การประยุกต์ระบบฮันนีพอตเพื่อเก็บล็อกวิเคราะห์การโจมตี

Application of Honeypot System for log Analysis

นางสาว ณัฐวรา เกษจันทร์

โครงงานสหกิจศึกษานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิทยาศาสตร์บัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยี ไทย-ญี่ปุ่น
พ.ศ. 2561

การประยุกต์ระบบฮันนีพอตเพื่อเก็บล็อกวิเคราะห์การโจมตี

Application of Honeypot System for log Analysis

นางสาว ณัฐวรา เกษจันทร์

โครงงานสหกิจศึกษานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

วิทยาศาสตร์บัณฑิต สาขาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีไทย - ญี่ปุ่น

ปีการศึกษา 2561

คณะกรรมการสอบ

…….. ประธานกรรมการสอบ

(อาจารย์ ตรีรัตน เมตต์การุณ์จิต)

…….. กรรมการสอบ

(อาจารย์ ลลิตา ณ หนองคาย)

…….. อาจารย์ที่ปรึกษา

(อาจารย์ ปราณิสา อิศรเสนา)

…….. ประธานสหกิจศึกษาสาขาวิชา

(อาจารย์ สลิลา ชีวกิดาการ)

ชื่อโครงงาน การประยุกต์ระบบฮันนีพอตเพื่อเก็บล็อกวิเคราะห์การโจมตี

Application of Honeypot System for log Analysis

ผู้เขียน นางสาวณัฐวรา เกษจันทร์

คณะวิชา เทคโนโลยีสารสนเทศ **สาขาวิชา** เทคโนโลยีสารสนเทศ

อาจารย์ที่ปรึกษา อาจารย์ ปราณิสา อิศรเสนา

พนักงานที่ปรึกษา คุณพงศกร เอกวิจิตรกุล

ชื่อบริษัท บริษัท โซซิเคียว จำกัด

ประเภทธุรกิจ/สินค้า Security

บทสรุป

บริษัท โซซีเคียว จำกัด มีความต้องการที่จะศึกษาพฤติกรรมของแฮกเกอร์ที่มีการโจมตีเข้ามาในระบบ ไม่ว่าจะเป็นการโจมตีของไวรัส จากแฮกเกอร์ เพื่อที่จะนำข้อมูลไปวิเคราะห์เพื่อป้องกันและนำไปสร้างเป็นโซลูชั่นอื่นๆ จึงเป็นที่มาของระบบฮันนีพอตและข้อมูลจากล็อกไฟล์ ซึ่งเป็นงานที่นักศึกษารับผิดชอบในการสร้างทั้งหมด เพื่อให้ทางบริษัทสามารถนำข้อมูลไปวิเคราะห์เพื่อนำไปสร้างโซลูชั่นของบริษัทและทำให้ระบบของบริษัทมีความปลอดภัยมากขึ้น

กิตติกรรมประกาศ

การที่ได้มีโอกาสมาปฏิบัติสหกิจศึกษาที่ บริษัท โซซีเคียว จำกัด เป็นโอกาสที่ดีโอกาสหนึ่ง ที่จะได้เรียนรู้วิธีการทำงานด้วยสถานการณ์จริง ลูกค้าจริง งานจริง ก่อนที่จะจบการศึกษาจากสถาบัน และเข้าสู่การทำงานจริงต่อไป ซึ่งการปฏิบัติสหกิจศึกษาครั้งนี้ ก็สำเร็จลุล่วงไปด้วยดี โดยได้รับการสนับสนุนให้คำแนะนำ คำปรึกษา จากบุคคลหลายๆ ท่าน รวมไปถึงบริษัท โซซีเคียว จำกัด ที่ให้โอกาสเข้ามาปฏิบัติสหกิจศึกษา

ขอขอบคุณพี่ๆ แผนก Security ทุกท่าน สำหรับความรู้ และแนวทางการปฏิบัติงาน ซึ่งทำให้เกิดประสบการณ์ที่เป็นประโยชน์อย่างมากในการปฏิบัติสหกิจศึกษาครั้งนี้ และยังทำให้รู้ถึงปัญหาที่เกิดขึ้นระหว่างการทำงาน ที่จะนำไปสู่แนวคิดที่จะแก้ปัญหา และนำมาสู่โครงงานสหกิจศึกษานี้ และขอขอบคุณอาจารย์ที่ปรึกษา อาจารย์ปราณิสา อิศรเสนา และคณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีไทย-ญี่ปุ่น ที่ให้การสนับสนุน ให้คำแนะนำ และให้ความช่วยเหลือตลอดระยะเวลาที่ปฏิบัติสหกิจศึกษา

นางสาว ณัฐวรา เกษจันทร์

ผู้จัดทำ

สารบัญ

สารบัญรูป

รูป **หน้า**

สารบัญตาราง

ตาราง **หน้า**

บทที่ 1
บทนำ

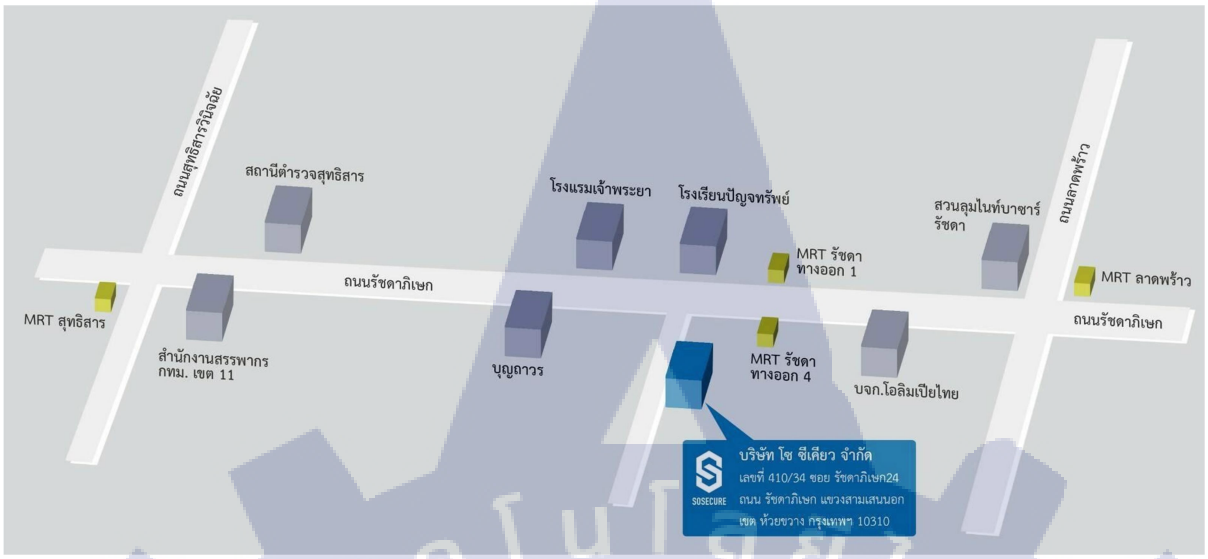
1.1 ชื่อและที่ตั้งของสถานประกอบการ

1.1.1. ชื่อสถานประกอบการ : บริษัท โซ ซิเคียว จำกัด

1.1.2. ที่ตั้งสถานประกอบการ : 410/34 ซอย รัชดาภิเษก24 ถนน
รัชดาภิเษก แขวงสามเสนนอก เขตห้วยขวาง
กรุงเทพมหานคร 10310

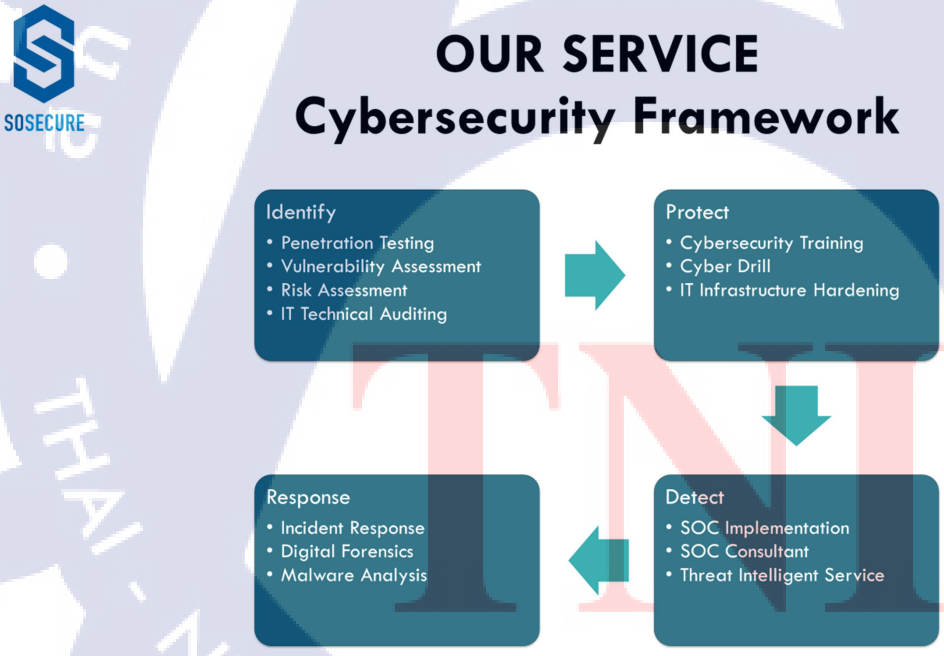
1.1.3. เบอร์โทรศัพท์ : โทรศัพท์ (66) 2 165 0660

ภาพที่ 1.1 แสดงตราสัญลักษณ์ของบริษัท โซ ซิเคียว จำกัด



ภาพที่ 1.2 แสดงที่ตั้งของบริษัท โซ ซีเคียว จำกัด

1.2 ลักษณะธุรกิจของสถานประกอบการ หรือการให้บริการหลักขององค์กร



ภาพที่ 1.3 แสดงกลุ่มบริการที่บริษัทให้บริการ

บริษัท โซ ซิเคียว จำกัด จัดตั้งขึ้นเพื่อตอบสนองความต้องการของตลาดในตอนนี้ ซึ่งเกี่ยวกับระบบรักษาความปลอดภัย ของโลกไซเบอร์ในปัจจุบัน ซึ่ง ณ ปัจจุบันข้อมูลในโลกออนไลน์มีการเข้าถึงได้ง่าย จึงทำให้มีบุคคลที่ไม่พึงประสงค์เป็นจำนวนมากเกิดขึ้น เพื่อที่จะทำการดึงข้อมูลของเจ้าของธุรกิจต่างๆ รวมถึงการเข้าถึงข้อมูลที่เป็นความลับขององค์กรต่างๆ ทางบริษัทจึงได้มีการรวบรวมบุคลากรที่เพรียบพร้อมทั้งคุณภาพในการทำงานและประสบการณ์ทางด้านนี้โดยเฉพาะ เพื่อดูแลความปลอดภัยของข้อมูลภายในองค์กรนั้นๆ

