp/[Blank password]"	HIGH
	2	FTP-Password: "anonymous/[Blank password]"	HIGH
Netbios-ns (137/udp)	3	Using NetBIOS to retrieve information from a Windows host	[illegible]
http (80/tcp)	4	WebDAV enabled	MEDIUM
	5	Test HTTP dangerous methods	HIGH
	6	Private IP address leaked in HTTP headers	[illegible]
Windows Terminal Services (3389/tcp)	7	Windows Terminal Service Enabled	[illegible]
	8	Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure Vulnerability	MEDIUM

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1-2 : ทำการ Disable user anonymous และทำการ เปลี่ยนรหัสผ่าน ftp ให้มีความซับซ้อนมากยิ่งขึ้น

ลำดับที่ 3 : ผู้บุกรุกสามารถเข้าถึงข้อมูลที่สำคัญเช่นคอมพิวเตอร์ชื่อเวิร์กกรุ๊ป, ชื่อปัจจุบันล็อกอินชื่อผู้ใช้ เป็นต้น แต่ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์แม่ข่าย

ลำดับที่ 4-6 : - ทำการ Disable WebDev

- ทำการ Disable Test HTTP dangerous method

ลำดับที่ 7-8 : - หากไม่มีการใช้งาน Windows Terminal Services ควรทำการ Disable

- หากจำเป็นต้องใช้งาน ไม่ควรมีการเปิดสิทธิ์แบบ Allow ควรมีการตรวจสอบสิทธิ์การใช้งาน

2.1.36 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 36: LOG-MANAGEMENT

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	LOG-MANAGEMENT
หน้าที่	Log Server
ระบบปฏิบัติการ	Windows Server 2003 SP2
IP Address	172.16.1.108

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 76 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย LOG-MANAGEMENT

No.	Port / Service	Port Number
1	nntp	119/tcp
2	VERITAS Backup	10000/tcp
3	Netbios-ns	137/udp
4	Microsoft-ds	445/tcp
5	ftp	21/tcp
6	Netbios-ssn	138/tcp
7	HP OpenView	2954/tcp
8	http	80/tcp
9	Smtp	25/tcp
10	Epmap	135/tcp
11	Radmin	4899/tcp
12	http-alt	8080/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 77 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย LOG-MANAGEMENT

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
ftp (21/tcp)	1	FTP-Password: "ftp/[Blank password]"	HIGH
	2	FTP-Password: "anonymous/[Blank password]"	HIGH
Netbios-ns (137/udp)	3	Using NetBIOS to retrieve information from a Windows host	[illegible]
http (80/tcp)	4	WebDAV enabled	MEDIUM
	5	OpenView Network Node Manager OpenView5.exe Action Parameter Traversal Arbitrary File Access	MEDIUM
	6	Test HTTP dangerous methods	HIGH
	7	Private IP address leaked in HTTP headers	[illegible]
Windows Terminal Services (3389/tcp)	8	Windows Terminal Service Enabled	[illegible]
	9	Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure Vulnerability	MEDIUM

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1-2 : ทำการ Disable user anonymous และทำการ เปลี่ยนรหัสผ่าน ftp ให้มีความซับซ้อนมากยิ่งขึ้น

ลำดับที่ 3 : ผู้บุกรุกสามารถเข้าถึงข้อมูลที่สำคัญเช่นคอมพิวเตอร์ชื่อเวิร์กกรุ๊ป, ชื่อปัจจุบันล็อกอินชื่อผู้ใช้ เป็นต้น แต่ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์แม่ข่าย

ลำดับที่ 4-7 : - ทำการ Disable WebDev

- ทำการ Disable Test HTTP dangerous method

ลำดับที่ 8-9 : -หากไม่มีการใช้งาน Windows Terminal Services ควรทำการ Disable

- หากจำเป็นต้องใช้งาน ไม่ควรมีการเปิดสิทธิ์แบบ Allow ควรมีการตรวจสอบสิทธิ์การใช้งาน

2.1.37 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 37: DDMNRE

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	DDMNRE
หน้าที่	DHCP
ระบบปฏิบัติการ	Windows Server 2003 SP2
IP Address	172.16.1.109

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 78 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย DDMNRE

No.	Port / Service	Port Number
1	Netbios-ns	137/udp
2	Windows Terminal Services	3389/tcp
3	Microsoft-ds	445/tcp
4	Epmap	135/tcp
5	Network blackjack	1025/tcp
6	Netbios-ssn	139/tcp
7	Domain	53/tcp
8	Domain	53/udp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 79 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย DDMNRE

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Netbios-ns (137/udp)	1	Using NetBIOS to retrieve information from a Windows host	LOW
Windows Terminal Services (3389/tcp)	2	Windows Terminal Service Enabled	LOW
	3	Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure Vulnerability	MEDIUM
Domain (53/udp)	4	DNS Cache Snooping	MEDIUM
	5	DNS Server Recursive Query Enabled	MEDIUM

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ผู้บุกรุกสามารถเข้าถึงข้อมูลที่สำคัญเช่นคอมพิวเตอร์ชื่อเวิร์กกรุ๊ป, ชื่อปัจจุบันล็อกอินชื่อผู้ใช้ เป็นต้น แต่ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์แม่ข่าย

ลำดับที่ 2-3 : - หากไม่มีการใช้งาน Windows Terminal Services ควรทำการ Disable

- หากจำเป็นต้องใช้งาน ไม่ควรมีการเปิดสิทธิ์แบบ Allow ควรมีการตรวจสอบสิทธิ์การใช้งาน

ลำดับที่ 4-5 : - ดูรายละเอียดเพิ่มเติมเกี่ยวกับการกำหนดค่า DNS:http://www.rootsecure.net/content/downloads/pdf/dns_cache_snooping.pdf

2.1.38 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 38: DNSMNRE

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	DNSMNRE
หน้าที่	DNS
ระบบปฏิบัติการ	Linux Kernal 2.6
IP Address	172.16.1.110

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 80 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย DNSMNRE

No.	Port / Service	Port Number
1	VERITAS Backup	10000/tcp
2	Ssh	22/tcp
3	Domain	53/tcp
4	Domain	53/udp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 81 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย DNSMNRE

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Domain (53/udp)	1	DNS Cache Snooping	MEDIUM
	2	DNS Server Recursive Query Enabled	MEDIUM

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1-2 : - ดูรายละเอียดเพิ่มเติมเกี่ยวกับการกำหนดค่า

DNS:http://www.rootsecure.net/content/downloads/pdf/dns_cache_snooping.pdf

2.1.39 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 39: ADMNRE

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	ADMNRE
หน้าที่	Domain Active Directory
ระบบปฏิบัติการ	Windows Server 2003 SP2
IP Address	172.16.1.111

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 82 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย ADMNRE

No.	Port / Service	Port Number
1	Domain	53/udp
2	Domain	53/tcp
3	Netbios-ns	137/udp
4	Microsoft-ds	445/tcp
5	Ntp	123/udp
6	Netbios-ssn	139/tcp
7	Epmap	135/tcp
8	Network blackjack	1025/tcp
9	Ldap	389/tcp
10	Windows Terminal Services	3389/tcp
11	Ldaps	636/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 83 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย ADMNRE

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Netbios-ns (137/udp)	1	Using NetBIOS to retrieve information from a Windows host	LOW
Windows Terminal Services (3389/tcp)	2	Windows Terminal Service Enabled	LOW
	3	Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure Vulnerability	MEDIUM
Domain (53/udp)	4	DNS Cache Snooping	MEDIUM
	5	DNS Server Recursive Query Enabled	MEDIUM
Ldap (389/tcp)	6	LDAP Allows anonymous binds	MEDIUM
	7	LDAP Allows null bases	MEDIUM

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ผู้บุกรุกสามารถเข้าถึงข้อมูลที่สำคัญเช่นคอมพิวเตอร์ชื่อเวิร์กกรุ๊ป, ชื่อบัจจุบันล็อกอินชื่อผู้ใช้ เป็นต้น แต่ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์แม่ข่าย

ลำดับที่ 2-3 : - หากไม่มีการใช้งาน Windows Terminal Services ควรทำการ Disable

- หากจำเป็นต้องใช้งาน ไม่ควรมีการเปิดสิทธิ์แบบ Allow ควรมีการตรวจสอบสิทธิ์การใช้งาน

ลำดับที่ 4-5 : - ดูรายละเอียดเพิ่มเติมเกี่ยวกับการกำหนดค่า DNS:http://www.rootsecure.net/content/downloads/pdf/dns_cache_snooping.pdf

ลำดับที่ 6-7 : - ทำการ Configure the LDAP Server so that it does not Allow NULL BINDs.

- ทำการ Disable NULL BASE queries on your LDAP Server

2.1.40 เครื่องคอมพิวเตอร์แม่ข่ายลำดับที่ 40: NMS

ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	NMS
หน้าที่	Network Management Server
ระบบปฏิบัติการ	Windows Server 2003 SP1
IP Address	172.16.201.1

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 84 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์แม่ข่าย NMS

No.	Port / Service	Port Number
1	Netbios-ns	137/udp
2	Windows Terminal Services	3389/tcp
3	Microsoft-ds	445/tcp
4	Epmap	135/tcp
5	http	80/tcp
6	Network blackjack	1025/tcp
7	Netbios-ssn	139/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 85 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์แม่ข่าย NMS

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Netbios-ns (137/udp)	1	Using NetBIOS to retrieve information from a Windows host	LOW
Windows Terminal Services (3389/tcp)	2	Windows Terminal Service Enabled	LOW
	3	Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure Vulnerability	MEDIUM
Microsoft-ds (445/tcp)	4	Vulnerability in Server Service Could Allow Remote Code Execution (917159)	HIGH

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
	5	Vulnerability in Server Service Could Allow Remote Code Execution (921883)	HIGH

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ผู้บุกรุกสามารถเข้าถึงข้อมูลที่สำคัญ เช่น คอมพิวเตอร์ชื่อเวิร์กกรุ๊ป (Work group), ชื่อปัจจุบันล็อกอินชื่อผู้ใช้ เป็นต้น แต่ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์แม่ข่าย

ลำดับที่ 2-3 : - หากไม่มีการใช้งาน Windows Terminal Services ควรทำการ Disable

- หากจำเป็นต้องใช้งาน ไม่ควรมีการเปิดสิทธิ์แบบ Allow ควรมีการตรวจสอบสิทธิ์การใช้งาน

ลำดับที่ 4-5 : - ติดตั้ง Patch: http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่

- ติดตั้ง Patch: http://www.microsoft.com/technet/security/bulletin/ms06-035.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่

- ติดตั้ง Patch: http://www.microsoft.com/technet/security/bulletin/ms06-040.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่

- ควรมีการตรวจสอบ พอร์ต 445 สำหรับการใช้งาน เพื่อป้องกันผู้บุกรุกจากภายนอก

2.2 ผลการสำรวจสถานภาพด้านความปลอดภัยอุปกรณ์เครือข่าย

2.2.1 อุปกรณ์เครือข่ายลำดับที่ 1: 192.168.4.27

หน้าที่	NetApp
ระบบปฏิบัติการ	Net App Release 7.2.3
IP Address	192.168.4.27

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 86 รายละเอียด Port / Service ที่เปิด ของอุปกรณ์เครือข่าย 192.168.4.27

No.	Port / Service	Port Number
1	telnet	23/tcp
2	VERITAS Backup	10000/tcp
3	Sunrpc	111/udp
4	Shell	514/tcp
5	Nfs	2049/udp
6	Netbios-ns	137/udp
7	Snmp	161/udp
8	Sunrpc	111/tcp
9	Ssh	22/tcp
10	Microsoft-ds	445/tcp
11	Ntp	123/udp
12	Netbios-ssn	139/tcp
13	http	80/tcp
14	https	443/tcp
15	Nfs	2049/tcp
16	Efs	520/udp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 87 รายละเอียดของช่องโหว่ที่พบ ของอุปกรณ์เครือข่าย 192.168.4.27

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
telnet (23/tcp)	1	A telnet Server is listening on the remote port	LOW
Shell (512/tcp)	2	Rsh Server Detection	MEDIUM
Nfs (2049/tcp)	3	Mountable NFS shares	MEDIUM
Snmp (161/udp)	4	Snmp-Password: "public"	HIGH
Netbios-ns (137/udp)	5	Using NetBIOS to retrieve information from a Windows host	LOW

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ทำการ Disable Telnet หากไม่มีการใช้งาน หรือเปลี่ยนจากการใช้ Telnet เป็น Ssh

ลำดับที่ 2 : ทำการ Disable Rsh หากไม่มีการใช้งาน

ลำดับที่ 3 : ทำการ Disable Nsf หากไม่มีการใช้งาน

ลำดับที่ 4 : ทำการ Disable Snmp หากไม่มีการใช้งาน หรือทำการเปลี่ยนรหัสผ่าน ให้มีความซับซ้อนมากยิ่งขึ้น

ลำดับที่ 5 : ผู้บุกรุกสามารถเข้าถึงข้อมูลที่สำคัญเช่นคอมพิวเตอร์ชื่อเวิร์กกรุ๊ป, ชื่อปัจจุบันล็อกอินชื่อผู้ใช้ เป็นต้น แต่ไม่มีผลกระทบ

2.2.2 อุปกรณ์เครือข่ายลำดับที่ 2: 172.16.1.254

หน้าที่	Switch
ระบบปฏิบัติการ	CISCO IOS 12.1
IP Address	172.16.1.254

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 88 รายละเอียด Port / Service ที่เปิด ของอุปกรณ์เครือข่าย 172.16.1.254

No.	Port / Service	Port Number
1	telnet	23/tcp
2	http	80/tcp
3	ftp	21/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 89 รายละเอียดของช่องโหว่ที่พบ ของอุปกรณ์เครือข่าย 172.16.1.254

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
telnet (23/tcp)	1	A telnet Server is listening on the remote port	

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1: ทำการ Disable Telnet หากไม่มีการใช้งาน หรือเปลี่ยนจากการใช้ Telnet เป็น Ssh

2.2.3 อุปกรณ์เครือข่ายลำดับที่ 3: 172.16.201.249

หน้าที่	Switch
ระบบปฏิบัติการ	CISCO IOS 12.4
IP Address	172.16.201.249

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 90 รายละเอียด Port / Service ที่เปิด ของอุปกรณ์เครือข่าย 172.16.201.249

No.	Port / Service	Port Number
1	telnet	23/tcp
2	http	80/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 91 รายละเอียดของช่องโหว่ที่พบ ของอุปกรณ์เครือข่าย 172.16.201.249

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
telnet (23/tcp)	1	A telnet Server is listening on the remote port	LOW
http (80/tcp)	2	Web Server Uses Basic Authentication	LOW

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ทำการ Disable Telnet หากไม่มีการใช้งาน หรือเปลี่ยนจากการใช้ Telnet เป็น Ssh

ลำดับที่ 2 : ทำการ Disable Http หากไม่มีการใช้งาน หรือเปลี่ยนจากการใช้ Http เป็น Https (443/tcp)

2.2.4 อุปกรณ์เครือข่ายลำดับที่ 4: 172.16.201.248

หน้าที่	Router
ระบบปฏิบัติการ	Allied Telesyn AR320 Router
IP Address	172.16.201.248

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 92 รายละเอียด Port / Service ที่เปิด ของอุปกรณ์เครือข่าย 172.16.201.248

No.	Port / Service	Port Number
1	telnet	23/tcp
2	http	80/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 93 รายละเอียดของช่องโหว่ที่พบ ของอุปกรณ์เครือข่าย 172.16.201.248

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
telnet (23/tcp)	1	Allied Telesyn Router/Switch found with default password	HIGH
http (80/tcp)	2	Web Server Uses Basic Authentication	LOW

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : - ทำการ Disable Telnet หากไม่มีการใช้งาน หรือเปลี่ยนจากการใช้ Telnet เป็น Ssh
- ทำการเปลี่ยนรหัสผ่านให้มีความซับซ้อนมากยิ่งขึ้น

ลำดับที่ 2 : ทำการ Disable Http หากไม่มีการใช้งาน หรือเปลี่ยนจากการใช้ Http เป็น Https (443/tcp)

2.2.5 อุปกรณ์เครือข่ายลำดับที่ 5: 172.16.201.254

หน้าที่	Router
ระบบปฏิบัติการ	Allied Telesyn AR320 Router
IP Address	172.16.201.254

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 94 รายละเอียด Port / Service ที่เปิด ของอุปกรณ์เครือข่าย 172.16.201.254

No.	Port / Service	Port Number
1	telnet	23/tcp
2	http	80/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 95 รายละเอียดของช่องโหว่ที่พบ ของอุปกรณ์เครือข่าย 172.16.201.254

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
telnet (23/tcp)	1	Allied Telesyn Router/Switch found with default password	HIGH
http (80/tcp)	2	Web Server Uses Basic Authentication	LOW

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : - ทำการ Disable Telnet หากไม่มีการใช้งาน หรือเปลี่ยนจากการใช้ Telnet เป็น Ssh

- ทำการเปลี่ยนรหัสผ่านให้มีความซับซ้อนมากยิ่งขึ้น

ลำดับที่ 2 : - ทำการ Disable Http หากไม่มีการใช้งาน หรือเปลี่ยนจากการใช้ Http เป็น Https (443/tcp)

2.2.6 อุปกรณ์เครือข่ายลำดับที่ 6: 172.16.201.253

หน้าที่	Router
ระบบปฏิบัติการ	Allied Telesyn AR320 Router
IP Address	172.16.201.253

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 96 รายละเอียด Port / Service ที่เปิด ของอุปกรณ์เครือข่าย 172.16.201.253

No.	Port / Service	Port Number
1	telnet	23/tcp
2	http	80/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 97 รายละเอียดของช่องโหว่ที่พบ ของอุปกรณ์เครือข่าย 172.16.201.253

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
telnet (23/tcp)	1	Allied Telesyn Router/Switch found with default password	HIGH
http (80/tcp)	2	Web Server Uses Basic Authentication	LOW

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : - ทำการ Disable Telnet หากไม่มีการใช้งาน หรือเปลี่ยนจากการใช้ Telnet เป็น Ssh

- ทำการเปลี่ยนรหัสผ่านให้มีความซับซ้อนมากยิ่งขึ้น

ลำดับที่ 2 : - ทำการ Disable Http หากไม่มีการใช้งาน หรือเปลี่ยนจากการใช้ Http เป็น Https (443/tcp)

2.2.7 อุปกรณ์เครือข่ายลำดับที่ 7: 172.16.201.252

หน้าที่	Switch
ระบบปฏิบัติการ	CISCO IOS 12.1
IP Address	172.16.201.252

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 98 รายละเอียด Port / Service ที่เปิด ของอุปกรณ์เครือข่าย 172.16.201.252

No.	Port / Service	Port Number
1	telnet	23/tcp
2	http	80/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 99 รายละเอียดของช่องโหว่ที่พบ ของอุปกรณ์เครือข่าย 172.16.201.252

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
telnet (23/tcp)	1	A telnet Server is listening on the remote port	LOW

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ทำการ Disable Telnet หากไม่มีการใช้งาน หรือเปลี่ยนจากการใช้ Telnet เป็น Ssh

2.2.8 อุปกรณ์เครือข่ายลำดับที่ 8: 172.16.201.251

หน้าที่	Switch
ระบบปฏิบัติการ	3Com SuperStack Switch
IP Address	172.16.201.251

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 100 รายละเอียด Port / Service ที่เปิด ของอุปกรณ์เครือข่าย 172.16.201.251

No.	Port / Service	Port Number
1	telnet	23/tcp
2	Ssh	22/tcp
3	Efs	520/udp
4	http	80/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 101 รายละเอียดของช่องโหว่ที่พบ ของอุปกรณ์เครือข่าย 172.16.201.251

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
telnet (23/tcp)	1	A telnet Server is listening on the remote port	LOW
http (80/tcp)	2	Web Server Uses Basic Authentication	LOW

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ทำการ Disable Telnet หากไม่มีการใช้งาน หรือเปลี่ยนจากการใช้ Telnet เป็น Ssh

ลำดับที่ 2 : ทำการ Disable Http หากไม่มีการใช้งาน หรือเปลี่ยนจากการใช้ Http เป็น Https (443/tcp)

2.2.9 อุปกรณ์เครือข่ายลำดับที่ 9: 192.168.16.126

หน้าที่	Firewall
ระบบปฏิบัติการ	Sun Solaris 8
IP Address	192.168.16.126

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 102 รายละเอียด Port / Service ที่เปิด ของอุปกรณ์เครือข่าย 192.168.16.126

No.	Port / Service	Port Number
1	ftp	21/tcp
2	Ssh	22/tcp
3	Domain	53/tcp
4	Domain	53/udp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 103 รายละเอียดของช่องโหว่ที่พบ ของอุปกรณ์เครือข่าย 192.168.16.126

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
ftp (21/tcp)	1	FTP Clear Text Authentication	LOW
Ssh (22/tcp)	2	OpenSSH < 3.7.1	HIGH
	3	OpenSSH X11 Forwarding Session Hijacking	MEDIUM
Domain (53/udp)	4	DNS Server Recursive Query Enabled	MEDIUM
	5	DNS Cache Snooping	MEDIUM
	6	Remote DNS Resolver Uses Non-Random Ports	HIGH

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ควรเปลี่ยนจากการใช้ ftp เป็น Ssh แทน

ลำดับที่ 2-3 : ควรทำการ Upgrade Ssh ให้มีเวอร์ชั่นที่สูงกว่า 3.7.1

ลำดับที่ 4-6 : - ควรมีการกำหนดสิทธิ์ การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

- ทำการ Contact your DNS Server vendor for a patch

2.2.10 อุปกรณ์เครือข่ายลำดับที่ 10: 172.16.200.251

หน้าที่	Switch
ระบบปฏิบัติการ	3Com SuperStack Switch
IP Address	172.16.200.251

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 104 รายละเอียด Port / Service ที่เปิด ของอุปกรณ์เครือข่าย 172.16.200.251

No.	Port / Service	Port Number
1	telnet	23/tcp
2	Ssh	22/tcp
3	Efs	520/udp
4	http	80/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 105 รายละเอียดของช่องโหว่ที่พบ ของอุปกรณ์เครือข่าย 172.16.200.251

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
telnet (23/tcp)	1	A telnet Server is listening on the remote port	LOW
http (80/tcp)	2	Web Server Uses Basic Authentication	LOW

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ทำการ Disable Telnet หากไม่มีการใช้งาน หรือเปลี่ยนจากการใช้ Telnet เป็น Ssh

ลำดับที่ 2 : ทำการ Disable Http หากไม่มีการใช้งาน หรือเปลี่ยนจากการใช้ Http เป็น Https (443/tcp)

2.2.11 อุปกรณ์เครือข่ายลำดับที่ 11: 172.16.203.2

หน้าที่	Switch
ระบบปฏิบัติการ	CISCO IOS 12.1
IP Address	172.16.203.2

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 106 รายละเอียด Port / Service ที่เปิด ของอุปกรณ์เครือข่าย 172.16.203.2

No.	Port / Service	Port Number
1	telnet	23/tcp
2	http	80/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 107 **รายละเอียดของช่องโหว่ที่พบ ของอุปกรณ์เครือข่าย** 172.16.203.2

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
telnet (23/tcp)	1	A telnet Server is listening on the remote port	LOW
http (80/tcp)	2	Web Server Uses Basic Authentication	LOW

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ทำการ Disable Telnet หากไม่มีการใช้งาน หรือเปลี่ยนจากการใช้ Telnet เป็น Ssh

ลำดับที่ 2 : ทำการ Disable Http หากไม่มีการใช้งาน หรือเปลี่ยนจากการใช้ Http เป็น Https (443/tcp)

2.2.12 อุปกรณ์เครือข่ายลำดับที่ 12: 192.168.16.125

หน้าที่	Switch
ระบบปฏิบัติการ	Switch Alcatel
IP Address	192.168.16.125

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 108 รายละเอียด Port / Service ที่เปิด ของอุปกรณ์เครือข่าย 192.168.16.125

No.	Port / Service	Port Number
1	ftp	21/tcp
2	https	443/tcp
3	http	80/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 109 รายละเอียดของช่องโหว่ที่พบ ของอุปกรณ์เครือข่าย 192.168.16.125

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
ftp (21/tcp)	1	FTP Clear Text Authentication	LOW
http (80/tcp)	2	Web Server Uses Plain Text Authentication Forms	MEDIUM
	3	HTTP TRACE / TRACK Methods	MEDIUM
https (443/tcp)	4	OpenSSL overflow via invalid certificate passing	HIGH

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ทำการ Disable Telnet หากไม่มีการใช้งาน หรือเปลี่ยนจากการใช้ Telnet เป็น Ssh

ลำดับที่ 2-3 : ทำการ Disable Http หากไม่มีการใช้งาน

ลำดับที่ 4 : ทำการ Upgrade OpenSSL to version 0.9.6k or 0.9.7c or newer

2.3. ผลการสำรวจสถานภาพด้านความปลอดภัยเครื่องคอมพิวเตอร์ลูกข่าย

2.3.1 เครื่องคอมพิวเตอร์ลูกข่ายลำดับที่ 1: HOME-9481A27B35

ชื่อเครื่องคอมพิวเตอร์ลูกข่าย	HOME-9481A27B35
หน้าที่	Personal Computer
ระบบปฏิบัติการ	Microsoft Windows XP Professional
IP Address	172.16.10.32

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 110 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์ลูกข่าย HOME-9481A27B35

No.	Port / Service	Port Number
1	Netbios-ns	137/udp
2	Windows Terminal Services	3389/tcp
3	Microsoft-ds	445/tcp
4	Netbios-ssn	139/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 111 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์ลูกข่าย HOME-9481A27B35

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Netbios-ns (137/udp)	1	Using NetBIOS to retrieve information from a Windows host	LOW
Windows Terminal Services (3389/tcp)	2	Windows Terminal Service Enabled	LOW
	3	Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure Vulnerability	MEDIUM

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ผู้บุกรุกสามารถเข้าถึงข้อมูลที่สำคัญ เช่น คอมพิวเตอร์ชื่อเวิร์กกรุ๊ป, ชื่อปัจจุบันล็อกอินชื่อผู้ใช้ เป็นต้น แต่ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์

ลำดับที่ 2-3 : - หากไม่มีการใช้งาน Windows Terminal Services ควรทำการ Disable

- หากจำเป็นต้องใช้งาน ไม่ควรมีการเปิดสิทธิ์แบบ Allow ควรมีการตรวจสอบสิทธิ์การใช้งาน

2.3.2 เครื่องคอมพิวเตอร์ลูกข่ายลำดับที่ 2: EDIT1

ชื่อเครื่องคอมพิวเตอร์ลูกข่าย	EDIT1
หน้าที่	Personal Computer
ระบบปฏิบัติการ	Microsoft Windows XP Professional
IP Address	172.16.10.56

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 112 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์ลูกข่าย EDIT1

No.	Port / Service	Port Number
1	Netbios-ns	137/udp
2	http	80/tcp
3	Microsoft-ds	445/tcp
4	Netbios-ssn	139/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 113 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์ลูกข่าย EDIT1

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Netbios-ns (137/udp)	1	Using NetBIOS to retrieve information from a Windows host	LOW
Microsoft-ds (445/tcp)	2	SMB guest account for all users	MEDIUM
	3	SMB shares access	HIGH
http (80/tcp)	4	HTTP TRACE / TRACK Methods	MEDIUM
	5	Apache < 2.2.9 Multiple Vulnerabilities (DoS, XSS)	MEDIUM
	6	PHP < 5.2.4 Multiple Vulnerabilities	HIGH
	7	phpinfo.php	MEDIUM

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ผู้บุกรุกสามารถเข้าถึงข้อมูลที่สำคัญ เช่น คอมพิวเตอร์ชื่อเวิร์กกรุ๊ป, ชื่อปัจจุบันล็อกอินชื่อผู้ใช้ เป็นต้น แต่ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์

ลำดับที่ 2-3 : - ติดตั้ง Patch: http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่

- ติดตั้ง Patch: http://www.microsoft.com/technet/security/bulletin/ms06-035.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่

- ติดตั้ง Patch: http://www.microsoft.com/technet/security/bulletin/ms06-040.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่

- ควรมีการตรวจสอบ พอร์ต 445 สำหรับการใช้งาน เพื่อป้องกันผู้บุกรุกจากภายนอก

ลำดับที่ 4-7 : - ทำการอัพเกรด PHP ให้มี version สูงกว่า 5.2.4

- ทำการอัพเกรด Apache ให้มี version สูงกว่า 2.2.9

- ทำการ Disable HTTP TRACE / TRACK Methods

- ทำการ Disable file phpinfo.php

2.3.3 เครื่องคอมพิวเตอร์ลูกข่ายลำดับที่ 3: AB10OUTXXMOC004

ชื่อเครื่องคอมพิวเตอร์ลูกข่าย	AB10OUTXXMOC004
หน้าที่	Personal Computer
ระบบปฏิบัติการ	Microsoft Windows XP Professional
IP Address	172.16.10.63

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 114 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์ลูกข่าย AB10OUTXXMOC004

No.	Port / Service	Port Number
1	Netbios-ns	137/udp
2	Microsoft-ds	445/tcp
3	Ntp	123/udp
4	Netbios-ssn	139/tcp
5	Epmap	135/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 115 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์ลูกข่าย AB10OUTXXMOC004

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Netbios-ns (137/udp)	1	Using NetBIOS to retrieve information from a Windows host	LOW
Microsoft-ds (445/tcp)	2	SMB guest account for all users	MEDIUM
	3	SMB shares access	HIGH

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ผู้บุกรุกสามารถเข้าถึงข้อมูลที่สำคัญ เช่น คอมพิวเตอร์ชื่อเวิร์กกรุ๊ป, ชื่อปัจจุบันล็อกอินชื่อผู้ใช้ เป็นต้น แต่ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์

ลำดับที่ 2-3 : - ติดตั้ง Patch: http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่

- ติดตั้ง Patch: http://www.microsoft.com/technet/security /bulletin/ms06-035.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่

- ติดตั้ง Patch: http://www.microsoft.com/technet/security /bulletin/ms06-040.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่

- ควรมีการตรวจสอบ พอร์ต 445 สำหรับการใช้งาน เพื่อป้องกันผู้บุกรุกจากภายนอก

2.3.4 เครื่องคอมพิวเตอร์ลูกข่ายลำดับที่ 4: AA1CICTK01

ชื่อเครื่องคอมพิวเตอร์ลูกข่าย	AA1CICTK01
หน้าที่	Personal Computer
ระบบปฏิบัติการ	Microsoft Windows XP Professional
IP Address	172.16.10.64

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 116 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์ลูกข่าย AA1CICTK01

No.	Port / Service	Port Number
1	Netbios-ns	137/udp
2	Microsoft-ds	445/tcp
3	Epmap	135/tcp
4	Ntp	123/udp
5	Netbios-ssn	139/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 117 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์ลูกข่าย AA1CICTK01

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Netbios-ns (137/udp)	1	Using NetBIOS to retrieve information from a Windows host	LOW
Epmap (135/tcp)	2	RPC DCOM Interface DoS	HIGH

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ผู้บุกรุกสามารถเข้าถึงข้อมูลที่สำคัญ เช่น คอมพิวเตอร์ชื่อเวิร์กกรุ๊ป, ชื่อปัจจุบันล็อกอินชื่อผู้ใช้ เป็นต้น แต่ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์

ลำดับที่ 2 : ติดตั้ง Patch: http://www.microsoft.com/technet/security/bulletin/ms03-039.mspxสำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่

2.3.5 เครื่องคอมพิวเตอร์ลูกข่ายลำดับที่ 5: IBM-D9FE7233D4

ชื่อเครื่องคอมพิวเตอร์ลูกข่าย	IBM-D9FE7233D4
หน้าที่	Personal Computer
ระบบปฏิบัติการ	Microsoft Windows XP Professional
IP Address	172.16.10.71

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 118 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์ลูกข่าย IBM-D9FE233D4

No.	Port / Service	Port Number
1	Netbios-ns	137/udp
2	Microsoft-ds	445/tcp
3	Epmap	135/tcp
4	Ntp	123/udp
5	Netbios-ssn	139/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 119 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์ลูกข่าย IBM-D9FE233D4

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Netbios-ns (137/udp)	1	Using NetBIOS to retrieve information from a Windows host	LOW
Epmap (135/tcp)	2	RPC DCOM Interface DoS	HIGH

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ผู้บุกรุกสามารถเข้าถึงข้อมูลที่สำคัญ เช่น คอมพิวเตอร์ชื่อเวิร์กกรุ๊ป, ชื่อปัจจุบันล็อกอินชื่อผู้ใช้ เป็นต้น แต่ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์

ลำดับที่ 2 : ติดตั้ง Patch: http://www.microsoft.com/technet/security/bulletin/ms03-039.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่

2.3.6 เครื่องคอมพิวเตอร์ลูกข่ายลำดับที่ 6: TR14

ชื่อเครื่องคอมพิวเตอร์ลูกข่าย	TR14
หน้าที่	Personal Computer
ระบบปฏิบัติการ	Microsoft Windows XP Professional
IP Address	172.16.10.74

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 120 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์ลูกข่าย TR14

No.	Port / Service	Port Number
1	Netbios-ns	137/udp
2	Microsoft-ds	445/tcp
3	Epmap	135/tcp
4	Ntp	123/udp
5	Netbios-ssn	139/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 121 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์ลูกข่าย TR14

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Netbios-ns (137/udp)	1	Using NetBIOS to retrieve information from a Windows host	LOW
Microsoft-ds (445/tcp)	2	SMB guest account for all users	MEDIUM

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ผู้บุกรุกสามารถเข้าถึงข้อมูลที่สำคัญเช่นคอมพิวเตอร์ชื่อเวิร์กกรุ๊ป, ชื่อบัจจุบันล็อกอินชื่อผู้ใช้ เป็นต้น แต่ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์

ลำดับที่ 2 : ทำการ Disable User Guest

2.3.7 เครื่องคอมพิวเตอร์ลูกข่ายลำดับที่ 7: LENOVO-02AA5E49

ชื่อเครื่องคอมพิวเตอร์ลูกข่าย	LENOVO-02AA5E49
หน้าที่	Personal Computer
ระบบปฏิบัติการ	Microsoft Windows XP Professional
IP Address	172.16.10.86

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 122 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์ลูกข่าย LENOVO-02AA5E49

No.	Port / Service	Port Number
1	Netbio-ns	137/udp
2	Microsoft-ds	445/tcp
3	Epmap	135/tcp
4	Ntp	123/udp
5	Netbios-ssn	139/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 123 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์ลูกข่าย LENOVO-02AA5E49

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Netbios-ns (137/udp)	1	Using NetBIOS to retrieve information from a Windows host	LOW
Microsoft-ds (445/tcp)	2	SMB guest account for all users	MEDIUM

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ผู้บุกรุกสามารถเข้าถึงข้อมูลที่สำคัญเช่นคอมพิวเตอร์ชื่อเวิร์กกรุ๊ป, ชื่อปัจจุบันล็อกอินชื่อผู้ใช้ เป็นต้น แต่ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์

ลำดับที่ 2 : ทำการ Disable User Guest

2.3.8 เครื่องคอมพิวเตอร์ลูกข่ายลำดับที่ 8: TR44

ชื่อเครื่องคอมพิวเตอร์ลูกข่าย	TR44
หน้าที่	Personal Computer
ระบบปฏิบัติการ	Microsoft Windows XP Professional
IP Address	172.16.10.87

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 124 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์ลูกข่าย TR44

No.	Port / Service	Port Number
1	Netbios-ns	137/udp
2	ftp	21/tcp
3	Microsoft-ds	445/tcp
4	Netbios-ssn	139/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 125 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์ลูกข่าย TR44

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Netbios-ns (137/udp)	1	Using NetBIOS to retrieve information from a Windows host	LOW
Microsoft-ds (445/tcp)	2	SMB guest account for all users	MEDIUM
	3	SMB shares access	HIGH

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ผู้บุกรุกสามารถเข้าถึงข้อมูลที่สำคัญ เช่น คอมพิวเตอร์ชื่อเวิร์กกรุ๊ป, ชื่อปัจจุบันล็อกอินชื่อผู้ใช้ เป็นต้น แต่ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์

ลำดับที่ 2-3 : - ติดตั้ง Patch: http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่

- ติดตั้ง Patch: http://www.microsoft.com/technet/security

/bulletin/ms06-035.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่

- ติดตั้ง Patch: http://www.microsoft.com/technet/security

/bulletin/ms06-040.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่

- ควรมีการตรวจสอบ พอร์ต 445 สำหรับการใช้งาน เพื่อป้องกันผู้บุกรุกจากภายนอก

2.3.9 เครื่องคอมพิวเตอร์ลูกข่ายลำดับที่ 9: IBMC1044

ชื่อเครื่องคอมพิวเตอร์ลูกข่าย	IBMC1044
หน้าที่	Personal Computer
ระบบปฏิบัติการ	Microsoft Windows XP Professional
IP Address	172.16.10.114

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 126 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์ลูกข่าย IBMC1044

No.	Port / Service	Port Number
1	Netbios-ns	137/udp
2	VMware ESX/GSX	912/tcp
3	Daytime	13/tcp
4	Microsoft-ds	445/tcp
5	Epmap	135/tcp
6	Netbios-ssn	139/tcp
7	Time	37/tcp
8	ftp-ssl	990/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 127 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์ลูกข่าย IBMC1044

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Netbios-ns (137/udp)	1	Using NetBIOS to retrieve information from a Windows host	LOW
Epmap (135/tcp)	2	RPC DCOM Interface DoS	HIGH

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ผู้บุกรุกสามารถเข้าถึงข้อมูลที่สำคัญ เช่น คอมพิวเตอร์ชื่อเวิร์กกรุ๊ป, ชื่อปัจจุบันล็อกอินชื่อผู้ใช้ เป็นต้น แต่ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์

ลำดับที่ 2 : ติดตั้ง Patch: http://www.microsoft.com/technet/security/bulletin/ms03-039.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่

2.3.10 เครื่องคอมพิวเตอร์ลูกข่ายลำดับที่ 10: IBM-D9FE7233D4

ชื่อเครื่องคอมพิวเตอร์ลูกข่าย	IBM-D9FE7233D4
หน้าที่	Personal Computer
ระบบปฏิบัติการ	Microsoft Windows XP Professional
IP Address	172.16.11.70

(1) รายละเอียด Port / Service ที่เปิด

ตารางที่ 128 รายละเอียด Port / Service ที่เปิด ของเครื่องคอมพิวเตอร์ลูกข่าย IBM-D9FE7233D4

No.	Port / Service	Port Number
1	Netbios-ns	137/udp
2	Microsoft-ds	445/tcp
3	Epmap	135/tcp
4	VNC	5900/tcp
5	http	80/tcp
6	Ntp	123/udp
7	Netbios-ssn	139/tcp
8	Vnc-http	5800/tcp

(2) รายละเอียดของช่องโหว่ที่พบ

ตารางที่ 129 รายละเอียดของช่องโหว่ที่พบ ของเครื่องคอมพิวเตอร์ลูกข่าย IBM-D9FE7233D4

Port / Service	ลำดับที่	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Netbios-ns (137/udp)	1	Using NetBIOS to retrieve information from a Windows host	LOW
Microsoft-ds (445/tcp)	2	SMB guest account for all users	MEDIUM
	3	SMB shares access	HIGH

(3) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

ลำดับที่ 1 : ผู้บุกรุกสามารถเข้าถึงข้อมูลที่สำคัญ เช่น คอมพิวเตอร์ชื่อเวิร์กกรุ๊ป, ชื่อปัจจุบันล็อกอินชื่อผู้ใช้ เป็นต้น แต่ไม่มีผลกระทบกับเครื่องคอมพิวเตอร์

ลำดับที่ 2-3 : - ติดตั้ง Patch: http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่

- ติดตั้ง Patch: http://www.microsoft.com/technet/security/bulletin/ms06-035.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่

- ติดตั้ง Patch: http://www.microsoft.com/technet/security/bulletin/ms06-040.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่

- ควรมีการตรวจสอบ พอร์ต 445 สำหรับการใช้งาน เพื่อป้องกันผู้บุกรุกจากภายนอก

3. ผลการวิเคราะห์ช่องโหว่ในเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย

จากการสำรวจสถานภาพด้านความปลอดภัย ที่ปรึกษาได้นำผลที่ได้มาวิเคราะห์ ตรวจพบสาเหตุของการเกิดช่องโหว่ในเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย โดยสามารถสรุปประเด็น ดังนี้

3.1 การตั้งค่ารหัสผ่าน

เครื่องคอมพิวเตอร์แม่ข่าย ที่สามารถเจาะเข้าสู่ระบบได้ด้วยการสุ่มรหัสผ่านจากไฟล์ Dictionary ที่เก็บรหัสผ่านที่นิยมใช้กันไว้จำนวนมาก และทดสอบใช้รหัสผ่านจากไฟล์ดังกล่าวป้อนเข้าสู่หน้าจอ login ไปเรื่อย ๆ จนหมด หรือจนสามารถได้รหัสผ่านที่ถูกต้อง โดยวิธีการนี้ถูกเรียกอย่างเป็นทางการว่า Dictionary Attack

ตารางที่ 130 การตั้งค่ารหัสผ่านของเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่าย

เครื่องคอมพิวเตอร์แม่ข่าย	Service or Port	User	Password
192.168.16.2 (PXMNRE)	ftp	Anonymous	[blank password]
192.168.16.3 (DCS)	ftp	Anonymous	[blank password]
		ftp	[blank password]
192.168.16.9 (MISMNRE)	ftp	Anonymous	[blank password]
		ftp	[blank password]
172.16.1.37 (INVENT)	ftp	Anonymous	[blank password]
		ftp	[blank password]
172.16.1.45 (WAREHOUSE)	ftp	Anonymous	[blank password]
		ftp	[blank password]
172.16.1.61 (AVMNRE)	ftp	Anonymous	[blank password]
		ftp	[blank password]
172.16.1.107 (BACKUP-SERVER)	ftp	Anonymous	[blank password]
		ftp	[blank password]
172.16.1.108 (LOG-MANAGEMENT)	ftp	Anonymous	[blank password]
		ftp	[blank password]

(1) ผลกระทบ (Impact)

1) ทำให้ผู้บุกรุกสามารถสุ่มรหัสผ่าน ได้ง่าย

(2) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

1) ควรมีการติดตั้งค่ารหัสผ่านให้มีความซับซ้อนเพื่อป้องกันผู้บุกรุกสามารถเดาสุ่ม ได้ง่าย

2) ทำการ Disable user Anonymous ออกจากเครื่องคอมพิวเตอร์แม่ข่าย

3.2 การปรับปรุงเวอร์ชั่น Patch หรือ Hot Fix

3.2.1 ระบบปฏิบัติการ Microsoft Windows ไม่ได้ติดตั้ง Patch ที่เป็นเวอร์ชั่นปัจจุบัน ซึ่งได้แก่เครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ดังต่อไปนี้

ตารางที่ 131 เครื่องคอมพิวเตอร์แม่ข่ายที่ต้องมีการปรับปรุงเวอร์ชั่น Patch หรือ Hot Fix

ลำดับที่	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	หมายเลขไอพี	ระบบปฏิบัติการ	Security Patch ที่ยังไม่ได้ติดตั้ง
1	GISFILESERVER	172.16.1.36	Windows Server 2003 SP2	MS08-067
2	WAREHOUSE	172.16.1.45	Windows Server 2003 SP2	MS08-040
3	GISWEB	172.16.1.52	Windows Server 2003 SP1	MS08-067
4	GOOGLEMNRE	172.16.1.57	Windows Server 2003 SP1	MS08-040
5	NMS	172.16.201.1	Windows Server 2003 SP1	MS08-067 MS06-035 MS06-040
6	CICTDB	192.168.16.120	Windows XP SP2	MS03-039

ตารางที่ 132 เครื่องคอมพิวเตอร์ลูกข่ายที่ต้องมีการปรับปรุงเวอร์ชั่น Patch หรือ Hot Fix

ลำดับที่	ชื่อเครื่องคอมพิวเตอร์ลูกข่าย	หมายเลขไอพี	ระบบปฏิบัติการ	Security Patch ที่ยังไม่ได้ติดตั้ง
1	AA11CICTK01	172.16.10.64	Microsoft Windows XP Professional	MS03-039
2	MICROSOF-F44D0A	172.16.10.71	Microsoft Windows XP Professional	MS03-039
3	IBMC1044	172.16.10.114	Microsoft Windows XP Professional	MS03-039
4	EDIT1	172.16.10.56	Microsoft Windows XP Professional	MS08-067 MS06-035 MS06-040
5	AB10OUTXXMOC004	172.16.10.63	Microsoft Windows XP Professional	MS08-067 MS06-035 MS06-040
6	TR14	172.16.10.87	Microsoft Windows XP Professional	MS08-067 MS06-035 MS06-040

(1) ผลกระทบ (Impact)

- ทำให้ผู้บุกรุกสามารถเข้าสู่เครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย จากช่องโหว่ของ patch ได้ง่าย

(2) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- ควรมีการติดตั้ง patch ให้กับเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่าย เพื่อป้องกันผู้บุกรุก

3.2.2 เครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ที่ไม่ได้ Upgrade PHP ซึ่งได้แก่เครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ดังต่อไปนี้

ตารางที่ 133 เครื่องคอมพิวเตอร์แม่ข่ายที่ต้องมีการปรับปรุงเวอร์ชั่น PHP

ลำดับที่	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	หมายเลขไอพี	Patch ที่ยังไม่ได้ติดตั้ง
1	ZINC	192.168.16.4	upgrade PHP ver 4.4.1
2	COPPER	192.168.16.5	upgrade PHP ver 5.2.7
3	KNOWNLEDGE	192.168.16.8	upgrade PHP ver 4.4.1
4	EPROJECT	192.168.16.10	upgrade PHP ver 4.4.1
5	TEST1	172.16.1.5	upgrade PHP ver 4.4.1
6	TEST2	172.16.1.6	upgrade PHP ver 4.4.1
7	DATATRAINING	172.16.1.35	upgrade PHP ver 4.4.1
8	GISFILESERVER	172.16.1.36	upgrade PHP ver 4.4.1
9	INVENT	172.16.1.37	upgrade PHPmyadmin ver 2.6.4
10	INTEL_SERVER	172.16.1.47	upgrade PHP ver 4.4.9
11	LITHUIM	172.16.1.64	upgrade PHP ver 4.4.9
12	SERVER	172.16.1.65	upgrade PHP ver 4.4.9

ตารางที่ 134 เครื่องคอมพิวเตอร์ลูกข่ายที่ต้องมีการปรับปรุงเวอร์ชั่น PHP

ลำดับที่	ชื่อเครื่องคอมพิวเตอร์ลูกข่าย	หมายเลขไอพี	Patch ที่ยังไม่ได้ติดตั้ง
1	EDIT1	172.16.10.56	upgrade PHP ver 5.2.4

(1) ผลกระทบ (Impact)

- ทำให้ผู้บุกรุกสามารถเข้าสู่เครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายจากช่องโหว่ของ PHP ได้ง่าย

(2) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- ควรมีการติดตั้ง version PHP ให้กับเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่าย เพื่อป้องกันผู้บุกรุก

3.2.3 เครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ที่ไม่ได้ Upgrade Apache ซึ่งได้แก่เครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ดังต่อไปนี้

ตารางที่ 135 เครื่องคอมพิวเตอร์แม่ข่ายที่ต้องมีการปรับปรุงเวอร์ชั่น Apache

ลำดับที่	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	หมายเลขไอพี	Patch ที่ยังไม่ได้ติดตั้ง
1	PXMNRE	192.168.16.2	upgrade apache ver 2.2.9
2	ZINC	192.168.16.4	upgrade apache ver 2.0.59
3	COPPER	192.168.16.5	upgrade apache ver 2.2.9
4	E-PETITION	192.168.16.7	แก้ไข redirectMatch
5	DATATRAINING	172.16.1.35	upgrade apache ver 1.3.37 and update apache's configuration file(s)
6	GISFILESERVER	172.16.1.36	upgrade apache ver 1.3.37 and update apache's configuration file(s)
7	INTEL_SERVER	172.16.1.47	upgrade apache ver 2.0.59
8	LITHUIM	172.16.1.64	upgrade apache ver 1.3.37
9	SERVER	172.16.1.65	upgrade apache ver 1.3.42
10	CICTDB	192.168.16.120	upgrade apache ver. 1.3.28

ตารางที่ 136 เครื่องคอมพิวเตอร์ลูกข่ายที่ต้องมีการปรับปรุงเวอร์ชั่น Apache

ลำดับที่	ชื่อเครื่องคอมพิวเตอร์ลูกข่าย	หมายเลขไอพี	Patch ที่ยังไม่ได้ติดตั้ง
1	EDIT1	172.16.10.56	upgrade apache ver 2.2.9

(1) ผลกระทบ (Impact)

- ทำให้ผู้บุกรุกสามารถเข้าสู่เครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายจากช่องโหว่ของ Apache ได้ง่าย

(2) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- ควรมีการติดตั้ง version Apache ให้กับเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่าย เพื่อป้องกันผู้บุกรุก

3.2.4 เครื่องคอมพิวเตอร์แม่ข่ายที่ไม่ได้ Upgrade MySql ซึ่งได้แก่เครื่องคอมพิวเตอร์แม่ข่ายดังต่อไปนี้

ตารางที่ 137 เครื่องคอมพิวเตอร์แม่ข่ายที่ต้องมีการปรับปรุงเวอร์ชั่น MySql

ลำดับที่	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	หมายเลขไอพี	Patch ที่ยังไม่ได้ติดตั้ง
1	ZINC	192.168.16.4	update mysql ver. 4.0.25
2	KNOWNLEDGE	192.168.16.8	update mysql ver. 4.0.25
3	MISMNRE	192.168.16.9	update mysql ver. 4.0.25
4	TEST1	172.16.1.5	update mysql ver. 4.0.25
5	GISFILESERVER	172.16.1.36	update mysql ver. 4.0.25

(1) ผลกระทบ (Impact)

- ทำให้ผู้บุกรุกสามารถเข้าสู่เครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายจากช่องโหว่ของ Apache ได้ง่าย

(2) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- ควรมีการติดตั้ง version MySql ให้กับเครื่องคอมพิวเตอร์แม่ข่าย เพื่อป้องกันผู้บุกรุก

3.2.5 เครื่องคอมพิวเตอร์แม่ข่ายที่ไม่ได้ Upgrade Jboss ซึ่งได้แก่เครื่องคอมพิวเตอร์แม่ข่ายดังต่อไปนี้

ตารางที่ 138 เครื่องคอมพิวเตอร์แม่ข่ายที่ต้องมีการปรับปรุงเวอร์ชั่น Jboss

ลำดับที่	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	หมายเลขไอพี	Patch ที่ยังไม่ได้ติดตั้ง
1	E-PETITION	192.168.16.7	Upgrade Jboss EAP ver. 4.2.0.cp03/4.3.0. cp01

(1) ผลกระทบ (Impact)

- ทำให้ผู้บุกรุกสามารถเข้าสู่เครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายจากช่องโหว่ของ Jboss ได้ง่าย

(2) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- ควรมีการติดตั้ง version Jbossl ให้กับเครื่องคอมพิวเตอร์แม่ข่าย เพื่อป้องกันผู้บุกรุก

3.2.6 เครื่องคอมพิวเตอร์แม่ข่ายที่ไม่ได้ Upgrade ArgoSoft Mail ซึ่งได้แก่เครื่องคอมพิวเตอร์แม่ข่ายดังต่อไปนี้

ตารางที่ 139 เครื่องคอมพิวเตอร์แม่ข่ายที่ต้องมีการปรับปรุงเวอร์ชั่น ArgoSoft Mail

ลำดับที่	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย	หมายเลขไอพี	Patch ที่ยังไม่ได้ติดตั้ง
1	GISWEB	172.16.1.52	upgrade ArgoSoft Mail server 1.8.8.6 or later

(1) ผลกระทบ (Impact)

- ทำให้ผู้บุกรุกสามารถเข้าสู่เครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายจากช่องโหว่ของ AR ได้ง่าย

(2) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- ควรมีการติดตั้ง version AR ให้กับเครื่องคอมพิวเตอร์แม่ข่าย เพื่อป้องกันผู้บุกรุก

3.2.7 เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย ที่ไม่ได้ Upgrade OpenSSL ซึ่งได้แก่เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย ดังต่อไปนี้

ตารางที่ 140 เครื่องคอมพิวเตอร์แม่ข่ายที่ต้องมีการปรับปรุงเวอร์ชั่น OpenSSL

ลำดับที่	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย/อุปกรณ์เครือข่าย	หมายเลขไอพี	Patch ที่ยังไม่ได้ติดตั้ง
1	CICTDB	192.168.16.120	upgrade OpenSSL to ver. 0.9.6k
2	อุปกรณ์เครือข่าย	192.168.16.125	upgrade OpenSSL to ver. 0.9.6k or 0.9.7c or newer

(1) ผลกระทบ (Impact)

- ทำให้ผู้บุกรุกสามารถเข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย จากช่องโหว่ของ OpenSSL ได้ง่าย

(2) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- ควรมีการติดตั้ง version OpenSSL ให้กับเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย เพื่อป้องกันผู้บุกรุก

3.3 การเปิดใช้งาน Port / Service

จากผลลัพธ์ที่ได้จากการตรวจสอบสถานภาพด้านความปลอดภัยโดยใช้โปรแกรมในการตรวจสอบ ได้แก่ Internet Scanner (ISS), X-Scan และ Nessus พบว่าเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย มีการเปิดใช้งาน Port / Service เกินความจำเป็น เมื่อเทียบกับระบบงานของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย อาจส่งผลกระทบต่อการถูกบุกรุก ซึ่งอาจทำให้เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ทำงานช้าหรือผู้บุกรุกสามารถเข้าผ่านช่องทาง Port / Service ด้วยวิธีการต่าง ๆ กัน ตามแต่ Port / Service ที่เปิด เช่น การใช้ Exploit หรือการ Brute Force รหัสผ่าน ไปยังเครื่องคอมพิวเตอร์แม่ข่าย ทำให้สามารถได้ข้อมูลต่าง ๆ ภายในเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย หากผู้ดูแลระบบไม่ได้ทำการตรวจสอบ การเปิดใช้งาน Port / Service ต่าง ๆ ที่ไม่มีการใช้งาน หรือมีการใช้งานเสร็จสิ้นแล้วไม่ได้มีการปิด Port / Service ดังกล่าว บนเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ที่ปรึกษา ได้ดำเนินการวิเคราะห์ผลจากการตรวจสอบสถานภาพด้านความปลอดภัยของ สป.ทส. ทำให้พบว่า มี Port / Service ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย มีช่องโหว่ สามารถสรุป ได้ดังนี้

3.3.1 การเปิดใช้งาน Port / Service ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่อง คอมพิวเตอร์ลูกข่าย

ตารางที่ 141 การเปิดใช้งาน Port / Service ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ของ Microsoft-ds (445/tcp)

Port / Service	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย/อุปกรณ์เครือข่าย/เครื่องคอมพิวเตอร์ลูกข่าย	หมายเลขไอพี	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Microsoft-ds (445/tcp)	GISWEB NMS	172.16.1.52 172.16.201.1	SMB LanMan Pipe Server browse listing	[illegible]
	EDIT1	172.16.10.56	SMB shares access	HIGH
	AB10OUTXXMOC004 TR14 LENOVO-02AA5E49 TR44 IBM-D9FE7233D4 MMNRE CICTDB	172.16.10.63 172.16.10.74 172.16.10.86 172.16.10.87 172.16.11.70 172.16.1.62 192.168.16.120	Vulnerability in Server Service Could Allow Remote Code Execution (917159)	HIGH
			Vulnerability in Server Service Could Allow Remote Code Execution (921883)	HIGH

(1) ผลกระทบ (Impact)

- ช่องโหว่ของ Microsoft-ds ทำให้ผู้บุกรุกใช้ช่องทางเหล่านี้ทำการบุกรุก เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่ายได้
- ทำให้ผู้บุกรุกทำการเข้ามายึดเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่ายได้ ผ่าน Port เหล่านี้ได้โดยใช้การยิง Exploit ผ่านทาง Port ดังกล่าวได้

(2) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- ติดตั้ง Security Patch: http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ที่พบช่องโหว่
- ติดตั้ง Security Patch: http://www.microsoft.com/technet/security/bulletin/ms06-035.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ที่พบช่องโหว่
- ติดตั้ง Security Patch: http://www.microsoft.com/technet/security/bulletin/ms06-040.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ที่พบช่องโหว่
- ควรมีการตรวจสอบ พอร์ต 445 สำหรับการใช้งาน เพื่อป้องกันผู้บุกรุกจากภายนอก
- ทำการปิด shares หากไม่มีการใช้งาน หรือควรมีการกำหนดสิทธิ์ในการเข้าถึง file shares

ตารางที่ 142 การเปิดใช้งาน Port / Service ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ของ http (80/tcp), https (443/tcp)

Port / Service	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย/อุปกรณ์เครือข่าย/เครื่องคอมพิวเตอร์ลูกข่าย	หมายเลขไอพี	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
http (80/tcp) https (443/tcp)	EDOC	192.168.16.3	WebDAV enabled	MEDIUM
	DATATRAINING PXMNRE	172.16.1.35 192.168.16.2	Test HTTP dangerous methods	HIGH
	EDOC ZINC	192.168.16.3 192.168.16.4	PHP < 5.2.7 Multiple Vulnerabilities	HIGH
	COPPER E-PETITON	192.168.16.5 192.168.16.7	Web Server Cross Site Scripting	MEDIUM
	KNOWNLEDGR MISMNRE EPROJECT	192.168.16.8 192.168.16.9 192.168.16.10	Web Server Uses Plain Text Authentication Forms	MEDIUM

Port / Service	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย/อุปกรณ์เครือข่าย/เครื่องคอมพิวเตอร์ลูกข่าย	หมายเลขไอพี	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
	TEST1	172.16.1.5	phpinfo.php	MEDIUM
	TEST2	172.16.1.6	Apache < 2.2.9 Multiple Vulnerabilities (DoS,XSS)	MEDIUM
	GISFILESERVE	172.16.1.36		
	INVENT	172.16.1.37	Private IP address leaked in HTTP headers	LOW
	WAREHOUSE	172.16.1.45		
	INTEL_SERVER	172.16.1.47	Find if IIS Server Allows BASIC and/or NTLM authentication	LOW
	GISWEB	172.16.1.52		
	AVMNRE	172.16.1.61		
	LITHUIM	172.16.1.64	HTTP TRACE / TRACK Methods	MEDIUM
	SERVER	172.16.1.65		
	BACKUP-SERVER	172.16.1.107	PHP < 4.4.5 Multiple Vulnerabilities	HIGH
	LOG-MANAGEMENT	172.16.1.108		
	EDIT1	172.16.10.56	PHP < 4.4.1 / 5.0.6 Multiple Vulnerabilities	HIGH
	CICTDB	192.168.16.120		
	TEST3	172.16.1.20	Apache mod_proxy_ftp Directory Component Wildcard Character Globbing XSS	MEDIUM
	อุปกรณ์เครือข่าย	172.16.201.249		
	อุปกรณ์เครือข่าย	172.16.201.248		
	อุปกรณ์เครือข่าย	172.16.201.254		
	อุปกรณ์เครือข่าย	172.16.201.253	Web Server hosting copyrighted material	MEDIUM
	อุปกรณ์เครือข่าย	172.16.201.251		
	อุปกรณ์เครือข่าย	172.16.200.251	JBoss Enterprise Application Platform (EAP) Status Servlet Request Remote Information Disclosure	MEDIUM
	อุปกรณ์เครือข่าย	172.16.203.2		
	อุปกรณ์เครือข่าย	192.168.16.125		

Port / Service	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย/อุปกรณ์เครือข่าย/เครื่องคอมพิวเตอร์ลูกข่าย	หมายเลขไอพี	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
			Test HTTP dangerous methods	HIGH
			Apache UserDir Sensitive Information Disclosure	LOW
			Apache /Server-status accessible	MEDIUM
			Apache < 1.3.37	HIGH
			Apache < 1.3.41 Multiple Vulnerabilities (DoS, XSS)	MEDIUM
			PHP < 4.4.3 / 5.1.4 Multiple Vulnerabilities	HIGH
			PHP < 4.4.1 / 5.0.6 Multiple Vulnerabilities	HIGH
			AppServ appserv/main.php appserv_root Variable Remote File Inclusion	MEDIUM
			phpMyAdmin XSS	MEDIUM
			PHPMyAdmin < 2.6.4 Cross-Site Scripting Vulnerabilities	MEDIUM

(1) ผลกระทบ (Impact)

- ทำให้ผู้บุกรุกทำการเข้ามายึดเครื่องได้ ผ่าน Port เหล่านี้ได้โดยใช้ Remote Admin Exploit
- ทำให้ผู้บุกรุกสามารถทำการ Cross site scripting ทำให้เกิด Buffer overflow กับเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ได้

(1) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- ติดตั้ง Security Patch: http://www.microsoft.com/technet/security/bulletin/ms03-039.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่
- ทำการเปลี่ยนจากการใช้ พอร์ต 80 (www 80/tcp) เป็นพอร์ต 8080 (www 8080/tcp) หรือพอร์ต 443 (https 443/tcp) แทน เพื่อป้องกันการถูกบุกรุก
- ทำการปิดพอร์ต 80 บนเครื่องคอมพิวเตอร์แม่ข่าย หากไม่มีการใช้งานดังกล่าว
- หากไม่มีการใช้งาน WebDEV ควรทำการ Disable
- ทำการอัพเกรด IIS ให้เหมาะสมกับปัจจุบัน เพื่อป้องกัน การถูกบุกรุก
- ทำการอัพเกรด PHP ให้เหมาะสมกับปัจจุบัน เพื่อป้องการการถูกบุกรุก
- ทำการอัพเกรด Apache ให้เหมาะสมกับปัจจุบัน เพื่อป้องการการถูกบุกรุก
- ควรทำการ Delete file phpinfo.php เพื่อป้องกันผู้บุกรุกค้นหาข้อมูลจาก file ดังกล่าว
- หากมีการใช้งาน IIS ที่ Allows หรือมีการตั้งค่ารหัสผ่านที่ไม่ซับซ้อนก็อาจทำให้ผู้บุกรุกสามารถเข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย ดังนั้นควรมีการตรวจสอบการตั้งค่ารหัสผ่าน

ตารางที่ 143 การเปิดใช้งาน Port / Service ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ของ http-alt (8080/tcp)

Port / Service	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย/อุปกรณ์เครือข่าย/เครื่องคอมพิวเตอร์ลูกข่าย	หมายเลขไอพี	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
http-alt (8080/tcp)	WAREHOUSE	172.16.1.45	Tomcat snoop.jsp Cross-Site Scripting Vulnerability	MEDIUM
			Tomcat Hello World Sample App Cross-Site Scripting Vulnerability	MEDIUM
			Apache UserDir Sensitive Information Disclosure	LOW

(1) ผลกระทบ (Impact)

- ทำให้ผู้บุกรุกทำการเข้ามายึดเครื่องได้ ผ่าน Port เหล่านี้ได้โดยใช้ Remote Admin Exploit
- ทำให้ผู้บุกรุกสามารถทำการ Cross site scripting ทำให้เกิด Buffer overflow กับเครื่องคอมพิวเตอร์แม่ข่ายได้

(2) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- ทำการปิดพอร์ต 8080 บนเครื่องคอมพิวเตอร์แม่ข่าย หากไม่มีการใช้งานดังกล่าว
- ทำการตรวจสอบค่า remote proxy ที่เข้ามาภายในเครือข่ายเพื่อป้องกันการถูกบุกรุก
- ไม่ทำการ Deploy the Tomcat ทั้งในส่วนของตัวอย่าง หรือเอกสารต่าง ๆ ที่เกี่ยวกับ Web application ของเครื่องคอมพิวเตอร์แม่ข่าย

ตารางที่ 144 การเปิดใช้งาน Port / Service ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ของ Oracle Database (1521/tcp)

Port / Service	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย/อุปกรณ์เครือข่าย/เครื่องคอมพิวเตอร์ลูกข่าย	หมายเลขไอพี	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Oracle Database (1521/tcp)	DATATRAINING GISWEB CICTDB	172.16.1.35 172.16.1.52 192.168.16.120	Oracle SET TIME_ZONE Query Overflow	HIGH
			Oracle DBS_SCHEDULER Remote Command Execution	HIGH
			Oracle CREATE DATABASE LINK Query Overflow	HIGH
			Oracle Database 8i/9i Multiple Directory Traversal Vulnerabilities	MEDIUM
			Oracle SOAP / XML Remote Denial of Service	HIGH
			Unpassworded Oracle Listener Program (tnslsnr) Service	MEDIUM

(1) ผลกระทบ (Impact)

- ช่องโหว่ของ Port ดังกล่าวทำให้ผู้บุกรุกสามารถเข้ามาทำการยึดเครื่องคอมพิวเตอร์แม่ข่ายได้ โดยการยิง Exploit โดยผ่านทาง Port ดังกล่าว

(2) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- ทำการ Upgrade Oracle version 9.0.2.3 เพื่อป้องกันผู้บุกรุก
- ทำการ Update Patch Oracle เพื่อป้องการผู้บุกรุก
- ทำการ ใช้ CHANGE_PASSWORD command เพื่อทำการกำหนดค่ารหัสผ่าน

- ดูรายละเอียดเพิ่มเติม http://metalink.oracle.com
- ดูรายละเอียดเพิ่มเติม http://www.nextgenss.com/advisories/ora_time_zone.txt
- ดูรายละเอียดเพิ่มเติม http://www.oracle.com/technology/deploy/security/pdf/2004alert68.pdf
- ดูรายละเอียดเพิ่มเติม http://otn.oracle.com/deploy/security/pdf/2003alert54.pdf

ตารางที่ 145 การเปิดใช้งาน Port / Service ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ของ epmap (135/tcp)

Port / Service	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย/อุปกรณ์เครือข่าย/เครื่องคอมพิวเตอร์ลูกข่าย	หมายเลขไอพี	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
epmap (135/tcp)	AA11CICTK01 MICROSOF-F44D0A IBMC1044 CICTDB	172.16.10.64 172.16.10.71 172.16.10.114 192.168.16.120	RPC DCOM Interface DoS	HIGH

(1) ผลกระทบ (Impact)

- ช่องโหว่ของ RPC ทำให้ผู้บุกรุกสามารถเข้ามาทำการยึดเครื่องคอมพิวเตอร์ และได้สิทธิ์ admin เพื่อทำการจัดการเครื่องคอมพิวเตอร์แม่ข่ายได้

(2) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- ติดตั้ง Security Patch: http://www.microsoft.com/technet/security/bulletin/ms03-039.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่
- ควรมีการตรวจสอบ พอร์ต 135 สำหรับการใช้งาน เพื่อป้องการผู้บุกรุกจากภายนอก

ตารางที่ 146 การเปิดใช้งาน Port / Service ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ของ snmp (161/udp)

Port / Service	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย/อุปกรณ์เครือข่าย/เครื่องคอมพิวเตอร์ลูกข่าย	หมายเลขไอพี	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
snmp (161/udp)	UPS1849 อุปกรณ์เครือข่าย	172.16.1.13 192.168.4.27	Snmp-Password: "public"	HIGH

(1) ผลกระทบ (Impact)

- ช่องโหว่ของ SNMP ทำให้ผู้บุกรุกสามารถเดาพาสเวิร์ดได้ง่าย ซึ่งเป็นช่องทางที่ทำให้ผู้บุกรุก เข้าสู่เครื่องคอมพิวเตอร์แม่ข่ายได้ ซึ่งทำให้ผู้บุกรุก สามารถได้ข้อมูลเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายได้ เพื่อใช้เป็นข้อมูลเบื้องต้นในการดำเนินการต่อไป

(2) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- ทำการเปลี่ยน รหัสผ่าน SNMP บนเครื่องคอมพิวเตอร์แม่ข่าย ให้มีความซับซ้อนมากขึ้น เพื่อป้องกันผู้บุกรุกเดาสุ่ม ได้ง่าย
- ทำการ Disable SNMP บนเครื่องคอมพิวเตอร์แม่ข่าย หากไม่มีการใช้งาน

ตารางที่ 147 การเปิดใช้งาน Port / Service ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ของ ftp (21/tcp)

Port / Service	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย/อุปกรณ์เครือข่าย/เครื่องคอมพิวเตอร์ลูกข่าย	หมายเลขไอพี	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
ftp (21/tcp)	IS~WALLBOARD	192.168.16.12	FTP-Password: "ftp/[Blank password]"	HIGH
	NICNATURAL	192.168.16.14		
	FIREWALL	192.168.16.126	FTP-Password: "anonymous/[Blank password]"	HIGH
	INVENT	172.16.1.37		
	WAREHOUSE	172.16.1.45		
	AVMNRE	172.16.1.61	Anonymous FTP enabled	LOW
	BACKUP-SERVER	172.16.1.107	FTP Clear Text Authentication	LOW
	LOG-MANAGEMENT	172.16.1.108		
	FIREWALL	192.168.16.126		
	อุปกรณ์เครือข่าย	192.168.16.125		

(1) ผลกระทบ (Impact)

- ช่องโหว่ของ FTP ทำให้ผู้บุกรุกสามารถใช้เป็นช่องทางที่ทำให้ผู้บุกรุก เข้าสู่เครื่องคอมพิวเตอร์แม่ข่ายได้ ซึ่งทำให้ผู้บุกรุก สามารถทำการ execute command บนเครื่องคอมพิวเตอร์แม่ข่ายได้
- ทำให้ผู้บุกรุก สามารถเดาสุ่ม พาสเวิร์ด ได้ง่าย

(2) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- ทำการเปลี่ยน รหัสผ่าน FTP บนเครื่องคอมพิวเตอร์แม่ข่าย ให้มีความซับซ้อนมากขึ้น เพื่อป้องกันผู้บุกรุกเดาสุ่มได้ง่าย
- ทำการ disable user anonymous ออกจากเครื่องคอมพิวเตอร์แม่ข่าย
- ทำการอัพเกรด FTP บนเครื่องคอมพิวเตอร์แม่ข่าย หากมีความจำเป็นต้องใช้ FTP
- ทำการเปลี่ยนจากการใช้ FTP เป็น SSH เพื่อป้องกันผู้บุกรุกจากภายนอก

ตารางที่ 148 การเปิดใช้งาน Port / Service ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ของ telnet (23/tcp)

Port / Service	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย/อุปกรณ์เครือข่าย/เครื่องคอมพิวเตอร์ลูกข่าย	หมายเลขไอพี	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
telnet (23/tcp)	อุปกรณ์เครือข่าย	192.168.4.27	A Telnet Server is listening or the remote port	LOW
	อุปกรณ์เครือข่าย	172.16.1.254		
	อุปกรณ์เครือข่าย	172.16.201.249	Allied Telesyn Router/Switch found with default password	HIGH
	อุปกรณ์เครือข่าย	172.16.200.251		
	อุปกรณ์เครือข่าย	172.16.203.2		

(1) ผลกระทบ (Impact)

- มีการเปิดใช้งาน Telnet ซึ่งอาจทำให้ผู้บุกรุกสามารถ brute force รหัสผ่านหรือดักจับข้อมูล (sniff) เพื่อเอารหัสผ่านของเครื่องคอมพิวเตอร์แม่ข่ายได้

(2) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- ทำการปิดการใช้งาน Telnet ในเครื่องคอมพิวเตอร์แม่ข่าย และเปลี่ยนมาเป็นการใช้งาน Ssh แทน
- ทำการเปลี่ยน รหัสผ่าน Telnet ให้มีความซับซ้อนมากขึ้น เพื่อป้องกันผู้บุกรุกเดาสุ่มได้ง่าย
- ทำการ Disable Telnet บนเครื่องคอมพิวเตอร์แม่ข่าย หากไม่มีการใช้งานดังกล่าว

ตารางที่ 149 การเปิดใช้งาน Port / Service ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ของ smtp (25/tcp)

Port / Service	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย/อุปกรณ์เครือข่าย/เครื่องคอมพิวเตอร์ลูกข่าย	หมายเลขไอพี	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Smtp (25/tcp)	GISWEB	172.16.1.52	EXPN and VRFY commands	LOW

(1) ผลกระทบ (Impact)

- ช่องโหว่ของ SMTP เวอร์ชั่นนี้ ทำให้ผู้บุกรุกใช้ช่องทางเหล่านี้ทำการบุกรุกเข้าสู่เครื่องคอมพิวเตอร์แม่ข่ายได้

(2) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- ทำการเปลี่ยน รหัสผ่าน SMTP บนเครื่องคอมพิวเตอร์แม่ข่ายให้มีความซับซ้อนมากขึ้นเพื่อป้องกันผู้บุกรุกเดาสุ่มได้ง่าย
- ทำการ Disable SMTP บนเครื่องคอมพิวเตอร์แม่ข่ายหากไม่มีการใช้งาน
- ทำการอัพเกรด SMTP เวอร์ชั่นที่สูงกว่า

ตารางที่ 150 การเปิดใช้งาน Port / Service ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ของ Ms-sql-s (1433/tcp)

Port / Service	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย/อุปกรณ์เครือข่าย/เครื่องคอมพิวเตอร์ลูกข่าย	หมายเลขไอพี	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Ms-sql-s (1433/tcp)	WAREHIUSE GOOGLEMNRE	172.16.1.45 172.16.1.57	Vulnerabilities in Microsoft SQL Server Could Allow Elevation of Privilege (941203)	HIGH

(1) ผลกระทบ (Impact)

- ช่องโหว่ของ Ms-sql-s ทำให้ผู้บุกรุกสามารถใช้เป็นช่องทางที่ทำให้ผู้บุกรุกเข้าสู่เครื่องคอมพิวเตอร์แม่ข่ายได้ ซึ่งทำให้ผู้บุกรุกสามารถทำการ Brute Force ได้
- ทำการป้องกันการบุกรุกจากภายนอกโดยทำการ block Port ดังกล่าว (outside communication) โดยการกำหนดสิทธิ์ดังกล่าวที่อุปกรณ์ไฟร์วอลล์ (Firewall)

(2) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- ติดตั้ง Security Patch: http://www.microsoft.com/technet/security/bulletin/ms08-040.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่

ตารางที่ 151 การเปิดใช้งาน Port / Service ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ของ ssh (22/tcp)

Port / Service	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย/อุปกรณ์เครือข่าย/เครื่องคอมพิวเตอร์ลูกข่าย	หมายเลขไอพี	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Ssh (22/tcp)	FIREWALL	192.168.16.126	OpenSSH < 3.7.1	HIGH
			OpenSSH X11 Session Hijacking Vulnerability	MEDIUM

(1) ผลกระทบ (Impact)

- ช่องโหว่ของ SSH ทำให้ผู้บุกรุกใช้ช่องทางเหล่านี้ทำการบุกรุก เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย ได้

(2) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- ทำการ Upgrade SSH เพื่อป้องกันผู้บุกรุก

ตารางที่ 152 การเปิดใช้งาน Port / Service ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ของ Windows Terminal Services (3389/tcp)

Port / Service	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย/อุปกรณ์เครือข่าย/เครื่องคอมพิวเตอร์ลูกข่าย	หมายเลขไอพี	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Windows Terminal Services (3389/tcp)	EDOC	192.168.16.3	Windows Terminal Service Enabled	
	MISMNRE	192.168.16.9		
	TEST1	172.16.1.5	Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure Vulnerability	MEDIUM
	TOT	172.16.1.25		
	DOCFILESERV1	172.16.1.27		
	DOCFILESERV2	172.16.1.32		
	DATATRAINING	172.16.1.35		
	GISFILESERVER	172.16.1.36		
	WAREHOUSE	172.16.1.45		
	INTEL_SERVER	172.16.1.47		
	GISWEB	172.16.1.52		
	GOOGLEMNRE	172.16.1.57		
	AVMNRE	172.16.1.61		
	LITHUIM	172.16.1.64		
	BACKUP-SERVER	172.16.1.107		
	LOG-MANAGEMENT	172.16.1.108		
	DDMNRE	172.16.1.109		
	ADMNRE	172.16.1.111		
	NMS	172.16.201.1		
	HOME-9481A27B35	172.16.10.32		
	MMNRE	172.16.1.62		

(1) ผลกระทบ (Impact)

- ผู้บุกรุกสามารถใช้ช่องทางเหล่านี้ทำการบุกรุก เข้าสู่เครื่องคอมพิวเตอร์แม่ข่ายได้ โดยวิธีการ exploit ผ่านทาง Port/Services ดังกล่าวได้
- ผู้บุกรุกสามารถใช้ Port/Services ดังกล่าว ในการที่จะลองทำการสุ่ม user และ password โดยวิธีการ Dictionary Attack เพื่อที่จะ login เข้าสู่เครื่องคอมพิวเตอร์แม่ข่ายได้

(2) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- หากไม่มีการใช้งาน Windows Terminal Services ควรทำการ Disable เพื่อป้องกันผู้บุกรุก
- หากจำเป็นต้องใช้งาน Windows Terminal Services ไม่ควรมีการเปิดสิทธิ์ แบบ Allow ควรมีการตรวจสอบสิทธิ์การใช้งาน

ตารางที่ 153 การเปิดใช้งาน Port / Service ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ของ ldap (389/tcp)

Port / Service	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย/อุปกรณ์เครือข่าย/เครื่องคอมพิวเตอร์ลูกข่าย	หมายเลขไอพี	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Ldap (389/tcp)	EDOC ADMNRE	192.168.16.3 172.16.1.111	LDAP Allows anonymous binds	MEDIUM
			LDAP Allows null bases	MEDIUM
			Use LDAP search request to retrieve information from NT Directory Services	MEDIUM

(1) ผลกระทบ (Impact)

- ผู้บุกรุกสามารถใช้ช่องทางเหล่านี้ทำการบุกรุก เข้าสู่เครื่องคอมพิวเตอร์แม่ข่ายได้ โดยวิธีการ exploit ผ่านทาง Port/Services ดังกล่าวได้

(2) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- ทำการ กำหนดค่า LDAP Server so that it does not Allow NULL BINDs.
- ทำการ Disable NULL BASE queries on your LDAP Server

ตารางที่ 154 การเปิดใช้งาน Port / Service ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ของ Mysql (3306/tcp)

Port / Service	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย/อุปกรณ์เครือข่าย/เครื่องคอมพิวเตอร์ลูกข่าย	หมายเลขไอพี	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Mysql (3306/tcp)	ZINC KNOWNLEDGE MISMNRE TEST1 GISFILESERVER	192.168.16.4 192.168.16.8 192.168.16.9 172.16.1.5 172.16.1.36	MySQL User-Defined Function Buffer Overflow Vulnerability	MEDIUM
			MySQL Remote Insecure Default Password Vulnerability	HIGH
			MySQL mysqlhotcopy script insecure temporary file	MEDIUM
			MySQL multiple flaws (2)	MEDIUM
			MySQL buffer overflow	MEDIUM
			MySQL Anonymous Login Handshake Remote Information Disclosure	MEDIUM

(1) ผลกระทบ (Impact)

- ผู้บุกรุกสามารถใช้ช่องทางเหล่านี้ทำการบุกรุก เข้าสู่เครื่องคอมพิวเตอร์แม่ข่ายได้ โดยวิธีการ exploit ผ่านทาง Port/Services ดังกล่าวได้
- ทำให้ผู้บุกรุกสามารถเดาสุ่มรหัสผ่าน ได้ง่าย

(2) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- ทำการ Upgrade MySql ให้มี version 4.0.25 / 4.1.13 / 5.0.7-beta หรือเป็นอย่างน้อย
- ทำการตั้งค่ารหัสผ่าน ที่มีความซับซ้อน เพื่อป้องกันผู้บุกรุกสามารถเดาสุ่มได้ง่าย
- ควรมีการกำหนดสิทธิ์ IP เครื่องคอมพิวเตอร์ที่จะทำการเข้าถึง Database

ตารางที่ 155 การเปิดใช้งาน Port / Service ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ของ Gds_db (3050/tcp)

Port / Service	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย/อุปกรณ์เครือข่าย/เครื่องคอมพิวเตอร์ลูกข่าย	หมายเลขไอพี	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Gds_db (3050/tcp)	GISFILESERVER	172.16.1.36	Firebird DataBase Server Buffer Overflow	HIGH

(1) ผลกระทบ (Impact)

- The version of Firebird มีความเสี่ยงที่ทำให้ผู้บุกรุกสามารถทำการบุกรุกเข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย และทำให้เครื่องคอมพิวเตอร์แม่ข่ายเกิดการ buffer overflow โดยการส่งคำสั่ง specially-crafted 'op_connect' request, a remote, และผู้บุกรุกสามารถทำการ execute code on the affected host with SYSTEM privileges

(2) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- ทำการ Upgrade to Firebird 2.0.1 or later.
- รายละเอียดเพิ่มเติม http://dvlabs.tippingpoint.com/advisory/TPTI-07-11
- รายละเอียดเพิ่มเติม http://www.firebirdsql.org/rlsnotes/Firebird-2.0.1-ReleaseNotes.pdf

ตารางที่ 156 การเปิดใช้งาน Port / Service ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ของ pop3 (110/tcp)

Port / Service	ชื่อเครื่องคอมพิวเตอร์แม่ข่าย/อุปกรณ์เครือข่าย/เครื่องคอมพิวเตอร์ลูกข่าย	หมายเลขไอพี	รายละเอียดช่องโหว่ (Vulnerability Descriptions)	ระดับความเสี่ยง (Risk Factor)
Pop3 (110/tcp)	GISWEB	172.16.1.52	ArGoSoft Mail Server _DUMP Command System Information Disclosure	MEDIUM

(1) ผลกระทบ (Impact)

- ผู้บุกรุกสามารถใช้ช่องทางเหล่านี้ทำการบุกรุกเข้าสู่เครื่องคอมพิวเตอร์แม่ข่ายได้ โดยวิธีการ exploit ผ่านทาง Port/Services ดังกล่าวได้

(2) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- ทำการ Upgrade ArGoSoft Mail Server 1.8.8.6 หรือเป็นอย่างน้อย
- ทำการ Disable POP3 หากไม่มีการใช้งานดังกล่าว

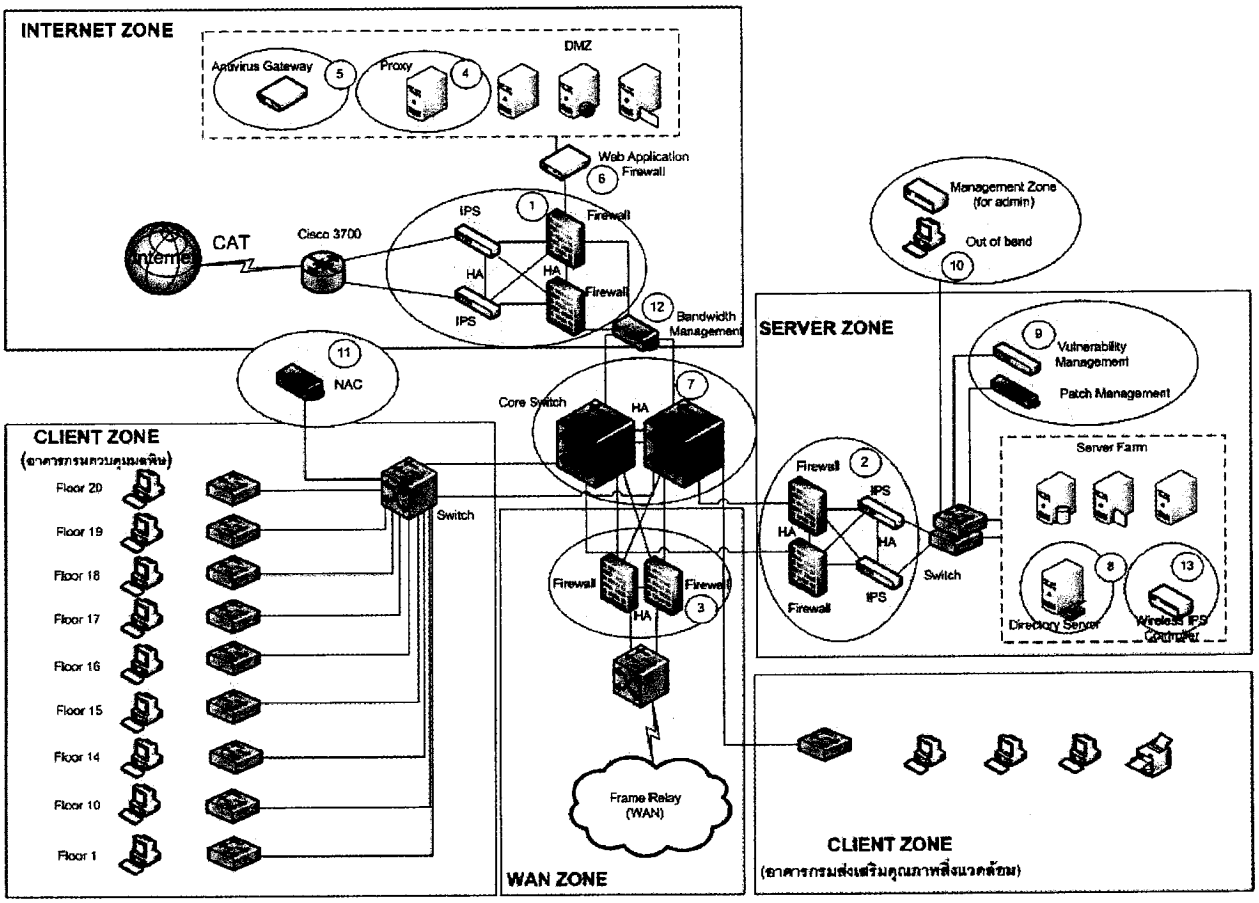
สรุปผลการดำเนินการ

จากผลการวิเคราะห์การสำรวจสถานภาพด้านความปลอดภัยเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ที่มีความเสี่ยงสูงและควรได้รับการปรับปรุงระบบความปลอดภัยเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย เนื่องจากอาจเป็นสาเหตุที่ให้ผู้บุกรุกสามารถใช้ในการบุกรุกเข้าถึงระบบเครือข่ายของ สป.ทส. เห็นควรดำเนินการปรับปรุงเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ลูกข่าย ดังต่อไปนี้

1. ติดตั้ง Security Patch: http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่
2. ติดตั้ง Security Patch: http://www.microsoft.com/technet/security/bulletin/ms06-035.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่
3. ติดตั้ง Security Patch: http://www.microsoft.com/technet/security/bulletin/ms06-040.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่
4. ติดตั้ง Security Patch: http://www.microsoft.com/technet/security/bulletin/ms03-039.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่
5. ติดตั้ง Security Patch: http://www.microsoft.com/technet/security/bulletin/ms08-040.mspx สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พบช่องโหว่
6. ควรมีการตรวจสอบ พอร์ต 137-139 และ 445 สำหรับการใช้งาน เพื่อป้องกันผู้บุกรุกจากภายนอก
7. ทำการปิด shares หากไม่มีการใช้งาน หรือควรมีการกำหนดสิทธิ์ในการเข้าถึง file shares
8. ทำการเปลี่ยนจากการใช้ พอร์ต 80 (www 80/tcp) เป็นพอร์ต 8080 (www 8080/tcp) หรือพอร์ต 443 (https 443/tcp) แทน เพื่อป้องกันการถูกบุกรุก
9. ทำการปิดพอร์ต 80 บนเครื่องคอมพิวเตอร์แม่ข่าย หากไม่มีการใช้งานดังกล่าว
10. หากไม่มีการใช้งาน WebDEV ควรทำการ Disable
11. หากมีการใช้งาน IIS ที่ Allows หรือมีการตั้งค่ารหัสผ่านที่ไม่ซับซ้อนก็อาจทำให้ผู้บุกรุกสามารถเข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย ดังนั้นควรมีการตรวจสอบการตั้งค่ารหัสผ่าน
12. ทำการอัพเกรด IIS ให้เหมาะสมกับปัจจุบัน เพื่อป้องกัน การถูกบุกรุก
13. ทำการอัพเกรด PHP ให้เหมาะสมกับปัจจุบัน เพื่อป้องการการถูกบุกรุก
14. ทำการอัพเกรด Apache ให้เหมาะสมกับปัจจุบัน เพื่อป้องการการถูกบุกรุก
15. ควรทำการ Delete file phpinfo.php เพื่อป้องกันผู้บุกรุกค้นหาข้อมูลจาก file ดังกล่าว

16. ทำการปิดพอร์ต 8080 บนเครื่องคอมพิวเตอร์แม่ข่าย หากไม่มีการใช้งานดังกล่าว
17. ทำการตรวจสอบค่า remote proxy ที่เข้ามาภายในเครือข่ายเพื่อป้องกันการถูกบุกรุก
18. ไม่ทำการ Deploy the Tomcat ทั้งในส่วนของตัวอย่าง หรือเอกสารต่าง ๆ ที่เกี่ยวกับ Web application ของเครื่องคอมพิวเตอร์แม่ข่าย
19. ทำการ Upgrade Oracle version 9.0.2.3 เพื่อป้องกันผู้บุกรุก
20. ทำการ Update Patch Oracle เพื่อป้องการผู้บุกรุก
21. ทำการ ใช้ CHANGE_PASSWORD command เพื่อทำการกำหนดค่ารหัสผ่าน
22. ควรมีการตรวจสอบ พอร์ต 135 สำหรับการใช้งาน เพื่อป้องการผู้บุกรุกจากภายนอก
23. ทำการเปลี่ยน รหัสผ่าน SNMP บนเครื่องคอมพิวเตอร์แม่ข่าย ให้มีความซับซ้อนมากขึ้น เพื่อป้องกันผู้บุกรุกเดาสุ่ม ได้ง่าย
24. ทำการ Disable SNMP บนเครื่องคอมพิวเตอร์แม่ข่าย หากไม่มีการใช้งาน
25. ทำการเปลี่ยน รหัสผ่าน ftp บนเครื่องคอมพิวเตอร์แม่ข่าย ให้มีความซับซ้อนมากขึ้น เพื่อป้องกันผู้บุกรุกเดาสุ่ม ได้ง่าย
26. ทำการ disable user anonymous ออกจากเครื่องคอมพิวเตอร์แม่ข่าย
27. ทำการอัพเกรด ftp บนเครื่องคอมพิวเตอร์แม่ข่าย หากมีความจำเป็นต้องใช้ ftp
28. ทำการเปลี่ยนจากการใช้ ftp เป็น ssh เพื่อป้องกันผู้บุกรุกจากภายนอก
29. ทำการปิดการใช้งาน Telnet ในเครื่องคอมพิวเตอร์แม่ข่าย และเปลี่ยนมาเป็นการใช้งาน ssh แทน
30. ทำการเปลี่ยน รหัสผ่าน TELNET ให้มีความซับซ้อนมากขึ้น เพื่อป้องกันผู้บุกรุกเดาสุ่ม ได้ง่าย
31. ทำการ Disable TELNET บนเครื่องคอมพิวเตอร์แม่ข่าย หากไม่มีการใช้งานดังกล่าว
32. ทำการเปลี่ยนรหัสผ่าน SMTP บนเครื่องคอมพิวเตอร์แม่ข่าย ให้มีความซับซ้อนมากขึ้น เพื่อป้องกันผู้บุกรุกเดาสุ่ม ได้ง่าย
33. ทำการ Disable SMTP บนเครื่องคอมพิวเตอร์แม่ข่าย หากไม่มีการใช้งาน
34. ทำการอัพเกรด SMTP เวอร์ชั่นที่สูงกว่า
35. ทำการ Upgrade SSH เพื่อป้องกันผู้บุกรุก
36. หากไม่มีการใช้งาน Windows Terminal Services ควรทำการ Disable เพื่อป้องกันผู้บุกรุก
37. หากจำเป็นต้องใช้งาน Windows Terminal Services ไม่ควรมีการเปิดสิทธิ์ แบบ Allow ควรมีการตรวจสอบสิทธิ์การใช้งาน
38. ทำการ กำหนดค่า LDAP Server so that it does not Allow NULL BINDs.
39. ทำการ Disable NULL BASE queries on your LDAP Server
40. ทำการ Upgrade MySql ให้มี version 4.0.25 / 4.1.13 / 5.0.7-beta หรือเป็นอย่างน้อย

41. ทำการตั้งค่าพาสเวิร์ด ที่มีความซับซ้อน เพื่อป้องกันผู้บุกรุกสามารถเดาสุ่มได้ง่าย
42. ควรมีการกำหนดสิทธิ์ IP เครื่องคอมพิวเตอร์ที่จะทำการเข้าถึงฐานข้อมูล (Database)
43. ทำการ Upgrade to Firebird 2.0.1 or later.
44. ทำการ Upgrade ArGoSoft Mail Server 1.8.8.6 หรือเป็นอย่างน้อย
45. ทำการ Disable POP3 หากไม่มีการใช้งานดังกล่าว
46. แนะนำการออกแบบความปลอดภัยระบบเครือข่ายและคอมพิวเตอร์เพิ่มเติมให้แก่ สป.ทส. ดังนี้



รูปที่ 4 แนะนำการออกแบบความปลอดภัยระบบเครือข่ายและคอมพิวเตอร์

- ติดตั้งอุปกรณ์ไฟร์วอลล์ (Firewall) และอุปกรณ์ป้องกันผู้บุกรุก (IPS) บริเวณช่องทางสื่อสารไปยังเครือข่ายอินเทอร์เน็ต ติดตั้งเป็นลักษณะ HA (High Availability) โดยเปลี่ยนเป็นอุปกรณ์ไฟร์วอลล์จากเครื่องคอมพิวเตอร์แม่ข่าย (Server) เป็น appliance (ดูตำแหน่งการจัดวางอุปกรณ์ที่ 1 จากรูปที่ 4)

- ปรับแต่งค่า Configuration ของอุปกรณ์ไฟร์วอลล์ (Firewall) ที่ติดตั้งใหม่ในข้อที่ 1 ให้ส่งข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไปยัง Centralized Log Server
- ติดตั้งอุปกรณ์ไฟร์วอลล์ (Firewall) และอุปกรณ์ป้องกันผู้บุกรุก (IPS) บริเวณช่องทางสื่อสารระหว่างอุปกรณ์สวิทช์หลัก (Core Switch) และ Server Farm Switch เพื่อป้องกันผู้บุกรุก โดยควรเลือกยี่ห้อของผลิตภัณฑ์ต่างชนิดกับอุปกรณ์ไฟร์วอลล์ (Firewall) ที่ติดตั้งที่ช่องทางสื่อสารเชื่อมโยงกับเครือข่ายอินเทอร์เน็ต (ดูตำแหน่งการจัดวางอุปกรณ์ที่ 2 จากรูปที่ 4)
- ติดตั้งอุปกรณ์ไฟร์วอลล์ (Firewall) และอุปกรณ์ป้องกันผู้บุกรุก (IPS) บริเวณช่องทางสื่อสารระหว่างอุปกรณ์สวิทช์หลัก (Core Switch) และอุปกรณ์ Router ที่เชื่อมโยงกับเครือข่ายภายนอก (WAN) เพื่อป้องกันผู้บุกรุก (ดูตำแหน่งการจัดวางอุปกรณ์ที่ 3 จากรูปที่ 4)
- ติดตั้งระบบ Proxy เพื่อใช้ในการพิสูจน์ตัวตนของผู้ใช้งานอินเทอร์เน็ต (ดูตำแหน่งการจัดวางอุปกรณ์ที่ 4 จากรูปที่ 4 และตารางที่157)
- ติดตั้งโปรแกรมป้องกันไวรัสให้กับเครื่องคอมพิวเตอร์ลูกข่ายทั้งหมด และให้อัพเดทฐานข้อมูลของโปรแกรมป้องกันไวรัสผ่าน Antivirus Server เท่านั้น
- ติดตั้งอุปกรณ์ป้องกันไวรัสคอมพิวเตอร์สำหรับ http และ ftp ที่ Gateway โดยต้องเลือกยี่ห้อของผลิตภัณฑ์เป็นต่างชนิดกับโปรแกรมป้องกันไวรัสคอมพิวเตอร์ที่เครื่องคอมพิวเตอร์ลูกข่าย (ดูตำแหน่งการจัดวางอุปกรณ์ที่ 5 จากรูปที่ 4)
- ติดตั้งอุปกรณ์ Web Application Firewall ที่เส้นทางเชื่อมโยงไปยัง Web Server เพื่อป้องกันผู้บุกรุกโจมตีเว็บไซต์ของ สป.ทส. (ดูตำแหน่งการจัดวางอุปกรณ์ที่ 6 จากรูปที่ 4)
- ติดตั้งอุปกรณ์สวิทช์หลัก (Core Switch) เพิ่มเติมอีก 1 เครื่อง โดยติดตั้งเป็นลักษณะ HA (High Availability) กับอุปกรณ์สวิทช์หลักเดิมที่มีอยู่แล้ว เพื่อสามารถทำงานทดแทนกันได้ในกรณีที่อุปกรณ์สวิทช์หลักเครื่องใดเครื่องหนึ่งเสีย (ดูตำแหน่งการจัดวางอุปกรณ์ที่ 7 จากรูปที่ 4)
- ติดตั้งระบบ Directory Service เพื่อพิสูจน์ตนของผู้ใช้งานระบบเครือข่ายของสป.ทส. (ดูตำแหน่งการจัดวาง Directory Server ได้จากตำแหน่งการจัดวางอุปกรณ์ที่ 8 จากรูปที่ 4)
- ติดตั้งอุปกรณ์ VM (Vulnerability Management) และ Patch Management เพื่อบริหารจัดการช่องโหว่และปิดช่องโหว่ที่พบใน Server Farm (ดูตำแหน่งการจัดวางอุปกรณ์ที่ 9 จากรูปที่ 4)