1.3 รูปแบบการจัดองค์กรและการบริหารองค์กร

บริษัท โซ ซิเคียว จำกัด เป็นบริษัทที่ทำเกี่ยวกับ การให้คำแนะนำระบบ ป้องการการโจรกรรมข้อมูล โดยแบ่งเป็นแผนกต่างๆ โดยแต่ละแผนกจะมีความเชี่ยญชาญ เฉพาะด้านไป เช่นการจัดการระบบ ทดสอบการเจาะข้อมูลก็จะมีทีมงานที่มีความเชี่ยวชาญในการจัดการ ทางด้านนี้โดยเฉพาะโดยทางบริษัทจะมีการแบ่งหลายๆแผนก เพื่อจัดการและดูแลได้อย่างทั่วถึง

ภาพที่ 1.4 รูปแบบการจัดการองค์กร

1.4 ตำแหน่งและหน้าที่งานที่นักศึกษาได้รับมอบหมาย

1.4.1. ตำแหน่ง : วิศวกรความปลอดภัย (Security Engineer)

1.4.2. สังกัด : ทีมรักษาความปลอดภัย (Security Team)

1.4.3. แผนก : Security

1.4.4. หน้าที่ : Security support

1.5 พนักงานที่ปรึกษา และ ตำแหน่งของพนักงานที่ปรึกษา

1.5.1. ชื่อ	:	คุณ พงศกร เอกวิจิตรกุล
1.5.2. ตำแหน่ง	:	Pentester
1.5.3. โทรศัพท์	:	(66) 8 03505639
1.5.4. Email	:	ca.pongsakorn_st@tni.ac.th

1.6 ระยะเวลาที่ปฏิบัติงาน

1.6.1. วันที่ทำงานวันแรก	:	วันพุธที่ 4 มิถุนายน 2561
1.6.2. วันที่ทำงานวันสุดท้าย	:	วันศุกร์ที่ 28 กันยายน 2561
1.6.3. เวลาเริ่มงาน	:	9:00 น.
1.6.4. เวลาเลิกงาน	:	18:00 น.

1.7 ที่มาและความสำคัญของปัญหา

ใน 2 เดือนแรกที่ทำงาน นักศึกษาได้พบว่าทางบริษัทมีความต้องการที่จะศึกษาพฤติกรรมของแฮกเกอร์ที่มีการโจมตีเข้ามาในระบบ เพื่อที่จะนำข้อมูลไปวิเคราะห์เพื่อป้องกันและนำไปสร้างเป็นโซลูชั่นอื่นๆ แต่ยังขาดบริการที่จะมาวิเคราะห์พฤติกรรมของแฮกเกอร์ วิธีการของแฮกเกอร์ที่ใช้ในการเจาะระบบ หลังจากแฮกเกอร์ยึดระบบหลังจากนั้นแฮกเกอร์ทำอะไรกับระบบบ้างเพื่อที่จะได้นำข้อมูลในส่วนนี้นำไปสร้างเป็นผลิตภัณฑ์ที่ใช้ป้องกันต่อไป

1.8 วัตถุประสงค์หรือจุดมุ่งหมายของโครงงาน

1. เพื่อตรวจจับพฤติกรรมของแฮกเกอร์ในการเข้ามาในระบบ
2. เพื่อศึกษาวิธีการของแฮกเกอร์ในการโจมตีระบบ
3. เพื่อนำข้อมูลจากล็อกไฟล์ไปวิเคราะห์ในการสร้างผลิตภัณฑ์

1.9 ผลที่คาดว่าจะได้รับจากการปฏิบัติงานหรือโครงงานที่ได้รับมอบหมาย

1. ระบบสามารถตรวจจับพฤติกรรมของแฮกเกอร์ในการเข้ามาในระบบ
2. ระบบสามารถเพิ่มความสะดวกในการกรองและตรวจจับวิธีการของแฮกเกอร์แล้วสรุปข้อมูลบางส่วนจาก ล็อกไฟล์ได้
3. ได้รับประสบการณ์จากการสร้างระบบฮันนีพอตและข้อมูลจากล็อกไฟล์
4. ได้รับความพึงพอใจในการใช้งานระบบ จากการนำไปใช้งานจริงของวิศวกร

1.10 นิยามศัพท์เฉพาะ

ตารางที่ 1.1 แสดงนิยามศัพท์เฉพาะ

คำศัพท์	**นิยาม**
ล็อกไฟล์	บันทึกการใช้งานเครื่อง ในที่นี่มีหลายแบบ ได้แก่ 1. ล็อกไฟล์ที่ได้จากโปรแกรม 2. ล็อกไฟล์ที่ได้จากเว็บ
IDS	รับแจ้งเตือนเมื่อมีผู้บุกรุกเข้ามาในระบบ
Honeypot	เครื่องจำลองใช้สำหรับศึกษาพฤติกรรมของแฮกเกอร์โดยให้แฮกเกอร์โจมตีเข้ามา
Splunk	รับแสดงล็อกต่างๆ

บทที่ 2
ทฤษฎีและเทคโนโลยีที่ใช้ในการปฏิบัติงาน

ในการปฏิบัติงานสหกิจศึกษาครั้งนี้ เป็นการนำความรู้ทางด้านทฤษฎีและเทคโนโลยีมาใช้ในการปฏิบัติงานทุกส่วนตลอดการปฏิบัติงานสหกิจศึกษา ซึ่งเป็นการนำความรู้ทั้งที่เคยเรียนมาประยุกต์ ใช้และเป็นการศึกษาเรียนรู้สิ่งใหม่ ๆ ที่ได้จากการปฏิบัติงาน ทฤษฎีและเทคโนโลยีที่เกี่ยวข้อง มีดังนี้

2.1 ทฤษฎีที่เกี่ยวข้อง

2.1.1 ความรู้เกี่ยวกับ Routing

Routing เป็นโปรโตคอลที่ใช้รวบรวมเส้นทางของ network address วงต่างๆที่ต้องการติดต่อข้าม network โดยจะแลกเปลี่ยนข้อมูลของอุปกรณ์ที่ทำงานอยู่ในระดับ layer 3 เพื่อให้อุปกรณ์เหล่านี้สามารถส่งข้อมูล (IP packet) ไปยังคอมพิวเตอร์ปลายทางได้อย่างถูกต้อง Router จะรู้ว่าไปยัง IP ปลายทางได้ทาง Interface ใด หรือไปทาง Router ตัวไหน ได้จาก routing table นั่นเอง ตัวอย่าง Routing Protocol ได้แก่ RIP (Routing Information Protocol) , OSPF (Open Shortest Path First), IGRP (Interior Gateway Routing Protocol) (Cisco Proprietary), EIGRP (Enhanced Interior Gateway Routing Protocol) (Cisco Proprietary) ,BGP (Border Gateway Protocol) เป็นต้น Routing Protocol ทำงานอยู่บน Layer 3 ของ OSI 7 Layers

Routing Protocol แบ่งเป็น 2 กลุ่มใหญ่ๆคือ 1.กลุ่ม Static (Static Route และ Default Route)
2.กลุ่ม Dynamic และ Dynamic ยังแบ่งเป็น 2 กลุ่มคือ IGP (Routing ที่ใช้ภายในหน่วยงาน หรือภายในองค์กรตัวเอง ไม่ได้คุยต่าง ISP) และ EGP (Routing ที่ใช้คุยข้ามองค์กร หรือหน่วยงาน หรือต่าง ISP กัน หรือใช้คุยระหว่าง ISP)

2.1.2 ความรู้เกี่ยวกับ IDS

Intrusion detection system (IDS) คือ software หรือ hardware ที่ใช้ตรวจสอบการเชื่อมต่อที่ไม่พึงประสงค์ หรือความพยายามที่จะเข้ามาทำอันตรายต่อเครือข่าย โดยการโจมตีนั้นอาจจะเกิดจาก cracker, Worm หรือ Malware ต่างๆ ข้อเสีย Intrusion detection system (IDS) ไม่สามารถที่จะตรวจสอบ Packet ที่

เข้ารหัสได้ องค์ประกอบของ Ids นั้นมีหลายหลายส่วนแต่ส่วนประกอบของ Intrusion detection system (IDS)ที่สำคัญนั้นมีอยู่สามส่วนได้แก่

1. Sensor คือส่วนที่จะสร้างเหตุการณ์ที่เกี่ยวกับความปลอดภัยขึ้นมา

2. Console คือส่วนที่จะตรวจจับเหตุการณ์ต่าง, แจ้งเตือน รวมไปถึงการควบคุม Sensor

3. Engine เป็นส่วน ที่จะบันทึกเหตุการณ์จาก sensor ลงใน Database และจะแจ้งเตือนตามกฎที่ได้ตั้งเอาไว้ใน IDS

2.1.3 ความรู้เกี่ยวกับ Sniffer

Sniffer คือโปรแกรมที่เอาไว้ดักจับข้อมูล บนระบบ Network เนื่องจากคอมพิวเตอร์เน็ตเวิร์คเป็นระบบการสื่อสารที่ใช้ร่วมกัน คอมพิวเตอร์สามารถรับข้อมูลที่คอมพิวเตอร์เครื่องอื่นตั้งใจจะส่งไป ให้อีกเครื่องหนึ่ง การดักจับข้อมูลที่ผ่านไปมาระหว่าง เน็ตเวิร์คเรียกว่า sniffing คล้ายๆ การดักฟังโทรศัพท์ แต่การดักฟังโทรศัพท์จะทำได้ทีละเครื่อง แต่ sniffer สามารถทำได้ทั้ง network

2.2 เทคโนโลยีที่ใช้ในการปฏิบัติงาน

2.2.1 Splunk

Splunk คือ ซอฟท์แวร์ที่สามารถ ค้นหา แสดงรายงาน ตรวจสอบ และ วิเคราะห์ ข้อมูล สามารถดูข้อมูลแบบ Live Streaming หรือ ดูข้อมูลเก่าในลักษณะข้อมูลทางสถิติได้ Splunk รองรับการทำงานแบบ Real Time

ภาพที่ 2.1 แสดงตราสัญลักษณ์ของ Splunk

ที่มา : https://www.ictsecurity.com.au/wp-content/uploads/2018/07/splunk.png

2.1.1.1 ข้อดีของ Splunk

- ความง่ายและยืดหยุ่นในการใช้งานให้ตอบโจทย์ความต้องการขององค์กร
- สามารถเชื่อมต่อกับอุปกรณ์รักษาความปลอดภัย, อุปกรณ์เครือข่าย และ Threat Intelligence ได้อย่างอิสระ
- ประยุกต์ใช้ได้กับระบบ E-Commerce/Retail Analytics
- สามารถวิเคราะห์ข้อมูลอะไรก็ได้