- จัดทำช่องทางสื่อสารใหม่สำหรับการบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่ายระยะไกล (Remote Access) โดยให้แยกออกจากช่องทางสื่อสารสำหรับผู้ใช้งานทั่วไป (ดูตำแหน่งของ Management Zone ได้จากรูป ตำแหน่งที่ 10 จากรูปที่ 4)
- ติดตั้งระบบตรวจจับ ป้องกันและกักกันการบุกรุก สำหรับเครื่องคอมพิวเตอร์ในระบบเครือข่าย (Network Access Control : NAC หรือ Endpoint Security) เพื่อตรวจสอบเครื่องคอมพิวเตอร์ลูกข่ายก่อนอนุญาตให้ใช้งานระบบเครือข่ายภายใน (ดูตำแหน่งการจัดวางอุปกรณ์ที่ 11 จากรูปที่ 4)
- ติดตั้งอุปกรณ์ Bandwidth Management เพื่อบริหารจัดการข้อมูลที่ผ่านไปยังอินเทอร์เน็ต (ดูตำแหน่งการจัดวางอุปกรณ์ที่ 12 จากรูปที่ 4)
- ติดตั้งระบบป้องกันผู้บุกรุกสำหรับเครือข่ายไร้สาย (Wireless IPS) เพื่อป้องกันผู้บุกรุกผ่านทางเครือข่ายไร้สาย (ดูตำแหน่งการจัดวางอุปกรณ์ที่ 13 จากรูปที่ 4)

47. คำแนะนำในการติดตั้งอุปกรณ์เพิ่มเติมดังรายการต่อไปนี้

ตารางที่ 157 คำแนะนำในการติดตั้งอุปกรณ์เพิ่มเติม

ลำดับ	รายการ	ผลิตภัณฑ์ลำดับที่ 1	ผลิตภัณฑ์ลำดับที่ 2	ผลิตภัณฑ์ลำดับที่ 3	งบประมาณต่อปี (บาท)	งบประมาณในการบำรุงรักษาต่อปี (บาท)
1	อุปกรณ์ไฟร์วอลล์ และ อุปกรณ์ป้องกันผู้บุกรุกสำหรับ Internet	Juniper Netscreen	Checkpoint	Cisco	1,500,000.-	150,000.-
2	อุปกรณ์ไฟร์วอลล์และ อุปกรณ์ป้องกันผู้บุกรุกสำหรับ Server Farm	Juniper Netscreen	Checkpoint	Cisco	2,500,000.-	250,000.-
3	อุปกรณ์ไฟร์วอลล์หรือ อุปกรณ์ป้องกันผู้บุกรุกจากเครือข่าย WAN	Juniper Netscreen	Checkpoint	Cisco	1,500,000.-	150,000.-
4	ระบบ Proxy	Bluecoat	Microsoft ISA	Squid	1,500,000.-	150,000.-
5	อุปกรณ์ป้องกันไวรัสสำหรับ http, ftp และ Content	Bluecoat	ContentKeeper	Web Washer	1,500,000.-	150,000.-
6	Web Application Firewall	Radware	Imperva	Net Continuum	2,000,000.-	200,000.-
7	อุปกรณ์ CoreSwitch	Cisco	Nortel	3Com	5,000,000.-	500,000.-
8	ระบบพิสูจน์ตัวตน	Microsoft Active Directory	LDAP (UNIX)	-	3,000,000.-	300,000.-
9	Vulnerability Management	StillSecure	Foundstone	Internet Scanner	1,000,000.-	100,000.-
10	ระบบตรวจจับ ป้องกันการบุกรุก และกักกันเครื่องคอมพิวเตอร์ลูกข่ายในระบบเครือข่าย (NAC)	Mirage	Consentry	TippingPoint	2,000,000.-	200,000.-
11	Bandwidth Management	Packeteer	PacketLogic	-	1,500,000.-	150,000.-
12	อุปกรณ์ Wireless IPS	Air-Tight	Air-Defence	Air-Magnet	1,500,000.-	150,000.-
13	Patch Management System	PatchLink	Microsoft SCCM	-	2,000,000.-	200,000.-

หมายเหตุ

- ราคาตลาด ตรวจสอบในช่วงเดือนธันวาคม 2551
- หลังจากติดตั้งอุปกรณ์ความปลอดภัยตามที่เสนอแล้ว สป.ทส. ควรจะจัดให้มีการฝึกอบรมสำหรับผู้ที่รับผิดชอบดูแลอุปกรณ์ที่ติดตั้งนี้ หรือควรจัดหา outsource ที่มีความเชี่ยวชาญเพื่อเข้ามาดูแลบำรุงรักษาและปรับแต่งค่า Configuration ของอุปกรณ์เหล่านี้

ที่ปรึกษา ขอขอบคุณ สป.ทส. ที่ให้โอกาสในการสำรวจสถานภาพด้านความปลอดภัย และขอขอบคุณทุกฝ่ายที่เกี่ยวข้องในการประสานงานในการสำรวจสถานภาพความปลอดภัยครั้งนี้ ซึ่งทำให้การดำเนินงานครั้งนี้สำเร็จลุล่วงเป็นอย่างดี ที่ปรึกษา แนะนำว่าควรจะมีการสำรวจสถานภาพด้านความปลอดภัยเป็นประจำอย่างน้อยปีละ 1 ครั้ง และก่อนที่จะมีการสำรวจสถานภาพด้านความปลอดภัยแต่ละครั้ง ควรจะดำเนินการแก้ไขตามที่ทางที่ปรึกษา แนะนำ เพื่อให้มั่นใจว่าการสำรวจครั้งต่อ ๆ ไปนั้น จะไม่พบช่องโหว่เดิมที่เคยพบไปก่อนหน้านี้

ส่วนที่ 2.2

รายงานผลการทดสอบเจาะระบบจากภายนอก

ความนำ

การทดสอบเจาะระบบจากภายนอก (Black-box Penetration Testing) เป็นการทดสอบเจาะระบบโดยกำหนดสถานการณ์จำลองของการโจมตีจุดอ่อน และนำไปสู่ความสูญเสียด้านความปลอดภัย (CIA) ซึ่งในการทดสอบนั้น จะเป็นการจำลองสถานการณ์เป็นผู้บุกรุกจากภายนอกซึ่งไม่มีข้อมูลใด ๆ เกี่ยวกับระบบที่จะทดสอบหรือมีข้อมูลบางส่วนเท่านั้น ผู้ทดสอบจะหาข้อมูลเกี่ยวกับเป้าหมายด้วยตนเองก่อนที่จะทดสอบเจาะระบบ สิ่งที่แตกต่างระหว่างผู้ทดสอบและผู้บุกรุก คือ ผู้บุกรุกมักจะเจาะระบบโดยต้องการบรรลุความต้องการบางอย่าง โดยไม่คำนึงถึงความเสียหายต่อองค์กรที่ถูกเจาะระบบ แต่ผู้ทดสอบจะดำเนินการทดสอบโดยไม่ประสงค์ที่จะทำให้เกิดความเสียหายใด ๆ การทดสอบเจาะระบบจึงเป็นประโยชน์กับองค์กร โดยใช้ผลของการทดสอบเจาะระบบทำการป้องกันและเพิ่มความปลอดภัย ก่อนที่ผู้บุกรุกจะสร้างความเสียหายให้กับองค์กร โดยเป้าหมายของผู้บุกรุกที่ใช้ในการเจาะระบบจากภายนอกนั้นประกอบด้วยเว็บไซต์ขององค์กร และอุปกรณ์เครือข่ายไร้สายขององค์กร

ในปัจจุบันองค์กรต่าง ๆ ทั้งภาครัฐและเอกชนต่างมีเว็บไซต์เพื่อให้บริการหรืออำนวยความสะดวกแก่บุคคลภายนอก โดยสามารถใช้งานได้จากทุกสถานที่ที่สามารถเชื่อมต่ออินเทอร์เน็ต แต่ความสะดวกสบายเหล่านั้นก็อาจตกเป็นเป้าหมายของผู้ไม่หวังดี ซึ่งอาจค้นพบช่องโหว่ในเว็บไซต์เหล่านั้น และดำเนินการเจาะระบบจนสร้างความเสียหายให้แก่องค์กรทั้งในด้านชื่อเสียง การเข้าถึงข้อมูลที่เป็นความลับ และด้านการเงินเป็นต้น ดังนั้นเว็บไซต์ขององค์กรจึงควรได้รับการตรวจสอบ และดำเนินการแก้ไขเพื่อให้เว็บไซต์ขององค์กรมีความปลอดภัย

นอกจากที่ผู้บุกรุกจะเจาะระบบจากภายนอกผ่านทางเว็บไซต์ขององค์กรแล้ว ผู้บุกรุกยังเจาะระบบจากภายนอกผ่านทางอุปกรณ์เครือข่ายไร้สายขององค์กร เนื่องจากในปัจจุบันอุปกรณ์เครือข่ายไร้สายได้รับความนิยมอย่างมากในการนำมาใช้เพื่อเชื่อมต่อเข้ากับระบบเครือข่ายภายในขององค์กร จากความสะดวกสบายของผู้ใช้งาน โดยเพียงแค่อยู่ในรัศมีของระบบเครือข่ายไร้สายก็สามารถเชื่อมต่อได้ทันที แต่อย่างไรก็ตามความสะดวกสบายเหล่านี้ก็นำมาซึ่งความไม่ปลอดภัยของระบบเครือข่ายด้วยเช่นกัน ดังนั้นการติดตั้งระบบเครือข่ายไร้สายจึงจำเป็นจะต้องมีการตรวจสอบในเรื่องความปลอดภัยก่อนเปิดใช้งาน โดยวิธีที่จะทำให้แน่ใจในความปลอดภัยคือ ทำการทดสอบเจาะระบบอุปกรณ์เครือข่ายไร้สาย ซึ่งเริ่มต้นจากการสำรวจเพื่อค้นหาสัญญาณของ Access Point ที่เปิดใช้งานอยู่ (War Driving) หลังจากนั้นจึงระบุเป้าหมายและใช้เครื่องมือเพื่อทดสอบเจาะระบบเครือข่ายไร้สาย

สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อมมีความประสงค์ที่จะดำเนินการทดสอบเจาะระบบจากภายนอก (Black-box Penetration Testing) โดยมีเป้าหมายในการทดสอบเจาะระบบจากภายนอกผ่านทางเว็บไซต์ในครั้งนี้ทั้งหมด 2 URL และอุปกรณ์เครือข่ายไร้สายทั้งหมด 3 SSID ประกอบด้วย

การทดสอบเจาะระบบจากภายนอกผ่านทางเว็บไซต์

1. http://www.warehouse.mnre.go.th/
2. http://petition.mnre.go.th/

การทดสอบเจาะระบบจากภายนอกผ่านทางอุปกรณ์เครือข่ายไร้สาย

1. mnre-ap (กรมส่งเสริมคุณภาพสิ่งแวดล้อม ชั้น 10)
2. linksys-mnre (กรมส่งเสริมคุณภาพสิ่งแวดล้อม ชั้น 10)
3. mnre-ap (กรมควบคุมมลพิษ ชั้น 1)

ในการทดสอบเจาะระบบจากภายนอกครั้งนี้ บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด ได้ดำเนินการตามขอบเขตการดำเนินงานดังต่อไปนี้

- ขอบเขตการดำเนินงานข้อ 3.2.1.2: ทดสอบการเจาะระบบจากภายนอก (Black Box Penetration Test) ตามรายละเอียดดังนี้
    1) เครื่องคอมพิวเตอร์แม่ข่าย Web Server ไม่น้อยกว่า 2 URL
    2) อุปกรณ์เครือข่ายไร้สาย (Wireless Local Area Network) ไม่น้อยกว่า 3 เครื่อง
- ขอบเขตการดำเนินงานข้อ 3.2.2: ตรวจสอบความปลอดภัยของระบบคอมพิวเตอร์ระดับ Application ภายใต้การควบคุมด้วยอุปกรณ์รักษาความปลอดภัยในปัจจุบัน เช่น การทดสอบ Web Application Security ของ Web Server ที่เชื่อมต่ออยู่กับระบบอินเทอร์เน็ต
- ขอบเขตการดำเนินงานข้อ 3.2.3: ให้กำหนดสถานการณ์จำลองที่สามารถโจมตีจุดอ่อนและนำไปสู่ความสูญเสียด้านความปลอดภัย (CIA) เช่น จำลองสถานการณ์โจมตีจากอินเทอร์เน็ตภายนอก จำลองสถานการณ์เป็นผู้ที่สามารถเข้ามาในสถานที่ปฏิบัติงาน ได้แก่ พนักงาน ผู้รับจ้างเหมาะพัฒนาระบบแบบ Outsource หรือ Vendor ภายใต้สถานการณ์ที่ถูกกำหนด
- ขอบเขตการดำเนินงานข้อ 3.2.4: หลีกเลี่ยงแบบทดสอบที่อาจจะก่อให้เกิดการหยุดชะงักของระบบงาน เช่น การใช้แบบทดสอบ Denial of Service ตามความเห็นชอบของสำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อมที่จะกำหนดให้มีการทดสอบในเครื่องทดสอบแทน
- ขอบเขตการดำเนินงานข้อ 3.2.5: นำเสนอรายงานในรูปแบบแสดงระดับความเสี่ยงโดยเปรียบเทียบกับการควบคุมและวิธีปฏิบัติงานตามความเห็นชอบของสำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม พร้อมข้อเสนอแนะและแนวทางที่เหมาะสมในการปรับปรุง รวมทั้งออกแบบระบบความปลอดภัยของระบบเครือข่ายและความปลอดภัยคอมพิวเตอร์ของสำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม รองรับการขยายการบริการ และรองรับกฎ ระเบียบและข้อบังคับด้านความมั่นคงปลอดภัยระบบสารสนเทศและการสื่อสาร หรือมาตรฐานด้านความปลอดภัยระบบสารสนเทศที่เกี่ยวข้อง

- ขอบเขตการดำเนินงานข้อ 3.2.6: เมื่อค้นพบช่องโหว่ หรือข้อมูลสำคัญ ซึ่งอาจจะทำให้สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อมตกอยู่ในสถานะหรือสภาวะต่อการรั่วไหล หรือหยุดชะงักของระบบคอมพิวเตอร์ ต้องมีการแจ้งเตือนเพื่อขออนุญาตดำเนินงานต่อไป
- ขอบเขตการดำเนินงานข้อ 3.2.7: หากเจ้าหน้าที่ดำเนินการค้นพบช่องโหว่ที่นอกเหนือจากรายการที่แจ้งไว้ จะต้องแจ้งให้สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อมให้ความเห็นชอบก่อนเข้าดำเนินการ ทั้งนี้ในระหว่างการดำเนินโครงการฯ ที่ปรึกษาจะต้องจัดเจ้าหน้าที่เพื่อให้คำแนะนำ ตอบคำถาม และให้การช่วยเหลือทางโทรศัพท์และพร้อมที่จะเข้าไปช่วยในกรณีเร่งด่วน โดยต้องอยู่ในขอบเขตการดำเนินโครงการฯ
- ขอบเขตการดำเนินงานข้อ 3.2.8: ดำเนินการวิเคราะห์และให้คำแนะนำ ในกรณีที่ระบบเครือข่ายของสำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม จำเป็นต้องได้รับการติดตั้งระบบ หรืออุปกรณ์เพิ่มเติม เพื่อเป็นการเพิ่มระดับการรักษาความปลอดภัยของระบบเครือข่ายและความปลอดภัยคอมพิวเตอร์ของสำนักงานปลัดกระทรวงทรัพย์ฯ สามารถเสนอเพื่อดำเนินการได้ทั้งนี้จะต้องไม่คิดค่าใช้จ่ายเพิ่มเติม

ซึ่งเป้าหมายในการทดสอบดังกล่าวเป็นส่วนหนึ่งในโครงการจัดจ้างที่ปรึกษาประเมินความเสี่ยงด้านสารสนเทศและการแก้ปัญหา บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด ได้เสร็จสิ้นการทดสอบเจาะระบบจากภายนอก (Black-box Penetration Testing) ทั้งหมดแล้ว ซึ่งหลังจากที่ได้ดำเนินการทดสอบเจาะระบบจากภายนอก (Black-box Penetration Testing) เสร็จสิ้นแล้ว บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด ได้จัดทำรายงานผลการทดสอบเจาะระบบจากภายนอก (Black-Box Penetration Test Report) เพื่อนำเสนอผลการทดสอบต่อสำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม เพื่อให้ฝ่ายต่าง ๆ ที่เกี่ยวข้องได้รับทราบ และดำเนินการแก้ไขต่อไป

เพื่อความสะดวกในการอ่านรายงานฉบับนี้ บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด จะเปลี่ยนการนำเสนอจากชื่อเต็มเป็นการใช้ชื่อย่อ ดังนี้

ชื่อเต็ม	ชื่อย่อที่ใช้
สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม	สป.ทส.
บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด	ที่ปรึกษา
โครงการจัดจ้างที่ปรึกษาและประเมินความเสี่ยงด้านสารสนเทศและการแก้ไขปัญหา	โครงการฯ

บทสรุปสำหรับผู้บริหาร

ในการทดสอบเจาะระบบจากภายนอกครั้งนี้ ที่ปรึกษาได้ทดสอบเจาะระบบจากภายนอกทั้งหมด 2 ส่วน คือการทดสอบเจาะระบบเว็บไซต์ของ สป.ทส. ทั้งหมด 2 URL และการทดสอบเจาะระบบอุปกรณ์เครือข่ายไร้สายของ สป.ทส. ทั้งหมด 3 SSID ซึ่งสามารถสรุปผลการทดสอบได้ดังนี้

1. การทดสอบเจาะระบบภายนอก

1.1 การทดสอบเจาะระบบจากภายนอกผ่านทางเว็บไซต์

1.1.1 http://www.warehouse.mnre.go.th/

ที่ปรึกษาพบว่าเว็บไซต์ http://www.warehouse.mnre.go.th/ มีความเสี่ยงที่จะถูกเจาะระบบอยู่ในระดับสูง โดยสาเหตุที่ความเสี่ยงอยู่ในระดับสูงเนื่องจากในการทดสอบสามารถเข้าถึงระบบบริหารจัดการเว็บไซต์ดังกล่าวได้ ซึ่งหากผู้บุกรุกสามารถเข้าถึงระบบในลักษณะเดียวกัน ก็จะสามารถแก้ไขเปลี่ยนแปลงหน้าเว็บไซต์ซึ่งจะทำให้องค์กรเสื่อมเสียชื่อเสียง

1.1.2 http://petition.mnre.go.th/

ที่ปรึกษาพบว่าเว็บไซต์ http://petition.mnre.go.th/ มีความเสี่ยงที่จะถูกเจาะระบบอยู่ในระดับสูง โดยสาเหตุที่ความเสี่ยงอยู่ในระดับสูงเนื่องจากในการทดสอบสามารถเข้าถึงระบบบริหารจัดการเว็บไซต์ดังกล่าวได้ในลักษณะเดียวกับเว็บไซต์ http://www.warehouse.mnre.go.th/ ซึ่งหากผู้บุกรุกสามารถเข้าถึงระบบในลักษณะเดียวกับการทดสอบครั้งนี้ ก็จะสามารถแก้ไขเปลี่ยนแปลงหน้าเว็บไซต์ซึ่งจะทำให้องค์กรเสื่อมเสียชื่อเสียง

1.2 การทดสอบเจาะระบบจากภายนอกผ่านทางอุปกรณ์เครือข่ายไร้สาย

1.2.1 mnre-ap (กรมส่งเสริมคุณภาพสิ่งแวดล้อม ชั้น 10)

ที่ปรึกษาพบว่าอุปกรณ์เครือข่ายไร้สาย mnre-ap ซึ่งตั้งอยู่ที่กรมส่งเสริมคุณภาพสิ่งแวดล้อม ชั้น 10 มีความเสี่ยงที่จะถูกเจาะระบบอยู่ในระดับสูง เนื่องจากมีการเข้ารหัสในลักษณะ WEP ซึ่งทำให้หากถอดรหัสดังกล่าวได้ ก็จะสามารถใช้งานอุปกรณ์เครือข่ายไร้สายและทำให้สามารถเข้าถึงเครื่องคอมพิวเตอร์ภายในองค์กรรวมทั้งเครื่องคอมพิวเตอร์แม่ข่าย

1.2.2 linksys-mnre (กรมส่งเสริมคุณภาพสิ่งแวดล้อม ชั้น 10)

ที่ปรึกษาพบว่าอุปกรณ์เครือข่ายไร้สาย linksys-mnre ซึ่งตั้งอยู่ที่กรมส่งเสริมคุณภาพสิ่งแวดล้อม ชั้น 10 มีความเสี่ยงที่จะถูกเจาะระบบอยู่ในระดับต่ำ เนื่องจากมีการเข้ารหัสในลักษณะ WPA-PSK

1.2.3 mnre-ap (กรมควบคุมมลพิษ ชั้น 1)

อุปกรณ์เครือข่ายไร้สาย mnre-ap ซึ่งตั้งอยู่ที่กรมควบคุมมลพิษ ชั้น 1 มีความเสี่ยงที่จะถูกเจาะระบบอยู่ในระดับสูง เนื่องจากมีการเข้ารหัสในลักษณะ WEP ซึ่งทำให้หากถอดรหัสดังกล่าวได้ ก็จะสามารถใช้งานอุปกรณ์เครือข่ายไร้สายและทำให้สามารถเข้าถึงเครื่องคอมพิวเตอร์ภายในองค์กรได้

ในการประเมินระดับความเสี่ยงของเป้าหมายที่จะทดสอบนั้น ที่ปรึกษามีการแบ่งระดับความเสี่ยงทางด้านเทคนิคเพื่อให้เจ้าหน้าที่ที่เกี่ยวข้องมีความเข้าใจว่าสิ่งที่พบจากการเจาะระบบเว็บไซต์และอุปกรณ์เครือข่ายไร้สายของ สป.ทส. นั้นมีความรุนแรงในระดับใด ซึ่งในการคำนวณหาระดับความเสี่ยงนั้นได้จากการคำนวณจาก ผลกระทบและโอกาสที่จะเกิด โดยสามารถแสดงรายละเอียดได้ดังนี้

ตารางที่ 1 นิยามระดับความรุนแรงในการประเมินความเสี่ยงทางด้านเทคนิคของที่ปรึกษา

ระดับ	ผลกระทบทางเทคนิค	โอกาสที่จะเกิด
สูง (HIGH)	สามารถเข้าไปบริหารจัดการระบบได้เปรียบเสมือนเป็นเจ้าของระบบนั้น	ผู้บุกรุกสามารถเข้าถึงระบบได้อย่างง่ายดาย โดยไม่ต้องใช้วิธีการที่ซับซ้อน
ปานกลาง (MEDIUM)	สามารถจำกัดสิทธิ์ในการควบคุมระบบ หรือเข้าไปแก้ไขค่าต่าง ๆ ของระบบได้	จากช่องโหว่ที่เกิดขึ้น ผู้บุกรุกสามารถทำการเข้าถึงระบบและเปลี่ยนสิทธิ์ของการควบคุมระบบได้โดยไม่จำเป็นต้องใช้โปรแกรม Exploit ทำการยึดเครื่องเป้าหมาย
ต่ำ (LOW)	เป็นข้อมูลที่แสดงนั้นเป็นประโยชน์ต่อการโจมตี หรือใช้ข้อมูลเครื่องดังกล่าว เป็นเป้าหมายในการยึดเครื่องต่อไปในระบบ	ช่องโหว่ที่เกิดขึ้นนั้น อาจถูกโจมตีได้ยาก เนื่องจากต้องอาศัยความชำนาญของผู้บุกรุกในการยึดเครื่องเป้าหมาย

จากระดับความรุนแรงผลกระทบทางเทคนิค และโอกาสที่จะเกิด สามารถนำมาคำนวณหาความเสี่ยงทางเทคนิคได้โดยคำนวณจากสูตร

ความเสี่ยงทางเทคนิค = (ผลกระทบทางเทคนิค x โอกาสที่จะเกิด)

ซึ่งเมื่อนำระดับความรุนแรงของผลกระทบทางเทคนิค และโอกาสที่จะเกิด ทั้งหมด (สูง กลาง และ ต่ำ) มาคำนวณหาความเสี่ยงทางเทคนิคจากสูตรข้างต้นจะสามารถสรุปผลได้ดังตารางที่ 2 ซึ่งที่ปรึกษาจะใช้การประเมินความเสี่ยงในลักษณะนี้เพื่อประเมินหาความเสี่ยงที่พบในเป้าหมายการทดสอบ

ตารางที่ 2 ผลการคำนวณความเสี่ยงทางเทคนิค (Technical Risk)

		โอกาสที่จะเกิด		
		สูง	ปานกลาง	ต่ำ
ผลกระทบทางเทคนิค	สูง	สูง	สูง	ปานกลาง
	ปานกลาง	สูง	ปานกลาง	ปานกลาง
	ต่ำ	ต่ำ	ต่ำ	ต่ำ

เมื่อพบความเสี่ยงด้านเทคนิคในเว็บไซต์ และอุปกรณ์เครือข่ายไร้สายของ สป.ทส. จะเกิดความสูญเสียด้านความปลอดภัยต่อ สป.ทส. ที่แตกต่างกันไป โดยที่ปรึกษาได้สรุปประเภทของความสูญเสียด้านความปลอดภัยดังแสดงในตารางที่ 3 เพื่อให้เจ้าหน้าที่ที่เกี่ยวข้องมีความเข้าใจว่าหากผู้บุกรุกสามารถเจาะระบบเว็บไซต์ และอุปกรณ์เครือข่ายไร้สายของ สป.ทส. จะทำให้ส่งผลกระทบกับ สป.ทส. ในลักษณะใด

ตารางที่ 3 ประเภทของความสูญเสียด้านความปลอดภัย

ประเภท	รายละเอียด
Confidentiality	ผลกระทบที่ก่อให้เกิดการสูญเสียข้อมูลที่เป็นความลับ
Integrity	ผลกระทบที่เกี่ยวข้องกับความถูกต้องสมบูรณ์ของข้อมูล
Availability	ผลกระทบที่เกี่ยวข้องกับความพร้อมใช้งานของระบบ

ในการทดสอบเจาะระบบเว็บไซต์ให้กับ สป.ทส. ที่ปรึกษาได้ดำเนินการทดสอบตามมาตรฐานของ OWASP ซึ่งมีการกำหนดมาตรฐานเกี่ยวกับช่องโหว่ทางเว็บแอพพลิเคชั่น ตัวอย่างหนึ่งของมาตรฐาน OWASP ที่ได้รับการยอมรับคือ OWASP Top 10 ซึ่งเป็นการประกาศช่องโหว่ทางเว็บแอพพลิเคชั่น 10 อันดับแรกที่สร้างความเสียหายให้กับเว็บไซต์ต่าง ๆ ทั่วโลก ซึ่งมาตรฐานของ OWASP Top 10 เวอร์ชั่นล่าสุดคือ OWASP Top 10 ของปี ค.ศ.2007 และนอกเหนือจากช่องโหว่ทางเว็บแอพพลิเคชั่น 10 อันดับแรกแล้ว โดยปกติในการทดสอบเจาะระบบเว็บไซต์ต่าง ๆ ก็จะพบช่องโหว่ทางเว็บแอพพลิเคชั่นอื่น ๆ นอกเหนือจากช่องโหว่ทางเว็บแอพพลิเคชั่น 10 อันดับแรก ซึ่งในการทดสอบเจาะระบบ ที่ปรึกษาจะรายงานช่องโหว่ที่พบทั้งช่องโหว่ทางเว็บแอพพลิเคชั่น 10 อันดับแรก และช่องโหว่อื่น ๆ ที่พบทั้งหมดให้กับ สป.ทส.

1. ผลการทดสอบเจาะระบบจากภายนอกผ่านทางเว็บไซต์

ในการทดสอบนั้น จะเป็นการจำลองสถานการณ์เป็นผู้บุกรุกจากภายนอกซึ่งไม่มีข้อมูลใด ๆ เกี่ยวกับระบบที่จะทดสอบหรือมีข้อมูลบางส่วนเท่านั้น โดยแสดงรายละเอียดการทดสอบเจาะระบบแต่ละเว็บไซต์ดังนี้

1.1 ผลการทดสอบเจาะระบบจากภายนอกผ่านทางเว็บไซต์ http://www.warehouse.mnre.go.th/

ตารางที่ 4 ผลกระทบทางเทคนิค โอกาสที่จะเกิด และความเสี่ยงทางเทคนิคของเว็บไซต์

http://www.warehouse.mnre.go.th

ผลกระทบทางเทคนิค: ระดับสูง
สิ่งที่พบ เว็บไซต์ http://www.warehouse.mnre.go.th/ มีผลกระทบทางเทคนิคอยู่ในระดับสูง เนื่องจากผู้ทดสอบพบช่องทางในการเข้าถึงระบบล็อกอินภายในหน้าแรกของเว็บไซต์ อีกทั้งผู้ทดสอบยังสามารถใช้ระบบลืมรหัสผ่านในการคาดเดาแอคเคานท์ที่มีในระบบ และพบว่าแอคเคานท์ของผู้ดูแลระบบมีการใช้รหัสผ่านที่ง่ายต่อการคาดเดา ซึ่งทั้งหมดนี้ทำให้สามารถเข้าไปบริหารจัดการระบบได้ และนำไปสู่การยึดครองเว็บไซต์ของ สป.ทส. ซึ่งมีผลกระทบอยู่ในระดับสูง
โอกาสที่จะเกิด: ระดับปานกลาง
สิ่งที่พบ เว็บไซต์ http://www.warehouse.mnre.go.th/ มีโอกาสที่จะถูกเจาะระบบจากผู้บุกรุกในระดับปานกลาง เนื่องจากมีโอกาสที่ผู้บุกรุกสามารถเข้าถึงช่องโหว่ดังเช่นที่พบในการทดสอบครั้งนี้ และสามารถคาดเดารหัสผ่านของผู้ดูแลระบบจนทำให้สามารถเข้าไปบริหารจัดการระบบได้
ความเสี่ยงทางเทคนิค: ระดับสูง
สิ่งที่พบ เว็บไซต์ http://www.warehouse.mnre.go.th/ มีความเสี่ยงทางเทคนิคอยู่ในระดับสูง ซึ่งได้จากการคำนวณผลกระทบทางเทคนิค (ระดับสูง) และโอกาสที่จะเกิด(ระดับปานกลาง) นำมาเปรียบเทียบกับตารางที่ 2.2 ทำให้พบว่าความเสี่ยงทางเทคนิคอยู่ในระดับสูง

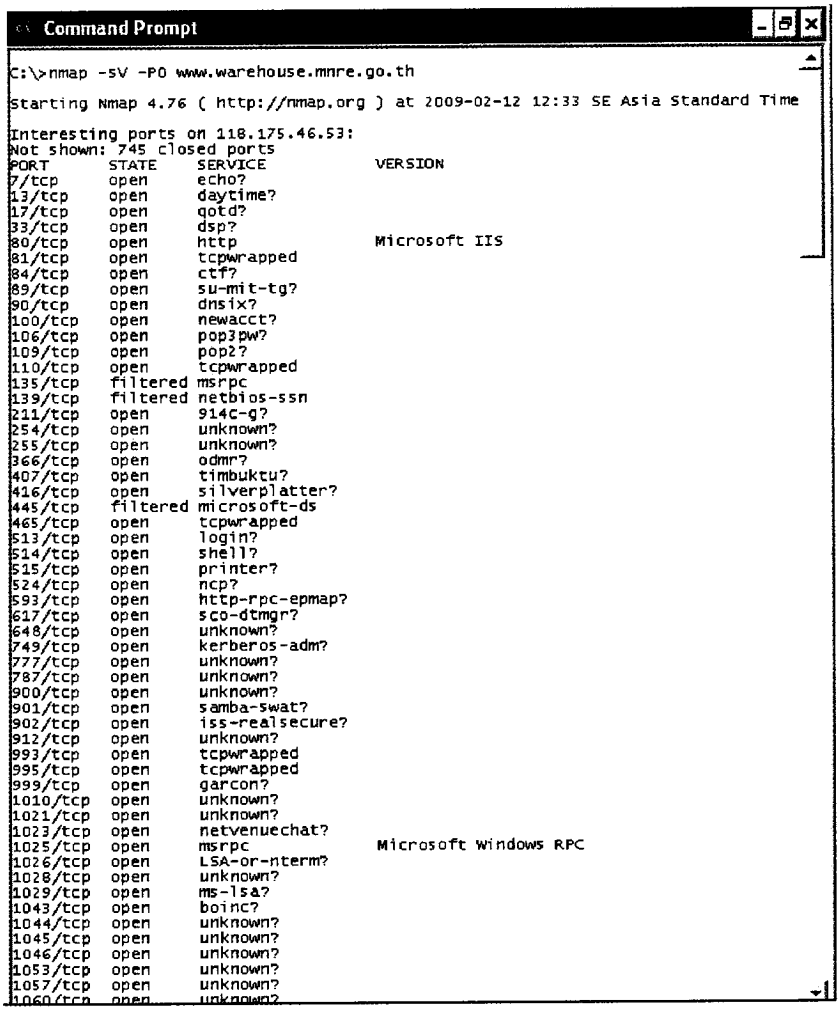
ตารางที่ 5 ความสูญเสียด้าน Confidentiality Integrity และ Availability ของเว็บไซต์

http://www.warehouse.mnre.go.th

ความสูญเสียด้าน Confidentiality: มีผลกระทบ
สิ่งที่พบ ความสูญเสียด้าน Confidentiality คือผลกระทบที่ก่อให้เกิดการสูญเสียข้อมูลที่เป็นความลับ ซึ่งจากการทดสอบสามารถยึดครองเว็บไซต์ดังกล่าวของ สป.ทส. ได้ ทำให้มีโอกาสที่ผู้บุกรุกจะสามารถเข้าถึงข้อมูลที่เป็นความลับภายในเว็บไซต์ดังกล่าว
ความสูญเสียด้าน Integrity: ไม่มีผลกระทบ
สิ่งที่พบ ไม่พบปัจจัยที่ส่งผลต่อความสูญเสียด้าน Integrity
ความสูญเสียด้าน Availability: มีผลกระทบ
สิ่งที่พบ ความสูญเสียด้าน Availability คือผลกระทบที่เกี่ยวข้องกับความพร้อมใช้งานของระบบ ซึ่งจากการทดสอบสามารถยึดครองเว็บไซต์ดังกล่าวของ สป.ทส. ได้ ทำให้มีโอกาสที่ผู้บุกรุกจะปรับโฉมหน้าของเว็บไซต์ ซึ่งทำให้ผู้ใช้งานไม่สามารถใช้งานเว็บไซต์ดังกล่าวได้

ขั้นตอนในการทดสอบ

1. ผู้ทดสอบทำการสแกนพอร์ตเครื่องเป้าหมาย โดยใช้โปรแกรม Nmap ซึ่งผลจากการสแกนพอร์ต ทำให้ผู้ทดสอบสามารถทราบหมายเลขพอร์ตที่เปิดอยู่ สถานะของพอร์ต และเซอร์วิส (Service) ที่ใช้พอร์ตดังกล่าว ข้อมูลทั้งหมดเป็นข้อมูลเบื้องต้น เพื่อให้ผู้ทดสอบสามารถทราบช่องทางในการทดสอบระบบ ดังแสดงในรูปที่ 1

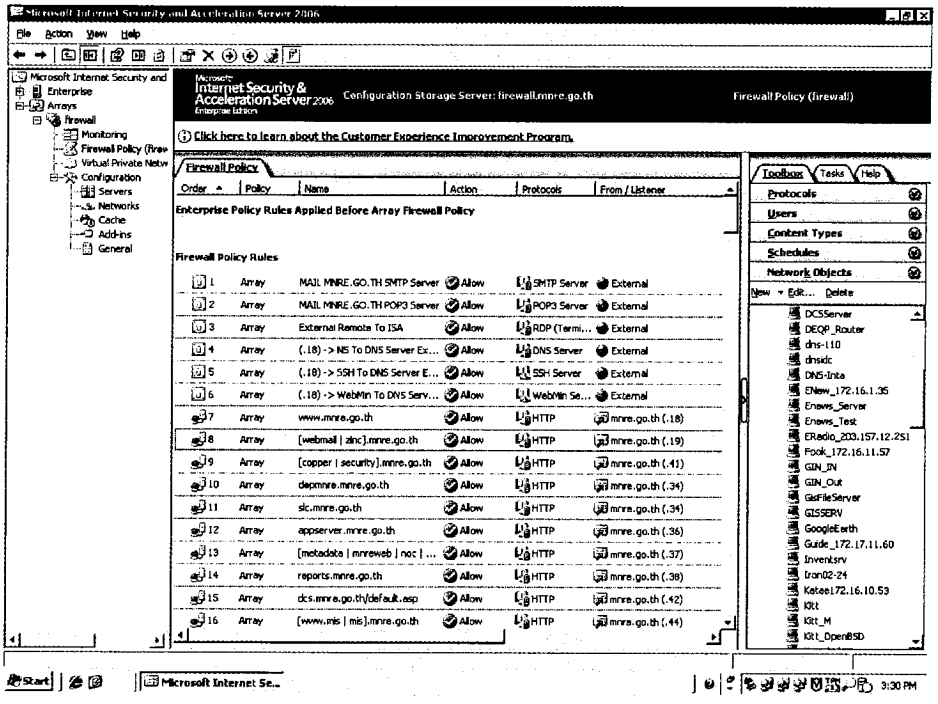


```
Command Prompt

C:\>nmap -sV -P0 www.warehouse.mnre.go.th

Starting Nmap 4.76 ( http://nmap.org ) at 2009-02-12 12:33 SE Asia Standard Time

Interesting ports on 118.175.46.53:
Not shown: 745 closed ports
PORT      STATE    SERVICE           VERSION
7/tcp     open     echo?
13/tcp    open     daytime?
17/tcp    open     qotd?
33/tcp    open     dsp?
80/tcp    open     http              Microsoft IIS
81/tcp    open     tcpwrapped
84/tcp    open     ctf?
89/tcp    open     su-mit-tg?
90/tcp    open     dnsix?
100/tcp   open     newacct?
106/tcp   open     pop3pw?
109/tcp   open     pop2?
110/tcp   open     tcpwrapped
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
211/tcp   open     914c-g?
254/tcp   open     unknown?
255/tcp   open     unknown?
366/tcp   open     odmr?
407/tcp   open     timbuktu?
416/tcp   open     silverplatter?
445/tcp   filtered microsoft-ds
465/tcp   open     tcpwrapped
513/tcp   open     login?
514/tcp   open     shell?
515/tcp   open     printer?
524/tcp   open     ncp?
593/tcp   open     http-rpc-epmap?
617/tcp   open     sco-dtmgr?
648/tcp   open     unknown?
749/tcp   open     kerberos-adm?
777/tcp   open     unknown?
787/tcp   open     unknown?
900/tcp   open     unknown?
901/tcp   open     samba-swat?
902/tcp   open     iss-realsecure?
912/tcp   open     unknown?
993/tcp   open     tcpwrapped
995/tcp   open     tcpwrapped
999/tcp   open     garcon?
1010/tcp  open     unknown?
1021/tcp  open     unknown?
1023/tcp  open     netvenuechat?
1025/tcp  open     msrpc             Microsoft Windows RPC
1026/tcp  open     LSA-or-nterm?
1028/tcp  open     unknown?
1029/tcp  open     ms-lsa?
1043/tcp  open     boinc?
1044/tcp  open     unknown?
1045/tcp  open     unknown?
1046/tcp  open     unknown?
1053/tcp  open     unknown?
1057/tcp  open     unknown?
1060/tcp  open     unknown?
```

รูปที่ 1 การทดสอบใช้โปรแกรม Nmap ทำการสแกนพอร์ตของเป้าหมาย

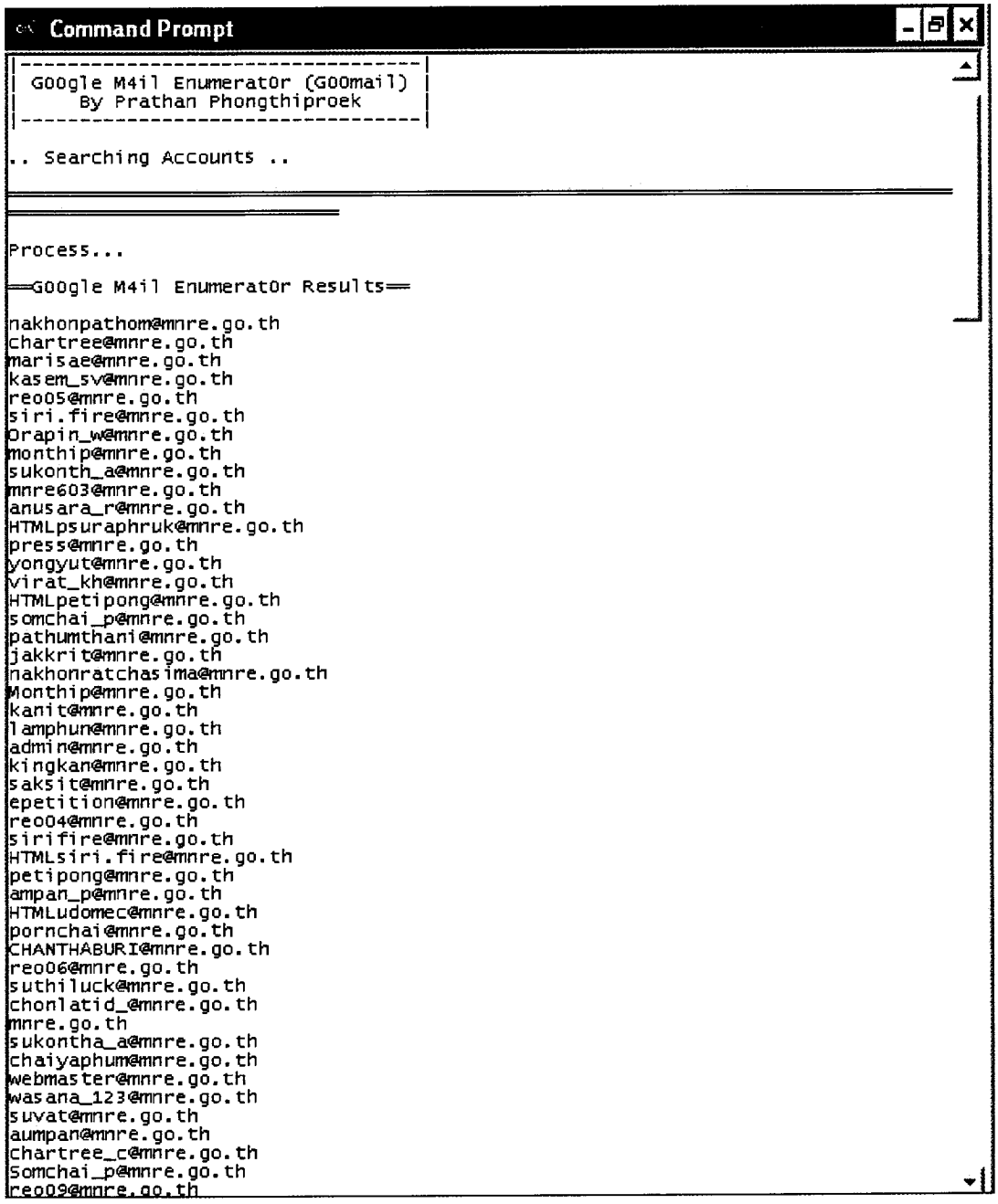
2. จากผลการสแกนพอร์ต ทำให้ผู้ทดสอบพบว่าเป้าหมายมีการใช้งาน Terminal Service ทำให้ผู้ทดสอบสามารถทำการ Remote Desktop ไปยังเครื่องเป้าหมายได้โดยตรง หลังจากนั้นได้ทดสอบคาดเดาบัญชีผู้ใช้ และรหัสผ่าน คือ administrator/password ปรากฏว่าสามารถเข้าสู่ระบบได้สำเร็จ ด้วยสิทธิ์ของผู้ดูแลระบบ รวมถึงสามารถเพิ่มผู้ใช้ (User) acis และเพิ่มสิทธิ์ให้อยู่ในกลุ่มของผู้ดูแลระบบได้สำเร็จ ดังแสดงในรูปที่ 2 และสามารถเข้าถึงระบบจัดการการทำงานของ Firewall (ISA Server) ได้ทั้งหมด ดังแสดงในรูปที่ 3

รูปที่ 2 การเข้าสู่ระบบ ด้วยสิทธิ์ของผู้ดูแลระบบผ่าน Remote Desktop



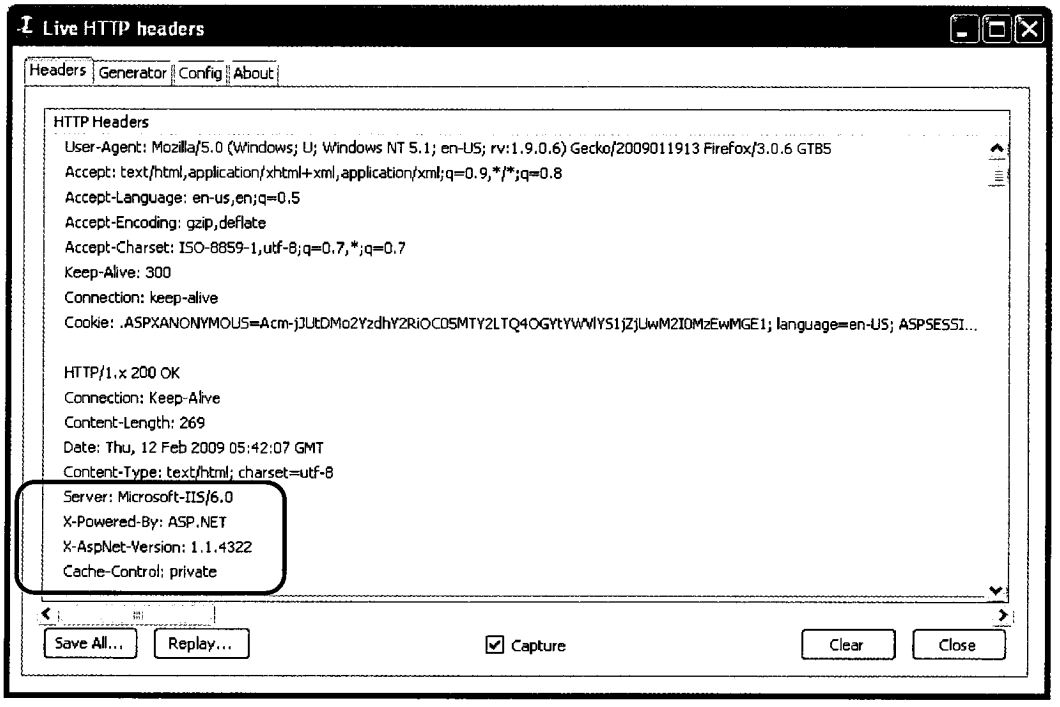
รูปที่ 3 การเข้าถึงระบบจัดการการทำงานของ Firewall (ISA Server)

3. ผู้ทดสอบได้ใช้โปรแกรม Goomail สแกนหาอีเมล์ของยูเซอร์ภายในองค์กร (@mnre.go.th) ที่ปรากฏบนอินเทอร์เน็ต และสามารถรวบรวมอีเมล์ของพนักงานภายในองค์กรได้จำนวนมาก ซึ่งมีความเสี่ยง เนื่องจากข้อมูลดังกล่าวอาจใช้ในการโจมตีแบบ Social Engineering ได้ เช่นหลอกลวงพนักงานภายในองค์กรเพื่อให้เปลี่ยนรหัสผ่านของผู้ดูแลระบบ เป็นต้น ดังแสดงในรูปที่ 4



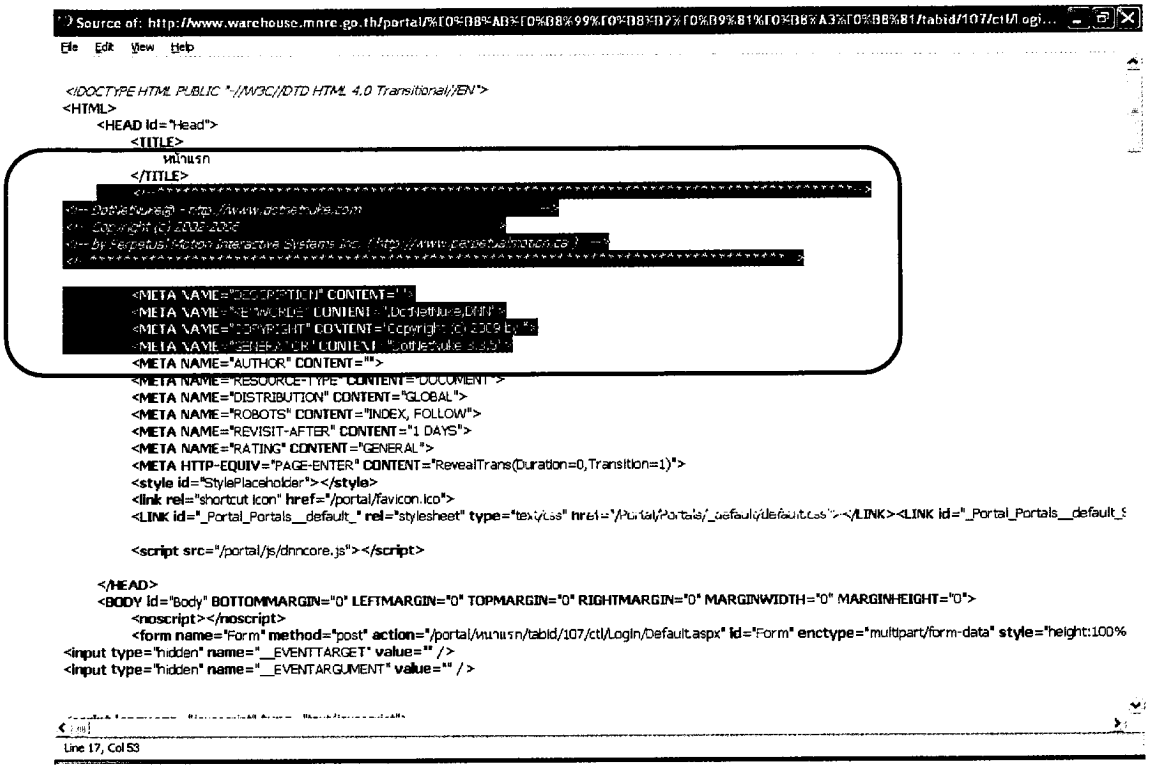
รูปที่ 4 การใช้โปรแกรม Goomail รวบรวมอีเมล์ของพนักงานภายในองค์กร (@mnre.go.th) จากอินเทอร์เน็ต

4. ผู้ทดสอบใช้โปรแกรม Live HTTP Header ทำการดักจับ HTTP Header ของเว็บไซต์เพื่อรวบรวมรายละเอียดของเว็บเซิร์ฟเวอร์ ซึ่งทำให้ผู้ทดสอบทราบว่าเว็บไซต์ดังกล่าวมีการใช้งาน IIS6.0 และ ASP.NET ดังแสดงในรูปที่ 5



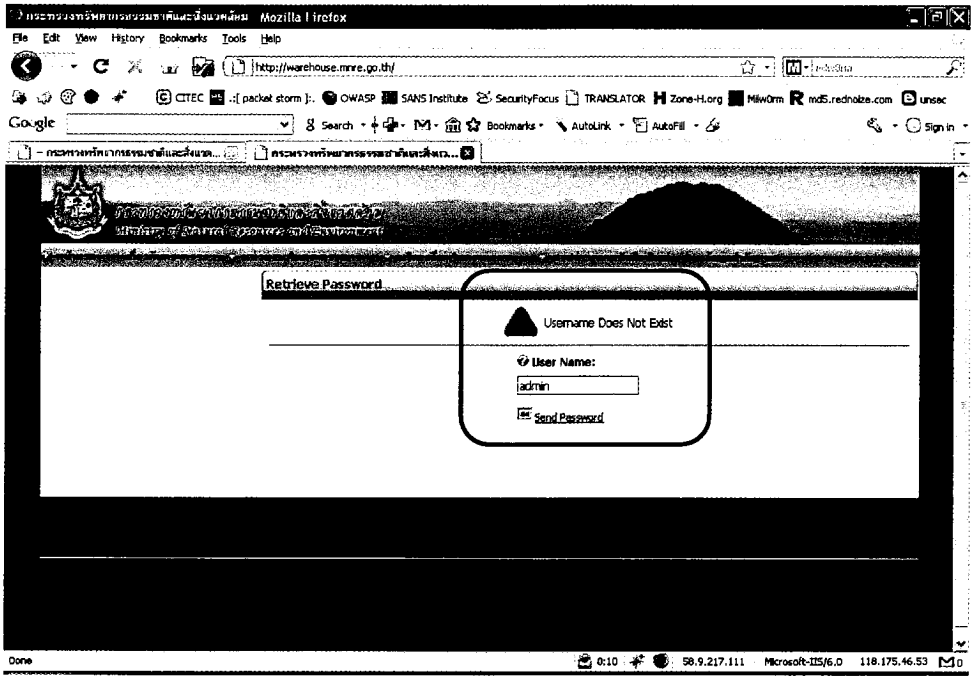
รูปที่ 5 การใช้โปรแกรม Live HTTP Header **ดักจับ** Header **ของเว็บไซต์** http://www.warehouse.mnre.go.th

5. ผู้ทดสอบสำรวจซอร์สโค๊ด (Source code) ซึ่งทำให้ทราบว่าเว็บแอพพลิเคชั่นดังกล่าวใช้งาน Web Content Management System (WCMS) ของ DotNetNuke เวอร์ชั่น 3.3.5 ดังแสดงในรูปที่ 6 และหลังจากนั้นผู้ทดสอบได้สำรวจหาช่องโหว่ของ DotNetNuke เวอร์ชั่นดังกล่าว แต่จากการสำรวจไม่พบว่ามีช่องโหว่ใด ๆ

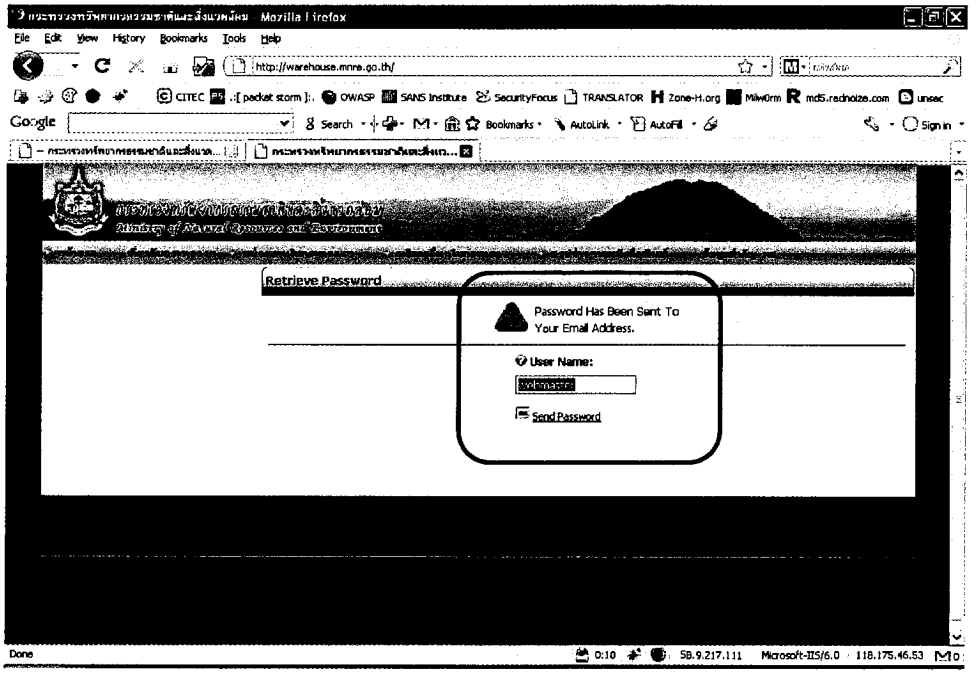


รูปที่ 6 การสำรวจซอร์สโค๊ดของเว็บแอพพลิเคชั่น

6. ผู้ทดสอบสามารถเข้าสู่ระบบล็อกอินได้ เนื่องจากผู้ทดสอบพบลิงค์ (Link) สำหรับเข้าสู่ระบบล็อกอินในหน้าแรกของเว็บ หลังจากนั้นได้ทดสอบเข้าสู่ระบบลืมรหัสผ่านเพื่อพยายามค้นหาบัญชีผู้ใช้ภายในระบบ และพบว่าระบบลืมรหัสผ่านมีการแจ้งผลไม่เหมาะสม เนื่องจากหากมีการใส่บัญชีผู้ใช้ที่มีอยู่ในระบบ ระบบจะแสดงข้อความว่า "Password Has Been Sent To Your Email Address" แต่หากบัญชีผู้ใช้ดังกล่าวไม่มีอยู่จริงในระบบ ระบบจะแสดงข้อความว่า "Username Does Not Exist" ซึ่งลักษณะของการแสดงข้อความดังกล่าวเป็นช่องโหว่ที่ทำให้สามารถค้นหาบัญชีผู้ใช้ที่มีการใช้งานอยู่ได้ด้วยการคาดเดา ดังแสดงในรูปที่ 7 และ 8



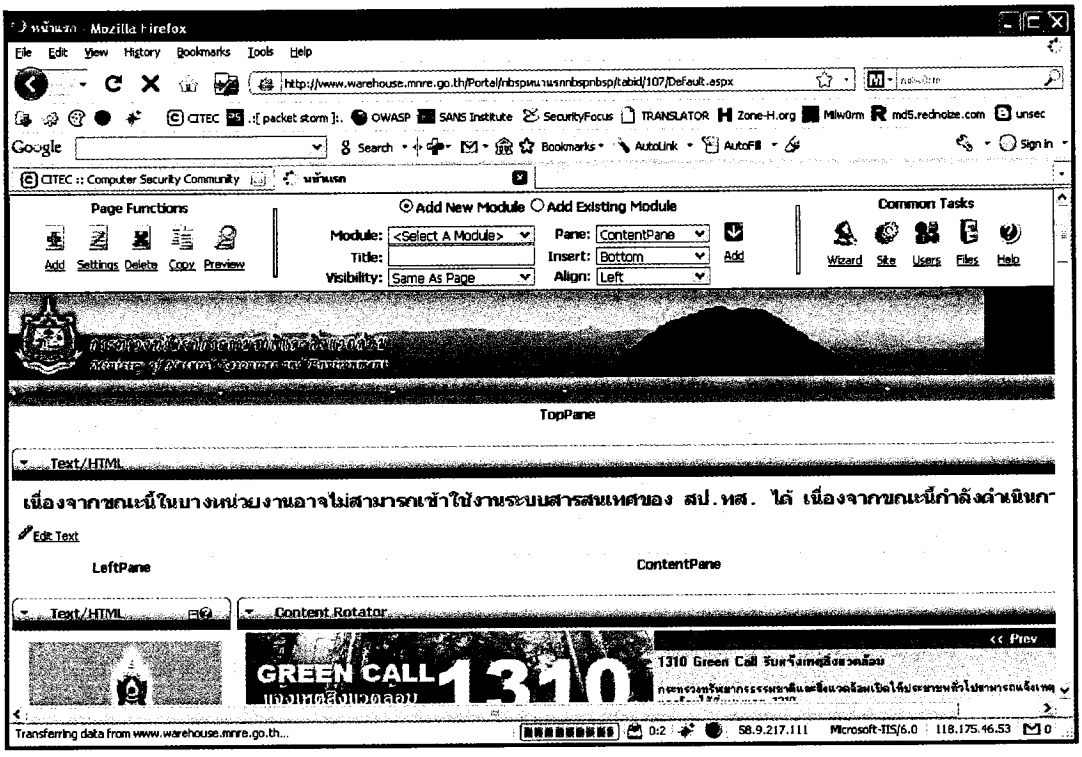
รูปที่ 7 การทดสอบคาดเดาบัญชีผู้ใช้ภายในระบบ กรณีไม่มีบัญชีผู้ใช้ภายในระบบ



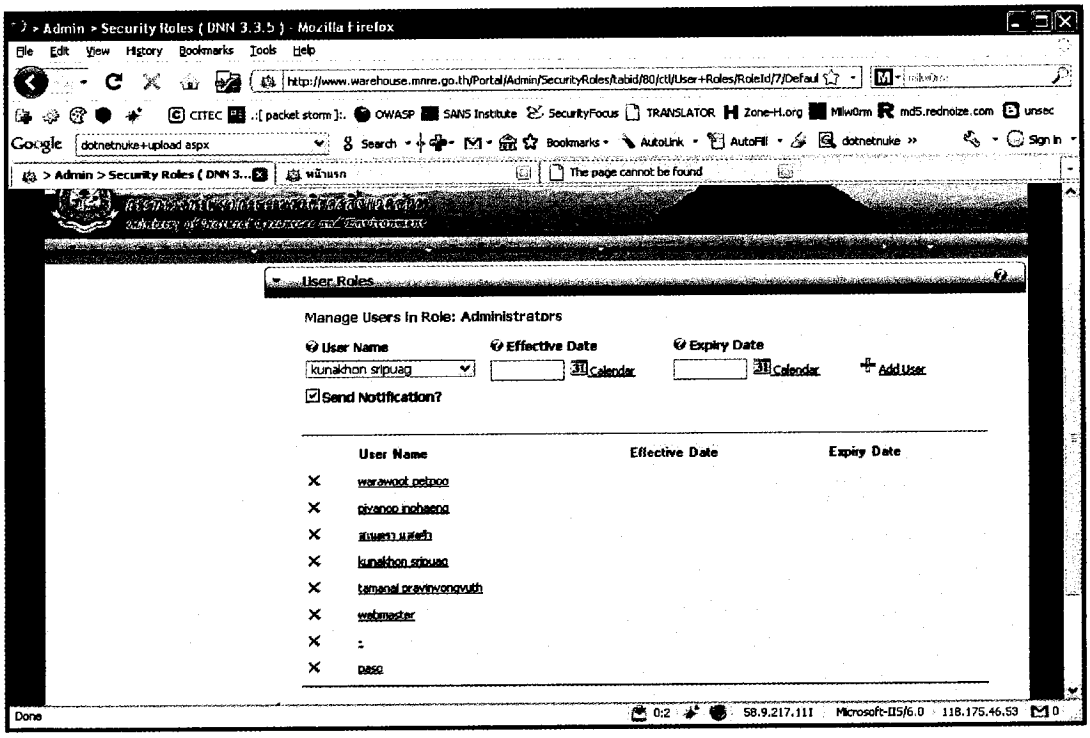
รูปที่ 8 การทดสอบคาดเดาบัญชีผู้ใช้ภายในระบบ กรณีมีบัญชีผู้ใช้ภายในระบบ

7. ผู้ทดสอบได้ทดลองคาดเดาบัญชีผู้ใช้ที่ผู้ดูแลระบบมักจะใช้งาน และทำให้ทราบว่าระบบใช้บัญชีผู้ใช้คือ webmaster จากนั้นจึงได้ทดลองคาดเดารหัสผ่านที่ง่ายต่อการเดาคือ webadmin ซึ่งสามารถเข้าถึงระบบจัดการเว็บไซต์ได้สำหรับผู้ดูแลระบบได้สำเร็จ และสามารถเปลี่ยนแปลงเนื้อหาภายในระบบได้ทั้งหมด รวมถึงสามารถเพิ่มบัญชี

(Account) หรือเปลี่ยนรหัสผ่านภายในระบบได้ทั้งหมด ดังแสดงในรูปที่ 9 และ 10

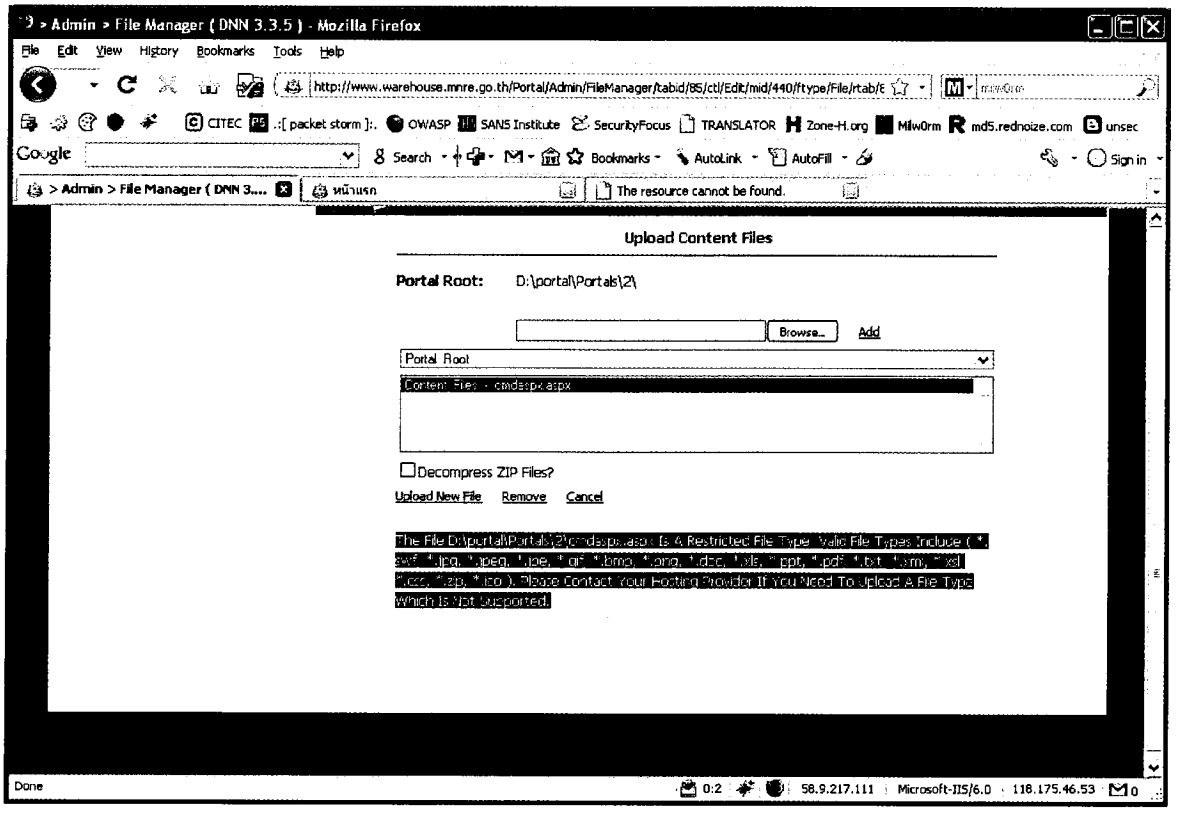


รูปที่ 9 การทดสอบคาดเดารหัสผ่าน



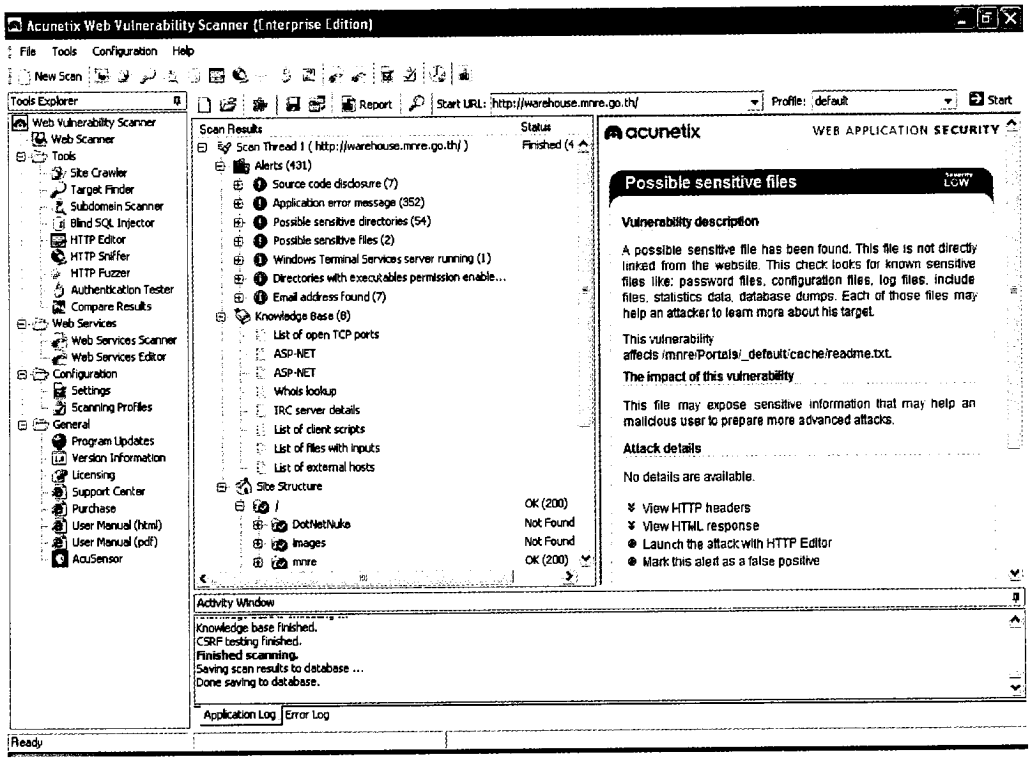
รูปที่ 10 การทดสอบการเพิ่ม เปลี่ยนแปลง ลบยูเซอร์ ภายในระบบจัดการเว็บไซต์

8. ผู้ทดสอบพยายามทำการอัพโหลดไฟล์ (Upload) แปลกปลอมเข้าสู่ระบบดังแสดงในรูปที่ 11 ซึ่งหากเว็บไซต์ไม่มีการป้องกันการรับไฟล์แปลกปลอมก็จะทำให้ผู้บุกรุกสามารถใช้ไฟล์แปลกปลอมดังกล่าวเป็นเครื่องมือในการเจาะระบบ แต่จากการทดสอบพบว่าระบบไม่ยอมรับไฟล์นอกเหนือจากที่กำหนด ซึ่งแสดงว่าเว็บไซต์สามารถป้องกันการโจมตีในลักษณะดังกล่าว



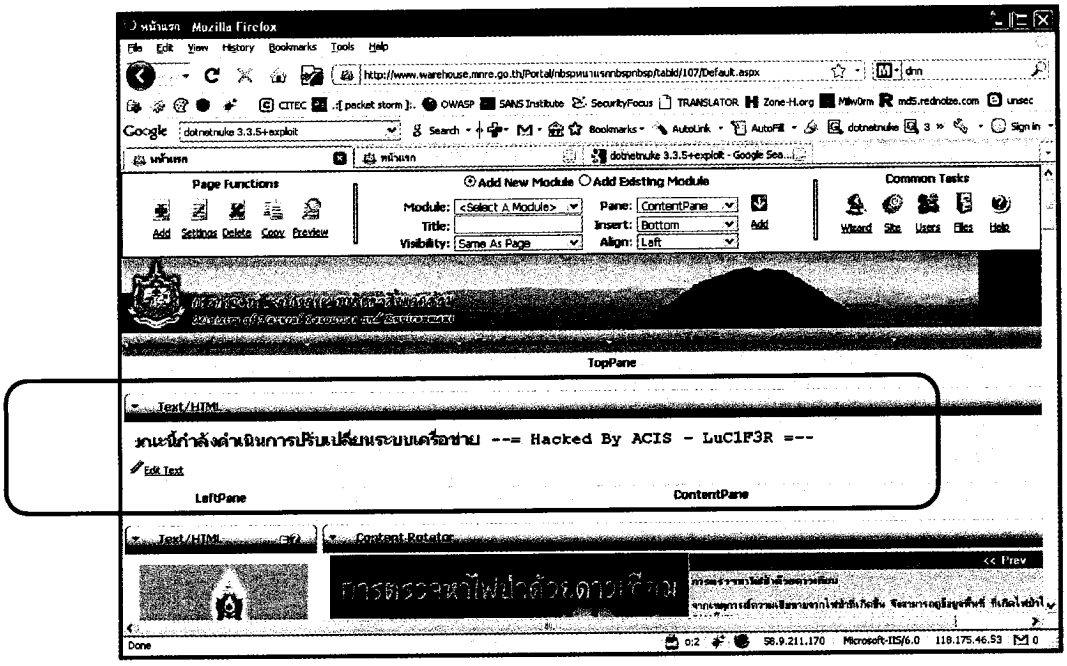
รูปที่ 11 การทดสอบการอัพโหลดไฟล์แปลกปลอมเข้าสู่ระบบ

9. เพื่อให้มั่นใจว่าเว็บไซต์ไม่มีช่องโหว่ใด ๆ นอกเหนือจากนี้ ผู้ทดสอบใช้โปรแกรม Acunetix ดังแสดงในรูปที่ 12 ซึ่งเป็นโปรแกรมสำหรับสแกนหาช่องโหว่ทางเว็บแอพพลิเคชั่น (Web application) ทำการสแกนหาช่องโหว่ แต่ไม่พบว่ามีช่องโหว่ เพิ่มเติม



รูปที่ 12 การทดสอบโดยใช้โปรแกรม Acunetix สแกนช่องโหว่ทางเว็บแอพพลิเคชั่น

10. ผู้ทดสอบจำลองสถานการณ์ให้เห็นว่าหากผู้บุกรุกพบช่องโหว่ และสามารถเจาะระบบได้เช่นเดียวกับการทดสอบครั้งนี้ ก็จะสามารถปรับโฉมหน้าเว็บไซต์ได้ตามที่ผู้บุกรุกต้องการ ดังแสดงในรูปที่ 13 ซึ่งรูปดังกล่าวเกิดจากการสมมุติขึ้นเท่านั้น ผู้ทดสอบไม่ได้แก้ไขหรือปรับโฉมหน้าเว็บไซต์ดังกล่าว



รูปที่ 13 การจำลองสถานการณ์ปรับโฉมหน้าเว็บไซต์

สิ่งที่พบจากการทดสอบ

จากการทดสอบเจาะระบบเว็บไซต์ http://www.warehouse.mnre.go.th/ ผู้ทดสอบพบว่าสามารถเจาะระบบเว็บไซต์ดังกล่าวได้ง่าย เนื่องจากผู้ทดสอบพบช่องทางในการเข้าถึงระบบล็อกอินภายในหน้าแรกของเว็บไซต์ อีกทั้งผู้ทดสอบยังสามารถใช้ระบบลืมรหัสผ่านในการคาดเดาแอคเคานท์ที่มีในระบบ และพบว่าแอคเคานท์ของผู้ดูแลระบบมีการใช้รหัสผ่านที่ง่ายต่อการคาดเดา ซึ่งทั้งหมดนี้สามารถนำไปสู่การยึดครองเว็บไซต์ของ สป.ทส.

จากการทดสอบสามารถสรุปสิ่งที่พบจากการทดสอบได้ดังนี้

- สามารถทราบรายละเอียดของเว็บเซิร์ฟเวอร์ (Web server) ได้จาก HTTP Header และไฟล์ phpinfo.php
- สามารถ Remote Desktop ไปยังเครื่องเป้าหมาย และเข้าสู่ระบบเพื่อครอบครองทรัพยากรของเครื่อง Firewall ได้สำเร็จ
- จากการสำรวจซอร์สโค๊ด (Source code) ทำให้พบว่าเว็บไซต์ดังกล่าวใช้ Web Content Management System (WCMS) ของ DotNetNuke
- สามารถเข้าถึงระบบล็อกอินของเว็บไซต์ได้โดยง่าย
- ระบบมีการแจ้งเตือนข้อความการลืมรหัสผ่านไม่เหมาะสม ทำให้สามารถคาดเดาบัญชีผู้ใช้ภายในระบบได้
- สามารถเข้าถึงระบบจัดการเว็บไซต์ของผู้ดูแลระบบได้ รวมถึงสามารถเปลี่ยนแปลงเนื้อหาทั้งหมดภายในเว็บไซต์ได้

หากผู้บุกรุกพบช่องโหว่ดังกล่าว จะก่อให้เกิดความสูญเสียต่อ สป.ทส. ดังนี้

- **ความสูญเสียด้าน** Confidentiality

ความสูญเสียด้าน Confidentiality คือผลกระทบที่ก่อให้เกิดการสูญเสียข้อมูลที่เป็นความลับ ซึ่งจากการทดสอบสามารถยึดครองเว็บไซต์ดังกล่าวของ สป.ทส. ได้ ทำให้มีโอกาสที่ผู้บุกรุกจะสามารถเข้าถึงข้อมูลที่เป็นความลับภายในเว็บไซต์ดังกล่าว

- **ความสูญเสียด้าน** Availability

ความสูญเสียด้าน Availability คือผลกระทบที่เกี่ยวข้องกับความพร้อมใช้งานของระบบ ซึ่งจากการทดสอบสามารถยึดครองเว็บไซต์ดังกล่าวของ สป.ทส. ได้ ทำให้มีโอกาสที่ผู้บุกรุกจะปรับโฉมหน้าของเว็บไซต์ ซึ่งทำให้ผู้ใช้งานไม่สามารถใช้งานเว็บไซต์ดังกล่าวได้

คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- Ability to Guess Administrative Username and Password

  ความเสี่ยงทางเทคนิค: สูง

พบว่าระบบล็อกอินมีการใช้ชื่อผู้ใช้และรหัสผ่านที่ง่ายต่อการคาดเดา เนื่องจากทั้งบัญชีผู้ใช้ และรหัสผ่านปรากฏใน Dictionary ทำให้สามารถใช้โปรแกรมสำหรับคาดเดารหัสผ่าน (Brute Force Attack) เพื่อคาดเดารหัสผ่านได้โดยง่าย จึงควรแก้ไขโดยการเปลี่ยนแปลงบัญชีผู้ใช้ และรหัสผ่านให้ยากต่อการคาดเดา เช่นรหัสผ่านต้องประกอบไปด้วยตัวอักษรตัวเล็ก ตัวใหญ่ ตัวเลข ตัวอักขระพิเศษผสมกัน และมีความยาวไม่ต่ำกว่า 8 ตัวอักษร

- Ability to Gain Access to Administrative Control Management (**สอดคล้องกับมาตรฐาน** OWASP **ปี ค.ศ.** 2007 **ข้อ** 10)

  ความเสี่ยงทางเทคนิค: สูง

พบว่ามีการใช้บัญชีผู้ใช้ และรหัสผ่าน ที่ง่ายต่อการคาดเดา รวมถึงมีลิงค์ที่เข้าสู่ระบบล็อกอินการจัดการข้อมูลบนเว็บไซต์ จึงควรแก้ไขโดยการซ่อนลิงค์ (Link) สำหรับเข้าสู่ระบบล็อกอินของเว็บไซต์

- Information Leakage and Improper Handling (**สอดคล้องกับมาตรฐาน** OWASP**ปี ค.ศ.** 2007**ข้อ** 6)

  ความเสี่ยงทางเทคนิค: ปานกลาง

เนื่องจากระบบลืมรหัสผ่านมีการแจ้งเตือนข้อความไม่เหมาะสม ทำให้สามารถคาดเดาบัญชีผู้ใช้ที่มีอยู่จริงในระบบได้ จึงควรแก้ไขโดยแสดงข้อความแจ้งเตือนให้เหมือนกัน ทั้งกรณียูเซอร์ดังกล่าวมีอยู่จริง หรือไม่มีในระบบ

- Server Info in HTTP Headers

  ความเสี่ยงทางเทคนิค: ต่ำ

  ควรทำการปิด หรือสร้างข้อมูล Header หลอก เพื่อป้องกันการรวบรวมข้อมูลผ่านทาง Header ของเว็บไซต์

- Email Address Found from Internet

  ความเสี่ยงทางเทคนิค: ต่ำ

ผู้ทดสอบสามารถรวบรวมอีเมล์ (E-mail) ของพนักงานภายในองค์กรได้ จากอินเทอร์เน็ต ซึ่งมีความเสี่ยงในการโจมตีแบบ Social Engineering จึงควรแก้ไขโดยการกำหนดนโยบายภายในองค์กร ไม่ให้ใช้อีเมล์ดังกล่าวในการโพสข้อความภายนอกองค์กร เช่นเว็บบอร์ดสาธารณะ

1.2 ผลการทดสอบเจาะระบบจากภายนอกผ่านทางเว็บไซต์ http://petition.mnre.go.th/

ตารางที่ 6 แสดงผลกระทบทางเทคนิค โอกาสที่จะเกิด และความเสี่ยงทางเทคนิคของเว็บไซต์

http://petition.mnre.go.th

ผลกระทบทางเทคนิค: ระดับสูง
สิ่งที่พบ เว็บไซต์ http://petition.mnre.go.th/ มีผลกระทบทางเทคนิคอยู่ในระดับสูง เนื่องจากผู้ทดสอบพบช่องทางในการเข้าถึงระบบล็อกอินภายในหน้าแรกของเว็บไซต์ อีกทั้งผู้ทดสอบยังสามารถใช้ระบบลืมรหัสผ่านในการคาดเดาแอคเคานท์ที่มีในระบบ และพบว่าแอคเคานท์ของผู้ดูแลระบบมีการใช้รหัสผ่านที่ง่ายต่อการคาดเดา ซึ่งทั้งหมดนี้ทำให้สามารถเข้าไปบริหารจัดการระบบได้ และนำไปสู่การยึดครองเว็บไซต์ของ สป.ทส. ซึ่งมีผลกระทบอยู่ในระดับสูง
โอกาสที่จะเกิด: ระดับปานกลาง
สิ่งที่พบ เว็บไซต์ http://petition.mnre.go.th/ มีโอกาสที่จะถูกเจาะระบบจากผู้บุกรุกในระดับปานกลาง เนื่องจากมีโอกาสที่ผู้บุกรุกสามารถเข้าถึงช่องโหว่ดังเช่นที่พบในการทดสอบครั้งนี้ และสามารถคาดเดารหัสผ่านของผู้ดูแลระบบจนทำให้สามารถเข้าไปบริหารจัดการระบบได้
ความเสี่ยงทางเทคนิค: ระดับสูง
สิ่งที่พบ เว็บไซต์ http://petition.mnre.go.th/ มีความเสี่ยงทางเทคนิคอยู่ในระดับสูง ซึ่งได้จากการคำนวณผลกระทบทางเทคนิค (ระดับสูง) และโอกาสที่จะเกิด(ระดับปานกลาง) นำมาเปรียบเทียบกับตารางที่ 2.2 ทำให้พบว่าความเสี่ยงทางเทคนิคอยู่ในระดับสูง

ตารางที่ 7 แสดงความสูญเสียด้าน Confidentiality Integrity **และ** Availability **ของเว็บไซต์**

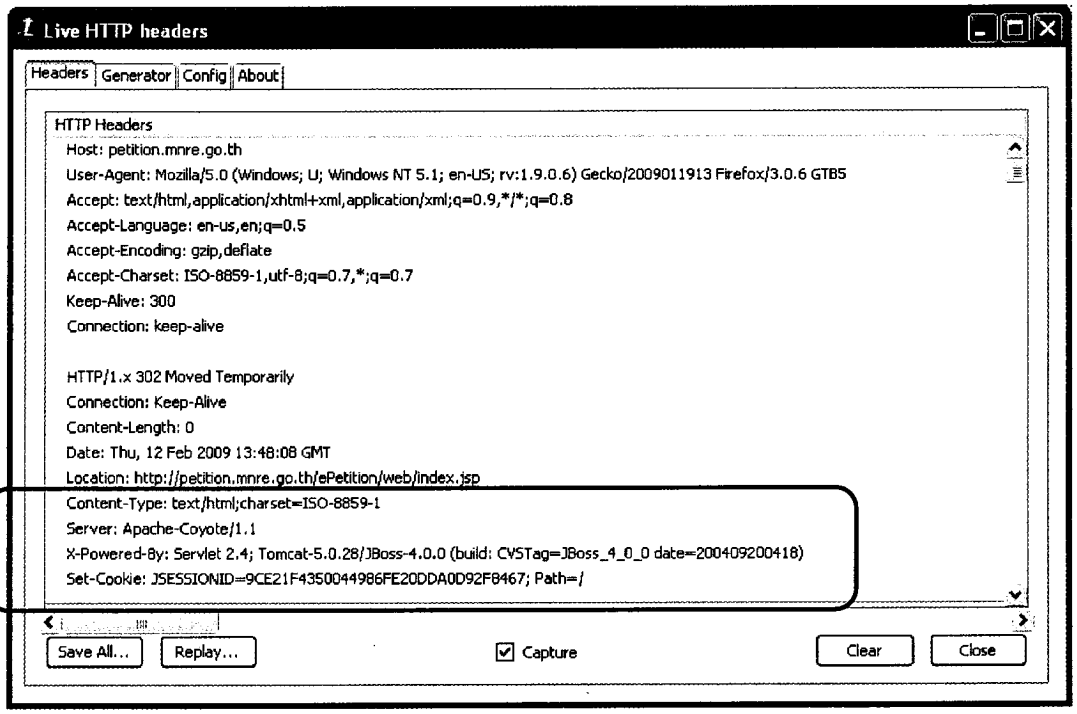
http://petition.mnre.go.th

ความสูญเสียด้าน Confidentiality: มีผลกระทบ
สิ่งที่พบ ความสูญเสียด้าน Confidentiality คือผลกระทบที่ก่อให้เกิดการสูญเสียข้อมูลที่เป็นความลับ ซึ่งจากการทดสอบสามารถยึดครองเว็บไซต์ดังกล่าวของ สป.ทส. ได้ ทำให้มีโอกาสที่ผู้บุกรุกจะสามารถเข้าถึงข้อมูลที่เป็นความลับภายในเว็บไซต์ดังกล่าว
ความสูญเสียด้าน Integrity: ไม่มีผลกระทบ
สิ่งที่พบ ไม่พบปัจจัยที่ส่งผลต่อความสูญเสียด้าน Integrity

ความสูญเสียด้าน Availability: มีผลกระทบ
สิ่งที่พบ ความสูญเสียด้าน Availability คือผลกระทบที่เกี่ยวข้องกับความพร้อมใช้งานของระบบ ซึ่งจากการทดสอบสามารถยึดครองเว็บไซต์ดังกล่าวของ สป.ทส. ได้ ทำให้มีโอกาสที่ผู้บุกรุกจะปรับโฉมหน้าของเว็บไซต์ ซึ่งทำให้ผู้ใช้งานไม่สามารถใช้งานเว็บไซต์ดังกล่าวได้

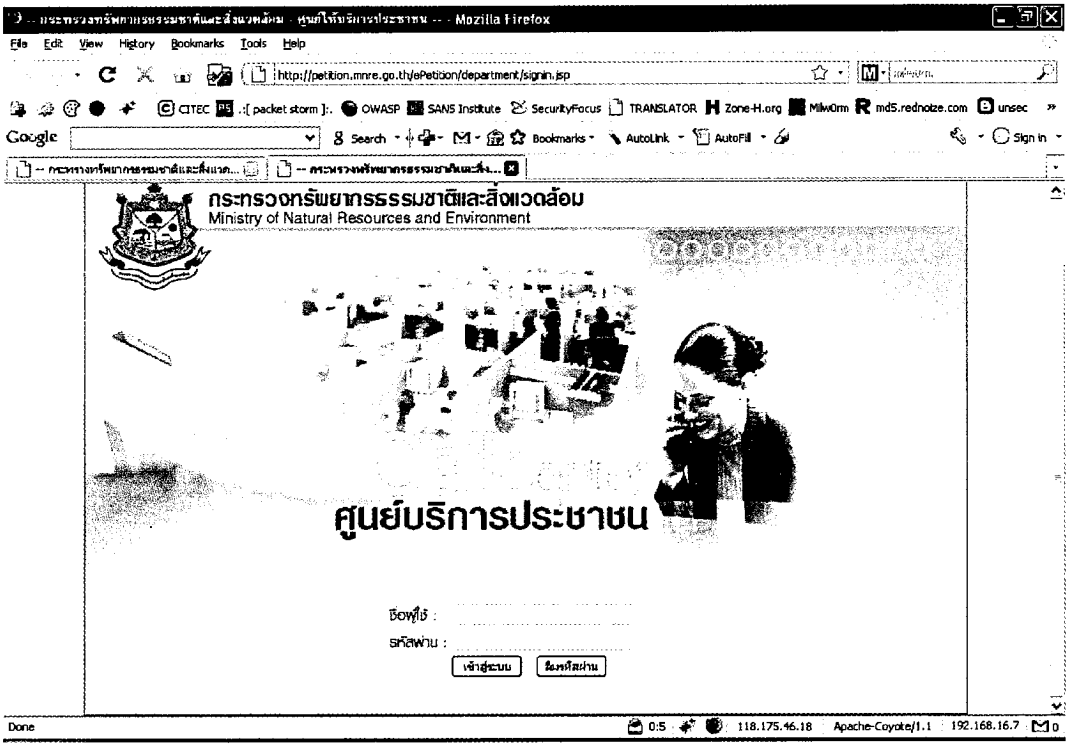
ขั้นตอนในการทดสอบ

1. ผู้ทดสอบใช้โปรแกรม Live HTTP Header ทำการดักจับ HTTP Header ของเว็บไซต์เพื่อรวบรวมรายละเอียดของเว็บเซิร์ฟเวอร์ ซึ่งทราบว่าเป็น Apache-Coyote/1.1, Servlet 2.4/Tomcat-5.0.28/Jboss-4.0.0 ดังแสดงในรูปที่ 14



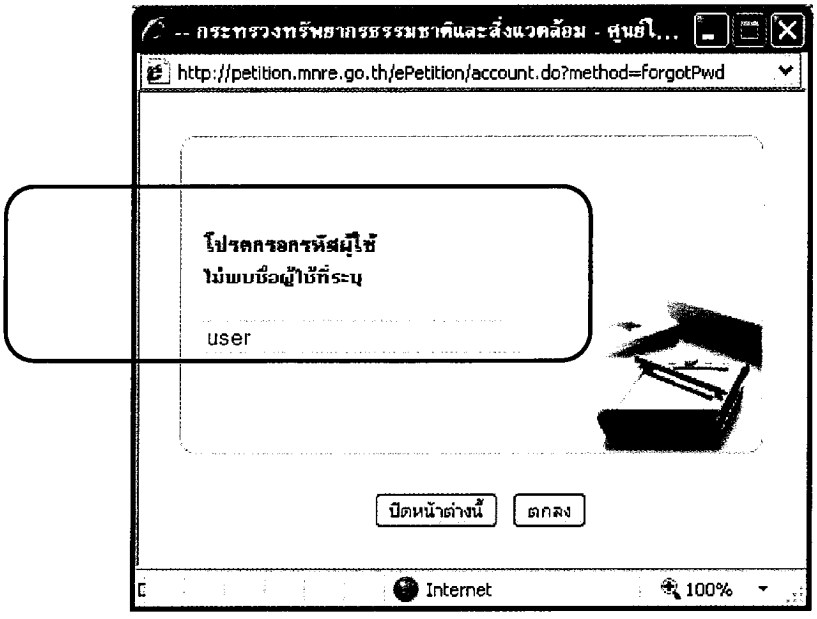
รูปที่ 14 การใช้โปรแกรม Live HTTP Header **ดักจับ** Header **ของเว็บไซต์** http://petition.mnre.go.th/

2. ผู้ทดสอบพบลิงค์ (Link) สำหรับเข้าสู่ระบบล็อกอินของเว็บไซต์ เนื่องจากมีการแสดง ลิงค์(Link) ดังกล่าวในหน้าแรกของเว็บ ทำให้ผู้ทดสอบสามารถเข้าสู่ระบบล็อกอินได้โดยตรง ดังแสดงในรูปที่ 15



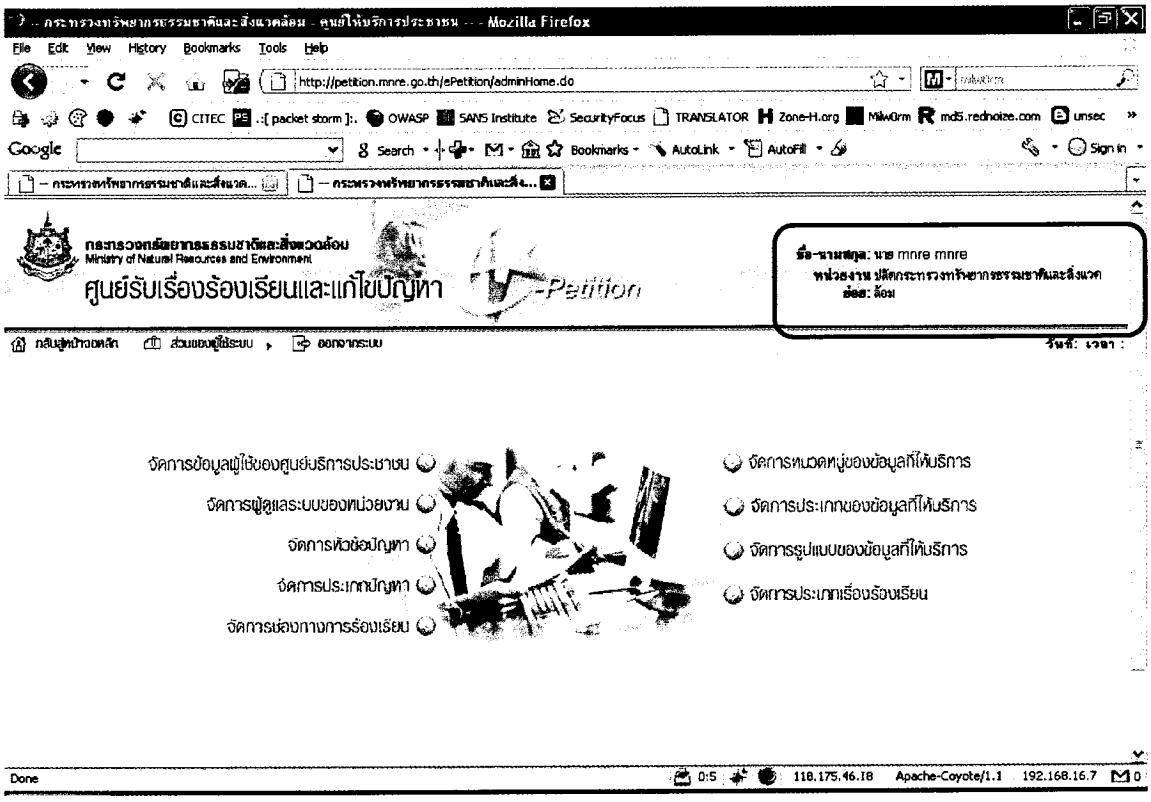
รูปที่ 15 การเข้าถึงระบบล็อกอินผู้ทดสอบสามารถเข้าถึงระบบล็อกอินได้โดยตรง