2.1.1.2 ข้อเสียของ Splunk

- ใช้งานยากจำเป็นต้องทราบคำสั่งที่ใช้ในการค้นหา
- ราคาสูง

2.2.2 MikroTik Router

MikroTik Router อุปกรณ์ที่ใช้งานด้านระบบเครือข่ายสัญชาติลัตเวีย สามารถปรับแต่งและตั้งค่าฟังชั่นต่างๆได้อย่างอิสระเพื่อให้สอดคล้องกับการใช้งาน ออกแบบให้รองรับงานด้านบริหารจัดการ Network มีราคาถูก การใช้งานไม่จำเป็นต้องพึ่ง Sever PC ทำให้ประหยัดไฟและประหยัดพื้นที่การใช้งาน

นอกจากนี้ยังมีขนาด router ที่เล็กสะดวกต่อการติดตั้ง Config ได้ง่าย รวมทั้งมีฟังก์ชั่น Authenticate ที่ทำให้ก่อนการเข้าใช้งาน Hotspot wifi ต้อง Login เข้าสู่ระบบก่อนเพื่อความปลอดภัยในการเข้าใช้งาน Internet wifi ในองค์กรต่างๆ Mikrotik จะถูกรันบนระบบปฏิบัติการ RounterOS คือระบบปฏิบัติการของ Mikrotik ถูกติดตั้งไว้บน Hardware ทุกรุ่นโดยที่คุณไม่จำเป็นต้องเสียเงินค่า License นอกจากยังสามารถนำ RouterOS ไปติดตั้งไว้บน Severและ PC ที่มีสเปคการใช้งาน

ภาพที่ 2.2 แสดงตราสัญลักษณ์ MikroTik

ที่มา : https://designs.mikrotik.com/images/large/mikrotik.png

2.2.2.1 ข้อดีของ MikroTik

- ราคาถูก

- สามารถทำ router แบบ virtualize ได้ไม่ต้องใช้ฮาร์แวร์จริง

2.2.2.2 ข้อเสียของ MikroTik

- ตั้งค่ายาก

- เชื่อถือได้ไม่เท่าแบรนด์หลัก

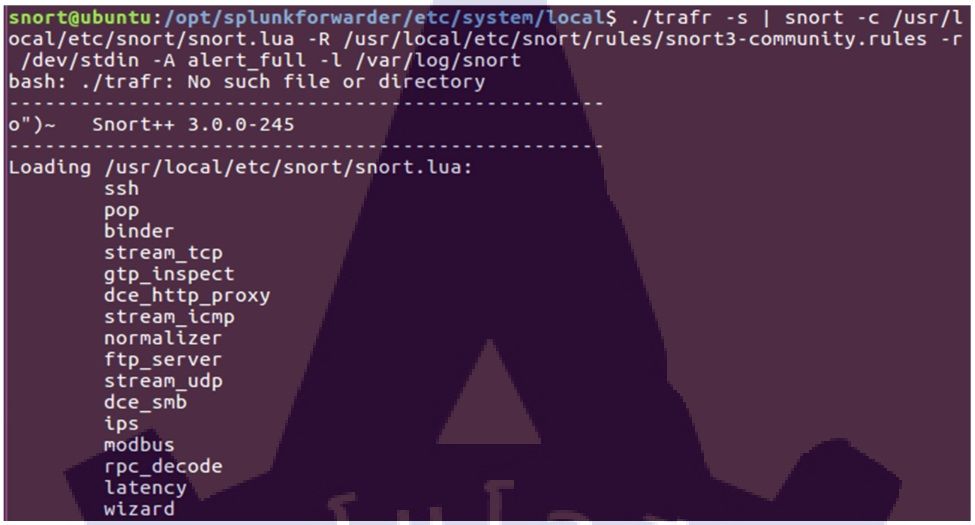
2.2.3 Snort

Snort เป็นเครื่องมือที่ใช้ตรวจจับการบุกรุกทางเครือข่าย (network intrusion detection) การทำงานของ Snort จะใช้ไลบรารี (library) พื้นฐานชื่อ libpcab ซึ่งใช้กันโดยทั่วไปในบรรดา network sniffer

Snort สามารถทำ protocol analysis, content searching/matching, ตรวจจับการบุกรุก

ภาพที่ 2.3 แสดงตราสัญลักษณ์ Snort

ที่มา : https://goo.gl/X3T4vv



ภาพที่ 2.3 แสดงหน้าจอของโปรแกรม snort ขณะใช้งาน

ที่มา : โปรแกรม Snort

2.2.3.1 ข้อดีของซอฟต์แวร์ Snort

- ง่ายต่อการติดตั้ง

- เป็น IDS แบบ open source สามารถใช้ได้กับหลายระบบปฏิบัติการ

2.2.3.2 ข้อเสียของซอฟต์แวร์ Snort

- ใช้ยากต้องมีพื้นฐานในการเขียน rule

บทที่ 3
แผนงานการปฏิบัติงานและขั้นตอนการดำเนินงาน

ในการปฏิบัติงานสหกิจศึกษาครั้งนี้ มีการนำความรู้มากมาย จากทั้งที่ได้เรียนรู้ระหว่างการปฏิบัติงาน และที่ได้เรียนรู้จากในห้องเรียน ขั้นตอนการดำเนินงาน และการวางแผน จึงเป็นสิ่งสำคัญที่จะต้องวางแผน เพื่อลดความผิดพลาดที่อาจจะเกิดขึ้นในการทำงาน

3.1 แผนงานการฝึกงาน

ตารางที่ **3.1** แสดงแผนการสร้างระบบฮันนีพอตและข้อมูลจากล็อกไฟล์

หัวข้องาน / เดือน	มิ.ย.		ก.ค.		ส.ค.		ก.ย.	
ศึกษาข้อมูลเกี่ยวกับระบบงาน								
ศึกษาและวางแผนการทำโครงงาน								
ทำงานทั่วไป								
สร้างระบบ Honeypot								
ทดสอบระบบที่สร้างขึ้น								
จัดทำเอกสารคู่มือระบบ								

3.2 รายละเอียดที่นักศึกษาปฏิบัติในการฝึกงาน

ภายในระยะเวลาปฏิบัติงานสหกิจศึกษาตลอดระยะเวลา 4 เดือน ได้รับมอบหมายให้ทำงานคือ การทดสอบเจาะระบบ การทดสอบเจาะระบบหลายครั้งของบริษัทมักพบว่ามีช่องโหว่ใหม่ๆเกิดขึ้นรวมถึงวิธีการที่ใช้ทดสอบเจาะระบบก็มีความหลายหลายมากขึ้น ดังนั้นเพื่อให้เกิดความง่ายในการตรวจพบช่อง

โหว่และวิธีการโจมตีใหม่ๆ รวมถึงพฤติกรรมของแฮกเกอร์ที่เข้ามาในระบบทำให้เห็นถึงแนวทางการสร้างระบบฮันนีพอตและข้อมูลจากล็อกไฟล์ โดยมีรายละเอียดดังนี้

3.2.1 การออกแบบการโครงสร้างของระบบ

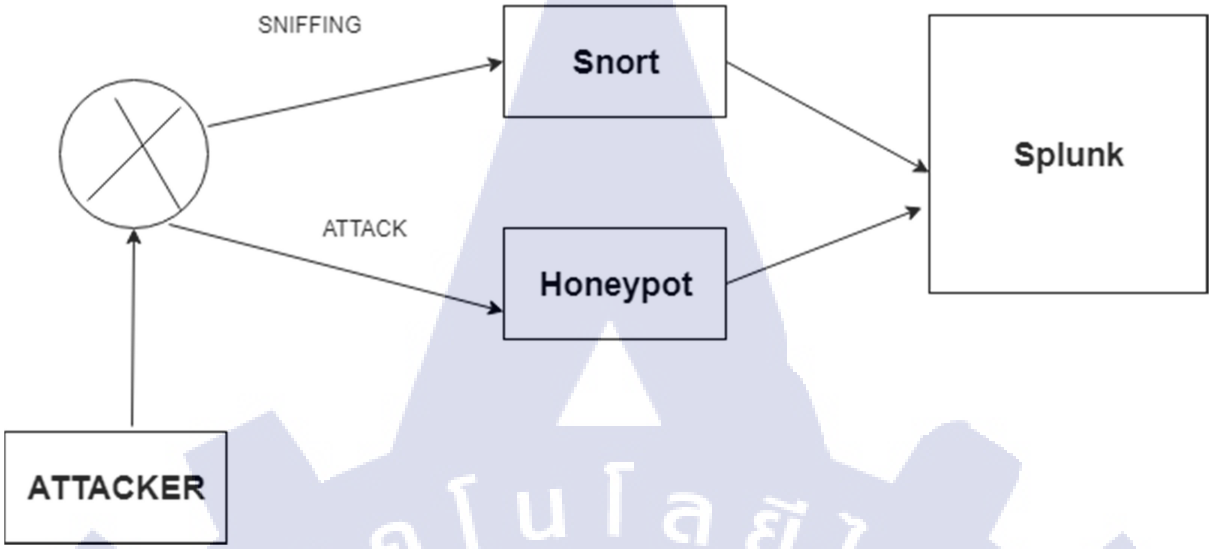
โครงสร้างของระบบฮันนีพอตและข้อมูลจากล็อกไฟล์ ได้ถูกออกแบบโดยใช้การวิเคราะห์จากความต้องการของวิศวกรในทีมติดตั้ง โดยได้สังเกตเห็นความต้องการของระบบ ดังนี้

1. ระบบสามารถใช้งานได้เมื่อโดนโจมตีแล้วระบบต้องไม่ล่ม
2. ระบบเมื่อถูกโจมตีสามารถส่งล็อกไปเก็บและประมวลผลได้
3. ระบบสามารถตรวจจับและแยกประเภทของการโจมตี
4. ผลลัพธ์ที่ได้จากระบบสามารถนำไปวิเคราะห์รูปแบบการโจมตี พฤติกรรมและวิธีที่ใช้ในการโจมตีได้

จากความต้องการข้างต้นความต้องการถูกนำไปวิเคราะห์และได้ออกมาเป็นแนวทางการสร้างระบบดังนี้