3. ผู้ทดสอบได้เข้าสู่ระบบล็อกอินของเว็บไซต์ และเข้าสู่ระบบลืมรหัสผ่านเพื่อคาดเดาบัญชีผู้ใช้ที่มีอยู่ในระบบ ซึ่งหากคาดเดาบัญชีผู้ใช้ที่ไม่มีอยู่ในระบบ ระบบจะแสดงข้อความ "ไม่พบชื่อผู้ใช้ที่ระบุ" แต่หากมีบัญชีผู้ใช้ในระบบจริง ระบบจะไม่แสดงข้อความดังกล่าว ดังแสดงในรูปที่ 16 ซึ่งลักษณะของการแสดงข้อความดังกล่าวเป็นช่องโหว่ที่ทำให้สามารถค้นหาบัญชีผู้ใช้ที่มีการใช้งานอยู่ได้ด้วยการคาดเดา



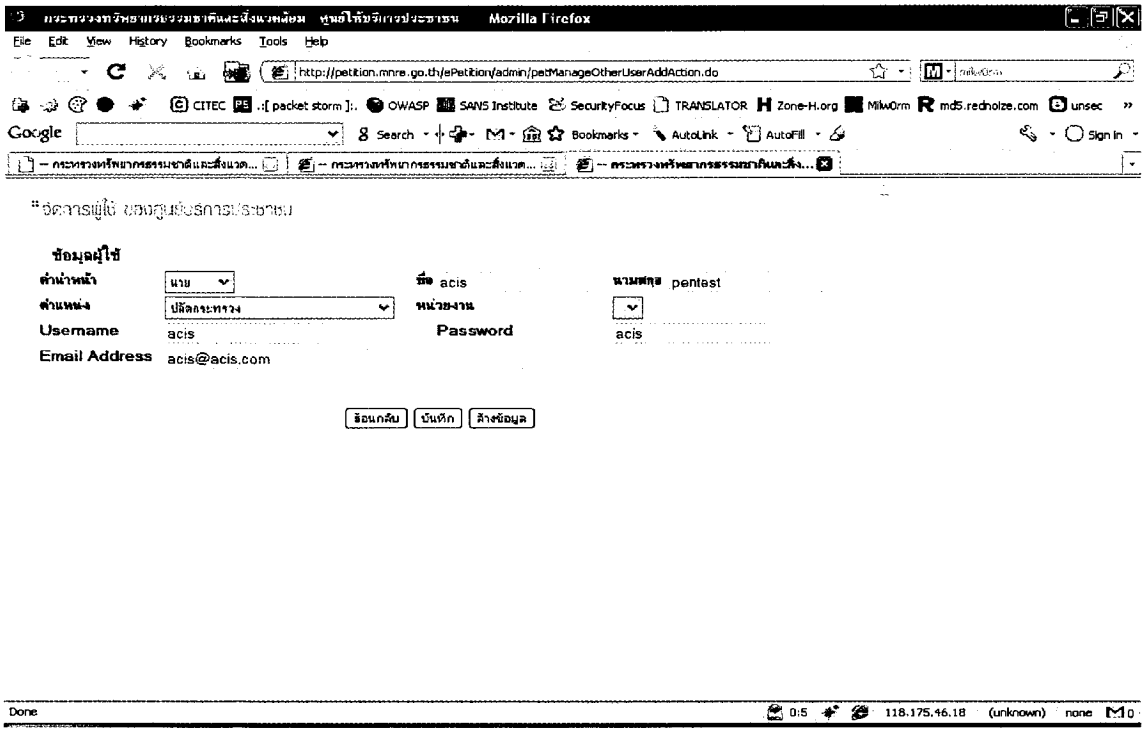
รูปที่ 16 การทดสอบระบบลืมรหัสผ่าน

4. ผู้ทดสอบทดลองคาดเดาบัญชีผู้ใช้และรหัสผ่านที่ง่ายต่อการคาดเดา และพบว่าระบบใช้งาน บัญชีผู้ใช้และรหัสผ่านคือ mnre/mnre ซึ่งสามารถเข้าสู่ระบบจัดการเว็บไซต์ได้ด้วยสิทธิ์ของปลัดกระทรวง ดังแสดงในรูปที่ 17

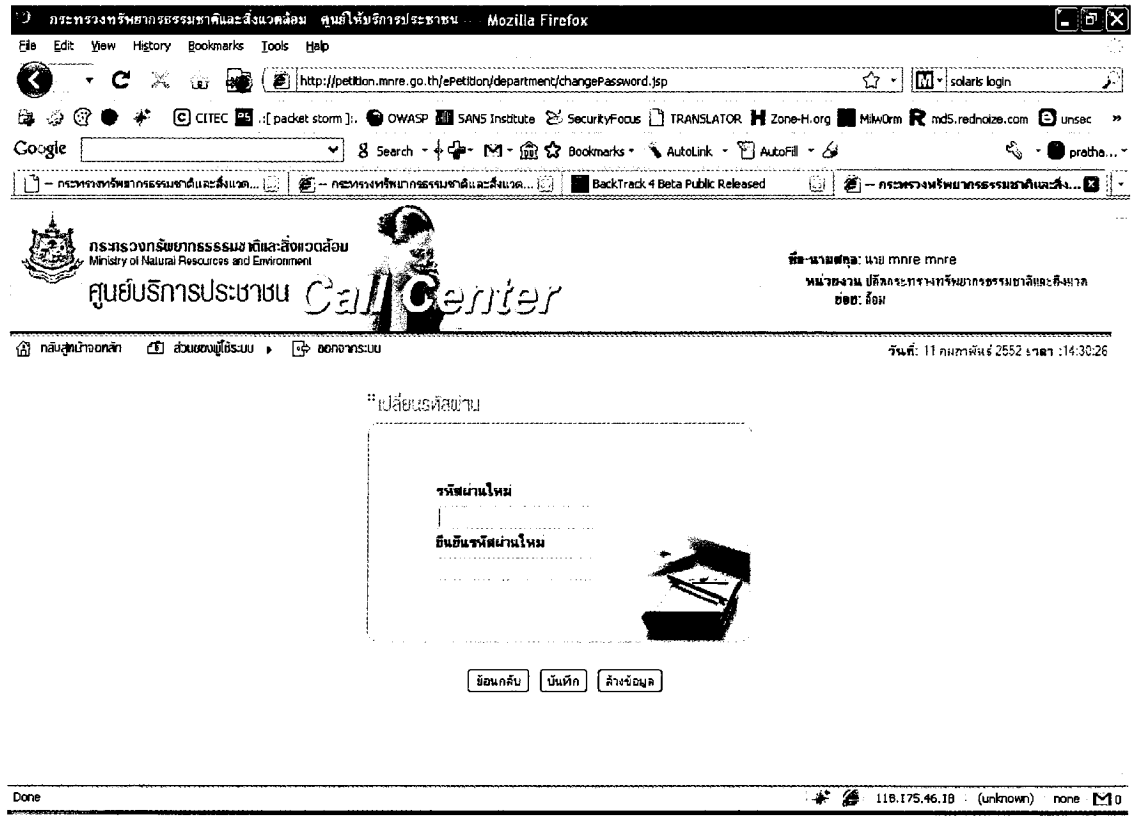


รูปที่ 17 การทดสอบเข้าระบบจัดการเว็บไซต์

5. ผู้ทดสอบสามารถเพิ่มแอคเคานท์ภายในระบบ รวมถึงเปลี่ยนแปลงรหัสผ่านของยูเซอร์ mnre ได้ ดังแสดงในรูปที่ 18 และ 19

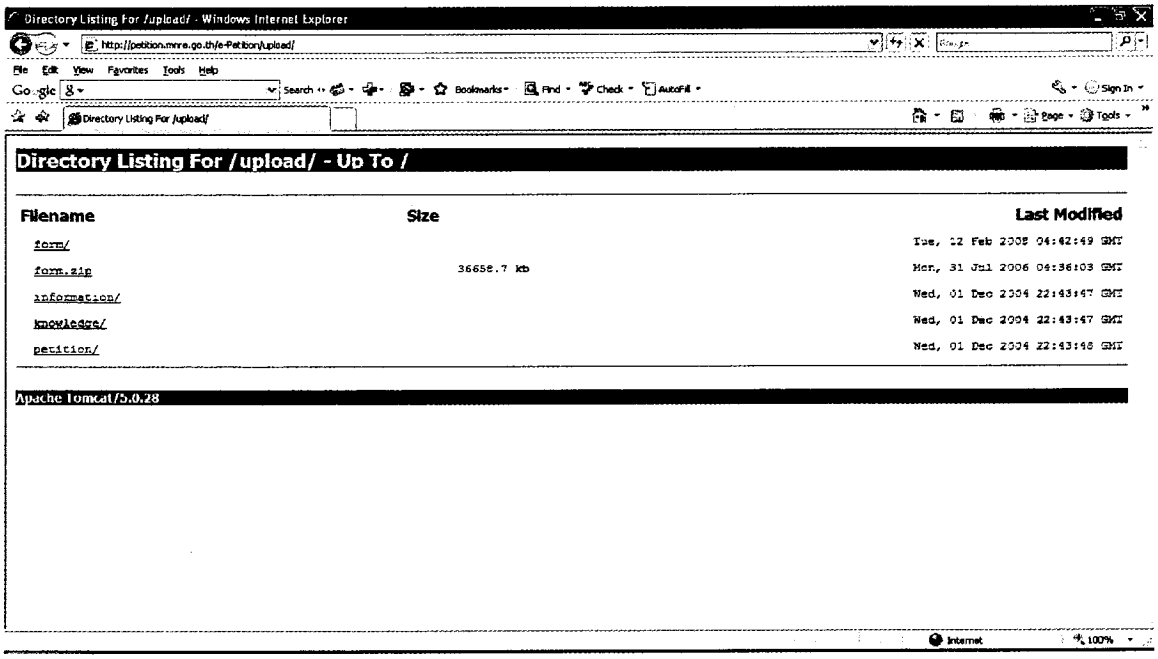


รูปที่ 18 การทดสอบเพิ่มแอคเคานท์

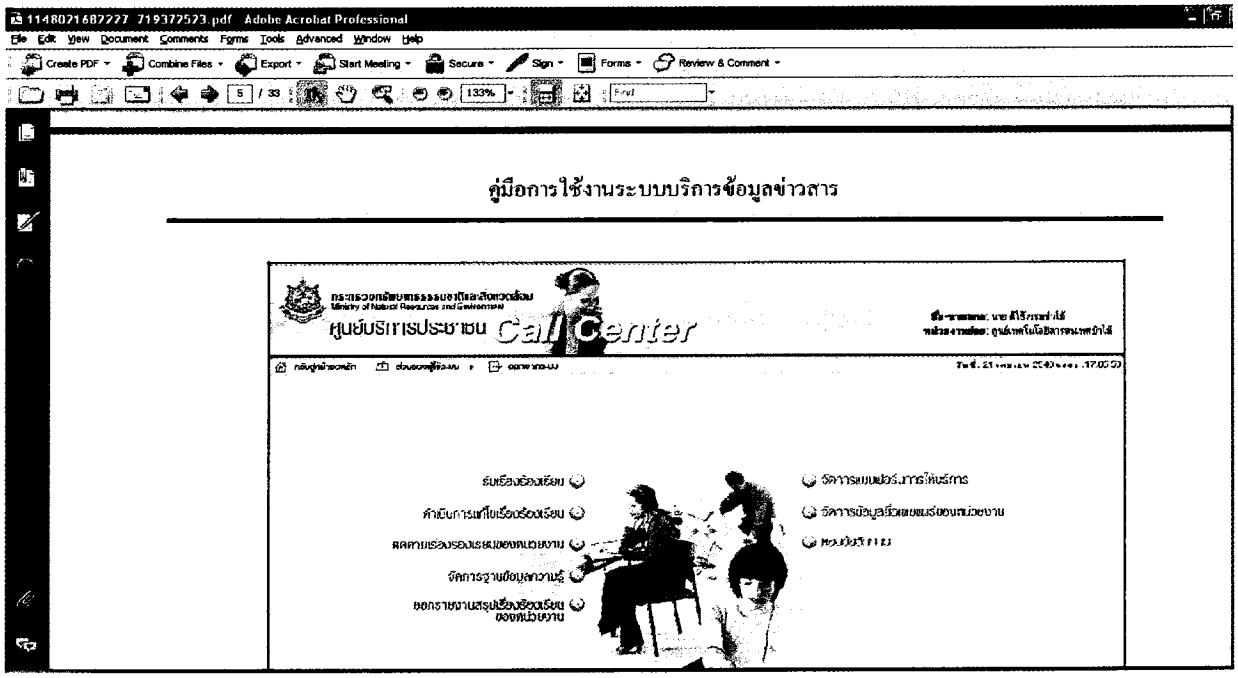


รูปที่ 19 การทดสอบเปลี่ยนแปลงรหัสผ่านของแอคเคานท์

6. ผู้ทดสอบพบว่าระบบมีช่องโหว่ของการทำ Directory Listing เนื่องจากสามารถทำการ Directory Listing ได้ที่พาท /upload ทำให้สามารถทราบถึงไดเร็กทอรี่ (Directory) และไฟล์ทั้งหมดภายในพาทนั้น ๆ ซึ่งผู้ทดสอบสามารถดาวน์โหลดไฟล์ (Download file) สำคัญ ๆ ภายในระบบได้ เช่นคู่มือการใช้งานระบบเว็บไซต์ ดังแสดงในรูปที่ 20 และ 21

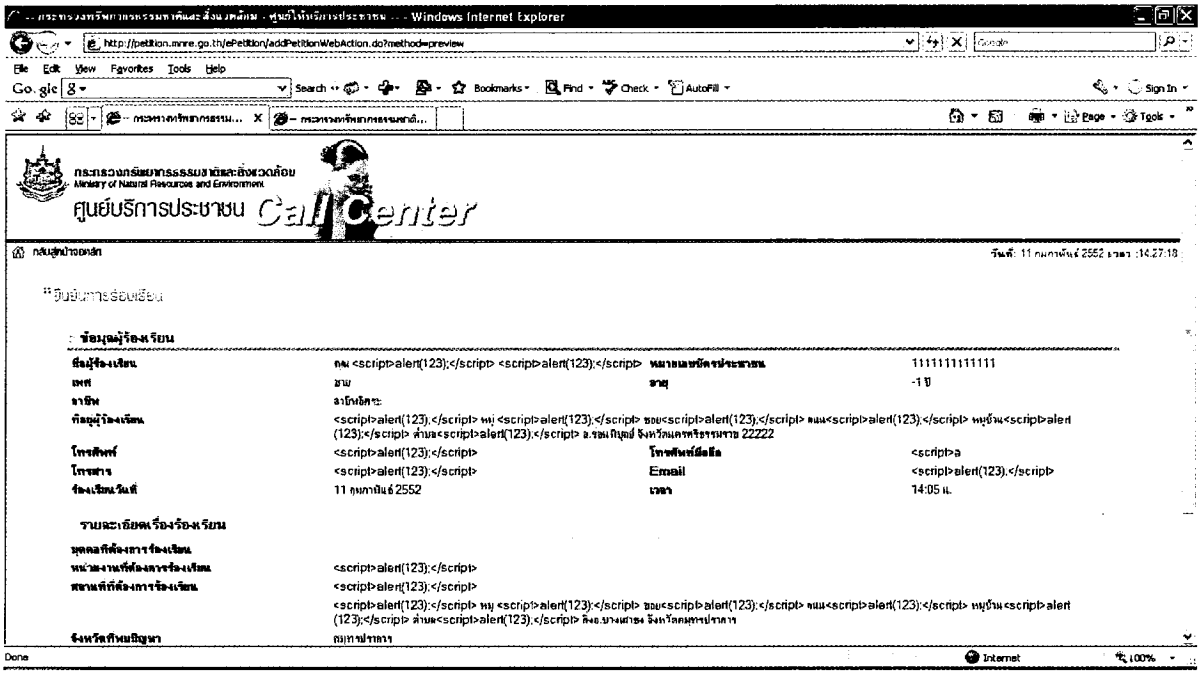


รูปที่ 20 การทดสอบช่องโหว่ Directory Listing



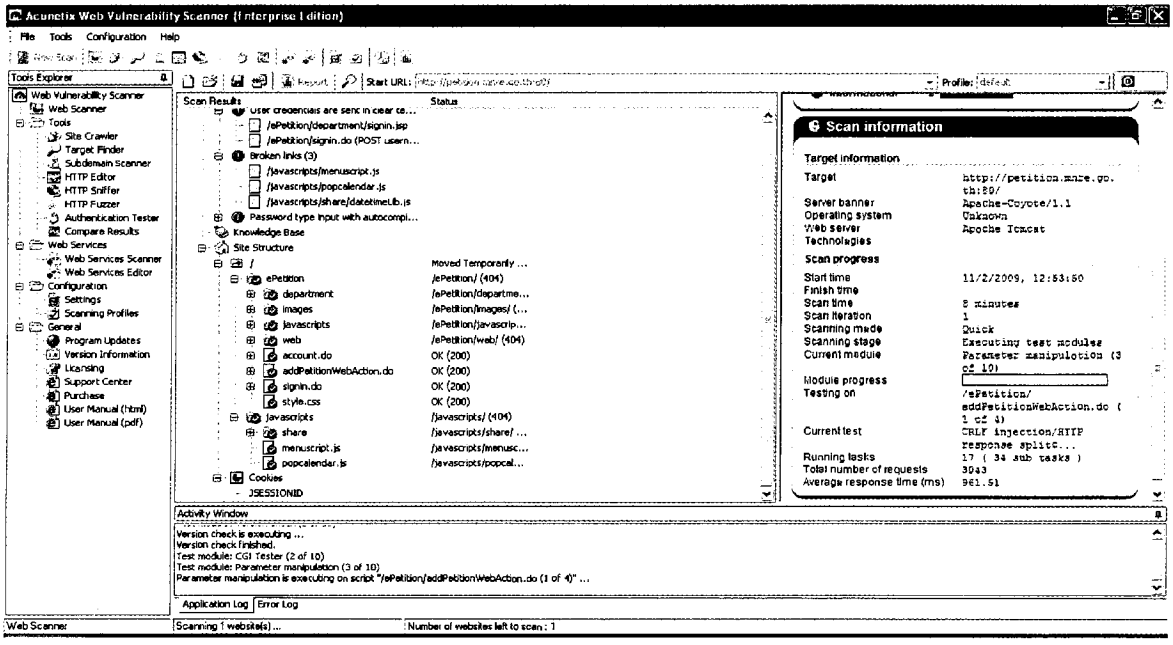
รูปที่ 21 การทดสอบดาวน์โหลดไฟล์คู่มือการใช้งานเว็บไซต์

7. ผู้ทดสอบทดลองหาช่องโหว่ของการโจมตีด้วยเทคนิค Cross Site Scripting โดยทำการส่งค่า JavaScript เข้าไปที่แบบฟอร์มการรับข้อมูล (Input form) ซึ่งหากเว็บไซต์มีช่องโหว่ดังกล่าวระบบจะรันคำสั่งที่ป้อนเข้าไป แต่จากการทดสอบไม่พบว่าเว็บไซต์ดังกล่าวมีช่องโหว่ของการโจมตีด้วยเทคนิค Cross Site Scripting ดังแสดงในรูปที่ 22



รูปที่ 22 การทดสอบช่องโหว่ Cross Site Scripting

8. เพื่อให้มั่นใจว่าเว็บไซต์ไม่มีช่องโหว่ใด ๆ นอกเหนือจากนี้ ผู้ทดสอบใช้โปรแกรม Acunetix ดังแสดงในรูปที่ 23 ซึ่งเป็นโปรแกรมสำหรับสแกนหาช่องโหว่ทางเว็บแอพพลิเคชั่น ทำการสแกนหาช่องโหว่ แต่ไม่พบว่ามีช่องโหว่ เพิ่มเติม



รูปที่ 23 การทดสอบโดยใช้โปรแกรม Acunetix สแกนช่องโหว่เว็บแอพพลิเคชั่น

สิ่งที่พบจากการทดสอบ

จากการทดสอบเจาะระบบเว็บไซต์ http://petition.mnre.go.th/ ผู้ทดสอบพบว่าสามารถเจาะระบบเว็บไซต์ดังกล่าวได้ง่าย เนื่องจากผู้ทดสอบพบช่องทางในการเข้าถึงระบบล็อกอินภายในหน้าแรกของเว็บไซต์ อีกทั้งผู้ทดสอบยังสามารถใช้ระบบลืมรหัสผ่านในการคาดเดาบัญชี (Account) ที่มีในระบบ และพบว่าบัญชีของผู้ดูแลระบบมีการใช้รหัสผ่านที่ง่ายต่อการคาดเดา ซึ่งทั้งหมดนี้สามารถนำไปสู่การยึดครองเว็บไซต์ของ สป.ทส.

จากการทดสอบสามารถสรุปสิ่งที่พบจากการทดสอบได้ดังนี้

- สามารถทราบรายละเอียดของเว็บเซิร์ฟเวอร์ได้จาก HTTP Header และไฟล์ phpinfo.php
- สามารถเข้าถึงไฟล์ Backup ของระบบได้
- สามารถทำการ Directory Listing ได้
- สามารถเข้าสู่ระบบภายในได้โดยไม่ต้องผ่านการพิสูจน์ตัวตน

หากผู้บุกรุกพบช่องโหว่ดังกล่าว จะก่อให้เกิดความสูญเสียต่อ สป.ทส. ดังนี้

- **ความสูญเสียด้าน** Confidentiality

ความสูญเสียด้าน Confidentiality คือผลกระทบที่ก่อให้เกิดการสูญเสียข้อมูลที่เป็นความลับ ซึ่งจากการทดสอบสามารถยึดครองเว็บไซต์ดังกล่าวของ สป.ทส. ได้ ทำให้มีโอกาสที่ผู้บุกรุกจะสามารถเข้าถึงข้อมูลที่เป็นความลับภายในเว็บไซต์ดังกล่าว

- **ความสูญเสียด้าน** Availability

ความสูญเสียด้าน Availability คือผลกระทบที่เกี่ยวข้องกับความพร้อมใช้งานของระบบ ซึ่งจากการทดสอบสามารถยึดครองเว็บไซต์ดังกล่าวของ สป.ทส. ได้ ทำให้มีโอกาสที่ผู้บุกรุกจะปรับโฉมหน้าของเว็บไซต์ ซึ่งทำให้ผู้ใช้งานไม่สามารถใช้งานเว็บไซต์ดังกล่าวได้

คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- Ability to Guess Administrative Username and Password

ความเสี่ยงทางเทคนิค: สูง

พบว่าระบบล็อกอินมีการใช้ชื่อผู้ใช้และรหัสผ่านที่ง่ายต่อการคาดเดา เนื่องจากทั้งบัญชีผู้ใช้ และรหัสผ่านปรากฏใน Dictionary ทำให้สามารถใช้โปรแกรมสำหรับคาดเดารหัสผ่าน (Brute Force Attack) เพื่อคาดเดารหัสผ่านได้โดยง่าย จึงควรแก้ไขโดยการเปลี่ยนแปลงบัญชีผู้ใช้ และรหัสผ่านให้ยากต่อการคาดเดา เช่นรหัสผ่านต้องประกอบไปด้วยตัวอักษรตัวเล็ก ตัวใหญ่ ตัวเลข ตัวอักขระพิเศษผสมกัน และมีความยาวไม่ต่ำกว่า 8 ตัวอักษร

- Ability to Gain Access to Administrative Control Management (**สอดคล้องกับมาตรฐาน** OWASP **ปี ค.ศ.** 2007 **ข้อ** 10)

  ความเสี่ยงทางเทคนิค: สูง

  พบว่ามีการใช้บัญชีผู้ใช้ และรหัสผ่าน ที่ง่ายต่อการคาดเดา รวมถึงมีลิงค์ที่เข้าสู่ระบบล็อกอินการจัดการข้อมูลบนเว็บไซต์ จึงควรแก้ไขโดยการซ่อนลิงค์ (Link) สำหรับเข้าสู่ระบบล็อกอินของเว็บไซต์

- Directory Listing Vulnerabilities (**สอดคล้องกับมาตรฐาน** OWASP **ปี ค.ศ.** 2007 **ข้อ** 4)

  ความเสี่ยงทางเทคนิค: กลาง

  ทำการป้องกัน Directory Listing โดยการตั้งค่าสิทธิ์การเข้าถึงพาทต่าง ๆ อย่างเหมาะสม

- Information Leakage and Improper Handling (**สอดคล้องกับมาตรฐาน** OWASP **ปี ค.ศ.** 2007 **ข้อ** 6)

  ความเสี่ยงทางเทคนิค: กลาง

  เนื่องจากระบบลืมรหัสผ่านมีการแจ้งเตือนข้อความไม่เหมาะสม ทำให้สามารถคาดเดาบัญชีผู้ใช้ที่มีอยู่จริงในระบบได้ จึงควรแก้ไขโดยแสดงข้อความแจ้งเตือนให้เหมือนกัน ทั้งกรณียูเซอร์ดังกล่าวมีอยู่จริง หรือไม่มีในระบบ

- Server info in HTTP Headers

  ความเสี่ยงทางเทคนิค: ต่ำ

  ควรทำการปิด หรือสร้างข้อมูล Header หลอก เพื่อป้องกันการรวบรวมข้อมูลผ่านทาง Header ของเว็บไซต์

2. ผลการวิเคราะห์ช่องโหว่

2.1 ผลการวิเคราะห์ช่องโหว่ที่พบในเว็บไซต์

จากการทดสอบเจาะระบบ ที่ปรึกษาได้นำช่องโหว่ที่พบมาวิเคราะห์ เพื่อหาสาเหตุของการเกิดช่องโหว่ในเว็บไซต์ โดยสามารถสรุปประเด็น ดังนี้

2.1.1 การตั้งค่าบัญชีผู้ใช้ และรหัสผ่านของผู้ดูแลระบบที่ง่ายต่อการคาดเดา

การตั้งค่าบัญชีผู้ใช้ และรหัสผ่านของผู้ดูแลระบบที่ง่ายต่อการคาดเดาส่งผลทำให้สามารถล็อกอินเข้าสู่ระบบด้วยสิทธิ์ของผู้ดูแลระบบ ซึ่งนำไปสู่การเข้าถึงระบบบริหารจัดการเว็บไซต์ ซึ่งหากผู้บุกรุกพบช่องโหว่ดังกล่าว ก็อาจจะสร้างความเสียหายให้กับเว็บไซต์ได้

(1) **ผลกระทบ** (Impact)

- หากผู้บุกรุกสามารถคาดเดารหัสผ่านได้ถูกต้อง ก็จะสามารถใช้ช่องทางดังกล่าวในการยึดครองเว็บไซต์ของ สป.ทส.

(2) **คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง**

- ควรแก้ไขโดยการเปลี่ยนแปลงบัญชีผู้ใช้ และรหัสผ่านให้ยากต่อการคาดเดา เช่นรหัสผ่านต้องประกอบไปด้วยตัวอักษรตัวเล็ก ตัวใหญ่ ตัวเลข ตัวอักขระพิเศษผสมกัน และมีความยาวไม่ต่ำกว่า 8 ตัวอักษร

2.1.2 การแสดงข้อความแจ้งเตือนข้อผิดพลาดที่ไม่เหมาะสม

ระบบลืมรหัสผ่านของทั้ง 2 เว็บไซต์ มีการแสดงข้อความแจ้งเตือนข้อผิดพลาดที่ไม่เหมาะสม ซึ่งหากมีบัญชีผู้ใช้อยู่ในระบบ จะมีการแสดงข้อความแจ้งเตือนในลักษณะหนึ่ง และหากไม่มีบัญชีผู้ใช้อยู่ในระบบ ก็จะมีการแสดงข้อความแจ้งเตือนในลักษณะที่แตกต่างกัน ซึ่งทำให้สามารถใช้ช่องโหว่ดังกล่าวในการคาดเดาบัญชีผู้ใช้ที่มีอยู่ในระบบ

(1) **ผลกระทบ** (Impact)

- ผู้บุกรุกสามารถใช้ช่องทางดังกล่าวในการคาดเดาบัญชี (Account) ที่มีอยู่ในระบบได้

(2) **คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง**

- ควรแก้ไขให้มีการแสดงข้อความแจ้งเตือนข้อผิดพลาดในลักษณะเดียวกัน

2.1.3 การตั้งค่า Configuration ที่ไม่เหมาะสม

ที่ปรึกษาพบว่าเว็บไซต์ยังมีการตั้งค่า Configuration ที่ไม่เหมาะสมในบางส่วน โดยสามารถทำ Directory Listing ได้ในบางพาท ซึ่งทำให้สามารถเห็นไฟล์ทั้งหมดภายในพาทดังกล่าว จึงควรแก้ไขสิทธิ์การเข้าถึงพาทดังกล่าว นอกจากนั้นยังสามารถดูข้อมูลของเว็บเซิร์ฟเวอร์ (Web Serer) ซึ่งอยู่ภายใน HTTP Header ได้อีกด้วย จึงควรแก้ไขด้วยการซ่อนการแสดงข้อความดังกล่าว

ในการสำรวจซอร์สโค๊ด (Source code) ของเว็บแอพพลิเคชั่นพบข้อความซึ่งแสดงให้เห็นว่าว่าระบบใช้งาน Web Content Management System (WCMS) ของ DotNetNuke ซึ่งแม้จะไม่พบว่า WCMS ดังกล่าวมีช่องโหว่ใด ๆ แต่ควรดำเนินการแก้ไขข้อความดังกล่าว เนื่องจากหากเวอร์ชั่นที่ใช้งานมีช่องโหว่ เว็บไซต์อาจถูกโจมตีจากผู้ไม่หวังดีได้โดยง่าย

(1) **ผลกระทบ** (Impact)

- ผู้บุกรุกสามารถใช้ช่องทางดังกล่าวในการรวบรวมข้อมูลสำหรับใช้เจาะระบบเว็บไซต์ของ สป.ทส.

(2) **คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง**

- ควรแก้ไขสิทธิ์การเข้าถึงพาทต่าง ๆ ภายในเว็บไซต์
- ซ่อนการแสดงข้อมูลของเว็บเซิร์ฟเวอร์ซึ่งอยู่ภายใน HTTP Header
- ลบข้อความภายในซอร์สโค๊ดซึ่งแสดงให้เห็นว่า ระบบใช้งาน Web Content Management System (WCMS) ของ DotNetNuke

2.2 ผลการทดสอบเจาะระบบจากภายนอกผ่านทางอุปกรณ์เครือข่ายไร้สาย

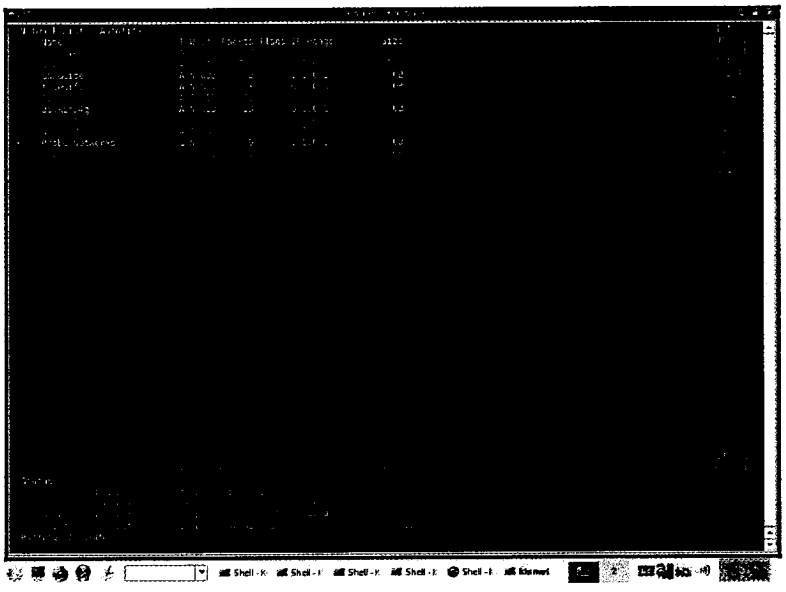
การทดสอบเจาะระบบเครือข่ายไร้สายของ สป.ทส. นั้นผู้ทดสอบทำเสมือนว่าผู้ทดสอบเป็นผู้ไม่หวังดี ต้องการเข้าถึงข้อมูลบางอย่างผ่านทางเครือข่ายไร้สายของ สป.ทส. โดยนำผลจากการสำรวจเพื่อค้นหาสัญญาณ Access Point (War Driving) มาเป็นข้อมูลเบื้องต้นในการดำเนินการทดสอบเจาะระบบเครือข่ายไร้สาย โดยแสดงรายละเอียดแต่ละ SSID ดังนี้

2.2.1 การสำรวจเพื่อค้นหาสัญญาณของ Access Point ที่เปิดใช้งานอยู่ (War Driving)

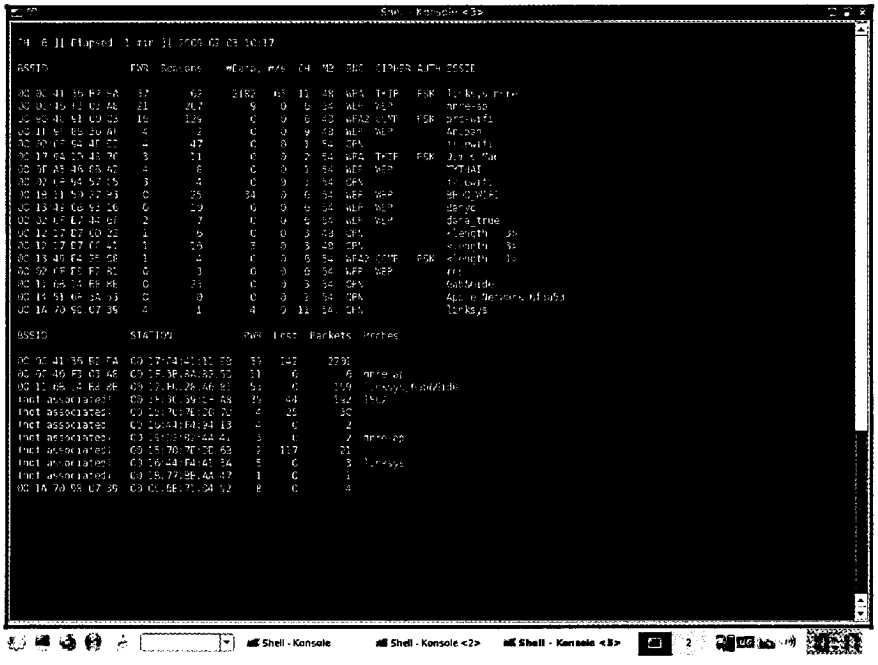
การทำ War Driving คือการค้นหาตำแหน่งของ Access Point ที่มีการเปิดใช้งานอย่างไม่ระมัดระวังเรื่องความปลอดภัย เช่นมีการใช้ค่า Default SSID ไม่มีการระบุค่า MAC Address ที่สามารถใช้งาน Access Point ดังกล่าว และไม่มีการเข้ารหัสด้วย WEP Key เป็นต้น ทำให้ผู้บุกรุกสามารถเข้ามาใช้งานระบบเครือข่ายไร้สายได้อย่างง่ายดาย โดยการทดสอบทำ War Driving ให้แก่ สป.ทส. นั้น ทางบริษัทฯได้ทำการสำรวจค้นหาสัญญาณของ Access Point ที่กระจายอยู่บริเวณภายในพื้นที่ทำงานของ สป.ทส. เพื่อตรวจสอบว่า Access Point เหล่านั้นมีการเปิดใช้งานโดยได้คำนึงถึงในเรื่องความปลอดภัยหรือไม่

เครื่องมือในการสำรวจเพื่อค้นหาสัญญาณของ Access Point ที่เปิดใช้งานอยู่ (War Driving) ในครั้งนี้คือ

- Kismet
- Airodump-ng



รูปที่ 24 ตัวอย่างโปรแกรม Kismet



รูปที่ 25 ตัวอย่างโปรแกรม Airodump-ng

ซึ่งจากการสำรวจสามารถสรุป Access Point ที่พบในพื้นที่ทำงานของ สป.ทส. ได้ดังนี้

- **กรมส่งเสริมคุณภาพสิ่งแวดล้อม (ชั้น 10)**

ตารางที่ 8 Access Point **ที่พบในบริเวณ กรมส่งเสริมคุณภาพสิ่งแวดล้อม (ชั้น 10)**

ลำดับที่	SSID	ความปลอดภัย
1	linksys-mnre	WPA-PSK
2	mnre-ap	WEP
3	prd-wifi	WPA2-PSK
4	Anupan	WEP
5	Truewifi	OPN
6	Jin's Mac	WPA-PSK
7	TYTHAI	WEP
8	BEDO_WIFI	WEP
9	Banyo	WEP
10	dana_true	WEP
11	Rcs	WEP
12	Gab&Gide	OPN

ลำดับที่	SSID	ความปลอดภัย
13	Apple Network 6f3a53	OPN
14	Linksys	OPN

- **ศูนย์บริการร่วมกรมส่งเสริมคุณภาพสิ่งแวดล้อม (กรมควบคุมมลพิษ ชั้น 1)**

ตารางที่ 9 Access Point ที่พบในบริเวณศูนย์บริการร่วมกรมส่งเสริมคุณภาพสิ่งแวดล้อม (กรมควบคุมมลพิษ ชั้น 1)

ลำดับที่	SSID	ความปลอดภัย
1	AvationF3	OPN
2	tsunami307_3	OPN
3	DMCR	WEP
4	mnre-ap	WEP

จากผลการสำรวจเพื่อค้นหาสัญญาณ Access Point ของ สป.ทส. พบว่า SSID ที่ทางที่ปรึกษาพบและเป็นของ สป.ทส.คือ mnre-ap และ linksys-mnre ส่วน SSID อื่นที่พบนั้นไม่ใช่ Access Point ที่สป.ทส. นำมาติดตั้งไว้ ซึ่งจะเห็นได้ว่า Access Point ที่ติดตั้งใช้งานของสป.ทส.จะใช้ WPA-PSK และ WEP ในการเข้ารหัสข้อมูลซึ่งถือว่ามีความปลอดภัยในระดับหนึ่ง แต่อย่างไรก็ตามเทคโนโลยีดังกล่าวยังมีความเสี่ยงที่ผู้บุกรุกจะเจาะผ่านเข้าไปยังระบบเครือข่ายภายในได้

2.2.2 ผลการทดสอบเจาะระบบจากภายนอกผ่านทางอุปกรณ์เครือข่ายไร้สาย mnre-ap (กรมส่งเสริมคุณภาพสิ่งแวดล้อม ชั้น 10)

ตารางที่ 10 ผลกระทบทางเทคนิค โอกาสที่จะเกิด และความเสี่ยงทางเทคนิคของอุปกรณ์เครือข่ายไร้สาย mnre-ap (กรมส่งเสริมคุณภาพสิ่งแวดล้อม ชั้น 10)

ผลกระทบทางเทคนิค: ระดับสูง
สิ่งที่พบ อุปกรณ์เครือข่ายไร้สาย mnre-ap (กรมส่งเสริมคุณภาพสิ่งแวดล้อม ชั้น 10) มีผลกระทบทางเทคนิคอยู่ในระดับสูงเนื่องจาก ผู้ทดสอบสามารถเชื่อมต่อเข้าอุปกรณ์เครือข่ายไร้สายดังกล่าวได้ และสามารถสแกนเครื่องคอมพิวเตอร์ที่เปิดใช้งานอยู่ในเครือข่ายภายใน ซึ่งรวมถึงเครื่องคอมพิวเตอร์แม่ข่ายของ สป.ทส. ซึ่งจะนำไปสู่การยึดครองเครื่องคอมพิวเตอร์แม่ข่ายของ สป.ทส. ต่อไป ซึ่งมีผลกระทบอยู่ในระดับสูง
โอกาสที่จะเกิด: ระดับปานกลาง
สิ่งที่พบ อุปกรณ์เครือข่ายไร้สาย mnre-ap (กรมส่งเสริมคุณภาพสิ่งแวดล้อม ชั้น 10) มีโอกาสที่จะถูกเจาะระบบจากผู้บุกรุกในระดับปานกลาง เนื่องจากมีการใช้ WEP ในการเข้ารหัสข้อมูล ซึ่งเป็นการเข้ารหัสที่สามารถถอดรหัสได้ จึงมีโอกาสที่จะถูกเจาะระบบจากผู้บุกรุกอยู่ในระดับสูง แต่ทั้งนี้อุปกรณ์เครือข่ายไร้สายดังกล่าวตั้งอยู่ในบริเวณชั้น 10 ซึ่งทำให้การเข้าถึงจากบุคคลภายนอกอาคารทำได้ยากขึ้น โอกาสที่จะเกิดจึงอยู่ในระดับปานกลาง
ความเสี่ยงทางเทคนิค: ระดับสูง
สิ่งที่พบ อุปกรณ์เครือข่ายไร้สาย mnre-ap (กรมส่งเสริมคุณภาพสิ่งแวดล้อม ชั้น 10) มีความเสี่ยงทางเทคนิคอยู่ในระดับสูง ซึ่งได้จากการคำนวณผลกระทบทางเทคนิค (ระดับสูง) และโอกาสที่จะเกิด(ระดับปานกลาง) นำมาเปรียบเทียบกับตารางที่ 2.2 ทำให้พบว่าความเสี่ยทางเทคนิคอยู่ในระดับสูง

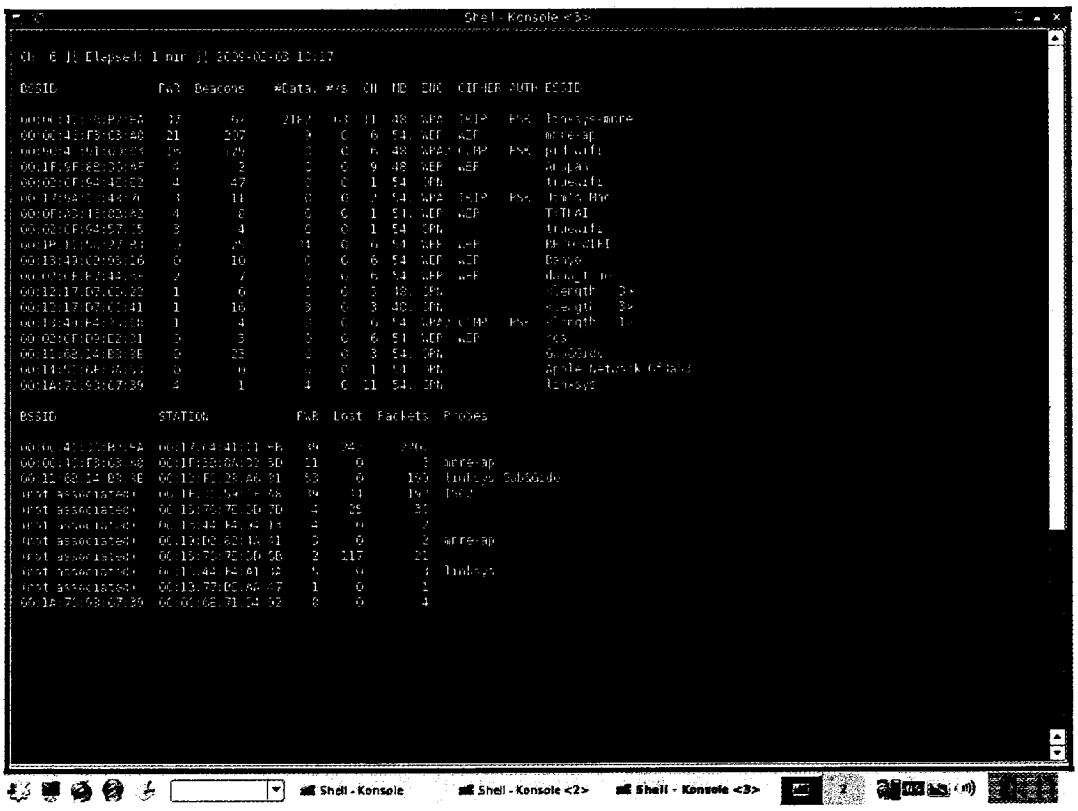
ตารางที่ 11 ความสูญเสียด้าน Confidentiality Integrity และ Availability ของอุปกรณ์เครือข่ายไร้สาย mnre-ap (กรมส่งเสริมคุณภาพสิ่งแวดล้อม ชั้น 10)

ความสูญเสียด้าน Confidentiality: มีผลกระทบ
สิ่งที่พบ ความสูญเสียด้าน Confidentiality คือผลกระทบที่ก่อให้เกิดการสูญเสียข้อมูลที่เป็นความลับ ซึ่งจากการทดสอบสามารถเข้าถึงอุปกรณ์เครือข่ายไร้สายดังกล่าวได้ และสามารถเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายภายใน สป.ทส. ทำให้มีโอกาสที่ผู้บุกรุกจะสามารถเข้าถึงข้อมูลที่เป็นความลับภายในเครื่องคอมพิวเตอร์แม่ข่ายเหล่านั้น
ความสูญเสียด้าน Integrity: ไม่มีผลกระทบ
สิ่งที่พบ ไม่พบปัจจัยที่ส่งผลต่อความสูญเสียด้าน Integrity
ความสูญเสียด้าน Availability: ไม่มีผลกระทบ
สิ่งที่พบ ไม่พบปัจจัยที่ส่งผลต่อความสูญเสียด้าน Availability

ขั้นตอนในการทดสอบ

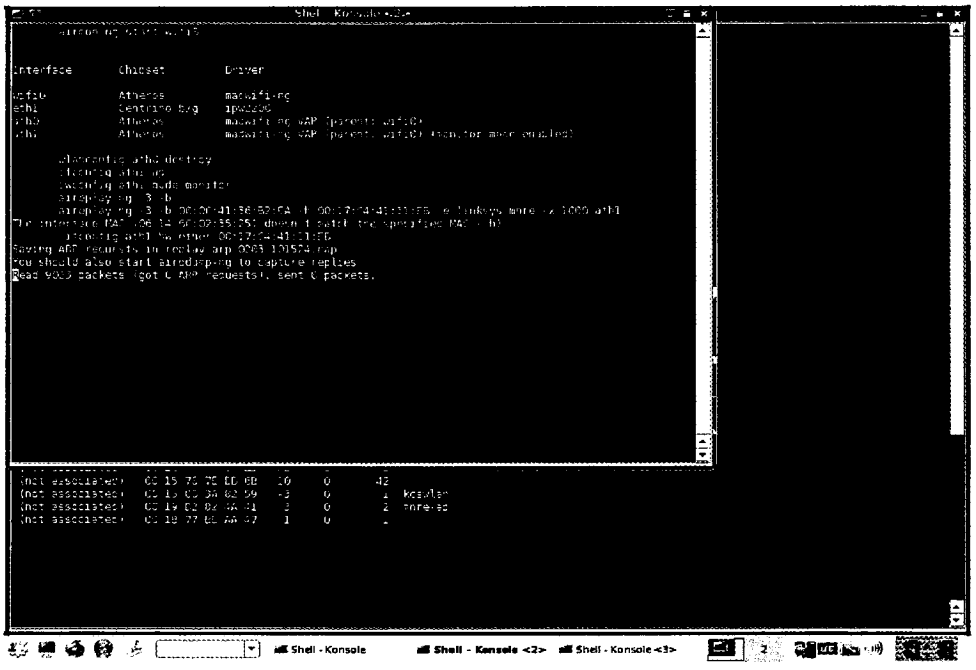
ขั้นตอนในการทดสอบสามารถสรุปออกมาดังนี้

1. ผู้ทดสอบใช้โปรแกรม airodump-ng เพื่อดักจับข้อมูลที่รับส่งระหว่าง Access Point mnre-ap และเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับ Access Point ดังกล่าว โดยที่ผู้ทดสอบจะต้องดักจับข้อมูลที่เรียกว่า Initial Vectors ให้ได้จำนวนที่เพียงพอจึงสามารถที่จะถอดรหัส WEP Key ได้ ดังแสดงในรูปที่ 26



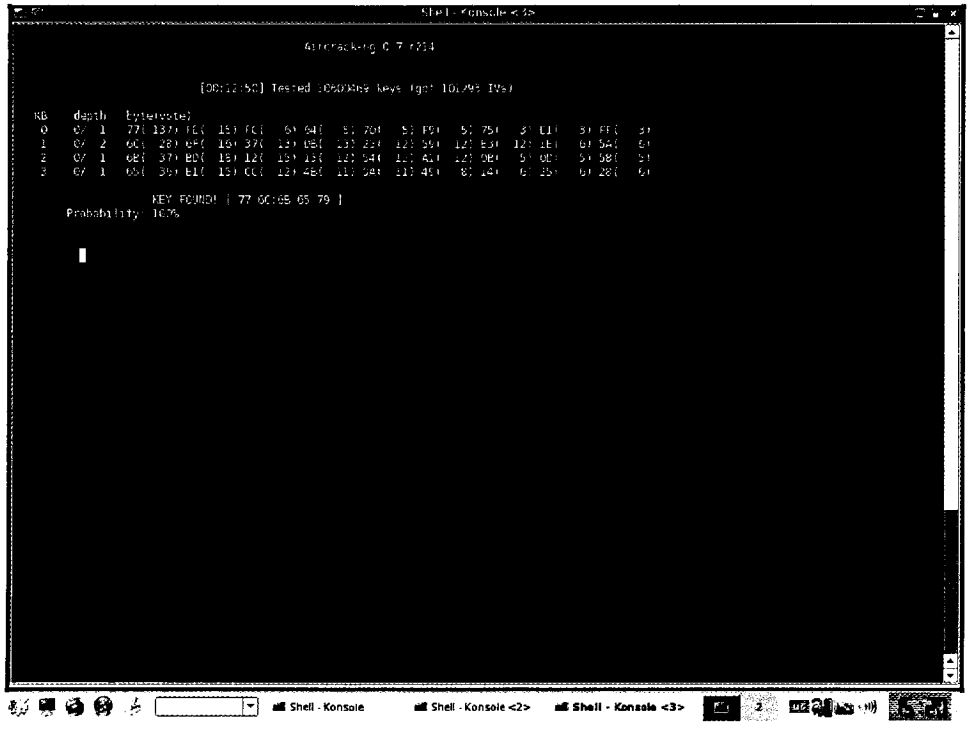
รูปที่ 26 การทดสอบโดยใช้โปรแกรม Airodump-ng เพื่อดักจับข้อมูล

2. ผู้ทดสอบได้ใช้โปรแกรม aireplay-ng เพื่อสร้าง (Generate) ข้อมูลให้มากขึ้น เพื่อทำให้สามารถดักเก็บค่า Initial Vectors (IVs) ได้รวดเร็วยิ่งขึ้น ดังแสดงในรูปที่ 27



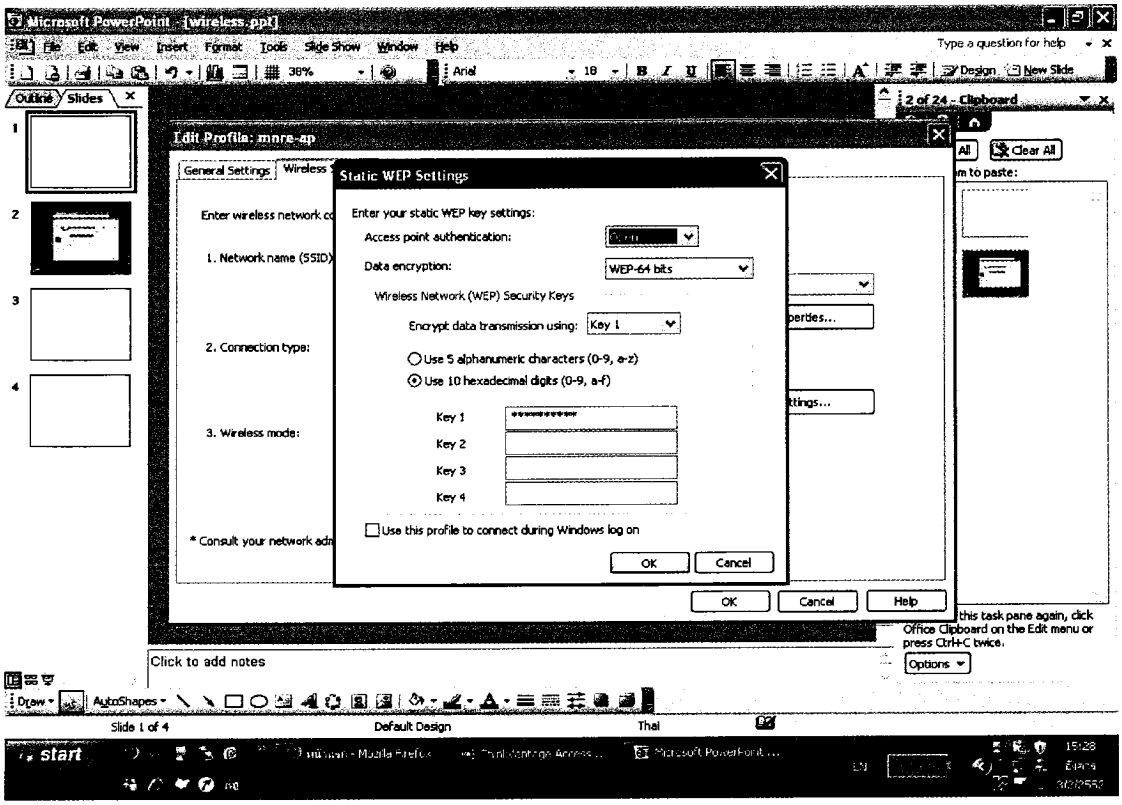
รูปที่ 27 การทดสอบโดยใช้โปรแกรม Aireplay-ng เพื่อสร้างข้อมูลให้มากขึ้นทำให้สามารถดักเก็บค่า IVs

3. ในการทดสอบนั้น ผู้ทดสอบจะปล่อยให้ airodump-ng เก็บข้อมูลระยะเวลาหนึ่ง และจากนั้นผู้ทดสอบได้ใช้โปรแกรม aircrack-ng เพื่อถอดรหัส WEP Key โดยสามารถทำได้สำเร็จดังแสดงในรูปที่ 28 โดย WEP Key ที่ถอดรหัสได้คือ 776C6579 หรือ wlkey



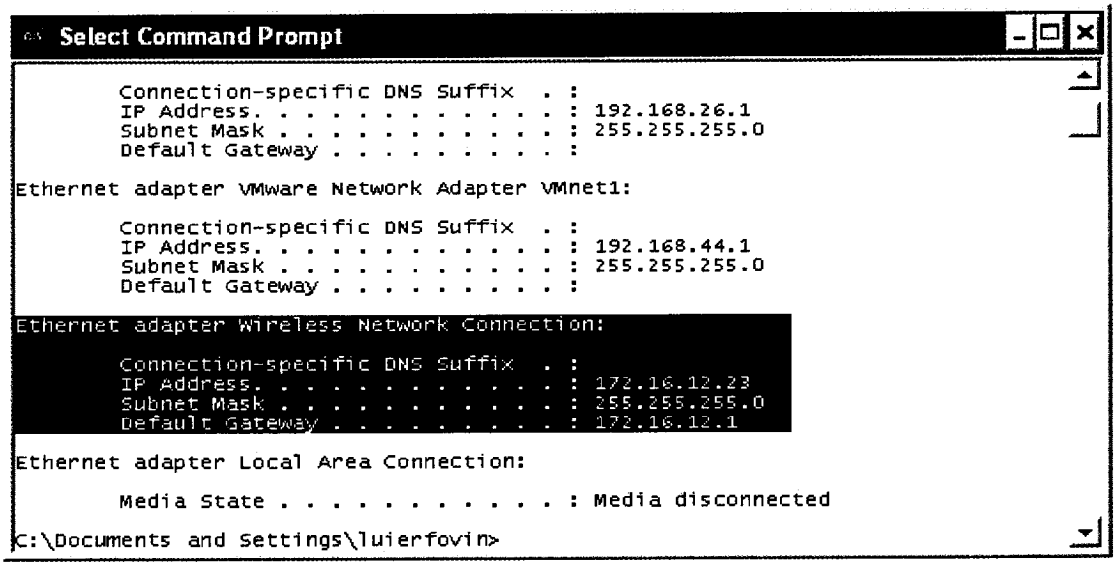
รูปที่ 28 การทดสอบโดยใช้โปรแกรม Aircrack-ng โดยสามารถถอดรหัส WEP Key

4. เมื่อผู้ทดสอบสามารถถอดรหัส WEP Key ได้สำเร็จ ผู้ทดสอบได้ทดลองเชื่อมต่อกับ Access Point mnre-ap ด้วย WEP Key ที่ได้ ดังแสดงในรูปที่ 29 โดยสามารถเชื่อมต่อได้สำเร็จ



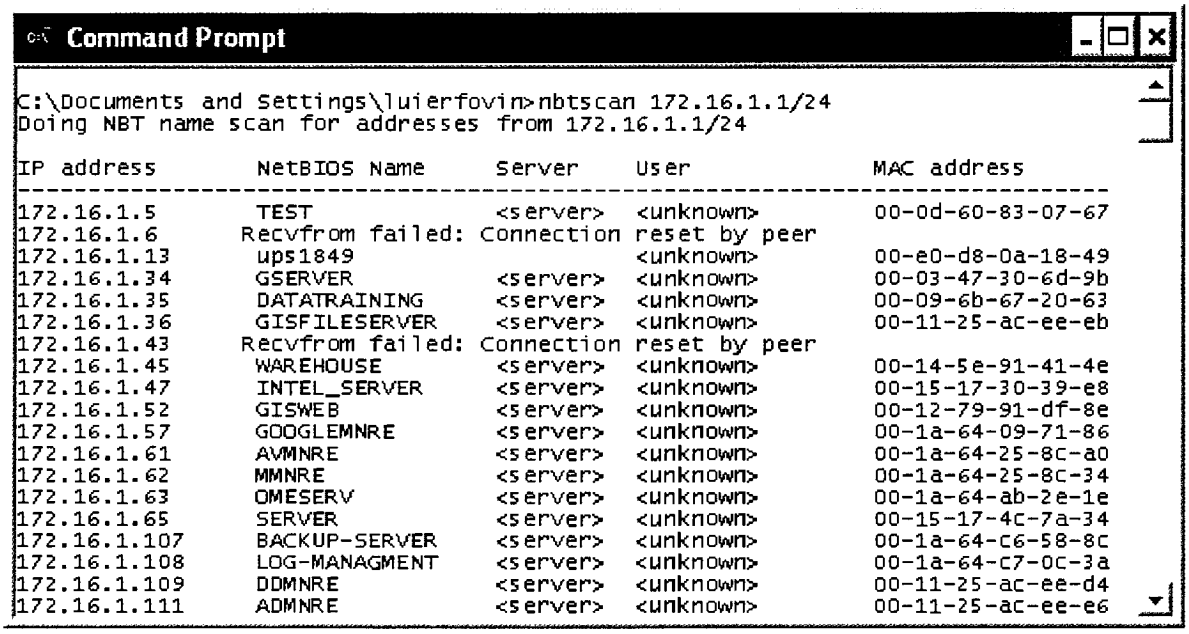
รูปที่ 29 การทดสอบเชื่อมต่อกับ mnrp-ap โดยใช้ WEP Key ที่ได้จากการถอดรหัส

5. ผู้ทดสอบได้รับหมายเลขไอพีหลังจากเชื่อมต่อเป็น 172.16.12.23 ดังแสดงในรูปที่ 30



รูปที่ 30 หมายเลขไอพีที่ได้รับจากการเชื่อมต่อ เครือข่ายไร้สาย mnre-ap (กรมส่งเสริมคุณภาพสิ่งแวดล้อม ชั้น 10)

6. จากหมายเลขไอพีดังกล่าวผู้ทดสอบได้ใช้โปรแกรม nbtscan เพื่อค้นหารายชื่อเครื่องคอมพิวเตอร์ภายในเครือข่าย โดยสามารถเห็นรายชื่อเครื่องคอมพิวเตอร์ที่อยู่ในเครือข่ายเดียวกับผู้ทดสอบ และยังสามารถเห็นเครื่องคอมพิวเตอร์แม่ข่ายของ สป.ทส. ซึ่งหมายความว่าหากผู้บุกรุกสามารถถอดรหัส WEP Key ได้สำเร็จ ก็จะสามารถเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายของ สป.ทส. ดังแสดงในรูปที่ 31



รูปที่ 31 การทดสอบโดยใช้โปรแกรม nbtscan เพื่อค้นหาเครื่องคอมพิวเตอร์แม่ข่าย

สิ่งที่พบจากการทดสอบ

จากการทดสอบเจาะระบบจากภายนอกผ่านทางอุปกรณ์เครือข่ายไร้สาย mnre-ap ซึ่งตั้งอยู่ที่กรมส่งเสริมคุณภาพสิ่งแวดล้อม ชั้น 10 ผู้ทดสอบพบว่าสามารถเจาะอุปกรณ์เครือข่ายไร้สายดังกล่าวได้ง่าย เนื่องจากมีการใช้ WEP ในการเข้ารหัสข้อมูล ซึ่งเป็นการเข้ารหัสที่สามารถถอดรหัสได้

จากการทดสอบสามารถสรุปสิ่งที่พบจากการทดสอบได้ดังนี้

- ผู้ทดสอบสามารถเชื่อมต่อเข้าอุปกรณ์เครือข่ายไร้สายดังกล่าวได้
- ผู้ทดสอบสามารถสแกนเครื่องคอมพิวเตอร์ที่เปิดใช้งานอยู่ในเครือข่ายภายใน ซึ่งรวมถึงเครื่องคอมพิวเตอร์แม่ข่ายของ สป.ทส.

หากผู้บุกรุกพบช่องโหว่ดังกล่าว จะก่อให้เกิดความสูญเสียต่อ สป.ทส. ดังนี้

- **ความสูญเสียด้าน** Confidentiality

ความสูญเสียด้าน Confidentiality คือผลกระทบที่ก่อให้เกิดการสูญเสียข้อมูลที่เป็นความลับ ซึ่งจากการทดสอบสามารถเข้าถึงอุปกรณ์เครือข่ายไร้สายดังกล่าวได้ และสามารถเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายภายใน สป.ทส. ทำให้มีโอกาสที่ผู้บุกรุกจะสามารถเข้าถึงข้อมูลที่เป็นความลับภายในเครื่องคอมพิวเตอร์แม่ข่ายเหล่านั้น

คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

จากสิ่งที่พบ ที่ปรึกษามีคำแนะนำเรื่องความปลอดภัยระบบเครือข่ายไร้สายให้สป.ทส.ดังนี้

สป.ทส. ควรพิจารณาใช้การพิสูจน์ตัวตนกับเครื่องคอมพิวเตอร์แม่ข่ายควบคู่กับ การเข้ารหัสข้อมูลด้วย WPA2 เนื่องจากการเข้ารหัสข้อมูลด้วย WEP ยังไม่มีความปลอดภัยเพียงพอ จึงมีความเสี่ยงที่ผู้บุกรุกสามารถถอดรหัส WEP Key และเชื่อมต่อเข้าสู่ระบบเครือข่ายภายในของสป.ทส.ได้

สป.ทส. ควรพิจารณาให้มีการซ่อน SSID ของเครือข่ายไร้สาย โดยปรับตั้งค่าของอุปกรณ์เครือข่ายให้ระงับใช้งานฟังก์ชั่น "Broadcast SSID" เพื่อป้องกันไม่ให้ผู้บุกรุกสามารถค้นหาเครือข่ายได้ง่าย

2.2.3 การทดสอบเจาะระบบจากภายนอกผ่านทางอุปกรณ์เครือข่ายไร้สาย linksys-mnre (กรมส่งเสริมคุณภาพสิ่งแวดล้อม ชั้น 10

ตารางที่ 12 ผลกระทบทางเทคนิค โอกาสที่จะเกิด และความเสี่ยงทางเทคนิคของอุปกรณ์เครือข่ายไร้สาย linksys-mnre (กรมส่งเสริมคุณภาพสิ่งแวดล้อม ชั้น 10)

ผลกระทบทางเทคนิค: ระดับต่ำ
สิ่งที่พบ อุปกรณ์เครือข่ายไร้สาย linksys-mnre (กรมส่งเสริมคุณภาพสิ่งแวดล้อม ชั้น 10) มีผลกระทบทางเทคนิคอยู่ในระดับต่ำเนื่องจากผู้ทดสอบไม่สามารถเจาะอุปกรณ์เครือข่ายไร้สายดังกล่าวได้ เนื่องจากมีการใช้ WPA-PSK ในการเข้ารหัสข้อมูล และมีการใช้รหัสผ่านที่ไม่ปรากฏอยู่ใน Wordlist
โอกาสที่จะเกิด: ระดับปานกลาง
สิ่งที่พบ อุปกรณ์เครือข่ายไร้สาย linksys-mnre (กรมส่งเสริมคุณภาพสิ่งแวดล้อม ชั้น 10) มีโอกาสที่จะถูกเจาะระบบจากผู้บุกรุกในระดับปานกลาง เนื่องจากอุปกรณ์เครือข่ายไร้สายดังกล่าวตั้งอยู่ในบริเวณชั้น 10 ซึ่งทำให้การเข้าถึงจากบุคคลภายนอกอาคารทำได้ยาก โอกาสที่จะเกิดจึงอยู่ในระดับปานกลาง
ความเสี่ยงทางเทคนิค: ระดับต่ำ
สิ่งที่พบ อุปกรณ์เครือข่ายไร้สาย linksys-mnre (กรมส่งเสริมคุณภาพสิ่งแวดล้อม ชั้น 10) มีความเสี่ยงทางเทคนิคอยู่ในระดับต่ำ ซึ่งได้จากการคำนวณผลกระทบทางเทคนิค (ระดับต่ำ) และโอกาสที่จะเกิด(ระดับปานกลาง) นำมาเปรียบเทียบกับตารางที่ 2.2 ทำให้พบว่าความเสี่ยทางเทคนิคอยู่ในระดับต่ำ

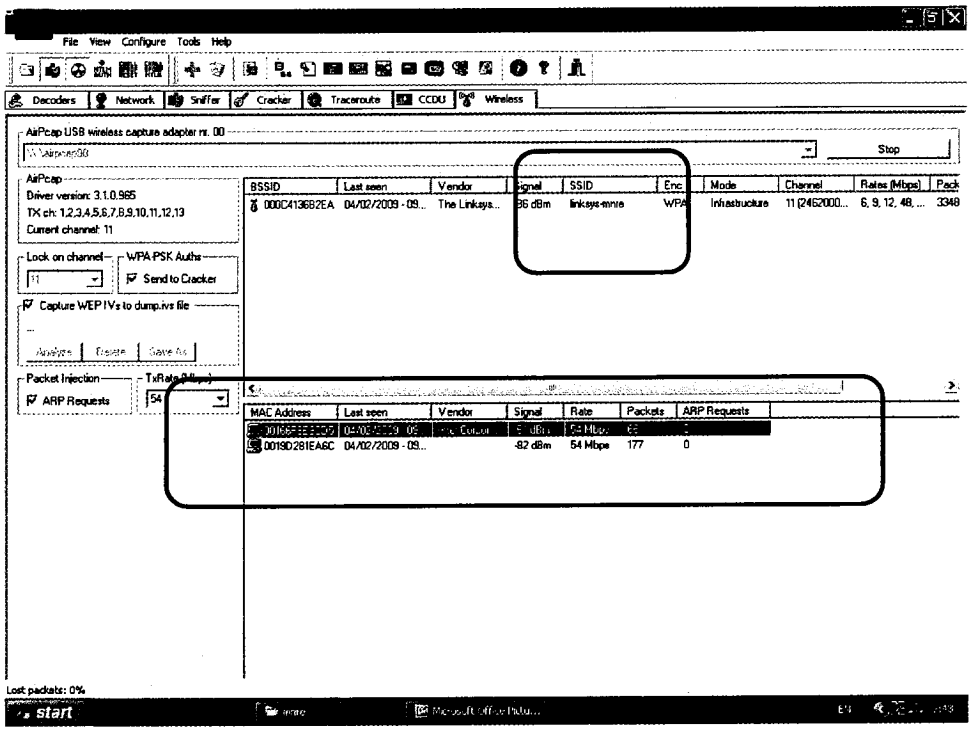
ตารางที่ 13 ความสูญเสียด้าน Confidentiality Integrity และ Availability ของอุปกรณ์เครือข่ายไร้สาย linksys-mnre (กรมส่งเสริมคุณภาพสิ่งแวดล้อม ชั้น 10)

ความสูญเสียด้าน Confidentiality: ไม่มีผลกระทบ
สิ่งที่พบ ไม่พบปัจจัยที่ส่งผลต่อความสูญเสียด้าน Confidentiality
ความสูญเสียด้าน Integrity: ไม่มีผลกระทบ
สิ่งที่พบ ไม่พบปัจจัยที่ส่งผลต่อความสูญเสียด้าน Integrity
ความสูญเสียด้าน Availability: ไม่มีผลกระทบ
สิ่งที่พบ ไม่พบปัจจัยที่ส่งผลต่อความสูญเสียด้าน Availability

ขั้นตอนในการทดสอบ

ขั้นตอนในการทดสอบสามารถสรุปออกมาดังนี้

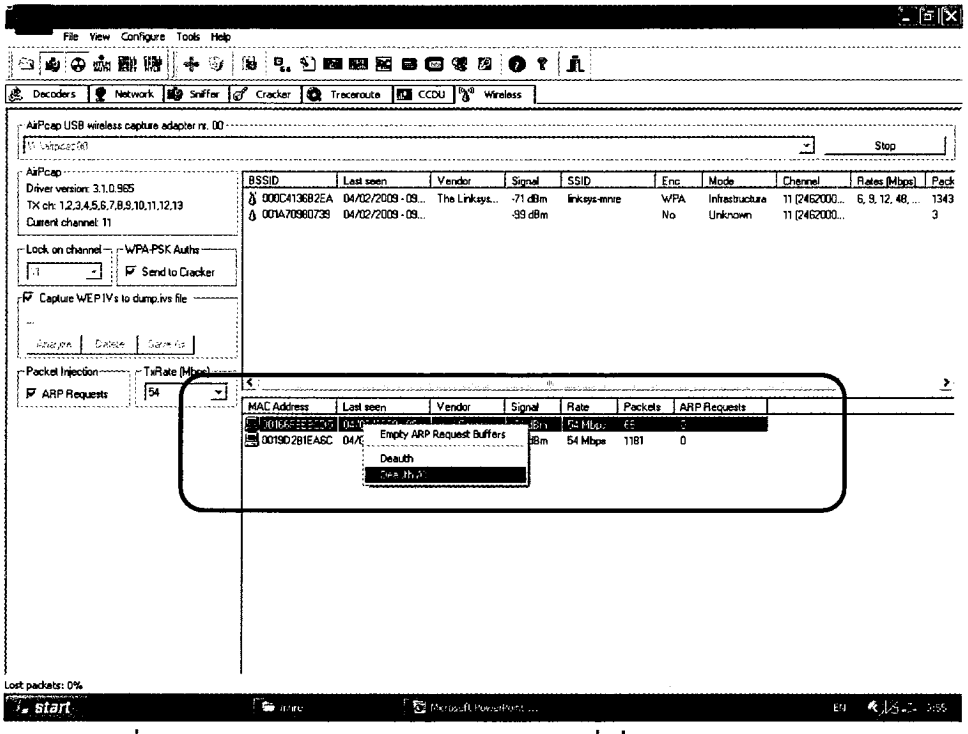
1. ผู้ทดสอบใช้โปรแกรม Cain ร่วมกับอุปกรณ์ AirPcap เพื่อดักจับข้อมูลการพิสูจน์ตัวตนของผู้ใช้งานเครือข่ายไร้สาย โดยเริ่มต้นผู้ทดสอบได้เปิดโปรแกรม Cain เลือกแถบ wireless เลือกอุปกรณ์เป็น AirPcap และเปิดการดักจับข้อมูลที่รับส่งกันระหว่าง Access Point และ เครื่องคอมพิวเตอร์ลูกข่าย ดังแสดงในรูปที่ 32



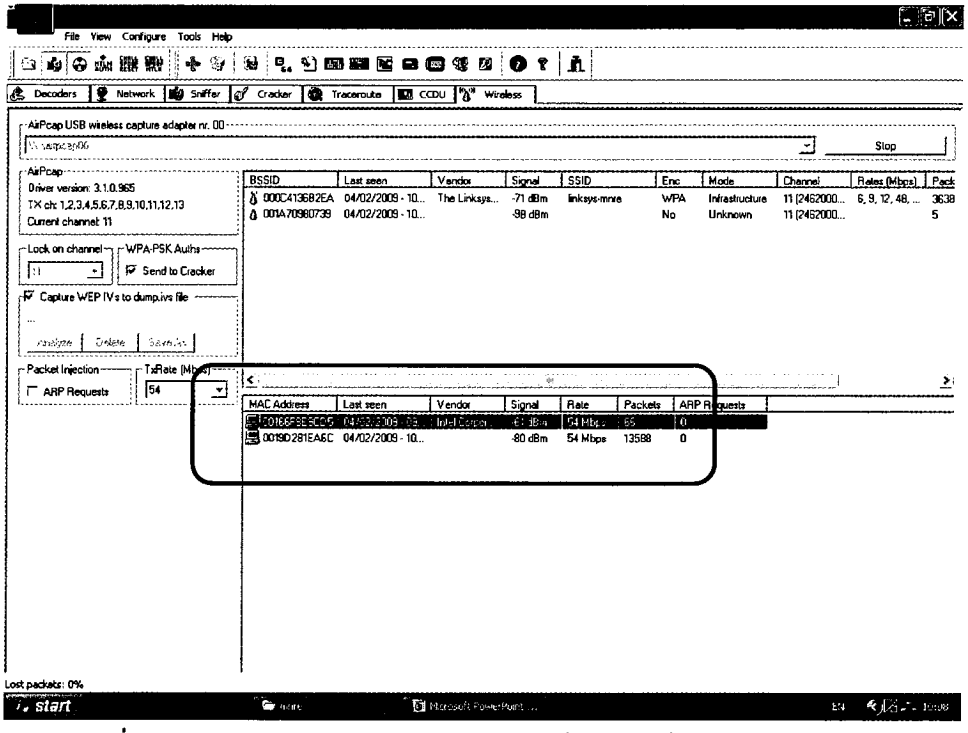
รูปที่ 32 การทดสอบโดยใช้โปรแกรม Cain เพื่อดักจับข้อมูลเครือข่ายไร้สาย

2. จากการใช้โปรแกรม Cain ดังภาพที่ 2.32 ผู้ทดสอบจะเห็นผู้ใช้งานที่เชื่อมต่อกับ linksys-mnre โดยขณะทดสอบพบว่ามีคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับ linksys-mnre จำนวน 2 เครื่อง

3. ผู้ทดสอบใช้การทำ Deauthtication จากโปรแกรม Cain เพื่อให้ผู้ใช้งานสูญเสียการเชื่อมต่อกับ Access Point linksys-mnre ดังแสดงในภาพที่ 33 และ 34

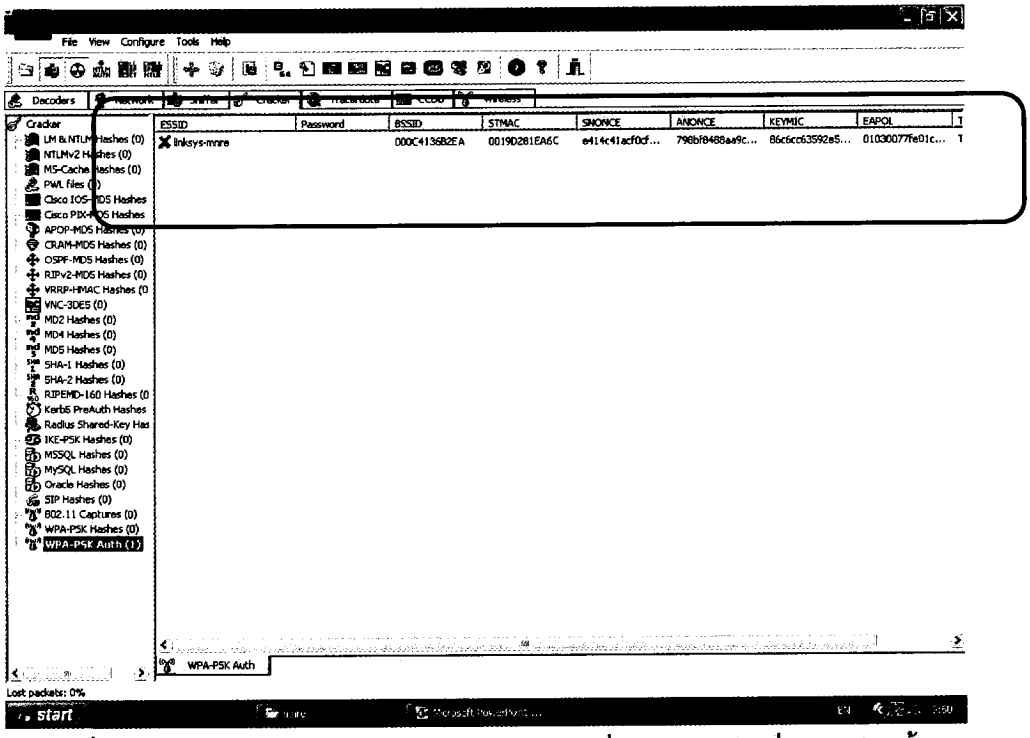


รูปที่ 33 การทำ Deauthentication กับผู้ใช้งานที่เชื่อมต่อกับ linksys-mnre



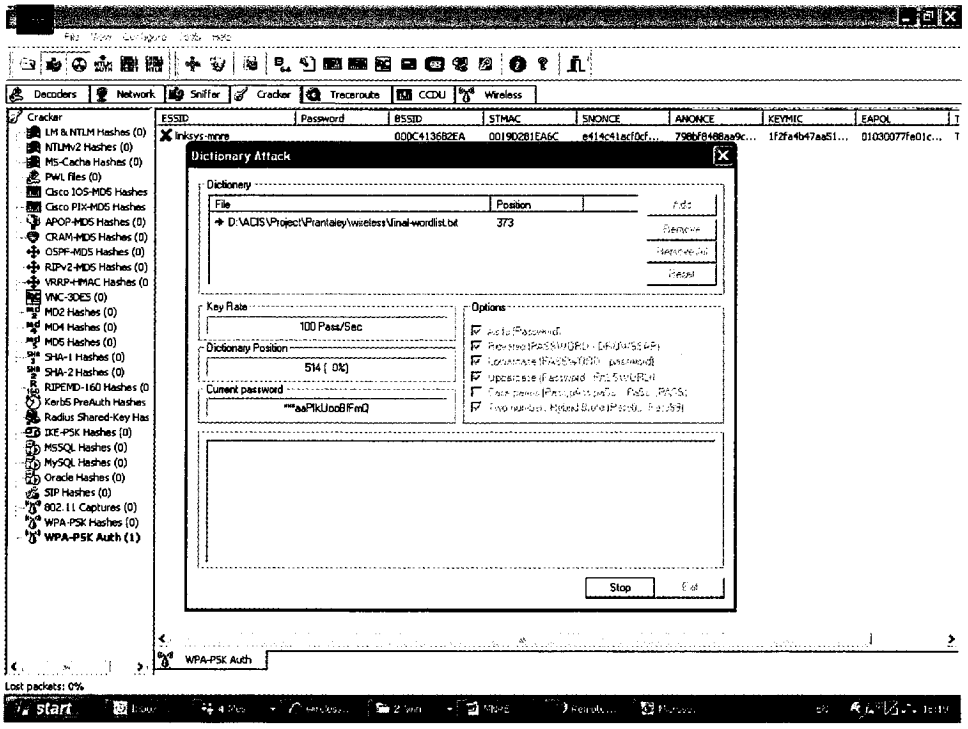
รูปที่ 34 ผลการทำ Deauthentication อุปกรณ์เครือข่ายไร้สาย linksys-mnre

4. จากนั้นเมื่อผู้ใช้งานเริ่มเชื่อมต่อกับ linksys-mnre อีกครั้ง ผู้ทดสอบจะสามารถดักข้อมูลการพิสูจน์ตัวตนได้ ดังแสดงในรูปที่ 35



รูปที่ 35 การทดสอบดักจับข้อมูลการพิสูจน์ตัวตนเมื่อผู้ใช้งานเข้าเชื่อมต่ออีกครั้ง

5. ผู้ทดสอบนำข้อมูลการพิสูจน์ตัวตนที่ได้มาค้นหารหัสผ่าน โดยวิธีการ Dictionary Attack ด้วย Wordlist ที่ผู้ทดสอบได้เตรียมไว้แล้ว ดังแสดงในรูปที่ 2.36 ซึ่งจากการทดสอบผู้ทดสอบไม่พบรหัสผ่านที่ถูกต้องจาก Wordlist ที่เตรียมไว้



รูปที่ 36 การทดสอบโดยใช้โปรแกรม Cain ทำ Dictionary Attack เพื่อค้นหารหัสผ่าน

สิ่งที่พบจากการทดสอบ

จากการทดสอบเจาะระบบจากภายนอกผ่านทางอุปกรณ์เครือข่ายไร้สาย linksys-mnre ซึ่งตั้งอยู่ที่กรมส่งเสริมคุณภาพสิ่งแวดล้อม ชั้น 10 ผู้ทดสอบไม่สามารถเจาะอุปกรณ์เครือข่ายไร้สายดังกล่าวได้ เนื่องจากมีการใช้ WPA-PSK ในการเข้ารหัสข้อมูล และมีการใช้รหัสผ่านที่ไม่ปรากฏอยู่ใน Wordlist

จากการทดสอบสามารถสรุปสิ่งที่พบจากการทดสอบได้ดังนี้

- สามารถดักข้อมูลการพิสูจน์ตัวตนเพื่อทำ Offline Dictionary Attack

คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

จากสิ่งที่พบ ที่ปรึกษามีคำแนะนำเรื่องความปลอดภัยระบบเครือข่ายไร้สายให้ สป.ทส. ดังนี้

- สป.ทส. ควรพิจารณาใช้การพิสูจน์ตัวตนกับเครื่องคอมพิวเตอร์แม่ข่ายควบคู่กับ การเข้ารหัสข้อมูลด้วย WPA2 เนื่องจากการใช้ WPA-PSK ผู้บุกรุกสามารถดักเก็บข้อมูลการพิสูจน์ตัวตนและใช้วิธีการ Offline Dictionary Attack เพื่อค้นหารหัสผ่านได้
- สป.ทส. ควรพิจารณาให้มีการซ่อน SSID ของเครือข่ายไร้สาย โดยปรับตั้งค่าของอุปกรณ์เครือข่ายให้ระงับใช้งานฟังก์ชั่น "Broadcast SSID" เพื่อป้องกันไม่ให้ผู้บุกรุกสามารถค้นหาเครือข่ายได้ง่าย และเปลี่ยนชื่อของ AP ไม่ให้ระบุเป็นชื่อ default ของผลิตภัณฑ์

2.2.4 การทดสอบเจาะระบบจากภายนอกผ่านทางอุปกรณ์เครือข่ายไร้สาย mnre-ap (กรมควบคุมมลพิษ ชั้น 1)

ตารางที่ 14 ผลกระทบทางเทคนิค โอกาสที่จะเกิด และความเสี่ยงทางเทคนิคของอุปกรณ์เครือข่ายไร้สาย mnre-ap (กรมควบคุมมลพิษ ชั้น 1)

ผลกระทบทางเทคนิค: ระดับสูง
สิ่งที่พบ อุปกรณ์เครือข่ายไร้สาย mnre-ap (กรมควบคุมมลพิษ ชั้น 1) มีผลกระทบทางเทคนิคอยู่ในระดับสูงเนื่องจาก ผู้ทดสอบสามารถเจาะอุปกรณ์เครือข่ายไร้สายดังกล่าวได้ เนื่องจากมีการใช้ WEP ในการเข้ารหัสข้อมูล ซึ่งเป็นการเข้ารหัสที่สามารถถอดรหัสได้ ทำให้สามารถเชื่อมต่อเข้าเครือข่ายไร้สายได้
โอกาสที่จะเกิด: ระดับสูง
สิ่งที่พบ อุปกรณ์เครือข่ายไร้สาย mnre-ap (กรมควบคุมมลพิษ ชั้น 1) มีโอกาสที่จะถูกเจาะระบบจากผู้บุกรุกในระดับสูง เนื่องจากมีการใช้ WEP ในการเข้ารหัสข้อมูล ซึ่งเป็นการเข้ารหัสที่สามารถถอดรหัสได้ จึงมีโอกาสที่จะถูกเจาะระบบจากผู้บุกรุกอยู่ในระดับสูง และอุปกรณ์เครือข่ายไร้สายดังกล่าวตั้งอยู่ในบริเวณชั้น 1 ซึ่งทำให้การเข้าถึงจากบุคคลภายนอกอาคารทำได้ง่าย โอกาสที่จะเกิดจึงอยู่ในระดับสูง
ความเสี่ยงทางเทคนิค: ระดับสูง
สิ่งที่พบ อุปกรณ์เครือข่ายไร้สาย mnre-ap (กรมควบคุมมลพิษ ชั้น 1) มีความเสี่ยงทางเทคนิคอยู่ในระดับสูง ซึ่งได้จากการคำนวณผลกระทบทางเทคนิค (ระดับสูง) และโอกาสที่จะเกิด(ระดับสูง) นำมาเปรียบเทียบกับตารางที่ 2.2 ทำให้พบว่าความเสี่ยทางเทคนิคอยู่ในระดับสูง

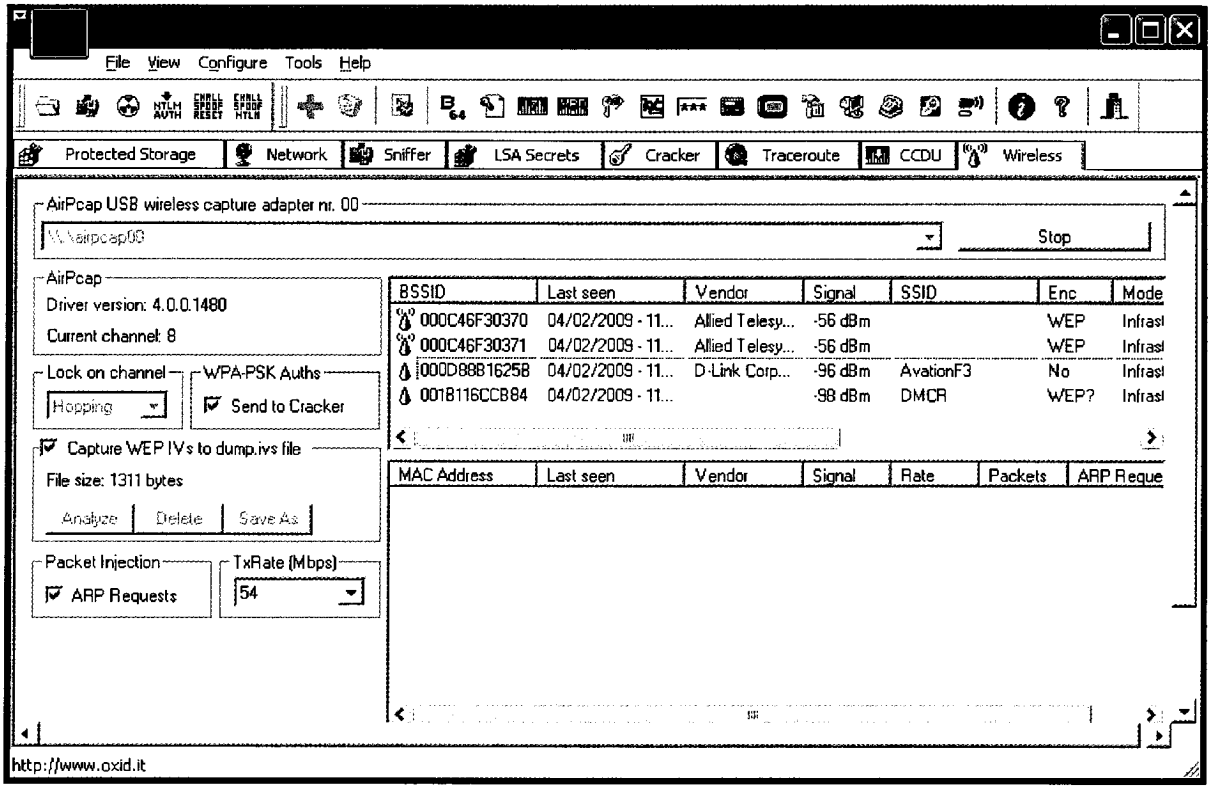
ตารางที่ 15 ความสูญเสียด้าน Confidentiality Integrity และ Availability ของอุปกรณ์เครือข่ายไร้สาย mnre-ap (กรมควบคุมมลพิษ ชั้น 1)

ความสูญเสียด้าน Confidentiality: มีผลกระทบ
สิ่งที่พบ ความสูญเสียด้าน Confidentiality คือผลกระทบที่ก่อให้เกิดการสูญเสียข้อมูลที่เป็นความลับ ซึ่งจากการทดสอบสามารถเข้าถึงอุปกรณ์เครือข่ายไร้สายดังกล่าวได้ ทำให้มีโอกาสที่ผู้บุกรุกจะสามารถเข้าถึงข้อมูลที่เป็นความลับภายในเครื่องคอมพิวเตอร์ที่กำลังใช้งานเครือข่ายไร้สาย
ความสูญเสียด้าน Integrity: ไม่มีผลกระทบ
สิ่งที่พบ ไม่พบปัจจัยที่ส่งผลต่อความสูญเสียด้าน Integrity
ความสูญเสียด้าน Availability: ไม่มีผลกระทบ
สิ่งที่พบ ไม่พบปัจจัยที่ส่งผลต่อความสูญเสียด้าน Availability

ขั้นตอนในการทดสอบ

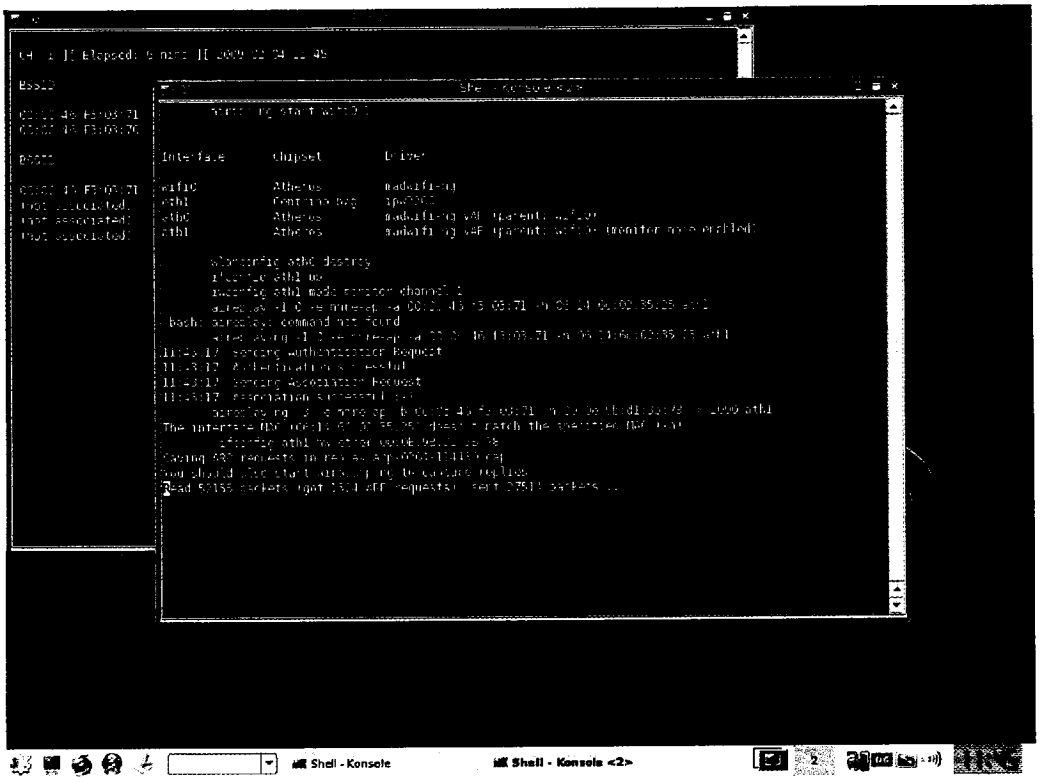
ขั้นตอนในการทดสอบสามารถสรุปออกมาดังนี้

1. ผู้ทดสอบใช้โปรแกรม Cain ควบคู่กับอุปกรณ์ AirPcap เพื่อดักเก็บข้อมูลที่รับส่งระหว่าง Access Point mnre-ap และเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับ Access Point ดังกล่าว ดังแสดงในรูปที่ 37 โดยที่ผู้ทดสอบจะต้องดักจับข้อมูลที่เรียกว่า Initial Vectors ให้ได้จำนวนที่เพียงพอจึงสามารถที่จะถอดรหัส WEP Key ได้



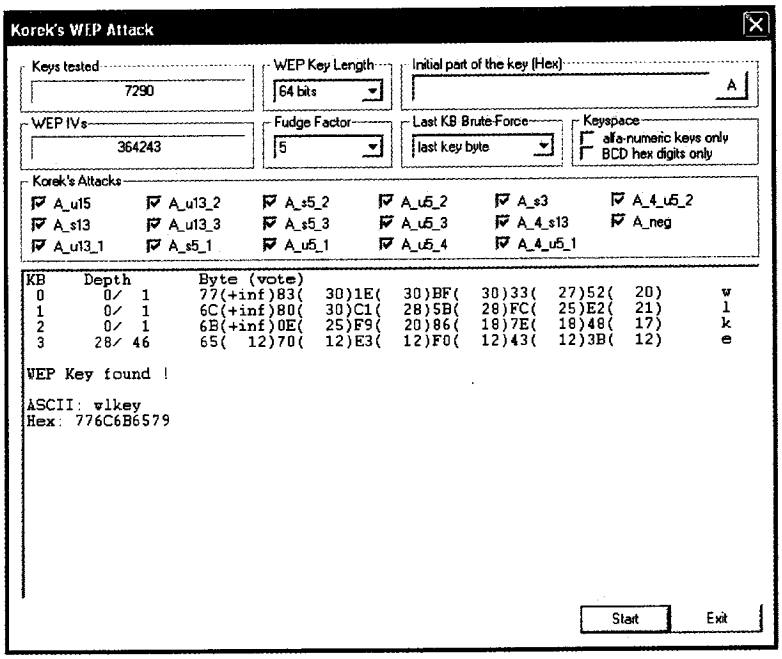
รูปที่ 37 การทดสอบโดยใช้โปรแกรม Cain เพื่อดักจับข้อมูล

2. ผู้ทดสอบใช้โปรแกรม aireplay-ng เพื่อสร้าง (Generate) ข้อมูลให้มากขึ้น ทำให้สามารถดักเก็บค่า Initial Vectors (IVs) ได้รวดเร็วยิ่งขึ้น ดังแสดงในรูปที่ 38



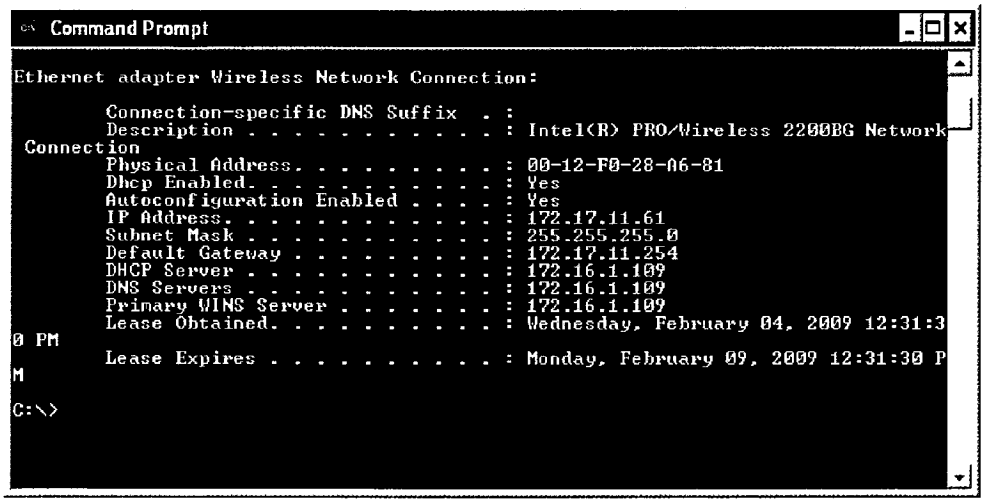
รูปที่ 38 การทดสอบโดยใช้โปรแกรม Aireplay-ng เพื่อสร้างข้อมูลให้มากขึ้นทำให้สามารถดักเก็บค่า IVs