1. แบ่งส่วนระบบออกเป็น 4 ส่วนได้แก่ ส่วนของเน็ตเวิร์ค ส่วนที่ใช้ศึกษาพฤติกรรมการโจมตี ส่วนตรวจจับการโจมตี ส่วนที่ใช้เก็บข้อมูลการโจมตีต่างๆ
2. ในส่วนของเน็ตเวิร์คสามารถดักจับข้อมูลและส่งล็อกไปให้ส่วนตรวจจับการโจมตีเพื่อนำไปวิเคราะห์
3. ส่วนที่ใช้ศึกษาพฤติกรรมโจมตี มีหน้าที่รองรับการโจมตีต่างๆรวมถึงมีช่องโหว่เพื่อใช้สำหรับศึกษาพฤติกรรมและวิธีการต่างๆที่ใช้ในการโจมตี
4. ส่วนตรวจจับการโจมตีสามารถที่จะตวจจับได้ว่าเป็นการโจมตีรูปแบบใด ส่งล็อกไปหาส่วนที่ใช้เก็บข้อมูลการโจมตี
5. ส่วนที่ใช้เก็บข้อมูลการโจมตี เป็นแหล่งรวมล็อกต่างๆเพื่อนำมาวิเคราะห์รูปแบบการโจมตี พฤติกรรมของแฮกเกอร์หลักจากยึดระบบได้

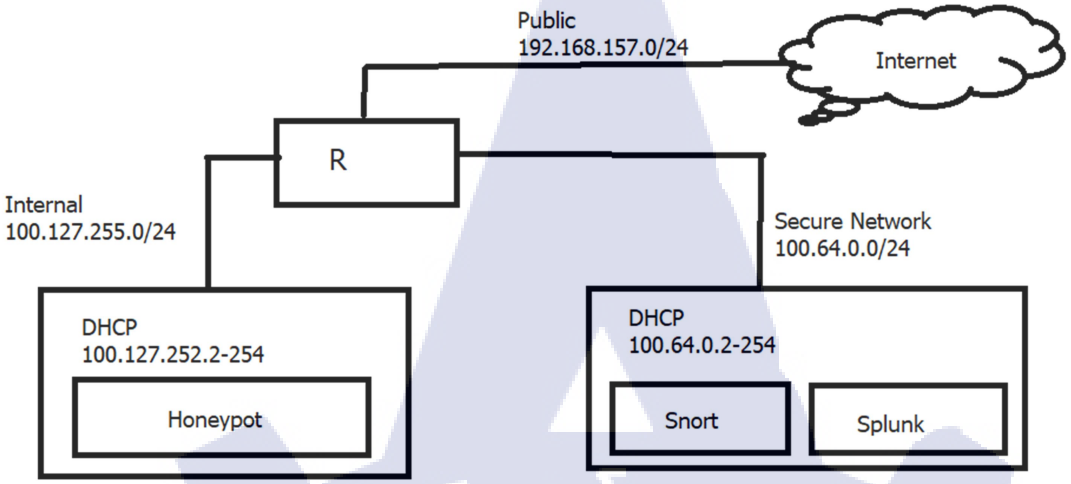
จากแนวทางการออกแบบระบบข้างต้น ทั้งหมดถูกนำไปรวมกันเป็นโครงสร้างของระบบ ดังที่แสดงในภาพที่ 3.1



ภาพที่ 3.1 แสดงโครงสร้างของระบบ

3.2.2 **การออกแบบระบบเน็ตเวิร์ค**

หลังจากเสร็จสิ้นการออกแบบโครงสร้างของระบบ การออกแบบระบบเน็ตเวิร์ค เป็นอีกหนึ่งสิ่งที่มีความสำคัญ และเป็นสิ่งที่จะแสดงถึงการติดต่อสื่อสารกันระหว่างระบบ



ภาพที่ 3.2 แสดงโครงสร้างเครือข่าย

จากภาพที่ 3.2 สามารถอธิบายได้ว่าในส่วนของเราเตอร์มีการติดต่อสามทางด้วยกัน คือในส่วนของ Public ใช้สำหรับการออกอินเทอร์เน็ตรวมถึงการรับแพกเกจจากภายนอกด้วย ซึ่งในที่นี้เพื่อให้แฮกเกอร์สามารถโจมตีจากภายนอกเข้ามาได้ เมื่อแฮกเกอร์โจมตีเข้ามา Router จะทำตัวเสมือนกระจก (mirror) ทำให้แพกเกจทะลุผ่านเราเตอร์เข้าไปหา honeypot ได้ สามารถแสดงได้ดังภาพ 3.3

```
[admin@Router] /system logging action> /ip add
[admin@Router] /ip address> pr
Flags: X - disabled, I - invalid, D - dynamic
 #    ADDRESS            NETWORK         INTERFACE
 0    100.127.255.1/24   100.127.255.0   Internal
 1    100.64.0.1/24      100.64.0.0      Secure Network
 2 D 192.168.157.128/24 192.168.157.0   Public Interface
[admin@Router] /ip address> _
```

ภาพที่ 3.3 แสดงถึงการตั้งค่าเครือข่ายในเราเตอร์ MikroTik

หลังจากนั้นมีการทำ DHCP ให้กับเครือข่ายทั้งสองวง ได้แก่ Internal และ Secure Network เพื่อการใช้งานสำหรับในอนาคตในกรณีที่ต้องการเพิ่มจำนวนเครื่อง DHCP คือการกำหนด IP Address แบบ

อัตโนมัติให้แก่เครื่องลูกข่ายในระบบเพราะ DHCP server จะเป็นตัวแจกจ่าย IP address ที่ไม่เหมือนกันให้กับเครื่องลูกข่าย โดย DHCP Server จะมีขอบเขตในการแจกจ่าย IP address ซึ่งผู้ดูแลระบบจะต้องกำหนดขึ้นมาเองในที่นี้คือ 100.64.0.0/24 และ 100.127.255.0/24 สามารถแสดงได้ดังภาพ 3.4

```
[admin@Router] /tool> ..
[admin@Router] > /ip dhcp-ser
[admin@Router] /ip dhcp-server> pr
Flags: D - dynamic, X - disabled, I - invalid
 #    NAME       INTERFACE    RELAY           ADDRESS-POOL    LEASE-TIME ADD-ARP
 0    dhcp1      Internal                     Internal        17w1d
 1    dhcp2      Secure Ne...                 Secure Network  17w1d
[admin@Router] /ip dhcp-server>
```

ภาพที่ 3.4 แสดงถึงการตั้งค่า DHCP ในเราเตอร์ MikroTik

```
[admin@Router] /ip dhcp-server network> pr
Flags: D - dynamic
 #   ADDRESS            GATEWAY          DNS-SERVER          WINS-SERVER     DOM
 0   100.64.0.0/24      100.64.0.1       100.64.0.1
 1   100.127.255.0/24   100.127.255.1    100.127.255.1
[admin@Router] /ip dhcp-server network>
```

ภาพที่ 3.5 แสดงถึงการตั้งค่า DHCP ในเราเตอร์ MikroTik

มีการสร้าง ip pool ซึ่งเสมือนกับคลังที่ใช้ในการเก็บ IP สามารถแสดงได้ดังภาพ 3.2.2.4

```
[admin@Router] /ip pool> pr
 # NAME                                            RANGES
 0 Internal                                        100.127.255.2-100.127.255.254
 1 Secure Network                                  100.64.0.2-100.64.0.254
[admin@Router] /ip pool>
```

ภาพที่ 3.6 แสดงถึงการตั้งค่า IP pool ในเราเตอร์ MikroTik

Nat (Network address Translation) คือ การแปลง Private IP ของเครื่องลูกข่ายให้เป็น Public IP เทคนิคแบบนี้อาจเรียกชื่อว่า IP Masquerade เป็นการซ่อนไอพีของเครื่องลูกข่าย ในที่นี้เพื่อป้องกันไม่ให้แฮกเกอร์ทราบ Private IP ของเครื่องต่างๆที่อยู่ภายในระบบ สามารถแสดงได้ดังภาพ 3.7

```
[admin@Router] /ip firewall nat> pr
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=srcnat action=masquerade src-address=100.127.255.0/24
      out-interface=Public Interface

 1    chain=srcnat action=masquerade src-address=100.64.0.0/24
      out-interface=Public Interface

 2    chain=dstnat action=dst-nat to-addresses=100.127.255.254
      dst-address=192.168.157.128
[admin@Router] /ip firewall nat> _
```

ภาพที่ 3.7 แสดงถึงการตั้งค่า Nat ในเราเตอร์ MikroTik

ในเราเตอร์ MikroTik มีการดักจับแพกเกจเพื่อส่งไปให้ snort ซึ่งเป็นการส่งข้อมูลแบบ stream โดยใช้โปรโตคอล TZSP (Tazmen Sniffer Protocal) ซึ่งอยู่ใน MikroTik สามารถแสดงได้ดังภาพ 3.8

```
[admin@Router] /tool sniffer> ..
[admin@Router] /tool> ..
[admin@Router] > /tool sni print
                    only-headers: no
                    memory-limit: 100KiB
                   memory-scroll: yes
                       file-name:
                      file-limit: 1000KiB
                streaming-enabled: yes
                 streaming-server: 100.64.0.254
                    filter-stream: yes
                 filter-interface: Public Interface
              filter-mac-address:
             filter-mac-protocol:
               filter-ip-address:
             filter-ipv6-address:
              filter-ip-protocol:
                     filter-port:
                      filter-cpu:
                 filter-direction: any
  filter-operator-between-entries: or
                          running: yes
[admin@Router] >
```

ภาพที่ 3.8 แสดงการตั้งค่าใน MikroTik

3.2.3 **การสร้างส่วนที่ใช้ศึกษาพฤติกรรมการโจมตี**

3.2.3.1 ติดตั้งแพกเกจ Openssl เวอร์ชั่นที่มีช่องโหว่ Heartbleed และแพกเกจ Libssl 1.0.0 แสดงได้ดังภาพ 3.9

```
root@honeypot:~# ls
libssl1.0.0_1.0.1-4ubuntu5.11_amd64.deb
openssl_1.0.1-4ubuntu5.11_amd64.deb
```