3. ในการทดสอบนั้น ผู้ทดสอบจะปล่อยให้ Cain เก็บข้อมูลระยะเวลาหนึ่ง และจากนั้นผู้ทดสอบได้ใช้โปรแกรม Cain เพื่อถอดรหัส WEP Key ดังแสดงในรูปที่ 39 โดยสามารถทำได้สำเร็จโดย WEP Key ที่ถอดรหัสได้คือ 776C6579 หรือ wlkey



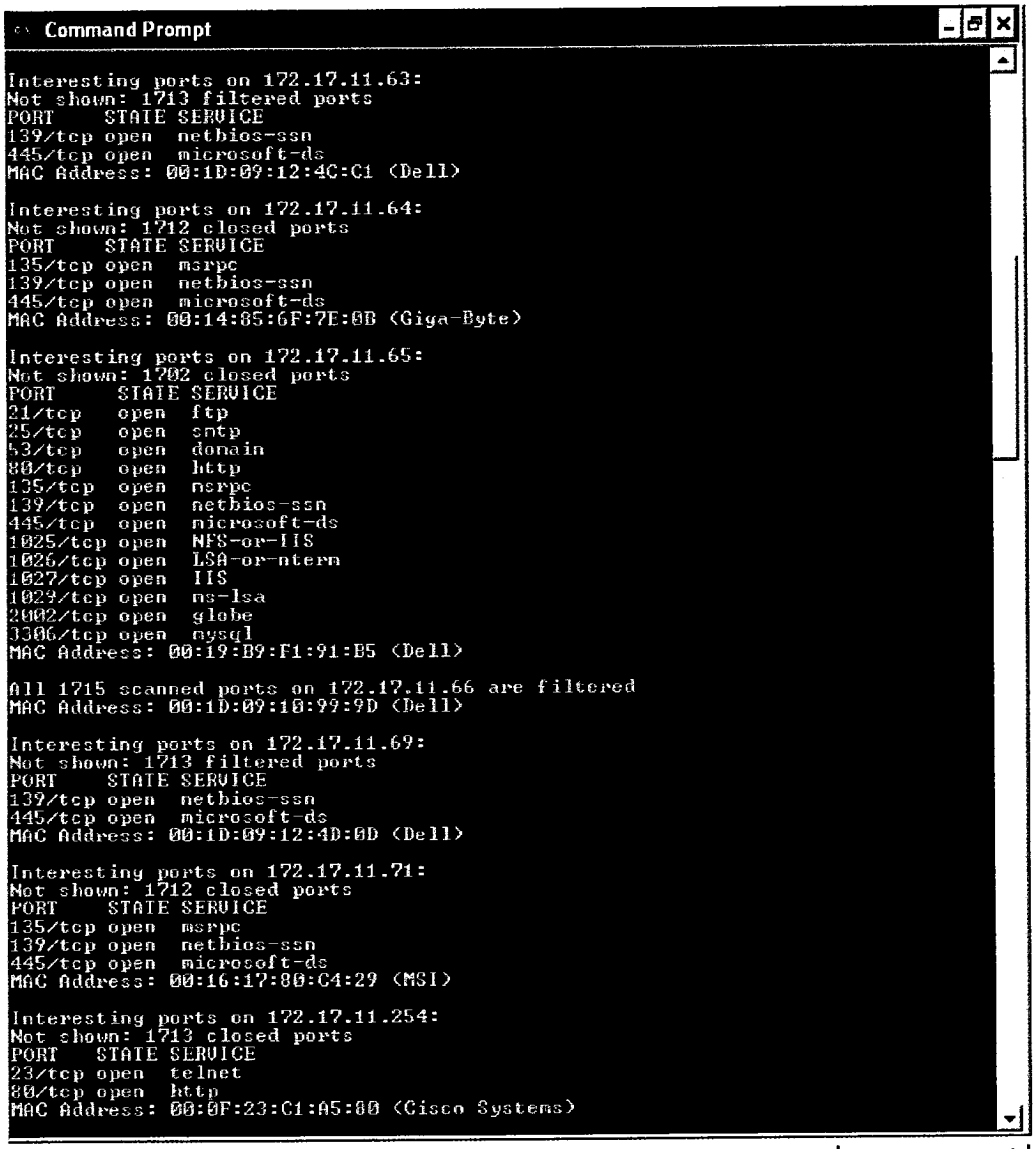
รูปที่ 39 การทดสอบโดยใช้โปรแกรม Cain เพื่อถอดรหัส WEP Key

4. เมื่อผู้ทดสอบสามารถถอดรหัส WEP Key ได้สำเร็จ ผู้ทดสอบได้ทดลองเชื่อมต่อกับ Access Point mnre-ap ด้วย WEP Key ที่ได้ โดยสามารถเชื่อมต่อได้สำเร็จ โดยผู้ทดสอบได้รับ IP Address หลังจากเชื่อมต่อเป็น 172.17.11.61 ดังแสดงในรูปที่ 40



รูปที่ 40 หมายเลขไอพีที่ได้รับจากการเชื่อมต่อเครือข่ายไร้สาย mnre-ap (กรมควบคุมมลพิษ ชั้น 1)

5. จากหมายเลขไอพีดังกล่าวผู้ทดสอบได้ใช้โปรแกรม nmap ซึ่งเป็นเครื่องมือสำหรับสแกนพอร์ตเครื่องเป้าหมาย ทำให้ผู้ทดสอบสามารถทราบหมายเลขพอร์ตที่เปิดอยู่, สถานะของพอร์ต และเซอร์วิสที่ใช้พอร์ตดังกล่าว ดังแสดงในรูปที่ 41 ข้อมูลทั้งหมดเป็นข้อมูลเบื้องต้นสำหรับเริ่มต้นเจาะระบบ ซึ่งเป็นการแสดงให้เห็นว่าหากผู้บุกรุกสามารถถอดรหัส WEP Key ได้สำเร็จก็จะสามารถเริ่มต้นเจาะระบบเครื่องคอมพิวเตอร์ที่พบภายในเครือข่ายดังกล่าว



รูปที่ 41 การทดสอบใช้โปรแกรม nmap ในการสแกน Port และ Service ของเครื่องคอมพิวเตอร์ที่พบ

สิ่งที่พบจากการทดสอบ

จากการทดสอบเจาะระบบจากภายนอกผ่านทางอุปกรณ์เครือข่ายไร้สาย mnre-ap ซึ่งตั้งอยู่ที่กรมควบคุมมลพิษ ชั้น 1 ผู้ทดสอบพบว่าสามารถเจาะอุปกรณ์เครือข่ายไร้สายดังกล่าวได้ง่าย เนื่องจากมีการใช้ WEP ในการเข้ารหัสข้อมูล ซึ่งเป็นการเข้ารหัสที่สามารถถอดรหัสได้

จากการทดสอบสามารถสรุปสิ่งที่พบจากการทดสอบได้ดังนี้

- สามารถเชื่อมต่อเข้าเครือข่ายไร้สายได้

หากผู้บุกรุกพบช่องโหว่ดังกล่าว จะก่อให้เกิดความสูญเสียต่อ สป.ทส. ดังนี้

- **ผลกระทบด้าน** Confidentiality

ความสูญเสียด้าน Confidentiality คือผลกระทบที่ก่อให้เกิดการสูญเสียข้อมูลที่เป็นความลับ ซึ่งจากการทดสอบสามารถเข้าถึงอุปกรณ์เครือข่ายไร้สายดังกล่าวได้ ทำให้มีโอกาสที่ผู้บุกรุกจะสามารถเข้าถึงข้อมูลที่เป็นความลับภายในเครื่องคอมพิวเตอร์ที่กำลังใช้งานเครือข่ายไร้สาย

คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

จากสิ่งที่พบ ที่ปรึกษามีคำแนะนำเรื่องความปลอดภัยระบบเครือข่ายไร้สายให้ สป.ทส. ดังนี้

- สป.ทส.ควรพิจารณาใช้การพิสูจน์ตัวตนกับเครื่องคอมพิวเตอร์แม่ข่ายควบคู่กับ การเข้ารหัสข้อมูลด้วย WPA2 เนื่องจากการเข้ารหัสข้อมูลด้วย WEP ยังไม่มีความปลอดภัยเพียงพอ จึงมีความเสี่ยงที่ผู้บุกรุกสามารถถอดรหัส WEP Key และเชื่อมต่อเข้าสู่ระบบเครือข่ายภายในของ สป.ทส. ได้

2.3 ผลการวิเคราะห์ช่องโหว่ที่พบในอุปกรณ์เครือข่ายไร้สาย

จากการทดสอบเจาะระบบ ที่ปรึกษาได้นำช่องโหว่ที่พบมาวิเคราะห์ เพื่อหาสาเหตุของการเกิดช่องโหว่ในอุปกรณ์เครือข่ายไร้สาย โดยสามารถสรุปประเด็น ดังนี้

2.3.1 Wireless Encryption

จากการทดสอบอุปกรณ์เครือข่ายไร้สายพบว่ามีการเข้ารหัสข้อมูลด้วย WEP หรือ WPA-PSK ซึ่งอาจส่งผลกระทบได้ดังนี้

(1) **ผลกระทบ** (Impact)

- ผู้บุกรุกสามารถใช้เครื่องมือ (Tools) ที่สามารถเจาะระบบผ่านระบบความปลอดภัยเหล่านี้ และเข้าถึงระบบเครือข่ายไร้สายของ สป.ทส.

(2) **คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง**

การป้องกันผู้บุกรุกจากการใช้งานระบบเครือข่ายไร้สาย โดยวิธีการใช้ WEP หรือ WPA-PSK นั้นปัจจุบันไม่สามารถจะทำได้แล้ว เนื่องจากวิธีการดังกล่าวได้มีเครื่องมือ (Tools) ที่สามารถจะเจาะระบบผ่านระบบความปลอดภัยเหล่านี้ และสามารถหาได้ง่ายจากอินเทอร์เน็ต โดยในปัจจุบันวิธีที่ดีที่สุดคือ ใช้การพิสูจน์ตัวตนผู้ใช้งานเครือข่ายไร้สายกับเครื่องคอมพิวเตอร์แม่ข่าย

2.3.2 SSID Broadcast

การปิดฟังก์ชั่น SSID Broadcast เป็นอีกวิธีหนึ่งที่ช่วยเพิ่มความปลอดภัยให้กับเครือข่ายไร้สาย แม้ว่าปัจจุบันจะมีเครื่องมือที่สามารถจะค้นหา SSID ที่ซ่อนอยู่ได้แล้ว แต่อย่างไรก็ตามการซ่อน SSID ก็เป็นการเพิ่มความยากให้แก่ผู้บุกรุกในการเจาะระบบเครือข่ายไร้สาย

(1) **ผลกระทบ** (Impact)

- การเปิดฟังก์ชั่น SSID Broadcast อาจเพิ่มโอกาสที่จะทำให้ผู้บุกรุกโจมตีอุปกรณ์เครือข่ายไร้สายของ สป.ทส.

(2) **คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง**

ควรปิดฟังก์ชั่น SSID Broadcast เพื่อลดโอกาสที่อุปกรณ์เครือข่ายไร้สายจะถูกโจมตีจากผู้บุกรุก

สรุปผลการดำเนินการ

จากผลการทดสอบเจาะระบบจากภายนอกทั้งหมด 2 ส่วน คือการทดสอบเจาะระบบเว็บไซต์ของ สป.ทส. ทั้งหมด 2 URL และการทดสอบเจาะระบบอุปกรณ์เครือข่ายไร้สายของ สป.ทส. ทั้งหมด 3 SSID ที่ปรึกษาได้นำเสนอไว้ในรายงานฉบับนี้แล้วนั้น ที่ปรึกษา จึงใคร่ขอเรียนผลการสำรวจ และข้อแนะนำในการปรับปรุงดังต่อไปนี้

1. **ผลการสำรวจ**

1.1 **เว็บไซต์** http://www.warehouse.mnre.go.th/

ที่ปรึกษาพบว่าเว็บไซต์ http://www.warehouse.mnre.go.th/ มีความเสี่ยงที่จะถูกเจาะระบบอยู่ในระดับสูง โดยสาเหตุที่ความเสี่ยงอยู่ในระดับสูงเนื่องจากในการทดสอบสามารถเข้าถึงระบบบริหารจัดการเว็บไซต์ดังกล่าวได้ ซึ่งหากผู้บุกรุกสามารถเข้าถึงระบบในลักษณะเดียวกัน ก็จะสามารถแก้ไขเปลี่ยนแปลงหน้าเว็บไซต์ซึ่งจะทำให้องค์กรเสื่อมเสียชื่อเสียง

1.2 **เว็บไซต์** http://petition.mnre.go.th/

ที่ปรึกษาพบว่าเว็บไซต์ http://petition.mnre.go.th/ มีความเสี่ยงที่จะถูกเจาะระบบอยู่ในระดับสูง โดยสาเหตุที่ความเสี่ยงอยู่ในระดับสูงเนื่องจากในการทดสอบสามารถเข้าถึงระบบบริหารจัดการเว็บไซต์ดังกล่าวได้ในลักษณะเดียวกับเว็บไซต์ http://www.warehouse.mnre.go.th/ ซึ่งหากผู้บุกรุกสามารถเข้าถึงระบบในลักษณะเดียวกับการทดสอบครั้งนี้ ก็จะสามารถแก้ไขเปลี่ยนแปลงหน้าเว็บไซต์ซึ่งจะทำให้องค์กรเสื่อมเสียชื่อเสียง

1.3 **อุปกรณ์เครือข่ายไร้สาย** mnre-ap (**กรมส่งเสริมคุณภาพสิ่งแวดล้อม ชั้น** 10)

ที่ปรึกษาพบว่าอุปกรณ์เครือข่ายไร้สาย mnre-ap ซึ่งตั้งอยู่ที่กรมส่งเสริมคุณภาพสิ่งแวดล้อม ชั้น 10 มีความเสี่ยงที่จะถูกเจาะระบบอยู่ในระดับสูง เนื่องจากมีการเข้ารหัสในลักษณะ WEP ซึ่งทำให้หากถอดรหัสดังกล่าวได้ ก็จะสามารถใช้งานอุปกรณ์เครือข่ายไร้สายและทำให้สามารถเข้าถึงเครื่องคอมพิวเตอร์ภายในองค์กรรวมทั้งเครื่องคอมพิวเตอร์แม่ข่าย

1.4 **อุปกรณ์เครือข่ายไร้สาย** linksys-mnre (**กรมส่งเสริมคุณภาพสิ่งแวดล้อม ชั้น** 10)

ที่ปรึกษาพบว่าอุปกรณ์เครือข่ายไร้สาย linksys-mnre ซึ่งตั้งอยู่ที่กรมส่งเสริมคุณภาพสิ่งแวดล้อม ชั้น 10 มีความเสี่ยงที่จะถูกเจาะระบบอยู่ในระดับต่ำ เนื่องจากมีการเข้ารหัสในลักษณะ WPA-PSK

2. **อุปกรณ์เครือข่ายไร้สาย** mnre-ap (**กรมควบคุมมลพิษ ชั้น** 1)

อุปกรณ์เครือข่ายไร้สาย mnre-ap ซึ่งตั้งอยู่ที่กรมควบคุมมลพิษ ชั้น 1 มีความเสี่ยงที่จะถูกเจาะระบบอยู่ในระดับสูง เนื่องจากมีการเข้ารหัสในลักษณะ WEP ซึ่งทำให้หากถอดรหัสดังกล่าวได้ ก็จะสามารถใช้งานอุปกรณ์เครือข่ายไร้สายและทำให้สามารถเข้าถึงเครื่องคอมพิวเตอร์ภายในองค์กรได้

3. คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

1. ระบบล็อกอินของเว็บไซต์มีการใช้ชื่อผู้ใช้และรหัสผ่านที่ง่ายต่อการคาดเดา เนื่องจากทั้งบัญชีผู้ใช้ และรหัสผ่าน ปรากฏใน Dictionary ทำให้สามารถใช้โปรแกรมสำหรับคาดเดารหัสผ่าน (Brute Force Attack) เพื่อคาดเดารหัสผ่านได้โดยง่าย จึงควรแก้ไขโดยการเปลี่ยนแปลงบัญชีผู้ใช้ และรหัสผ่านให้ยากต่อการคาดเดา เช่นรหัสผ่านต้องประกอบไปด้วยตัวอักษรตัวเล็ก ตัวใหญ่ ตัวเลข ตัวอักขระพิเศษผสมกัน และมีความยาวไม่ต่ำกว่า 8 ตัวอักษร

2. พบว่าเว็บไซต์ของ สป.ทส. มีลิงค์ (Link) ที่เข้าสู่ระบบล็อกอินการจัดการข้อมูลบนเว็บไซต์ จึงควรแก้ไขโดยการซ่อนลิงค์สำหรับเข้าสู่ระบบล็อกอินของเว็บไซต์

3. จากการที่ระบบลืมรหัสผ่านของเว็บไซต์มีการแจ้งเตือนข้อความไม่เหมาะสม ทำให้สามารถคาดเดาบัญชีผู้ใช้ที่มีอยู่จริงในระบบได้ จึงควรแก้ไขโดยแสดงข้อความแจ้งเตือนให้เหมือนกัน ทั้งกรณีผู้ใช้ (User) ดังกล่าวมีอยู่จริงหรือไม่มีในระบบ

4. สป.ทส. ควรป้องกันการทำ Directory Listing โดยการตั้งค่าสิทธิ์การเข้าถึงพาทต่าง ๆ อย่างเหมาะสม

5. สป.ทส. ควรทำการปิด หรือสร้างข้อมูล Header หลอก เพื่อป้องกันการรวบรวมข้อมูลผ่านทาง Header ของเว็บไซต์

6. สป.ทส. ควรกำหนดนโยบายภายในองค์กร ไม่ให้ใช้อีเมล์ดังกล่าวในการโพสข้อความภายนอกองค์กร เช่น เว็บบอร์ดสาธารณะ

7. สป.ทส. ควรพิจารณาใช้การพิสูจน์ตัวตนกับเครื่องคอมพิวเตอร์แม่ข่ายควบคู่กับ การเข้ารหัสข้อมูลด้วย WPA2 เนื่องจากการเข้ารหัสข้อมูลด้วย WEP และ WPA-PSK ยังไม่มีความปลอดภัยเพียงพอ จึงมีความเสี่ยงที่ผู้บุกรุกสามารถเข้าถึงระบบเครือข่ายภายในของ สป.ทส. ได้

8. สป.ทส. ควรพิจารณาให้มีการซ่อน SSID ของเครือข่ายไร้สายทุกจุด โดยปรับตั้งค่าของอุปกรณ์เครือข่ายให้ระงับใช้งานฟังก์ชั่น "Broadcast SSID" เพื่อป้องกันไม่ให้ผู้บุกรุกสามารถค้นหาเครือข่ายได้ง่าย และเปลี่ยนชื่อของ Access Point ไม่ให้ระบุเป็นชื่อ Default ของผลิตภัณฑ์

ภาคผนวก ก. คำศัพท์เฉพาะทางเทคนิค

OPN หมายถึง ระบบเครือข่ายไร้สายไม่มีการเข้ารหัส ผู้ใช้งานไม่จำเป็นต้องใส่ KEY หรือรหัสผ่านเพื่อเชื่อมต่อกับเครือข่ายไร้สาย

WEP (Wired Equivalent Privacy) หมายถึง มาตรฐานความปลอดภัยสำหรับเครือข่ายไร้สายโดยมีการเข้ารหัสข้อมูลโดยใช้ RC4 โดยผู้ใช้งานจะต้องใส่ WEP KEY เพื่อเชื่อมต่อเข้ากับระบบเครือข่ายไร้สาย

WPA-PSK (Wi-Fi Protected Access-Pre-Share Key) หมายถึง มาตรฐานความปลอดภัยสำหรับเครือข่ายไร้สายที่พัฒนาขึ้นมาภายหลัง WEP มีการเข้ารหัสข้อมูลที่เรียกว่า AES (Advanced Encryption Standard) โดย WPA แบบ Pre-Share Key นั้นไม่มีการพิสูจน์ตัวตนกับเครื่องคอมพิวเตอร์แม่ข่าย ผู้ใช้งานยังคงใช้การใส่รหัสผ่านเพื่อเชื่อมต่อกับระบบเครือข่ายไร้สาย

ภาคผนวก ข. มาตรฐาน OWASP

ช่องโหว่ทางเว็บแอพพลิเคชั่น 10 อันดับแรกของปี ค.ศ. 2007 ตามมาตรฐาน OWASP มีดังนี้

1. Cross Site Scripting (XSS)
2. Injection Flaws
3. Malicious File Execution
4. Insecure Direct Object Reference
5. Cross Site Request Forgery (CSRF)
6. Information Leakage and Improper Error Handling
7. Broken Authentication and Session Management
8. Insecure Cryptographic Storage
9. Insecure Communications
10. Failure to Restrict URL Access

ช่องโหว่ทางเว็บแอพพลิเคชั่น 10 อันดับแรกของปี ค.ศ. 2004 ตามมาตรฐาน OWASP มีดังนี้

1. Unvalidated Input
2. Broken Access Control
3. Broken Authentication and Session Management
4. Cross Site Scripting
5. Buffer Overflow
6. Injection Flaws
7. Improper Error Handling
8. Insecure Storage
9. Application Denial of Service
10. Insecure Configuration Management

ส่วนที่ 2.3

รายงานผลการทดสอบเจาะระบบเครือข่ายภายใน

ความนำ

การทดสอบเจาะระบบเครือข่ายภายใน (White-Box Penetration Testing) เป็นการกำหนดสถานการณ์จำลองของการโจมตีจุดอ่อน และนำไปสู่ความสูญเสียด้านความปลอดภัย (CIA) โดยในการทดสอบนั้น จะเป็นการจำลองสถานการณ์เป็นผู้บุกรุกที่สามารถเข้ามาในสถานที่ปฏิบัติงาน ได้แก่พนักงาน ผู้รับจ้างเหมาพัฒนาระบบแบบ Outsource หรือเวนเดอร์ ซึ่งอาจมีความประสงค์ที่ต้องการเจาะระบบเครือข่ายภายในองค์กร เพื่อพยายามค้นหาข้อมูลสำคัญ หรือยึดครองเครื่องคอมพิวเตอร์เป้าหมายให้สำเร็จ สิ่งที่แตกต่างระหว่างผู้ทดสอบและผู้บุกรุกคือ ผู้บุกรุกจะเจาะระบบเครือข่ายภายในโดยไม่คำนึงถึงความเสียหายต่อองค์กรที่ถูกเจาะระบบ แต่ผู้ทดสอบจะดำเนินการทดสอบโดยไม่ประสงค์ที่จะทำให้เกิดความเสียหายใด ๆ การทดสอบเจาะระบบจึงเป็นประโยชน์ต่อองค์กร เนื่องจากสามารถใช้ผลของการทดสอบเจาะระบบทำการป้องกันและเพิ่มความปลอดภัย ก่อนที่ผู้บุกรุกจะสร้างความเสียหายให้กับองค์กร

สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม มีความประสงค์ที่จะดำเนินการทดสอบเจาะระบบจากภายใน (White-box Penetration Testing) ให้กับเครื่องคอมพิวเตอร์แม่ข่ายจำนวน 2 หมายเลขไอพี ประกอบด้วย

1. เครื่องคอมพิวเตอร์แม่ข่ายหมายเลขไอพี 172.16.1.45
2. เครื่องคอมพิวเตอร์แม่ข่ายหมายเลขไอพี 192.168.16.7

ในการทดสอบเจาะระบบจากภายนอกครั้งนี้ บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด ได้ดำเนินการตามขอบเขตการดำเนินงานดังต่อไปนี้

- ขอบเขตการดำเนินงานข้อ 3.2.3: ให้กำหนดสถานการณ์จำลองที่สามารถโจมตีจุดอ่อนและนำไปสู่ความสูญเสียด้านความปลอดภัย (CIA) เช่น จำลองสถานการณ์โจมตีจากอินเทอร์เน็ตภายนอก จำลองสถานการณ์เป็นผู้ที่สามารถเข้ามาในสถานที่ปฏิบัติงาน ได้แก่ พนักงาน ผู้รับจ้างเหมาะพัฒนาระบบแบบ Outsource หรือ Vendor ภายใต้สถานการณ์ที่ถูกกำหนด

- ขอบเขตการดำเนินงานข้อ 3.2.4: หลีกเลี่ยงแบบทดสอบที่อาจจะก่อให้เกิดการหยุดชะงักของระบบงาน เช่น การใช้แบบทดสอบ Denial of Service ตามความเห็นชอบของสำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อมที่จะกำหนดให้มีการทดสอบในเครื่องทดสอบแทน

- ขอบเขตการดำเนินงานข้อ 3.2.5: นำเสนอรายงานในรูปแบบแสดงระดับความเสี่ยงโดยเปรียบเทียบกับการควบคุม และวิธีปฏิบัติงานตามความเห็นชอบของสำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม พร้อมข้อเสนอแนะและแนวทางที่เหมาะสมในการปรับปรุง รวมทั้งออกแบบระบบความปลอดภัยของระบบ

เครือข่ายและความปลอดภัยคอมพิวเตอร์ของสำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม รองรับการขยายการบริการ และรองรับกฎ ระเบียบและข้อบังคับด้านความมั่นคงปลอดภัยระบบสารสนเทศและการสื่อสาร หรือมาตรฐานด้านความปลอดภัยระบบสารสนเทศที่เกี่ยวข้อง

- ขอบเขตการดำเนินงานข้อ 3.2.6: เมื่อค้นพบช่องโหว่ หรือข้อมูลสำคัญ ซึ่งอาจจะทำให้สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อมตกอยู่ในสถานะหรือสภาวะต่อการรั่วไหล หรือหยุดชะงักของระบบคอมพิวเตอร์ ต้องมีการแจ้งเตือนเพื่อขออนุญาตดำเนินงานต่อไป

- ขอบเขตการดำเนินงานข้อ 3.2.7: หากเจ้าหน้าที่ดำเนินการค้นพบช่องโหว่ที่นอกเหนือจากรายการที่แจ้งไว้ จะต้องแจ้งให้สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อมให้ความเห็นชอบก่อนเข้าดำเนินการ ทั้งนี้ในระหว่างการดำเนินโครงการฯ ที่ปรึกษาจะต้องจัดเจ้าหน้าที่เพื่อให้คำแนะนำ ตอบคำถาม และให้การช่วยเหลือทางโทรศัพท์และพร้อมที่จะเข้าไปช่วยในกรณีเร่งด่วน โดยต้องอยู่ในขอบเขตการดำเนินโครงการฯ

- ขอบเขตการดำเนินงานข้อ 3.2.8: ดำเนินการวิเคราะห์และให้คำแนะนำ ในกรณีที่ระบบเครือข่ายของสำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม จำเป็นต้องได้รับการติดตั้งระบบ หรืออุปกรณ์เพิ่มเติม เพื่อเป็นการเพิ่มระดับการรักษาความปลอดภัยของระบบเครือข่ายและความปลอดภัยคอมพิวเตอร์ของสำนักงานปลัดกระทรวงทรัพย์ฯ สามารถเสนอเพื่อดำเนินการได้ทั้งนี้จะต้องไม่คิดค่าใช้จ่ายเพิ่มเติม

หลังจากที่ได้ดำเนินการทดสอบเจาะระบบจากภายใน (White-box Penetration Testing) เสร็จสิ้นแล้ว บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด ได้จัดทำเอกสารรายงานการทดสอบเจาะระบบเครือข่ายภายใน (White-box Penetration Test Report) เพื่อนำเสนอผลการทดสอบต่อสำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม เพื่อให้ฝ่ายต่าง ๆ ที่เกี่ยวข้องได้รับทราบและดำเนินการแก้ไขต่อไป

เพื่อความสะดวกในการอ่านรายงานฉบับนี้ บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด จะเปลี่ยนการนำเสนอจากชื่อเต็มเป็นการใช้ชื่อย่อ ดังนี้

ชื่อเต็ม	ชื่อย่อที่ใช้
สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม	สป.ทส.
บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด	ที่ปรึกษา
โครงการจัดจ้างที่ปรึกษาและประเมินความเสี่ยงด้านสารสนเทศและการแก้ไขปัญหา	โครงการฯ

บทสรุปสำหรับผู้บริหาร

ในการทดสอบเจาะระบบเครือข่ายภายในครั้งนี้ ที่ปรึกษาได้ทดสอบเจาะระบบระบบเครือข่ายภายในซึ่งเป็นเครื่องคอมพิวเตอร์แม่ข่ายทั้งหมด 2 หมายเลขไอพี ซึ่งสามารถสรุปผลการทดสอบได้ดังนี้

1. การทดสอบเจาะระบบเครือข่ายภายใน

1.1 เครื่องคอมพิวเตอร์แม่ข่าย: WAREHOUSE

ที่ปรึกษาพบว่าเครื่องคอมพิวเตอร์แม่ข่าย WAREHOUSE (หมายเลขไอพี 172.16.1.45) มีความเสี่ยงที่จะถูกเจาะระบบอยู่ในระดับปานกลาง ซึ่งแม้ว่าในการทดสอบจะไม่สามารถยึดครองเครื่องคอมพิวเตอร์แม่ข่ายดังกล่าว แต่สามารถเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายได้โดยตรง ซึ่งหากมีผู้ไม่หวังดีภายในองค์กร เช่นพนักงาน ผู้รับจ้างเหมาพัฒนาระบบแบบ Outsource หรือเวนเดอร์ ที่อาจมีความประสงค์ร้ายเข้ามาใช้งานเครือข่ายภายในองค์กร ก็สามารถเข้าถึง และโจมตีเครื่องคอมพิวเตอร์แม่ข่ายได้โดยตรง

1.2 เครื่องคอมพิวเตอร์แม่ข่าย: E-PETITION

ที่ปรึกษาพบว่าเครื่องคอมพิวเตอร์แม่ข่าย E-PETITION (หมายเลขไอพี 192.168.16.7) มีความเสี่ยงที่จะถูกเจาะระบบอยู่ในระดับปานกลาง ซึ่งแม้ว่าในการทดสอบจะไม่สามารถยึดครองเครื่องคอมพิวเตอร์แม่ข่ายดังกล่าว แต่สามารถเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายได้โดยตรง ซึ่งหากมีผู้ไม่หวังดีภายในองค์กร เช่นพนักงาน ผู้รับจ้างเหมาพัฒนาระบบแบบ Outsource หรือเวนเดอร์ ที่อาจมีความประสงค์ร้ายเข้ามาใช้งานเครือข่ายภายในองค์กร ก็สามารถเข้าถึง และโจมตีเครื่องคอมพิวเตอร์แม่ข่ายได้โดยตรง

ในการประเมินระดับความเสี่ยงของเป้าหมายที่จะทดสอบนั้น ที่ปรึกษามีการแบ่งระดับความเสี่ยงทางด้านเทคนิคเพื่อให้เจ้าหน้าที่ที่เกี่ยวข้องมีความเข้าใจว่าสิ่งที่พบจากการเจาะระบบเครื่องคอมพิวเตอร์แม่ข่ายของ สป.ทส. นั้นมีความรุนแรงในระดับใด ซึ่งในการคำนวณหาระดับความเสี่ยงนั้นได้จากการคำนวณจาก ผลกระทบและโอกาสที่จะเกิด โดยสามารถแสดงรายละเอียดได้ดังนี้

ดารางที่ 1 นิยามระดับความรุนแรงในการประเมินความเสี่ยงทางด้านเทคนิคของที่ปรึกษา

ระดับ	ผลกระทบทางเทคนิค	โอกาสที่จะเกิด
สูง (HIGH)	สามารถเข้าไปบริหารจัดการระบบได้เปรียบเสมือนเป็นเจ้าของระบบนั้น	ผู้บุกรุกสามารถเข้าถึงระบบได้อย่างง่ายดาย โดยไม่ต้องใช้วิธีการที่ซับซ้อน
ปานกลาง (MEDIUM)	สามารถจำกัดสิทธิ์ในการควบคุมระบบ หรือเข้าไปแก้ไขค่าต่าง ๆ ของระบบได้	จากช่องโหว่ที่เกิดขึ้น ผู้บุกรุกสามารถทำการเข้าถึงระบบและเปลี่ยนสิทธิ์ของการควบคุมระบบได้โดยไม่จำเป็นต้องใช้โปรแกรม Exploit ทำการยึดเครื่องเป้าหมาย
ต่ำ (LOW)	เป็นข้อมูลที่แสดงนั้นเป็นประโยชน์ต่อการโจมตี หรือใช้ข้อมูลเครื่องดังกล่าว เป็นเป้าหมายในการยึดเครื่องต่อไปในระบบ	ช่องโหว่ที่เกิดขึ้นนั้น อาจถูกโจมตีได้ยาก เนื่องจากต้องอาศัยความชำนาญของผู้บุกรุกในการยึดเครื่องเป้าหมาย

จากระดับความรุนแรงผลกระทบทางเทคนิค และโอกาสที่จะเกิด สามารถนำมาคำนวณหาความเสี่ยงทางเทคนิคได้โดยคำนวณจากสูตร

ความเสี่ยงทางเทคนิค = (ผลกระทบทางเทคนิค x โอกาสที่จะเกิด)

ซึ่งเมื่อนำระดับความรุนแรงของผลกระทบทางเทคนิค และโอกาสที่จะเกิด ทั้งหมด (สูง กลาง และ ต่ำ) มาคำนวณหาความเสี่ยงทางเทคนิคจากสูตรข้างต้นจะสามารถสรุปผลได้ดังตารางที่ 2 ซึ่งที่ปรึกษาจะใช้การประเมินความเสี่ยงในลักษณะนี้เพื่อประเมินหาความเสี่ยงที่พบในเป้าหมายการทดสอบ

ดารางที่ 2 ผลการคำนวณความเสี่ยงทางเทคนิค (Technical Risk)

		โอกาสที่จะเกิด		
		สูง	ปานกลาง	ต่ำ
ผลกระทบทางเทคนิค	สูง	สูง	สูง	ปานกลาง
	ปานกลาง	สูง	ปานกลาง	ปานกลาง
	ต่ำ	ต่ำ	ต่ำ	ต่ำ

เมื่อพบความเสี่ยงด้านเทคนิคในเครื่องคอมพิวเตอร์แม่ข่ายของ สป.ทส. จะเกิดความสูญเสียด้านความปลอดภัยต่อ สป.ทส. ที่แตกต่างกันไป โดยที่ปรึกษาได้สรุปประเภทของความสูญเสียด้านความปลอดภัยดังแสดงในตารางที่ 3

เพื่อให้เจ้าหน้าที่ที่เกี่ยวข้องมีความเข้าใจว่าหากผู้บุกรุกสามารถเจาะระบบเครื่องคอมพิวเตอร์แม่ข่ายของ สป.ทส. จะทำให้ส่งผลกระทบกับ สป.ทส. ในลักษณะใด

ตารางที่ 3 ประเภทของความสูญเสียด้านความปลอดภัย

ประเภท	รายละเอียด
Confidentiality	ผลกระทบที่ก่อให้เกิดการสูญเสียข้อมูลที่เป็นความลับ
Integrity	ผลกระทบที่เกี่ยวข้องกับความถูกต้องสมบูรณ์ของข้อมูล
Availability	ผลกระทบที่เกี่ยวข้องกับความพร้อมใช้งานของระบบ

1. ผลการทดสอบเจาะระบบเครือข่ายภายใน

1.1 ผลการทดสอบเจาะระบบเครื่องคอมพิวเตอร์แม่ข่าย: WAREHOUSE

ตารางที่ 4 ผลกระทบทางเทคนิค โอกาสที่จะเกิด และความเสี่ยงทางเทคนิคของเครื่องคอมพิวเตอร์แม่ข่าย: WAREHOUSE

ผลกระทบทางเทคนิค: ระดับปานกลาง
สิ่งที่พบ เครื่องคอมพิวเตอร์แม่ข่าย: WAREHOUSE มีผลกระทบทางเทคนิคอยู่ในระดับปานกลาง เนื่องจากถึงแม้ว่าผู้ทดสอบจะไม่สามารถเจาะระบบเครื่องคอมพิวเตอร์แม่ข่ายดังกล่าวได้ เนื่องจากผู้ทดสอบไม่พบช่องโหว่ที่ทำให้สามารถยึดครองเครื่องคอมพิวเตอร์แม่ข่ายได้สำเร็จ แต่หากผู้บุกรุกหรือผู้ไม่หวังดีทราบรหัสผ่าน (Password)ของเครื่องคอมพิวเตอร์แม่ข่ายดังกล่าว จะสามารถยึดครองเครื่องคอมพิวเตอร์แม่ข่ายได้โดยง่าย
โอกาสที่จะเกิด: ระดับต่ำ
สิ่งที่พบ เครื่องคอมพิวเตอร์แม่ข่าย: WAREHOUSE มีโอกาสที่จะถูกเจาะระบบจากผู้บุกรุกในระดับต่ำ เนื่องจากผู้ทดสอบไม่พบช่องโหว่ที่ทำให้สามารถยึดครองเครื่องคอมพิวเตอร์แม่ข่ายได้สำเร็จ
ความเสี่ยงทางเทคนิค: ระดับปานกลาง
สิ่งที่พบ เครื่องคอมพิวเตอร์แม่ข่าย: WAREHOUSE มีความเสี่ยงทางเทคนิคอยู่ในระดับปานกลาง ซึ่งได้จากการคำนวณผลกระทบทางเทคนิค (ระดับปานกลาง) และโอกาสที่จะเกิด(ระดับต่ำ) นำมาเปรียบเทียบกับตารางที่ 3.2 ทำให้พบว่าความเสี่ยงทางเทคนิคอยู่ในระดับปานกลาง

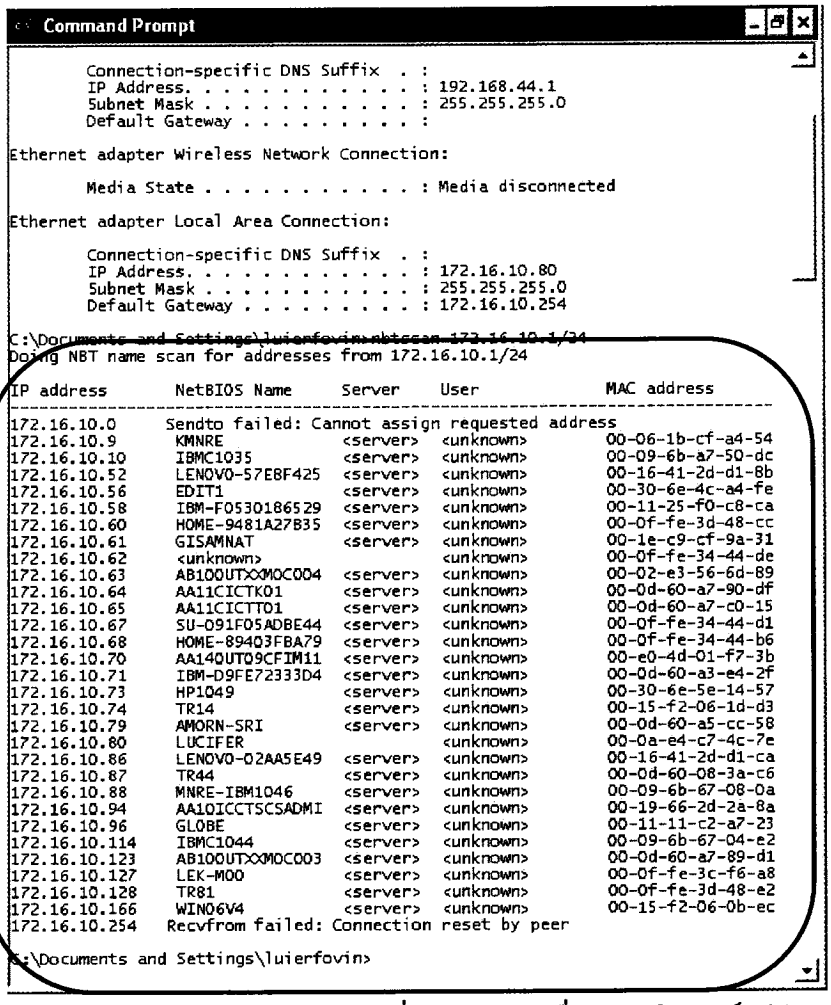
ดารางที่ 5 ความสูญเสียด้าน Confidentiality Integrity **และ** Availability **ของเครื่องคอมพิวเตอร์**

แม่ข่าย: WAREHOUSE

ความสูญเสียด้าน Confidentiality: **ไม่มีผลกระทบ**
สิ่งที่พบ
ไม่พบปัจจัยที่ส่งผลต่อความสูญเสียด้าน Confidentiality
ความสูญเสียด้าน Integrity: **ไม่มีผลกระทบ**
สิ่งที่พบ
ไม่พบปัจจัยที่ส่งผลต่อความสูญเสียด้าน Integrity
ความสูญเสียด้าน Availability: **ไม่มีผลกระทบ**
สิ่งที่พบ
ไม่พบปัจจัยที่ส่งผลต่อความสูญเสียด้าน Availability

ขั้นตอนในการทดสอบ

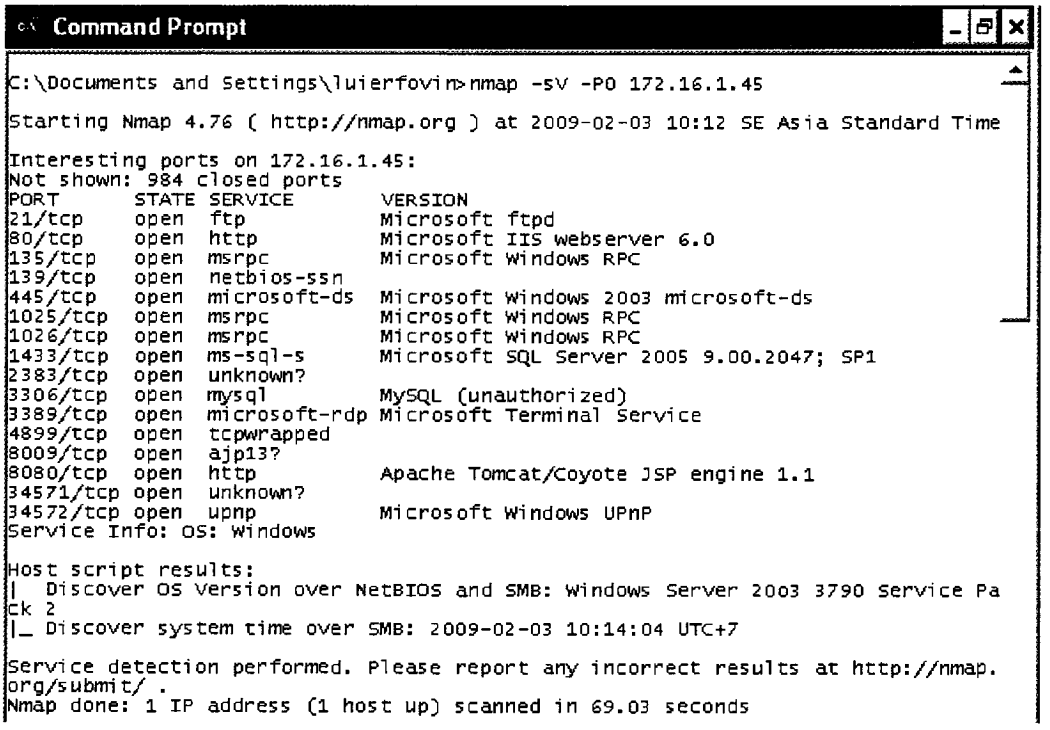
1. ผู้ทดสอบทดลองใช้โปรแกรม nbtscan เพื่อสแกนหาเครื่องคอมพิวเตอร์แม่ข่ายภายในเครือข่าย 172.16.10.1/24 ปรากฏว่าสามารถเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายต่าง ๆ ได้โดยตรง ดังแสดงในรูปที่ 1 ซึ่งหมายความว่าเครื่องคอมพิวเตอร์แม่ข่ายมีความเสี่ยงที่จะถูกโจมตีจากผู้ไม่หวังดีภายในองค์กร เช่นพนักงาน ผู้รับจ้างเหมาพัฒนาระบบแบบ Outsource หรือเวนเดอร์ ที่อาจมีความประสงค์ร้ายเข้ามาใช้งานเครือข่ายภายในองค์กร ก็สามารถเข้าถึง และโจมตีเครื่องคอมพิวเตอร์แม่ข่ายได้โดยตรง



```
Command Prompt

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.44.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

Ethernet adapter Wireless Network Connection:

        Media State . . . . . . . . . . . : Media disconnected

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 172.16.10.80
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.16.10.254

C:\Documents and Settings\luierfovin>nbtscan 172.16.10.1/24
Doing NBT name scan for addresses from 172.16.10.1/24

IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------------
172.16.10.0      Sendto failed: Cannot assign requested address
172.16.10.9      KMNRE            <server>  <unknown>        00-06-1b-cf-a4-54
172.16.10.10     IBMC1035         <server>  <unknown>        00-09-6b-a7-50-dc
172.16.10.52     LENOVO-57E8F425  <server>  <unknown>        00-16-41-2d-d1-8b
172.16.10.56     EDIT1            <server>  <unknown>        00-30-6e-4c-a4-fe
172.16.10.58     IBM-F0530186529  <server>  <unknown>        00-11-25-f0-c8-ca
172.16.10.60     HOME-9481A27B35  <server>  <unknown>        00-0f-fe-3d-48-cc
172.16.10.61     GISAMNAT         <server>  <unknown>        00-1e-c9-cf-9a-31
172.16.10.62     <unknown>                  <unknown>        00-0f-fe-34-44-de
172.16.10.63     AB100UTXXMOC004  <server>  <unknown>        00-02-e3-56-6d-89
172.16.10.64     AA11CICTK01      <server>  <unknown>        00-0d-60-a7-90-df
172.16.10.65     AA11CICTT01      <server>  <unknown>        00-0d-60-a7-c0-15
172.16.10.67     SU-091F05ADBE44  <server>  <unknown>        00-0f-fe-34-44-d1
172.16.10.68     HOME-89403FBA79  <server>  <unknown>        00-0f-fe-34-44-b6
172.16.10.70     AA140UT09CFIM11  <server>  <unknown>        00-e0-4d-01-f7-3b
172.16.10.71     IBM-D9FE72333D4  <server>  <unknown>        00-0d-60-a3-e4-2f
172.16.10.73     HP1049           <server>  <unknown>        00-30-6e-5e-14-57
172.16.10.74     TR14             <server>  <unknown>        00-15-f2-06-1d-d3
172.16.10.79     AMORN-SRI        <server>  <unknown>        00-0d-60-a5-cc-58
172.16.10.80     LUCIFER                    <unknown>        00-0a-e4-c7-4c-7e
172.16.10.86     LENOVO-02AA5E49  <server>  <unknown>        00-16-41-2d-d1-ca
172.16.10.87     TR44             <server>  <unknown>        00-0d-60-08-3a-c6
172.16.10.88     MNRE-IBM1046     <server>  <unknown>        00-09-6b-67-08-0a
172.16.10.94     AA1OICCTSCSADMI  <server>  <unknown>        00-19-66-2d-2a-8a
172.16.10.96     GLOBE            <server>  <unknown>        00-11-11-c2-a7-23
172.16.10.114    IBMC1044         <server>  <unknown>        00-09-6b-67-04-e2
172.16.10.123    AB100UTXXMOC003  <server>  <unknown>        00-0d-60-a7-89-d1
172.16.10.127    LEK-MOO          <server>  <unknown>        00-0f-fe-3c-f6-a8
172.16.10.128    TR81             <server>  <unknown>        00-0f-fe-3d-48-e2
172.16.10.166    WIN06V4          <server>  <unknown>        00-15-f2-06-0b-ec
172.16.10.254    Recvfrom failed: Connection reset by peer

C:\Documents and Settings\luierfovin>
```