ภาพที่ 3.9 แสดงแพกเกจที่ใช้ในการติดตั้ง

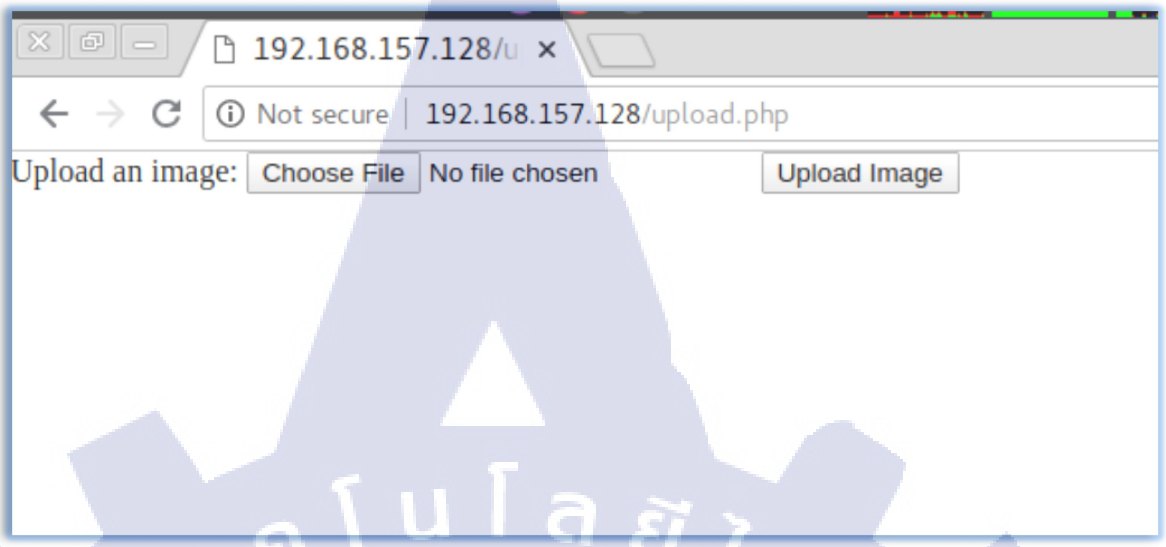
3.2.3.2 ทดสอบช่องโหว่โดยการใช้ NSE ดังภาพที่ 3.10

```
┌─[root@parrot]─[/home/pro]
└──╼ #nmap -p 443 --script ssl-heartbleed 192.168.157.128
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-24 11:12 +07
Nmap scan report for 192.168.157.128
Host is up (0.00056s latency).

PORT    STATE SERVICE
443/tcp open  https
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptog
raphic software library. It allows for stealing information intended to be prote
cted by SSL/TLS encryption.
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0
.2-beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for read
ing memory of systems protected by the vulnerable OpenSSL versions and could all
ow for disclosure of otherwise encrypted confidential information as well as the
 encryption keys themselves.
```

ภาพที่ 3.10 แสดงการใช้ NSE ในการทดสอบช่องโหว่ที่สร้างขึ้น

3.2.3.3 หลังจากนั้นเพิ่มช่องโหว่เพื่อให้แฮกเกอร์ใช้ในการอัพโหลดไฟล์ เพื่อใช้ดูว่าแฮกเกอรใช้อะไรในการเพิ่มสิทธิ์ตนเองให้เป็นผู้ใช้ที่มีสิทธิ์เต็มระบบ แสดงได้ดังภาพที่ 3.11



ภาพที่ 3.11 แสดงช่องโหว่ที่เพิ่มเข้ามา

3.2.4 การสร้างส่วนที่ใช้ตรวจจับการโจมตี

เนื่องจากโดยปกติ snort เป็น IDS (Intrusion detection system) มีหน้าที่ในการตรวจจับกาโจมตี ดังนั้นเราต้องการให้ snort สามารถส่งล็อกเพื่อให้ Splunk นำไปวิเคราะห์ข้อมูลจากที่ Snort ตรวจจับการโจมตีได้ เราจึงติดตั้งแพกเกจที่ชื่อว่า SplunkForwarder ตั้งค่าตามภาพที่ 3.12

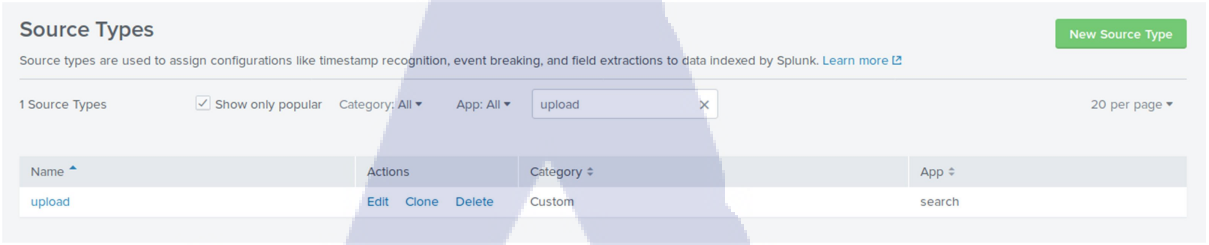
```
root@ubuntu:/opt/splunkforwarder/etc/system/local# more inputs.conf
[monitor:///var/log/snort/alert_full.txt]
index = snort
followTail = 1
sourcetype = snort


root@ubuntu:/opt/splunkforwarder/etc/system/local#
```

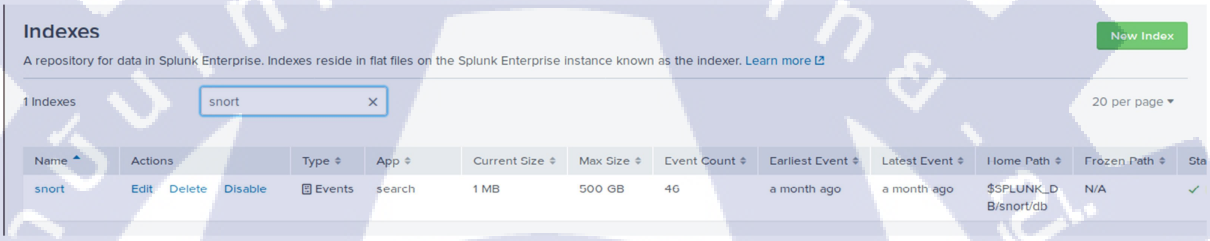
ภาพที่ 3.12 แสดงการตั้งค่า splunkforwarder

3.2.5 การสร้างส่วนที่ใช้เก็บข้อมูลการโจมตี

เพิ่ม SourceType และ Index ใน splunk ดังภาพ 3.13



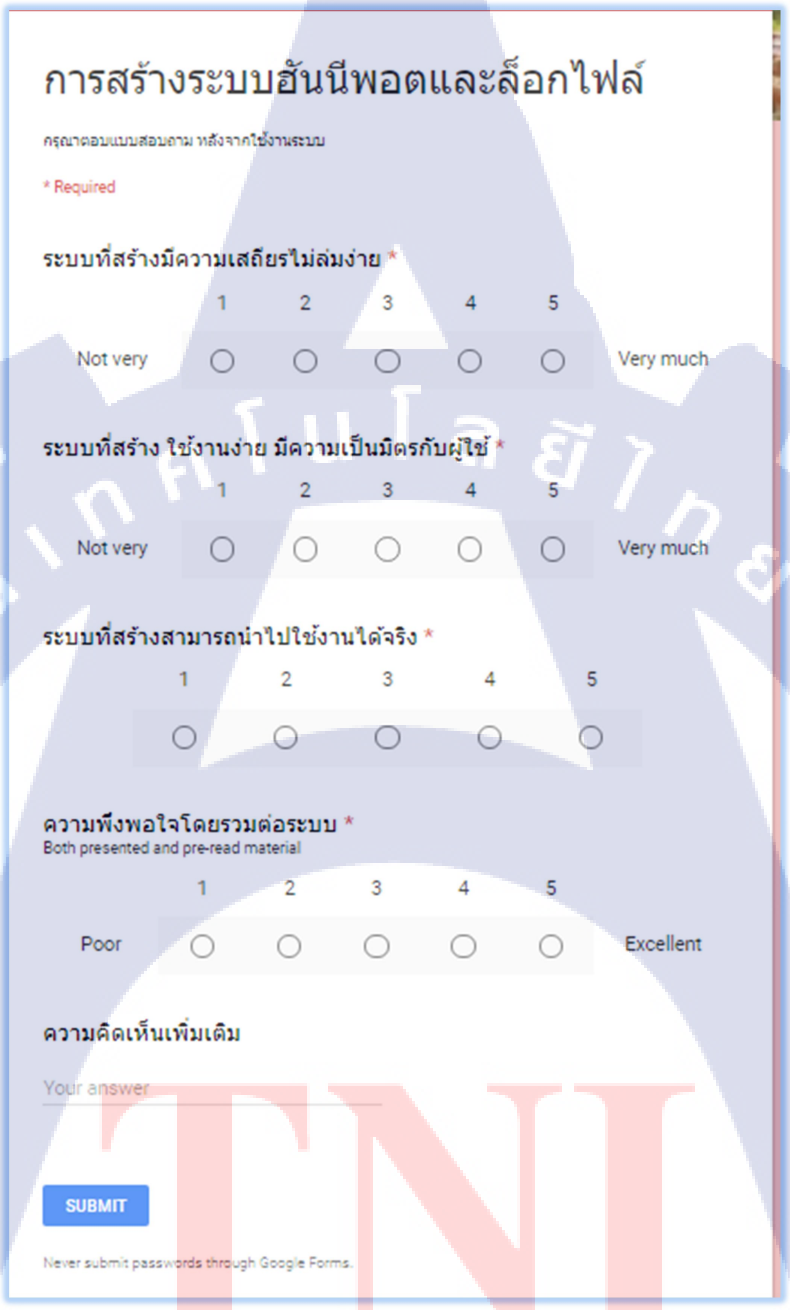
ภาพที่ 3.13 แสดงการเพิ่ม sourcetypes



ภาพที่ 3.14 แสดงการเพิ่ม Indexes

3.2.7 การออกแบบแบบสอบถามความพึงพอใจในการใช้งานระบบ

เมื่อระบบทั้งหมดถูกสร้างเรียบร้อยแล้ว การวัดผลเป็นอีกสิ่งหนึ่ง ที่มีความสำคัญอย่างยิ่ง ในการวัดผลนั้น อุปสรรคสำคัญ คือวิศวกรส่วนใหญ่ ไม่มีเวลาเพียงพอที่จะตอบแบบสอบถามขนาดยาวได้ อีกทั้งยังมีโอกาสที่จะเดินทางไปยังสำนักงานน้อย ดังนั้น แบบสอบถามที่ถูกส่งไป จะเป็นแบบสอบถามที่สั้น และใช้เวลาตอบน้อย ด้วยการถามแบบสรุป 3 ข้อ ซึ่งเป็นจุดประสงค์หลักของการสร้างระบบดังภาพที่ 3.2.7 ได้แก่ 1) ประสิทธิภาพของระบบ ในด้านความเสถียร 2) ประสิทธิภาพของระบบ ในด้านความสะดวกในการใช้งาน และ 3) ความพึงพอใจโดยรวม จากการใช้งานระบบของวิศวกร และเพื่อเป็นการเก็บ Feedback บางประการที่อาจไม่มีในคำถาม ผู้พัฒนาจึงถามเพิ่มเติมในข้อที่ 4 ถึงความคิดเห็นเพิ่มเติม ซึ่งแบบสอบถามทั้งหมดนี้ ถูกส่งไปในรูปของแบบฟอร์มอิเล็กทรอนิกส์ Google Form ทำให้สามารถสอบถามวิศวกรจำนวนมากได้ ภายในระยะเวลาอันสั้น



การสร้างระบบฮันนีพอตและล็อกไฟล์

กรุณาตอบแบบสอบถาม หลังจากใช้งานระบบ

* Required

ระบบที่สร้างมีความเสถียรไม่ล่มง่าย *

	1	2	3	4	5	
Not very	○	○	○	○	○	Very much

ระบบที่สร้าง ใช้งานง่าย มีความเป็นมิตรกับผู้ใช้ *

	1	2	3	4	5	
Not very	○	○	○	○	○	Very much

ระบบที่สร้างสามารถนำไปใช้งานได้จริง *

1	2	3	4	5
○	○	○	○	○

ความพึงพอใจโดยรวมต่อระบบ *
Both presented and pre-read material

	1	2	3	4	5	
Poor	○	○	○	○	○	Excellent

ความคิดเห็นเพิ่มเติม

Your answer

SUBMIT

Never submit passwords through Google Forms.

ภาพที่ 3.15 แสดงแบบสอบถามที่ถูกส่งไปยังวิศวกร

3.3 ขั้นตอนการดำเนินงานที่นักศึกษาปฏิบัติงาน

ตารางที่ 3.2 แสดงขั้นตอนการดำเนินงาน และงานที่ทำในแต่ละขั้นตอน

หัวข้อ	รายละเอียด
ศึกษาวิธีการทำงาน และปัญหาจากการทำงาน	- ศึกษาวิธีการทำงาน ทั้งงานที่ต้องใช้ความสามารถในการทดสอบระบบ และงานเอกสาร - Identify ปัญหาที่เกิดขึ้นในการทำงาน - คิดแนวทางการแก้ไขปัญหาที่เกิดขึ้นในการทำงาน
สร้างระบบเพื่อทดสอบความเป็นไปได้ในการแก้ปัญหา	- นำแนวคิดที่จะใช้ในการแก้ไขปัญหา มาสร้างเป็น ระบบ
สร้างระบบตัวจริง และทดสอบด้วยตนเอง	- นำแนวคิดที่สามารถทำได้จริง มาพัฒนาให้มีความยืดหยุ่นในการใช้งานเพิ่มขึ้น - วางโครงสร้างของระบบ - เริ่มสร้างระบบในแต่ละส่วนแล้วนำมาเชื่อมต่อกัน - ทดสอบด้วยตนเอง โดยนำข้อมูลที่เคยออกแบบมาใช้ในการสร้างระบบทั้งหมด - แก้ไขข้อผิดพลาดที่อาจเกิดขึ้นในการทำงาน
ส่งระบบให้นักทดสอบว่าแก้ปัญหาได้จริงหรือไม่	- จัดทำแบบสอบถาม เพื่อประเมินประสิทธิผลของระบบ - นำข้อมูลที่ได้จากแบบสอบถาม มาประมวลผลเพื่อสรุปประสิทธิผลของโปรแกรม
จัดทำรูปเล่ม	- นำแนวคิดที่สร้างระบบ มาสร้างเป็น diagram ต่างๆ - นำข้อมูลที่มีทั้งหมด จัดเรียงใหม่เป็นรูปเล่ม

บทที่ 4
สรุปผลการดำเนินงาน การวิเคราะห์และสรุปผลต่าง ๆ

4.1 ขั้นตอนและผลการดำเนินงาน

4.1.1 ผลการดำเนินงาน

4.1.1.1 ผลการศึกษาวิธีการทำงาน และปัญหาจากการทำงาน

จากการศึกษาวิธีการทำงาน การทดสอบเจาะระบบหลายครั้งของบริษัทมักพบว่ามีช่องโหว่ใหม่ๆเกิดขึ้น รวมถึงวิธีการที่ใช้ทดสอบเจาะระบบก็มีความหลายหลายมากขึ้น

โดยขั้นตอนการดำเนินงานโดยทั่วไป(ในส่วนของนักทดสอบระบบ) มีดังนี้

1. เก็บข้อมูลความต้องการจากลูกค้าว่าต้องการให้ทดสอบระบบแบบใด
2. วางแผนและเตรียมการทดสอบระบบ
3. เริ่มทดสอบระบบ
4. ทำรายงานและสิ่งที่แนะนำให้ทำ

การทำรายงานเป็นหัวใจหลักของการทดสอบระบบ เพราะทางผู้ทดสอบระบบจำเป็นจะต้องเขียนเนื้อหาสรุปใจความให้กระชับและเข้าใจง่าย อีกทั้งเอกสารยังต้องปรับความแน่นเชิงลึกของเนื้อหาตามระดับความรู้ความสามารถของบริษัทหรือผู้ดูแลอีกด้วย นอกจากนี้ช่องโหว่ต่างๆมีความสำคัญไม่แพ้กัน เพราะนักทดสอบระบบจำเป็นที่จะต้องมีความรู้เกี่ยวกับช่องโหว่ที่เกิดขึ้นใหม่ๆ เพื่อที่จะนำไปทดสอบให้กับลูกค้า รวมถึงให้ความรู้กับลูกค้าและแนวทางป้องกัน ดังนั้นระบบฮันนีพอตและล็อกไฟล์จึงมีความสำคัญเพราะจะช่วยให้เล็งเห็นถึงช่องโหว่ใหม่ๆ รวมถึงวิธีการที่แฮกเกอร์นั้นนำมาใช้โจมตีระบบ

4.1.1.2 ผลจากการสร้างระบบชั่วคราวเพื่อทดสอบความเป็นไปได้ในการแก้ปัญหา

จากแนวทางการแก้ไขปัญหาที่กล่าวไว้ข้างต้น ผู้พัฒนาจึงได้ทดสอบนำแนวทางการแก้ปัญหา ไปทดลองแก้ปัญหาจริง โดยการพัฒนาระบบฮันนีพอตและล็อกไฟล์ขึ้นแบบชั่วคราวว่าสามารถใช้งานได้จริง โดยแบ่งออกเป็นสองส่วนคือส่วนที่สร้างระบบและส่วนที่โจมตีระบบ โดยในส่วนโจมตีระบบเราจะให้นักทดสอบของบริษัททดลองโจมตีระบบและประเมินว่าระบบที่สร้างขึ้นเป็นไปตามเป้าหมายที่ตั้งไว้หรือไม่

4.1.1.3 ผลการสร้างระบบตัวจริง และทดสอบด้วยตนเอง

ในขั้นตอนการสร้างระบบตัวจริง และทดสอบระบบด้วยตนเอง ผู้พัฒนาได้เริ่มพัฒนาด้วยการแยกส่วนการทำงานแต่ละส่วนออกจากกัน ดังต่อไปนี้

1. แบ่งส่วนระบบออกเป็น 4 ส่วนได้แก่ ส่วนของเน็ตเวิร์ค ส่วนที่ใช้ศึกษาพฤติกรรมการโจมตี ส่วนตรวจจับการโจมตี ส่วนที่ใช้เก็บข้อมูลการโจมตีต่างๆ
2. ในส่วนของเน็ตเวิร์คสามารถดักจับข้อมูลและส่งล็อกไปให้ส่วนตรวจจับการโจมตีเพื่อนำไปวิเคราะห์
3. ส่วนที่ใช้ศึกษาพฤติกรรมโจมตี มีหน้าที่รองรับการโจมตีต่างๆรวมถึงมีช่องโหว่เพื่อใช้สำหรับศึกษาพฤติกรรมและวิธีการต่างๆที่ใช้ในการโจมตี
4. ส่วนตรวจจับการโจมตีสามารถที่จะตวจจับได้ว่าเป็นการโจมตีรูปแบบใด ส่งล็อกไปหาส่วนที่ใช้เก็บข้อมูลการโจมตี
5. ส่วนที่ใช้เก็บข้อมูลการโจมตีเป็นแหล่งรวมล็อกต่างๆเพื่อนำมาวิเคราะห์รูปแบบการโจมตีพฤติกรรมของแฮกเกอร์หลักจากยึดระบบได้

หลังจากที่ได้แยกส่วนการทำงานแล้ว ผู้พัฒนาได้ออกแบบและวางโครงสร้างการทำงาน โดยแบ่งการทำงานออกเป็น 2 ส่วนใหญ่ๆ ดังนี้

1. ส่วนโจมตีระบบ
2. ส่วนที่ใช้เก็บล็อกของระบบ

ภายในส่วนโจมตีระบบ จะประกอบด้วยช่องโหว่ต่างๆของระบบ, การเก็บล็อกต่างๆ , การส่งข้อมูลล็อกไฟล์ไปยังส่วนที่ใช่เก็บล็อกและวิเคราะห์

ภายในส่วนที่ใช้เก็บล็อกของระบบจะใช้พียงโปรแกรมสำเร็จรูป splunk ที่นำมาเก็บล็อกรวมถึงนำมาวิเคราะห์ล็อกต่างๆอีกด้วย จากการสร้างระบบจริง ได้เกิดปัญหาเล็กน้อย เช่น ไฟล์ vmdk เสีย , splunk ตัวฟรีไม่สามารถสร้าง dashboard ได้ ซึ่งเป็นปัญหาที่ไม่เคยทราบมาก่อน จึงแก้ปัญหาด้วยการศึกษาเพิ่มเติม

หลังจากระบบจริงถูกเขียนเสร็จแล้ว ผู้พัฒนาจึงทดสอบด้วยตนเอง ด้วยการใช้ข้อมูลที่เคยใช้งานเดิม นำมาทดสอบระบบที่สร้างขึ้นใหม่ ซึ่งมีผลลัพธ์ส่วนใหญ่ที่ถูกต้อง แต่ยังมีผลลัพธ์บางส่วนที่ยังไม่

ถูกต้อง ผู้สร้างระบบจึง Trace หาข้อผิดพลาด และแก้ไขข้อผิดพลาดที่พบ จนได้ผลลัพธ์ที่ไม่พบข้อผิดพลาดใด ๆ

4.1.1.4 ผลการส่งโปรแกรมให้นักทดสอบว่าแก้ปัญหาได้จริงหรือไม่

หลังจากที่โปรแกรมได้ถูกสร้างเรียบร้อยแล้ว ผู้สร้างได้ส่งระบบนี้ กระจายไปยังวิศวกรภายในทีมติดตั้ง เพื่อทดสอบและหาข้อผิดพลาดอีกครั้ง โดยในครั้งแรก โปรแกรมที่ถูกส่งไป ยังคงมีปัญหาเกิดขึ้นเพิ่มเติมมากมาย สรุปได้ดังต่อไปนี้

- ช่องโหว่ที่สร้าง สามารถโจมตีได้แต่ไม่สามารถได้สิทธิสูง
- การสร้างระบบ ควรจะมีการจัดทำคู่มือด้วย

จาก Feedback ที่ได้รับมาข้างต้น ผู้สร้างจึงดำเนินการ ย้อนกลับไปขั้นตอนตามข้อที่ 4.1.1.3 อีกครั้ง โดยระบุ และแก้ไขปัญหาที่เกิดขึ้น ดังนี้

- เพิ่มช่องโหว่เพื่อให้แฮกเกอร์สามารถยกระดับสิทธิ์ได้
- จัดทำคู่มือการใช้โปรแกรม แนบไปกับโปรแกรม