รูปที่ 1 การทดสอบโดยใช้โปรแกรม nbtscan เพื่อสำรวจหาเครื่องคอมพิวเตอร์แม่ข่ายขององค์กร

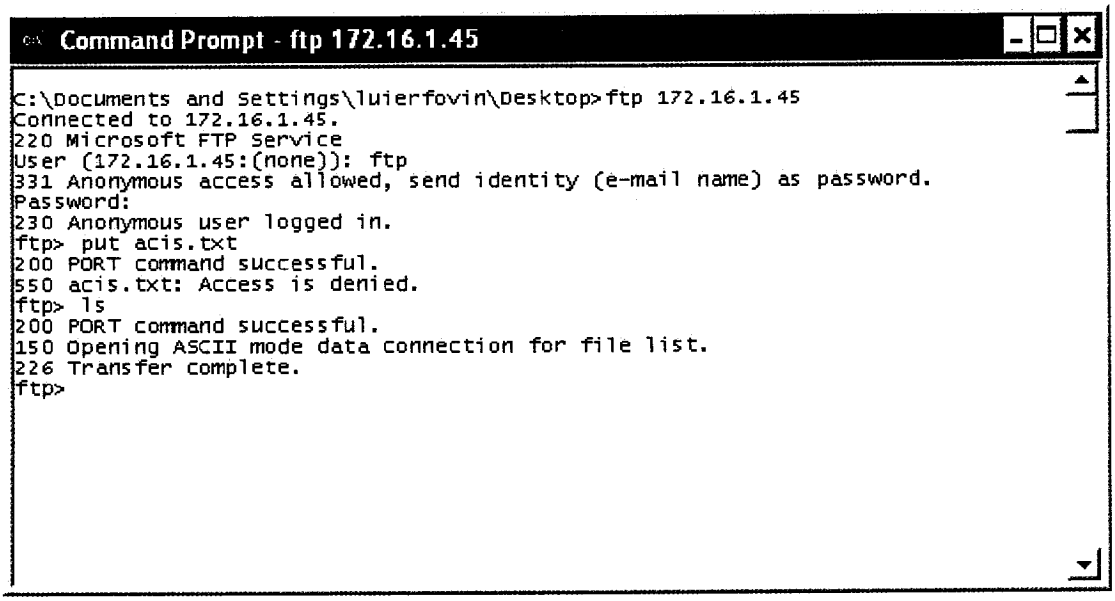
2. ผู้ทดสอบสแกนพอร์ตเครื่องเป้าหมาย โดยใช้โปรแกรม Nmap แสดงดังรูปที่ 2 ซึ่งผลจากการสแกนพอร์ตจะทำให้ผู้ทดสอบสามารถทราบหมายเลขพอร์ตที่เปิดอยู่ สถานะของพอร์ต และเซอร์วิสที่ใช้พอร์ตดังกล่าว ข้อมูลทั้งหมดเป็นข้อมูลเบื้องต้น เพื่อให้ผู้ทดสอบสามารถทราบช่องทางในการทดสอบระบบ



รูปที่ 2 การทดสอบโดยใช้โปรแกรม Nmap เพื่อสแกนพอร์ตเครื่องคอมพิวเตอร์แม่ข่ายหมายเลขไอพี 172.16.1.45

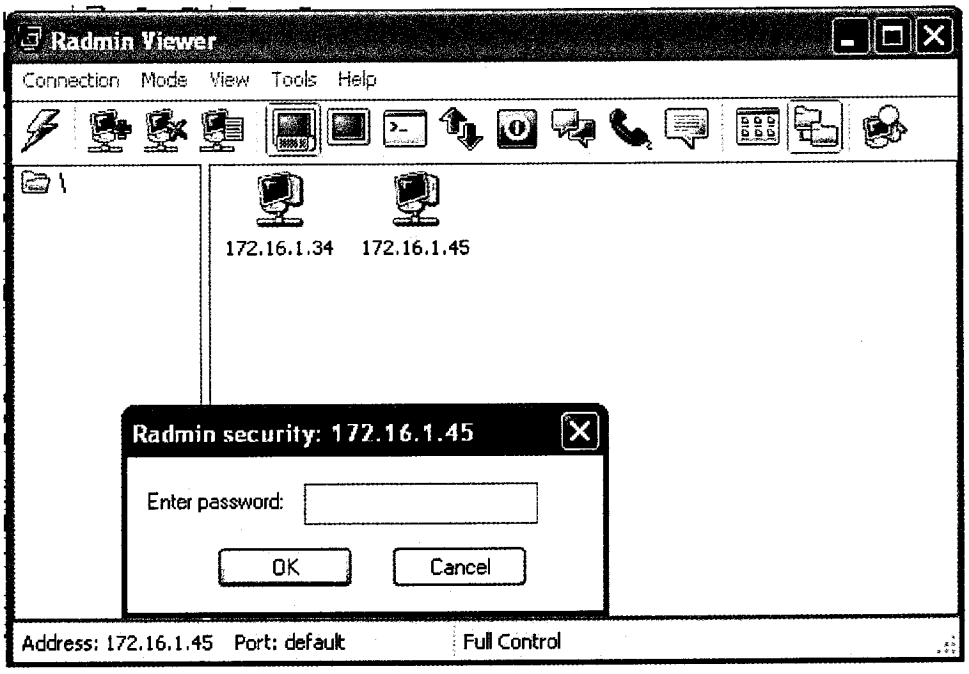
3. จากผลการสแกนพอร์ต แสดงดังรูปที่ 2 ทำให้ผู้ทดสอบทราบว่าสามารถเข้าถึงเซอร์วิสต่าง ๆ ได้โดยตรง เนื่องจากมีสถานะเป็น Open (ไม่ได้รับการฟิลเตอร์จากไฟร์วอลล์อย่างเหมาะสม) เช่น 21(FTP), 1433 (MSSQL), 3389 (Terminal Service), 4899 (Radmin) ผู้ทดสอบจึงได้เชื่อมต่อผ่านพอร์ตต่าง ๆ ไปยังเครื่องเป้าหมาย ซึ่งสามารถเข้าถึงได้โดยตรง และถือเป็นความเสี่ยง เนื่องจากหากผู้ทดสอบสามารถคาดเดาชื่อผู้ใช้ และรหัสผ่าน (Password)ได้ จะสามารถเข้าครอบครองทรัพยากรบนเครื่องคอมพิวเตอร์แม่ข่ายได้โดยง่าย

4. ผู้ทดสอบได้เข้าระบบ FTP และทดลองคาดเดารหัสผ่าน (Password)ที่ง่ายต่อการคาดเดา แต่ไม่สามารถล็อกอินเข้าระบบได้ แต่สามารถเข้าถึงด้วยสิทธิ์ Anonymous แต่สิทธิ์ดังกล่าว ไม่สามารถทำการดาวโหลดไฟล์ หรืออัพโหลดไฟล์ต่าง ๆ ได้ แสดงได้ดังรูปที่ 3

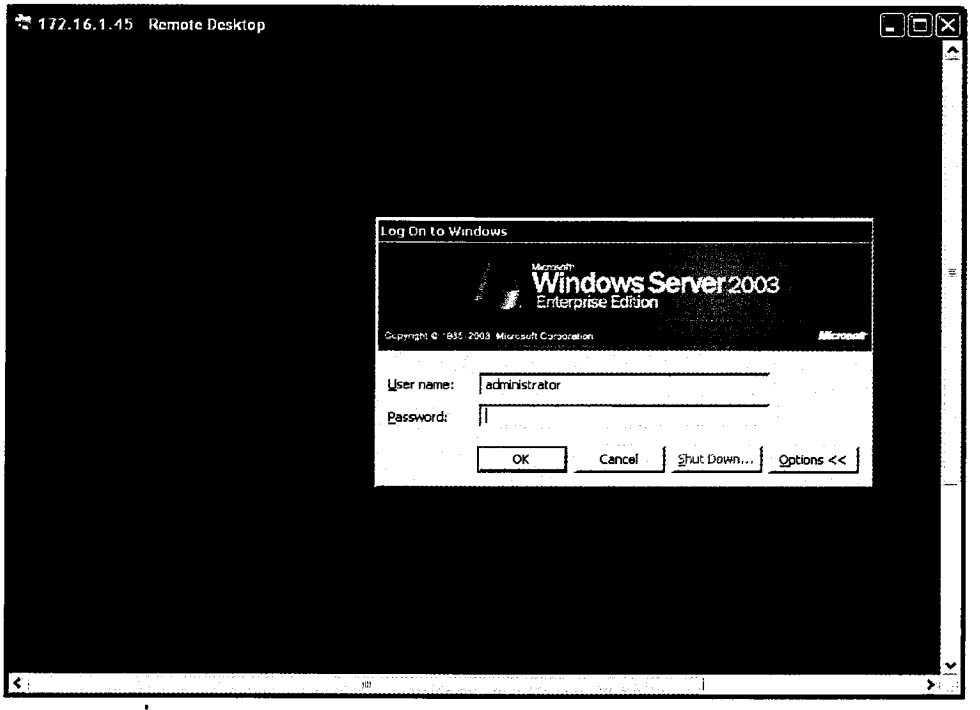


รูปที่ 3 การทดสอบเข้าถึงระบบ FTP ด้วยสิทธิ์ Anonymous

5. ผู้ทดสอบทำการเชื่อมต่อไปยัง Remote Desktop และ Radmin แสดงได้ดังรูปที่ 4 และ 5 โดยทำการคาดเดารหัสผ่าน (Password)ที่ง่ายต่อการคาดเดา แต่ไม่สามารถเข้าสู่ระบบภายในได้

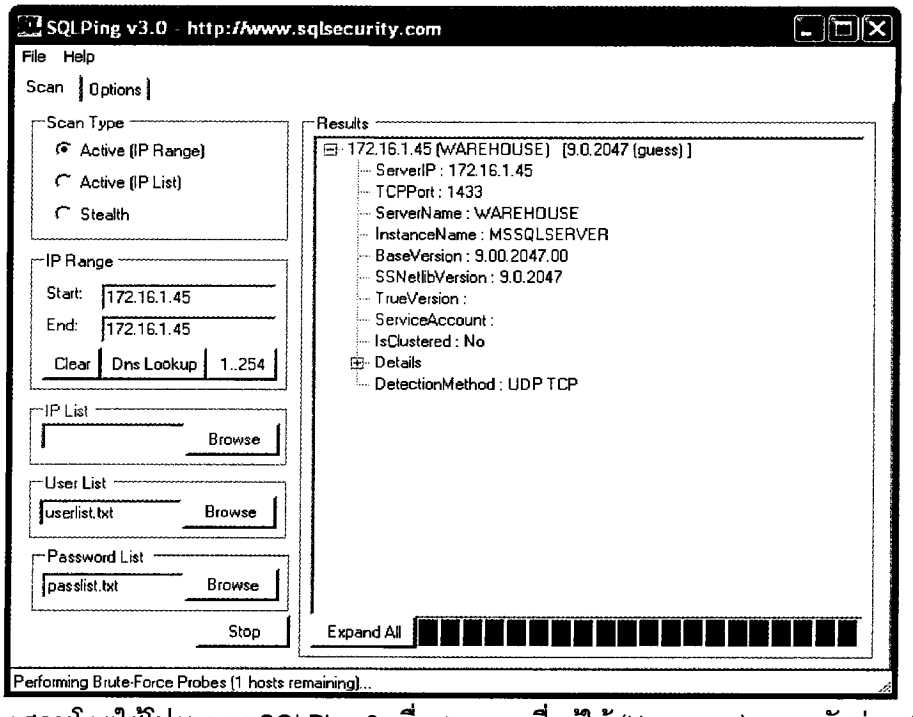


รูปที่ 4 การทดสอบคาดเดารหัสผ่าน (Password)ของ Radmin



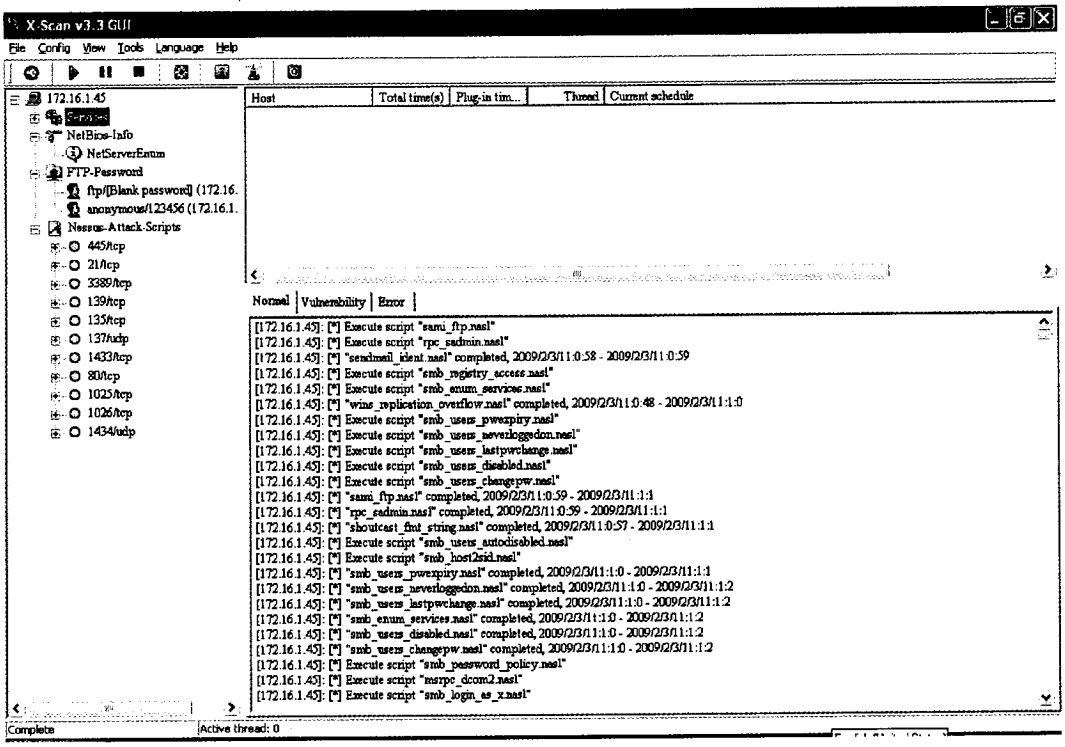
รูปที่ 5 การทดสอบคาดเดารหัสผ่าน (Password)ของ Remote Desktop

6. ผู้ทดสอบพบว่าเครื่องเป้าหมายมีการใช้งาน MSSQL จึงใช้โปรแกรม SQLPing3 ทำการสแกนหาชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)ที่ง่ายต่อการคาดเดา แสดงได้ดังรูปที่ 6 แต่ไม่สามารถเข้าถึงระบบได้ เนื่องจากมีการใช้รหัสผ่าน (Password)ที่ยากต่อการคาดเดา



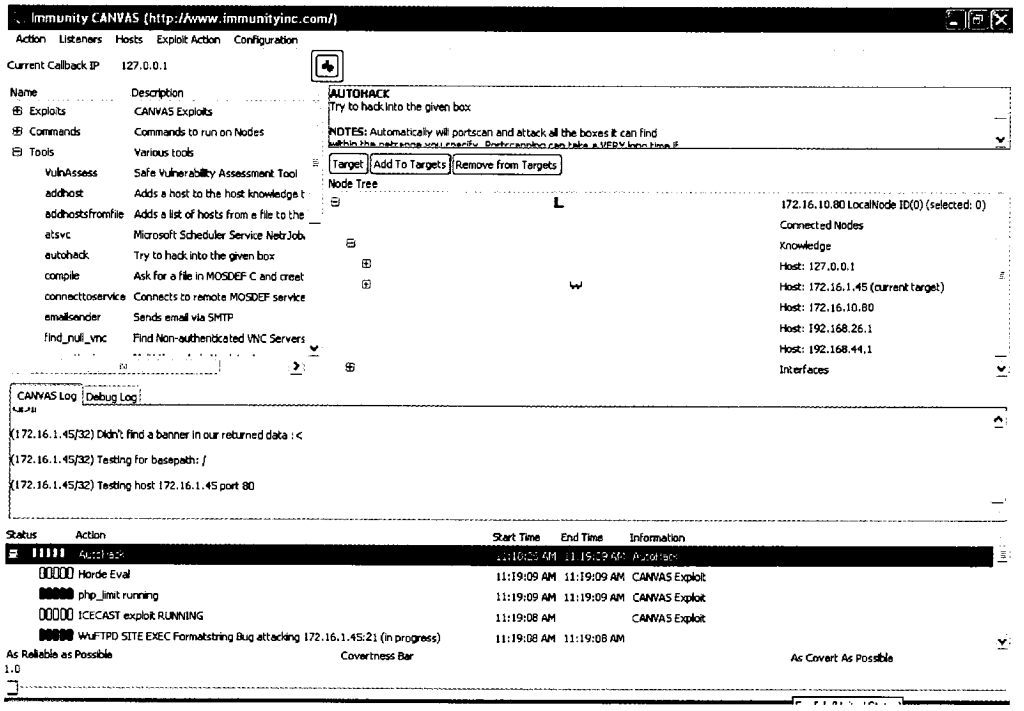
รูปที่ 6 การทดสอบโดยใช้โปรแกรม SQLPing 3 เพื่อสแกนหาชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) (Password)ของ MSSQL

7. ผู้ทดสอบใช้โปรแกรม X-scan ทำการสแกนช่องโหว่ของระบบปฏิบัติการวินโดวส์ และทดลองสุมชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)ที่ง่ายต่อการคาเดา ผ่านทางพอร์ตต่าง ๆ ที่สามารถเข้าถึงได้ แสดงได้ดังรูปที่ 7 แต่ไม่พบว่าระบบมีช่องโหว่ใด ๆ



รูปที่ 7 การทดสอบโดยใช้โปรแกรม X-scan สแกนหาช่องโหว่

8. ผู้ทดสอบใช้โปรแกรม CANVAS เพื่อสแกนหาช่องโหว่ของระบบปฏิบัติการวินโดวส์ แสดงได้ดังรูปที่ 8 แต่ไม่พบว่ามีช่องโหว่ใด ๆ เนื่องจากเครื่องเป้าหมายของ สป.ทส. มีความปลอดภัย



รูปที่ 8 การทดสอบโดยใช้โปรแกรม CANVAS สแกนหาช่องโหว่

สิ่งที่พบจากการทดสอบ

จากการทดสอบเจาะระบบเครื่องคอมพิวเตอร์แม่ข่าย WAREHOUSE ผู้ทดสอบไม่สามารถเจาะระบบเครื่องคอมพิวเตอร์แม่ข่ายดังกล่าวได้ เนื่องจากผู้ทดสอบไม่พบช่องโหว่ที่ทำให้สามารถยึดครองเครื่องคอมพิวเตอร์แม่ข่ายได้สำเร็จ แต่หากผู้บุกรุกหรือผู้ไม่หวังดีทราบรหัสผ่าน (Password)ของเครื่องคอมพิวเตอร์แม่ข่ายดังกล่าว ก็จะสามารถยึดครองเครื่องคอมพิวเตอร์แม่ข่ายได้โดยง่าย

จากการทดสอบสามารถสรุปสิ่งที่พบจากการทดสอบได้ดังนี้

- สามารถเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายได้โดยตรง
- สามารถเข้าถึงพอร์ตต่าง ๆ ของเครื่องคอมพิวเตอร์แม่ข่ายดังกล่าวได้
- สามารถล็อกอิน FTP ด้วยสิทธิ์ Anonymous แต่ไม่สามารถอัพโหลดไฟล์ใด ๆ ได้
- พบว่าเครื่องคอมพิวเตอร์แม่ข่ายดังกล่าวมีการใช้งานทั้ง Radmin และ Terminal Service

คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- Ability to Enumerate Server in Network

ผลกระทบทางเทคนิค: ปานกลาง

เนื่องจากไม่มีการฟิลเตอร์การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายอย่างเหมาะสม ทำให้ผู้ทดสอบสามารถเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายต่าง ๆ ได้โดยตรงซึ่งถือเป็นความเสี่ยง จึงควรแก้ไขโดยการฟิลเตอร์การเข้าถึงเครื่อง

คอมพิวเตอร์แม่ข่ายอย่างเหมาะสม โดยกำหนดเครือข่ายผู้ดูแลระบบที่สามารถเข้าถึงได้โดยตรง และเครือข่ายผู้ใช้งานที่ไม่สามารถเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

- Ports Open on the Firewall

ผลกระทบทางเทคนิค: ปานกลาง

เนื่องจากไม่มีการฟิลเตอร์การเข้าถึงพอร์ตและเซอร์วิสอย่างเหมาะสม ทำให้ผู้ทดสอบสามารถเข้าถึงพอร์ต สำคัญต่าง ๆ ได้โดยตรงซึ่งถือเป็นความเสี่ยง จึงควรแก้ไขโดยการฟิลเตอร์การเข้าถึงพอร์ตและเซอร์วิสของเครื่องคอมพิวเตอร์แม่ข่ายอย่างเหมาะสม โดยกำหนดเครือข่ายผู้ดูแลระบบที่สามารถเข้าถึงได้โดยตรง และเครือข่ายผู้ใช้งานที่ไม่สามารถเข้าถึงได้

1.2 ผลการทดสอบเจาะระบบเครื่องคอมพิวเตอร์แม่ข่าย: E-PETITION

ตารางที่ 6 ผลกระทบทางเทคนิค โอกาสที่จะเกิด และความเสี่ยงทางเทคนิคของเครื่องคอมพิวเตอร์แม่ข่าย: E-PETITION

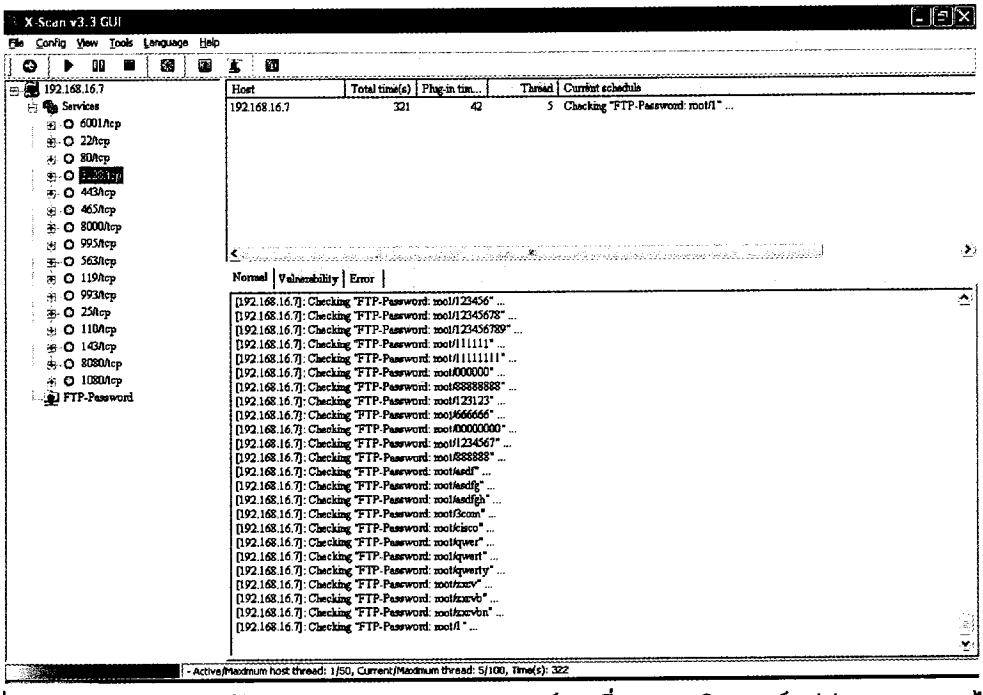
ผลกระทบทางเทคนิค: ระดับปานกลาง
สิ่งที่พบ เครื่องคอมพิวเตอร์แม่ข่าย: E-PETITION มีผลกระทบทางเทคนิคอยู่ในระดับปานกลาง เนื่องจากถึงแม้ว่าผู้ทดสอบจะไม่สามารถเจาะระบบเครื่องคอมพิวเตอร์แม่ข่ายดังกล่าวได้ เนื่องจากผู้ทดสอบไม่พบช่องโหว่ที่ทำให้สามารถยึดครองเครื่องคอมพิวเตอร์แม่ข่ายได้สำเร็จ แต่หากผู้บุกรุกหรือผู้ไม่หวังดีทราบรหัสผ่าน (Password)ของเครื่องคอมพิวเตอร์แม่ข่ายดังกล่าว ก็จะสามารถยึดครองเครื่องคอมพิวเตอร์แม่ข่ายได้โดยง่าย
โอกาสที่จะเกิด: ระดับต่ำ
สิ่งที่พบ เครื่องคอมพิวเตอร์แม่ข่าย: E-PETITION มีโอกาสที่จะถูกเจาะระบบจากผู้บุกรุกในระดับต่ำ เนื่องจากผู้ทดสอบไม่พบช่องโหว่ที่ทำให้สามารถยึดครองเครื่องคอมพิวเตอร์แม่ข่ายได้สำเร็จ
ความเสี่ยงทางเทคนิค: ระดับปานกลาง
สิ่งที่พบ เครื่องคอมพิวเตอร์แม่ข่าย: E-PETITION มีความเสี่ยงทางเทคนิคอยู่ในระดับปานกลาง ซึ่งได้จากการคำนวณผลกระทบทางเทคนิค (ระดับปานกลาง) และโอกาสที่จะเกิด(ระดับต่ำ) นำมาเปรียบเทียบกับตารางที่ 3.2 ทำให้พบว่าความเสี่ยงทางเทคนิคอยู่ในระดับปานกลาง

ตารางที่ 7 ความสูญเสียด้าน Confidentiality Integrity และ Availability ของเครื่องคอมพิวเตอร์แม่ข่าย: E-PETITION

ความสูญเสียด้าน Confidentiality: ไม่มีผลกระทบ
สิ่งที่พบ : ไม่พบปัจจัยที่ส่งผลต่อความสูญเสียด้าน Confidentiality
ความสูญเสียด้าน Integrity: ไม่มีผลกระทบ
สิ่งที่พบ : ไม่พบปัจจัยที่ส่งผลต่อความสูญเสียด้าน Integrity
ความสูญเสียด้าน Availability: ไม่มีผลกระทบ
สิ่งที่พบ : ไม่พบปัจจัยที่ส่งผลต่อความสูญเสียด้าน Availability

ขั้นตอนในการทดสอบ

1. ผู้ทดสอบใช้โปรแกรม X-scan เพื่อสแกนพอร์ต สแกนหาช่องโหว่ของระบบปฏิบัติการ และสแกนหาชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)ที่ง่ายต่อการคาดเดา แสดงได้ดังรูปที่ 9 ซึ่งจากการทดสอบไม่พบว่ามีช่องโหว่ใด ๆ



รูปที่ 9 การทดสอบโดยใช้โปรแกรม X-scan สแกนพอร์ตเครื่องคอมพิวเตอร์แม่ข่ายหมายเลขไอพี 192.168.16.7

2. จากผลการสแกนพอร์ตด้วยโปรแกรม X-scan ซึ่งแสดงในรูปที่ 9 ทำให้ผู้ทดสอบทราบว่าสามารถเข้าถึงเซอร์วิสต่าง ๆ ได้โดยตรง เนื่องจากมีสถานะเป็น Open (ไม่ได้รับการฟิลเตอร์จากไฟร์วอลล์อย่างเหมาะสม) ซึ่งถือเป็นความเสี่ยงของระบบ

3. จากผลการสแกนพอร์ตทำให้ผู้ทดสอบทราบว่าระบบมีการใช้ SSH ผู้ทดสอบจึงคาดเดารหัสผ่าน (Password)ที่ง่ายต่อการคาดเดา แต่ไม่สามารถเข้าสู่ระบบภายในได้ แสดงดังรูปที่ 10

รูปที่ 10 การทดสอบโดยใช้โปรแกรม Putty

สิ่งที่พบจากการทดสอบ

จากการทดสอบเจาะระบบเครื่องคอมพิวเตอร์แม่ข่าย E-PETITION ผู้ทดสอบไม่สามารถเจาะระบบเครื่องคอมพิวเตอร์แม่ข่ายดังกล่าวได้ เนื่องจากผู้ทดสอบไม่พบช่องโหว่ที่ทำให้สามารถยึดครองเครื่องคอมพิวเตอร์แม่ข่ายได้สำเร็จ

จากการทดสอบสามารถสรุปสิ่งที่พบจากการทดสอบได้ดังนี้

- สามารถเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายและพอร์ตต่าง ๆ ได้โดยตรง
- สามารถเข้าถึงพอร์ตต่าง ๆ ของเครื่องเป้าหมายได้
- พบว่ามีการใช้งาน SSH และสามารถเข้าถึงเซอร์วิสดังกล่าวได้โดยตรง

คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- Ability to Enumerate Server in Network

ผลกระทบทางเทคนิค: กลาง

เนื่องจากไม่มีการฟิลเตอร์การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายอย่างเหมาะสม ทำให้ผู้ทดสอบสามารถเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายต่าง ๆ ได้โดยตรง ซึ่งมีความเสี่ยง จึงควรแก้ไขโดยการฟิลเตอร์การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายอย่างเหมาะสม โดยกำหนดเครือข่ายผู้ดูแลระบบที่สามารถเข้าถึงได้โดยตรง และเครือข่ายผู้ใช้งานที่ไม่สามารถเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

- Ports Open on the Firewall

ผลกระทบทางเทคนิค: กลาง

เนื่องจากไม่มีการฟิลเตอร์การเข้าถึงพอร์ตและเซอร์วิสอย่างเหมาะสม ทำให้ผู้ทดสอบสามารถเข้าถึงพอร์ต สำคัญต่าง ๆ ได้โดยตรง ซึ่งมีความเสี่ยงสูง จึงควรแก้ไขโดยการฟิลเตอร์การเข้าถึงพอร์ตและเซอร์วิสของเครื่องคอมพิวเตอร์แม่ข่ายอย่างเหมาะสม โดยกำหนดเครือข่ายผู้ดูแลระบบที่สามารถเข้าถึงได้โดยตรง และเครือข่ายผู้ใช้งานที่ไม่สามารถเข้าถึงได้

2. ผลการวิเคราะห์ช่องโหว่ที่พบ

จากการทดสอบเจาะระบบ ที่ปรึกษาได้นำช่องโหว่ที่พบมาวิเคราะห์ เพื่อหาสาเหตุของการเกิดช่องโหว่ในระบบเครือข่ายภายใน โดยสามารถสรุปประเด็น ดังนี้

2.1 สามารถเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายและพอร์ตต่าง ๆ ได้โดยตรง

จากการทดสอบเจาะระบบ พบว่าสามารถเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายของ สป.ทส. ได้โดยตรง ซึ่งเป็นความเสี่ยงเนื่องจากพนักงาน ผู้รับจ้างเหมาพัฒนาระบบแบบ Outsource หรือเวนเดอร์ จะสามารถเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายและพอร์ตต่าง ๆ ได้โดยตรงเช่นกัน

(1) ผลกระทบ (Impact)

- มีโอกาสที่พนักงาน ผู้รับจ้างเหมาพัฒนาระบบแบบ Outsource หรือเวนเดอร์ จะสามารถเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย และสามารถเจาะระบบเครื่องคอมพิวเตอร์แม่ข่ายของ สป.ทส.

(2) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

- ควรแก้ไขโดยการฟิลเตอร์การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายอย่างเหมาะสม โดยกำหนดเครือข่ายผู้ดูแลระบบที่สามารถเข้าถึงได้โดยตรง และเครือข่ายผู้ใช้งานที่ไม่สามารถเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

2.2 การเปิดใช้งานเซอร์วิสที่มีหน้าที่การทำงานเดียวกัน

จากการทดสอบเจาะระบบ พบว่าเครื่องคอมพิวเตอร์แม่ข่าย WAREHOUSE มีการใช้งาน Radmin และ Terminal Service ซึ่งมีหน้าที่การทำงานเดียวกัน แต่หากมีการใช้งานทั้งสองโปรแกรม จะเป็นการเพิ่มช่องทางให้ผู้ไม่หวังดีโจมตีเครื่องคอมพิวเตอร์แม่ข่ายดังกล่าว

(1) ผลกระทบ (Impact)

มีโอกาสที่พนักงาน ผู้รับจ้างเหมาพัฒนาระบบแบบ Outsource หรือเวนเดอร์ จจะสามารถคาดเดา หรือรู้รหัสผ่าน (Password)ของ Radmin และ Terminal Service และสามารถเจาะระบบเครื่องคอมพิวเตอร์แม่ข่ายของ สป.ทส.

(2) คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

สป.ทส. ควรเลือกใช้ Radmin หรือ Terminal Service อย่างใดอย่างหนึ่ง เพื่อลดช่องทางที่จะถูกโจมตีจากผู้ไม่หวังดี ซึ่งอาจเป็น พนักงาน ผู้รับจ้างเหมาพัฒนาระบบแบบ Outsource หรือเวนเดอร์ ซึ่งสามารถเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายดังกล่าว

สรุปผลการดำเนินการ

จากผลการทดสอบเจาะระบบเครือข่ายภายในของ ของ สป.ทส. ทั้งหมด 2 หมายเลขไอพี ที่ปรึกษาได้นำเสนอไว้ในรายงานฉบับนี้แล้วนั้น ที่ปรึกษา จึงใคร่ขอเรียนผลการสำรวจ และข้อแนะนำในการปรับปรุงดังต่อไปนี้

ผลการสำรวจ

1. เครื่องคอมพิวเตอร์แม่ข่าย: WAREHOUSE

ที่ปรึกษาพบว่าเครื่องคอมพิวเตอร์แม่ข่าย WAREHOUSE (หมายเลขไอพี 172.16.1.45) มีความเสี่ยงที่จะถูกเจาะระบบอยู่ในระดับปานกลาง ซึ่งแม้ว่าในการทดสอบจะไม่สามารถยึดครองเครื่องคอมพิวเตอร์แม่ข่ายดังกล่าว แต่สามารถเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายได้โดยตรง ซึ่งหากมีผู้ไม่หวังดีภายในองค์กร เช่น พนักงาน ผู้รับจ้างเหมาพัฒนาระบบแบบ Outsource หรือเวนเดอร์ ที่อาจมีความประสงค์ร้ายเข้ามาใช้งานเครือข่ายภายในองค์กร ก็สามารถเข้าถึง และโจมตีเครื่องคอมพิวเตอร์แม่ข่ายได้โดยตรง

2. เครื่องคอมพิวเตอร์แม่ข่าย: E-PETITION

ที่ปรึกษาพบว่าเครื่องคอมพิวเตอร์แม่ข่าย E-PETITION (หมายเลขไอพี 192.168.16.7) มีความเสี่ยงที่จะถูกเจาะระบบอยู่ในระดับปานกลาง ซึ่งแม้ว่าในการทดสอบจะไม่สามารถยึดครองเครื่องคอมพิวเตอร์แม่ข่ายดังกล่าว แต่สามารถเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายได้โดยตรง ซึ่งหากมีผู้ไม่หวังดีภายในองค์กร เช่นพนักงาน ผู้รับจ้างเหมาพัฒนาระบบแบบ Outsource หรือเวนเดอร์ ที่อาจมีความประสงค์ร้ายเข้ามาใช้งานเครือข่ายภายในองค์กร ก็สามารถเข้าถึง และโจมตีเครื่องคอมพิวเตอร์แม่ข่ายได้โดยตรง

คำแนะนำ/ข้อเสนอแนะและแนวทางในการปรับปรุง

1. เนื่องจากไม่มีการฟิลเตอร์การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายอย่างเหมาะสม ทำให้ผู้ทดสอบสามารถเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายต่าง ๆ ได้โดยตรง ซึ่งมีความเสี่ยงสูง จึงควรแก้ไขโดยการฟิลเตอร์การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายอย่างเหมาะสม โดยกำหนดเครือข่ายผู้ดูแลระบบที่สามารถเข้าถึงได้โดยตรง และเครือข่ายผู้ใช้งานที่ไม่สามารถเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

2. เนื่องจากไม่มีการฟิลเตอร์การเข้าถึงพอร์ตและเซอร์วิสอย่างเหมาะสม ทำให้ผู้ทดสอบสามารถเข้าถึงพอร์ตสำคัญต่าง ๆ ได้โดยตรง ซึ่งมีความเสี่ยงสูง จึงควรแก้ไขโดยการฟิลเตอร์การเข้าถึงพอร์ตและเซอร์วิสของเครื่องคอมพิวเตอร์แม่ข่ายอย่างเหมาะสม โดยกำหนดเครือข่ายผู้ดูแลระบบที่สามารถเข้าถึงได้โดยตรง และเครือข่ายผู้ใช้งานที่ไม่สามารถเข้าถึงได้

ภาคผนวก ก. รายละเอียดการเข้าดำเนินการ

ADVANCED CERTIFIED INFORMATION SECURITY PROFESSIONAL CENTER

COPY

" Security Intelligence "

ที่ LT.ISCBU.BD.52-007

13 มกราคม 2552

เรื่อง ขอเข้าดำเนินงานสำรวจสถานภาพด้านความปลอดภัยของระบบเครือข่าย และระบบความปลอดภัยคอมพิวเตอร์พร้อมทั้งดำเนินงานถ่ายทอดความรู้และเทคโนโลยีควบคู่ไปกับการปฏิบัติงาน โครงการจัดจ้างที่ปรึกษาประเมินความเสี่ยงด้านสารสนเทศและการแก้ปัญหา

เรียน ประธานคณะกรรมการตรวจรับโครงการฯ

อ้างถึง สัญญาเลขที่ 0202/30/2552 ลงวันที่ 21 พฤศจิกายน 2551

ตามที่บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด ได้รับมอบหมายให้ดำเนินงานโครงการจัดจ้างที่ปรึกษาประเมินความเสี่ยงด้านสารสนเทศและการแก้ปัญหาของสำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม ตามสัญญาที่อ้างถึงนั้น โดยมีขอบเขตการดำเนินงานบางส่วนเกี่ยวข้องกับการสำรวจสถานภาพด้านความปลอดภัยของระบบเครือข่าย และระบบความปลอดภัยคอมพิวเตอร์ พร้อมทั้งดำเนินงานถ่ายทอดความรู้และเทคโนโลยีควบคู่ไปกับการปฏิบัติงานในแต่ละขั้นตอน

บริษัทฯ มีความประสงค์ใคร่ขอเข้าดำเนินงานดังกล่าว และขอเชิญบุคคลากรของทางสำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อมเข้าร่วมการดำเนินงานถ่ายทอดความรู้ และเทคโนโลยีควบคู่ไปกับการปฏิบัติงาน ตั้งแต่วันที่ 15 – 30 มกราคม 2552 โดยมีบุคลากรของบริษัทฯ ที่จะเข้าดำเนินงานดังต่อไปนี้

1. นายนิพนธ์ นาชิน
2. นายปิยะภัทร์ ชวีพัตน์
3. นายประวิทย์ ปิ่นเกตุ
4. นายจตุพล นิลพรัตน์
5. นายอนันต์ โชนี่
6. นายประธาน พงศ์ทิพย์ฤกษ์
7. นายนิสิต บุษราคัมมงคล

จึงเรียนมาเพื่อโปรดพิจารณา

ได้รับเรื่องแล้ว
13 / ม.ค. / 52

ขอแสดงความนับถือ

(นายสรวุฒิ ก้องกิดิกุล)
ผู้จัดการโครงการ
กลุ่มธุรกิจที่ปรึกษาด้านความปลอดภัยสารสนเทศ
บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด

ACIS PROFESSIONAL CENTER Co., Ltd.
2101, 21ST FLOOR, 62 THE MILLENNIA BUILDING, LUNGSUAN RD., LUMPINI, PATHUMWAN, BANGKOK 10330
TEL +66 0 2650 5771 FAX +66 0 2650 5776
http://www.acisonline.net

ADVANCED CERTIFIED INFORMATION SECURITY PROFESSIONAL CENTER

COPY

" Security Intelligence "

ที่ LT.ISCBU.BD.52-024

3 กุมภาพันธ์ 2552

เรื่อง ขอขยายระยะเวลาเข้าดำเนินงานสำรวจสถานภาพด้านความปลอดภัยของระบบเครือข่าย และระบบความปลอดภัยคอมพิวเตอร์พร้อมทั้งดำเนินงานถ่ายทอดความรู้และเทคโนโลยีควบคู่ไปกับการปฏิบัติงานโครงการจัดจ้างที่ปรึกษาประเมินความเสี่ยงด้านสารสนเทศและการแก้ปัญหา

เรียน ประธานคณะกรรมการตรวจรับโครงการฯ

อ้างถึง สัญญาเลขที่ 0202/30/2552 ลงวันที่ 21 พฤศจิกายน 2551
เอกสารเลขที่ LT.ISCBU.BD.52-007 ลงวันที่ 13 มกราคม 2552

ตามที่บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด ได้รับมอบหมายให้ดำเนินงานโครงการจัดจ้างที่ปรึกษาประเมินความเสี่ยงด้านสารสนเทศและการแก้ปัญหาของสำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม ตามสัญญาที่อ้างถึงนั้น โดยมีขอบเขตการดำเนินงานบางส่วนเกี่ยวข้องกับการสำรวจสถานภาพด้านความปลอดภัยของระบบเครือข่าย และระบบความปลอดภัยคอมพิวเตอร์ พร้อมทั้งดำเนินงานถ่ายทอดความรู้และเทคโนโลยีควบคู่ไปกับการปฏิบัติงานในแต่ละขั้นตอน

บริษัทฯ มีความประสงค์ใคร่ขอขยายระยะเวลาเข้าดำเนินงานดังกล่าวเพิ่มเติม และขอเชิญบุคคลากรของทางสำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อมเข้าร่วมการฝึกอบรมถ่ายทอดความรู้ และเทคโนโลยีควบคู่ไปกับการปฏิบัติงาน ตั้งแต่วันที่ 3 - 13 กุมภาพันธ์ 2552 โดยมีบุคลากรของบริษัทฯ ที่จะเข้าดำเนินงานดังต่อไปนี้

1. นายนิพนธ์ นาชิน
2. นายนิสิต บุษราคัมมงคล
3. นายประวิทย์ ปิ่นเกตุ
4. นายจตุพล นิลพรัตน์
5. นายอนันต์ โชนี่
6. นายประธาน พงศ์ทิพย์ฤกษ์

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ

(สราวุฒิ ก้องกิติกุล)
ผู้จัดการโครงการ
กลุ่มธุรกิจที่ปรึกษาด้านความปลอดภัยสารสนเทศ
บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด

( ) ลายมือชื่อ
ผู้รับเอกสาร
3 ก.พ. 52

ACIS PROFESSIONAL CENTER Co., Ltd.
2101, 21ST FLOOR, 62 THE MILLENNIA BUILDING, LUNGSUAN RD., LUMPINI, PATHUMWAN, BANGKOK 10330
TEL +66 0 2650 5771 FAX +66 0 2650 5776
http://www.acisonline.net

))

สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม

โครงการจัดจ้างที่ปรึกษาประเมินความเสี่ยงด้านสารสนเทศและการแก้ปัญหา

การดำเนินการสำรวจสถานภาพด้านความมปลอดภัยของระบบเครือข่ายและระบบความปลอดภัยคอมพิวเตอร์พร้อมทั้งถ่ายทอดความรู้และเทคโนโลยีควบคู่ไปกับการปฏิบัติงาน

Date/Time:	15 January 2009	Venue:	สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม

MNRE

No.	Name & Family Name	Signed
1	กฤตชัย เหมือนวัฒนากุล	
2	ชัยสิทธิ์ ลภกรัตน์	
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		

ACIS

No.	Name & Family Name	Signed
1	ณ:วิทย์ วิไลเกตุ	
2	[illegible]	
3	ฟิสิตา บุญรักษ์สมบูรณ์	
4		
5		
6		
7		
8		
9		
10		
11		
12		

Organized by: ACIS Professional Center Company Limited

))

สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม

โครงการจัดจ้างที่ปรึกษาประเมินความเสี่ยงด้านสารสนเทศและการแก้ปัญหา

การดำเนินการสำรวจสถานภาพด้านความมปลอดภัยของระบบเครือข่ายและระบบความปลอดภัยคอมพิวเตอร์พร้อมทั้งถ่ายทอดความรู้และเทคโนโลยีควบคู่ไปกับการปฏิบัติงาน

Date/Time:	20 January 2021	Venue:	สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม

MNRE

No.	Name & Family Name	Signed
1	กฤตธีร์ เสืองามขำ	
2	[illegible]	
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		

ACIS

No.	Name & Family Name	Signed
1	[illegible]	
2	[illegible]	
3	[illegible]	
4		
5		
6		
7		
8		
9		
10		
11		
12		

Organized by: ACIS Professional Center Company Limited

))

สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม

โครงการจัดจ้างที่ปรึกษาประเมินความเสี่ยงด้านสารสนเทศและการแก้ปัญหา

การดำเนินการสำรวจสถานภาพด้านความมปลอดภัยของระบบเครือข่ายและระบบความปลอดภัยคอมพิวเตอร์พร้อมทั้งถ่ายทอดความรู้และเทคโนโลยีควบคู่ไปกับการปฏิบัติงาน

Date/Time:	21 January 2009	Venue:	สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม

MNRE

No.	Name & Family Name	Signed
1	กฤตชัย เหลืองวิวัฒนกุล	
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		

ACIS

No.	Name & Family Name	Signed
1	ปกรณ์ ปิยนาฏ	
2	[illegible]	
3	[illegible]	
4		
5		
6		
7		
8		
9		
10		
11		
12		

Organized by: ACIS Professional Center Company Limited

สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม

โครงการจัดจ้างที่ปรึกษาประเมินความเสี่ยงด้านสารสนเทศและการแก้ปัญหา

การดำเนินการสำรวจสถานภาพด้านความมปลอดภัยของระบบเครือข่ายและระบบความปลอดภัยคอมพิวเตอร์พร้อมทั้งถ่ายทอดความรู้และเทคโนโลยีควบคู่ไปกับการปฏิบัติงาน

Date/Time:	3 February 2009	Venue:	สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม

MNRE

No.	Name & Family Name	Signed
1	[illegible]	[illegible]
2	[illegible]	[illegible]
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		

Organized by: ACIS Professional Center Company Limited

ACIS

No.	Name & Family Name	Signed
1	[illegible]	[illegible]
2	[illegible]	[illegible]
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		

))

สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม

โครงการจัดจ้างที่ปรึกษาประเมินความเสี่ยงด้านสารสนเทศและการแก้ปัญหา

[redacted]สำรวจสถานภาพด้านความมปลอดภัยของระบบเครือข่ายและระบบความปลอดภัยคอมพิวเตอร์พร้อมทั้งถ่ายทอดความรู้และเทคโนโลยีควบคู่ไปกับการปฏิบัติงาน

Date/Time:	4 February 2009	Venue:	สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม

MNRE

No.	Name & Family Name	Signed
1	กฤตชัย เหลืองวิวัฒนากุล	
2	ปิยะสิทธิ์ มากทรัพย์	
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		

ACIS

No.	Name & Family Name	Signed
1	[illegible]	
2	[illegible]	
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		

Organized by: ACIS Professional Center Company Limited

สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม

โครงการจัดจ้างที่ปรึกษาประเมินความเสี่ยงด้านสารสนเทศและการแก้ปัญหา

การดำเนินการสำรวจสถานภาพด้านความมปลอดภัยของระบบเครือข่ายและระบบความปลอดภัยคอมพิวเตอร์พร้อมทั้งถ่ายทอดความรู้และเทคโนโลยีควบคู่ไปกับการปฏิบัติงาน

Date/Time:	11 February 2009	Venue:	สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม

MNRE

No.	Name & Family Name	Signed
1	กฤตชัย เหลืองวิวัฒนากุล	
2	ปิยะเลิศ ลาภทรัพย์	
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		

Organized by: ACIS Professional Center Company Limited

ACIS

No.	Name & Family Name	Signed
1	[illegible]	
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		