หลังจากที่ได้แก้ไขระบบ และทดสอบด้วยตัวเองอีกครั้งว่าสามารถใช้งานได้ตามปกติแล้ว ผู้สร้างได้ส่งระบบที่แก้ไขแล้วไปยังวิศวกรเพื่อทดสอบอีกครั้ง ได้ Feedback กลับมาเป็นที่น่าพอใจ โดยวิศวกรส่วนใหญ่ระบุว่าระบบสามารถทำงานได้ถูกต้อง

บทที่ 5
บทสรุปและข้อเสนอแนะ

5.1 สรุปผลการดำเนินงาน

จากการปฏิบัติสหกิจศึกษาที่ บริษัท โซซิเคียว จำกัด เป็นระยะเวลา 4 เดือน ตั้งแต่วันที่ 30 พฤษภาคม 2559 จนถึงวันที่ 30 กันยายน 2559 งานและหน้าที่ที่ได้รับมอบหมาย ได้สำเร็จไปด้วยดี และยังได้รับประสบการณ์ใหม่ๆ ไม่ว่าจะเป็นทางด้านเทคนิค และด้านอื่น ๆ ทั้งการได้พบกับลูกค้า การทำเอกสาร การเตรียมงาน ตลอดจนการสื่อสารภายในองค์กร อีเมลล์ อีเมลล์กลุ่ม ลำดับขั้นตอนการทำงาน ฯลฯ

นอกจากที่ได้ความรู้และประสบการณ์ใหม่ๆ จากการปฏิบัติสหกิจศึกษาแล้ว ยังได้ทราบถึงปัญหาที่เกิดขึ้นในขั้นตอนการทำงาน ซึ่งนำไปสู่การแลกเปลี่ยนความคิดเห็นที่จะแก้ไขปัญหา เพื่อหาวิธีการแก้ไขปัญหาที่เหมาะสมที่สุดต่อไป

5.2 แนวทางการแก้ไขปัญหา

ในระหว่างการปฏิบัติสหกิจศึกษานั้น มีปัญหาเกิดขึ้นมากมาย ไม่ว่าจะเป็นปัญหาทางเทคนิค หรือปัญหาทางด้านอื่น ๆ โดยสรุปได้ ดังนี้

- ปัญหาด้านความรู้ความสามารถ
- การปฏิบัติตนเมื่ออยู่ในสถานที่ของลูกค้า / สำนักงาน
- การเปิดเผยข้อมูล
- มนุษยสัมพันธ์

5.2.1 ปัญหาด้านความรู้ความสามารถ

ในการปฏิบัติงานนั้น มีการใช้ความรู้ความสามารถของตนเองหลายอย่าง ซึ่งหลายอย่างนั้น เป็นเนื้อหาที่อยู่นอกเหนือจากที่เรียนในห้องเรียน และอีกหลายอย่างต้องใช้ประสบการณ์ในการทำงาน ดังนั้น การศึกษาหาความรู้เพิ่มเติมจึงเป็นสิ่งสำคัญ เพราะเทคโนโลยี ไม่ได้หยุดนิ่ง ๆ และมีการพัฒนาขึ้นเรื่อย ๆ ดังนั้น ผู้ปฏิบัติงานควรศึกษาหาความรู้ใหม่ ๆ ตามเทคโนโลยีที่พัฒนาไป อย่างสม่ำเสมอ

5.2.2 การปฏิบัติตนเมื่ออยู่ในสถานที่ของลูกค้า / สำนักงาน

การปฏิบัติตนในสถานที่ของลูกค้า หรือสำนักงานของบริษัทนั้น อาจส่งผลต่อภาพลักษณ์ และชื่อเสียงขององค์กร ดังนั้น นักศึกษาควรรู้ว่าต้องระวังอะไรบ้าง เช่น ระวังเผลอหลับระหว่างที่ทำงานในสถานที่ของลูกค้า ฯลฯ เพื่อไม่ให้เกิดปัญหาขึ้นมาในอนาคต

5.2.4 การเปิดเผยข้อมูล

ข้อมูลที่นักศึกษาได้รับมาระหว่างปฏิบัติสหกิจศึกษานั้น มีทั้งข้อมูลทั่วไป และข้อมูลที่เป็นความลับทั้งความลับของบริษัท และความลับของลูกค้า ดังนั้น นักศึกษาจะต้องระวังเป็นอย่างยิ่ง ในการเปิดเผยข้อมูลโดยเฉพาะบนเครือข่ายสังคมต่างๆ เช่น หากนักศึกษาเปิดเผยข้อมูลระบบรักษาความปลอดภัยของสถานที่ลูกค้า อาจส่งผลให้เกิดการเข้าถึงสถานที่ลูกค้าโดยไม่ได้รับอนุญาต และอาจก่อให้เกิดความเสียหายอีกด้วย

5.2.5 มนุษยสัมพันธ์

ในการทำงานนั้น เป็นไปไม่ได้ที่การทำงานทั้งหมด จะใช้คนเพียงคนเดียว ดังนั้น การทำงานจำเป็นต้องมีการสื่อสารกับผู้อื่น ดังนั้น นักศึกษาควรที่จะเรียนรู้การพูดคุย สื่อสารกับผู้อื่น ซึ่งจะไม่ได้เป็นประโยชน์เพียงแค่ทำงานได้ แต่จะมีประโยชน์ในการแก้ปัญหาต่างๆ ด้วยความช่วยเหลือจากผู้อื่นอีกด้วย

5.2.8 ความรับผิดชอบ

ในการทำงาน สิ่งที่สำคัญสิ่งหนึ่ง คือความรับผิดชอบ เพราะการที่รับงานมาแล้วนั้น หากไม่ทำให้เสร็จ จะก่อให้เกิดความเสียหายกับองค์กร เพราะไม่มีใครมาทำงานนั้นแทน ในระหว่างที่ผู้ปฏิบัติงานไม่ทำงานให้เสร็จ ดังนั้น หากรับงานมาแล้ว จะต้องทำให้เสร็จ ตามความต้องการที่ระบุ

5.2.9 การเก็บหลักฐาน

ในการทำงานจริงนั้น เป็นไปไม่ได้ที่ทุกคนในบริษัทจะไม่แสวงหาผลประโยชน์ ดังนั้น จะทำอะไรควรที่จะมีเอกสารยืนยันเป็นลายลักษณ์อักษร เช่น อีเมลล์แจ้งยืนยันปิดงาน เป็นต้น หากไม่มีการยืนยัน อาจทำให้เกิดการเปลี่ยนแปลงที่ไม่พึงประสงค์ได้ เช่น มีการขอแก้ไขหลังจากปิดงาน เนื่องจากต้องการฟังก์ชั่นเพิ่ม หากไม่มีการเก็บหลักฐานเอาไว้ การปิดงานที่ดำเนินการไปก่อนหน้า อาจหายไปได้ โดยไม่มีหลักฐานยืนยัน เป็นต้น

5.3 ข้อเสนอแนะจากการดำเนินงาน

จากปัญหาที่ได้พบในการทำงานในข้อที่ 5.2 จะเห็นได้ว่า การทำงานหลายอย่างยังคงต้องได้รับการปรับปรุง ดังนี้

- ผู้ปฏิบัติงานควรศึกษาหาความรู้เพิ่มเติมอย่างสม่ำเสมอ เนื่องจากเทคโนโลยีมีการพัฒนาตลอดเวลา
- ผู้ปฏิบัติงานควรรู้จัก ว่าลูกค้ามีนิสัยอย่างไร มิฉะนั้นอาจทำให้งานมีปัญหาได้
- ผู้ปฏิบัติงานควรทราบว่าข้อมูลที่อยู่ตรงหน้านั้น เป็นความลับมากน้อยเพียงใด และหลีกเลี่ยงการเปิดเผยข้อมูลใด ๆ ที่เกี่ยวข้องกับลูกค้า หรือบริษัท
- ผู้ปฏิบัติงานควรที่จะสามารถพูดคุยและสร้างความสนิทสนมกับผู้อื่นได้ หากสามารถทำได้ จะทำให้การทำงาน ง่ายขึ้น และมีปัญหาลดลง
- ควรคิดให้ดีก่อนที่จะตกลงรับงาน รับงานต่อเมื่อมั่นใจว่าสามารถทำได้ทันเวลาเท่านั้น เพื่อไม่ให้เป็นปัญหา
- การทำงานทุกขั้นตอน จะต้องมีการเก็บหลักฐานเอาไว้ โดยเฉพาะอีเมลล์ เพื่อให้สถานะของงานชัดเจน และป้องกันการเปลี่ยนแปลงที่ไม่พึงประสงค์ที่อาจเกิดขึ้น

เอกสารอ้างอิง

บัณฑิต จามรภูมิ (2552) , คัมภีร์ Ubuntu Linux Server เล่ม 1 , เอช เอ็น กรุ๊ป จำกัด

บัณฑิต จามรภูมิ (2553) , คัมภีร์ Ubuntu Linux Server เล่ม 2 , เอช เอ็น กรุ๊ป จำกัด

สุเมธ จิตภักดีบดินทร์ (2556) , ก้าวสู่นักทดสอบและก้องกันการเจาะระบบ , กรุงเทพมหานคร

ภาคผนวก ก

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
เลขที่ 1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์
สัปดาห์ที่ 1

ชื่อ-สกุลนักศึกษา ณัฐวรา นาคจันทร์ รหัสนักศึกษา 5812 1012 - 7
คณะวิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 4 ต.ค. 61	9	ศึกษา PDF OWASP	web application pentest	-
อังคาร 5 ต.ค. 61	9	ฝึกฝนเขียนสคริปต์	enumeration	-
พุธ 6 ต.ค. 61	9	ฝึกฝนเขียนสคริปต์	pentest	-
พฤหัสบดี 7 ต.ค. 61	9	ฝึกฝนเขียนสคริปต์	LM HASH	-
ศุกร์ 8 ต.ค. 61	9	ฝึกฝนเขียนสคริปต์	OWASP	-
เสาร์				
อาทิตย์				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	45	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	
จำนวนชั่วโมงในรายงานฉบับก่อน	-	ลงชื่อ ณัฐวรา นาคจันทร์	ลงชื่อ ดวงศักร ไกรสิทธา	
จำนวนชั่วโมงรวมทั้งหมด	45	วันเดือนปี 8/ต.ค./61	ตำแหน่ง Security engineering	
		นักศึกษา	วันเดือนปี 8/ต.ค./61	
			ผู้ควบคุมการปฏิบัติงาน	

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา / ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1221/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่ 2

ชื่อ-สกุลนักศึกษา ณัฐวรท เกษจินดา รหัสนักศึกษา 58121012-7
คณะวิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 11/06/61	9	เตรียมงาน cyber operation contest 2018	network vpn	-
อังคาร 12/06/61	9	support งาน cyber operation contest 2018	ปัญหาที่เกิดขึ้น แก้ไขที่ ctf	-
พุธ 13/06/61	9	ทำ pentest ผ่าน metasploit	pentest	-
พฤหัสบดี 14/06/61	9	ทำไลท์ pentest ผ่าน metasploit2	pentest	-
ศุกร์ 15/06/61	9	ศึกษางาน Project Beacon	Beacon	-
เสาร์ ../../..				
อาทิตย์ ../../..				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	45	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ ลงชื่อ ณัฐวรท (ณัฐวรท เกษจินดา) วัน/เดือน/ปี 15/06/61 นักศึกษา	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ ลงชื่อ ..... (ชยพัฒน์ เอกวิจิตรกุล) ตำแหน่ง Security engineering วัน/เดือน/ปี 15/06/61 ผู้ควบคุมการปฏิบัติงาน
จำนวนชั่วโมงในรายงานฉบับก่อน	45		
จำนวนชั่วโมงรวมทั้งหมด	90		

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา/ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

งานสหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1111/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่ 3

ชื่อ-สกุลนักศึกษา ณัฐวุฒ เกษจันทร์ รหัสนักศึกษา 58121012-7
คณะวิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 18 06 61	9	ฝึกฝนการเขียน	Use Case	-
อังคาร 19 06 61	9	หาข้อมูลเพิ่มเติมโปรเจค	วิธีการที่เพิ่มขึ้น	-
พุธ 20 06 61	9	ฝึกฝนการเขียน	OWASP	-
พฤหัสบดี 21 06 61	9	หาข้อมูลโปรเจคที่ใหม่	Pentest	-
ศุกร์ 22 06 61	9	ฝึกฝนการเขียน	ภาษา C	-
เสาร์...../...../.....				
อาทิตย์...../...../.....				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	45	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	
จำนวนชั่วโมงในรายงานฉบับก่อน	90	ลงชื่อ..... (ณัฐวุฒ เกษจันทร์) วัน/เดือน/ปี 22/06/61 นักศึกษา	ลงชื่อ..... (พงศกร เอกสิงคกุล) ตำแหน่ง Security engineering วัน/เดือน/ปี 22/06/61 ผู้ควบคุมการปฏิบัติงาน	
จำนวนชั่วโมงรวมทั้งหมด	135			

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา / ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1771/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่ 4

ชื่อ-สกุลนักศึกษา ณัฐวรา เกษจันทร์ รหัสนักศึกษา 58121012-7

คณะวิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 23 ต.ค. 61	9	LAB	wireshark	-
อังคาร 24 ต.ค. 61	9	LAB	encryption	-
พุธ 24 ต.ค. 61	9	การกู้คืนข้อมูล	recovery Data	-
พฤหัสบดี 25 ต.ค. 61	9	การลบข้อมูลถาวร	Wipe encryption disk	-
ศุกร์ 26 ต.ค. 61	9	ทำเอกสาร	encryption disk	-
เสาร์				
อาทิตย์				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	45	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ ลงชื่อ ณัฐวรา (ณัฐวรา เกษจันทร์) วัน/เดือน/ปี 29 ต.ค. 61 นักศึกษา	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ ลงชื่อ ( ) ตำแหน่ง security engineering วัน/เดือน/ปี 29/10/61 ผู้ควบคุมการปฏิบัติงาน
จำนวนชั่วโมงในรายงานฉบับก่อน	135		
จำนวนชั่วโมงรวมทั้งหมด	180		

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา/ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1771/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่ 5

ชื่อ-สกุลนักศึกษา ณัฐวรา เกษจันทร์ รหัสนักศึกษา 58121012-4

คณะวิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วันเดือนปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 2 ต.ค. 61	9	ลองใช้ Pentest	Dos attack	-
อังคาร 3 ต.ค. 61	9	ศึกษาข้อมูลเพิ่มเติม	Dos attack	-
พุธ 4 ต.ค. 61	9	ลองใช้ malware analysis	malware analysis	-
พฤหัสบดี 5 ต.ค. 61	9	ศึกษาข้อมูลเพิ่มเติม	malware	-
ศุกร์ 6 ต.ค. 61	9	สรุป Dos & malware analysis	Power Point	-
เสาร์				
อาทิตย์				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	45	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	
จำนวนชั่วโมงในรายงานฉบับก่อน	180	ลงชื่อ ณัฐวรา (ณัฐวรา เกษจันทร์)	ลงชื่อ (ผศ.ดร. เกวลิตรกุล)	
จำนวนชั่วโมงรวมทั้งหมด	225	วัน/เดือน/ปี 6/ต.ค./61 นักศึกษา	ตำแหน่ง Security Engineering วัน/เดือน/ปี 6/ต.ค./61 ผู้ควบคุมการปฏิบัติงาน	

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา / ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1521/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่ 6

ชื่อ-สกุลนักศึกษา กนิษวรา เกษวันหงู รหัสนักศึกษา 58121012-4
คณะ วิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 9 ก.ค. 61	9	ศึกษาเกี่ยวกับรูปแบบการโจมตี Worry	Threat	-
อังคาร 10 ก.ค. 61	9	ดำเนินการแก้ไขเกี่ยวกับรูปแบบการโจมตีไวรัส	Threat	-
พุธ 11 ก.ค. 61	9	ศึกษาวิธีแก้ไขเกี่ยวกับรูปแบบการโจมตีไวรัส	Threat	-
พฤหัสบดี 12 ก.ค. 61	9	ศึกษาโปรแกรม	Snort	-
ศุกร์ 13 ก.ค. 61	9	ศึกษาโปรแกรม	Snort	-
เสาร์				
อาทิตย์				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	45	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	
จำนวนชั่วโมงในรายงานฉบับก่อน	225	ลงชื่อ กนิษวรา (กนิษวรา เกษวันหงู)	ลงชื่อ (พงศกร ไกรจิตรกุล)	
จำนวนชั่วโมงรวมทั้งหมด	270	วัน/เดือน/ปี 13/07/61 นักศึกษา	ตำแหน่ง Security engineering วัน/เดือน/ปี 13/07/61 ผู้ควบคุมการปฏิบัติงาน	

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา / ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1111 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่ 4

ชื่อ-สกุลนักศึกษา ณัฐวรรธ หาญจันทร์ รหัสนักศึกษา 5812101127

คณะวิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วัน-เดือน ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 16 ก.ค. 61	9	ศึกษาเรื่อง web pentest	web security	-
อังคาร 17 ก.ค. 61	9	ทำแลป web pentest	web security	-
พุธ 18 ก.ค. 61	9	ทำสไลด์ web pentest	web security	-
พฤหัสบดี 19 ก.ค. 61	9	ศึกษาเรื่อง project	honeypot	-
ศุกร์ 20 ก.ค. 61	9	ศึกษาเรื่อง project	honeypot	-
เสาร์				
อาทิตย์				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	45	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ
จำนวนชั่วโมงในรายงานฉบับก่อน	270	ลงชื่อ ณัฐวรรธ	ลงชื่อ
จำนวนชั่วโมงรวมทั้งหมด	315	(ณัฐวรรธ เทศจันทร์)	(พวงทอง เดชาวิจิตรกุล)
		วัน/เดือน/ปี 20 ก.ค. 61	ตำแหน่ง Security engineering
		นักศึกษา	วัน/เดือน/ปี 20/07/61
			ผู้ควบคุมการปฏิบัติงาน

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา/ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1521/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่ 8

ชื่อ-สกุลนักศึกษา ณัฐวุฒ เกษจันทร์ รหัสนักศึกษา 5812101127
คณะวิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 23 ก.ค. 61	9	ศึกษาข้อมูล network security	network security	-
อังคาร 24 ก.ค. 61	9	ศึกษาเรื่อง network security	network security	-
พุธ 25 ก.ค. 61	9	ทำสไลด์ network security	network security	-
พฤหัสบดี 26 ก.ค. 61	9	ลักษณะ Project	honey pot	-
ศุกร์ ../../..		-		
เสาร์ ../../..				
อาทิตย์ ../../..				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	36	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ ลงชื่อ ณัฐวุฒ (ณัฐวุฒ เกษจันทร์) วัน/เดือน/ปี 26/07/61 นักศึกษา	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ ลงชื่อ (พงศกร เอกลิขิตกุล) ตำแหน่ง security engineering วัน/เดือน/ปี 26/07/61 ผู้ควบคุมการปฏิบัติงาน
จำนวนชั่วโมงในรายงานฉบับก่อน	315			
จำนวนชั่วโมงรวมทั้งหมด	351			

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา/ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์
สัปดาห์ที่ 9

ชื่อ-สกุลนักศึกษา กันยรัตน์ เกษจันทร์ รหัสนักศึกษา 58121012-7
คณะวิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วันเดือนปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์		-		
อังคาร 31 07 61	9	ศึกษาเรื่อง System Security	System Security	-
พุธ 1 08 61	9	ทำเอกสาร System Security	System Security	-
พฤหัสบดี 2 08 61	9	ทำสไลด์ System Security	System Security	-
ศุกร์ 3 08 61	9	ศึกษา Project	Splunk	-
เสาร์				
อาทิตย์				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	36	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	
จำนวนชั่วโมงในรายงานฉบับก่อน	351	ลงชื่อ กันยรัตน์ เกษจันทร์	ลงชื่อ พงศกร เดชวิชิตกุล	
จำนวนชั่วโมงรวมทั้งหมด	387	วัน/เดือน/ปี 3/08/61 นักศึกษา	ตำแหน่ง Security engineering วัน/เดือน/ปี 3/08/61 ผู้ควบคุมการปฏิบัติงาน	

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา/ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

หน่วยสหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่ 10

ชื่อ-สกุลนักศึกษา กิตติวรา เกษจันทร์ รหัสนักศึกษา 6521012-2

คณะวิชา คอมพิวเตอร์และสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วันเดือนปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้ ทักษะที่ได้รับ	ปัญหาและอุปสรรค
จันทร์ 6/08/61	9	เขียนต่อ Project	mikrotik	-
อังคาร 7/08/61	9	เรียน Project	mikrotik	-
พุธ 8/08/61	9	สอบ network	mikrotik	-
พฤหัสบดี 9/08/61	9	ทำต่อ mikrotik	mikrotik	-
ศุกร์ 10/08/61	9	สอบ flowchart	flowchart	-
เสาร์ ...../...../.....				
อาทิตย์ ...../...../.....				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	45	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	
จำนวนชั่วโมงในรายงานฉบับก่อน	384	ลงชื่อ..... (กิตติวรา เกษจันทร์) วันเดือนปี 10/08/61 นักศึกษา	ลงชื่อ..... (ผศ.ดร. ...) ตำแหน่ง Security engineering วันเดือนปี 10/08/61 ผู้ควบคุมการปฏิบัติงาน	
จำนวนชั่วโมงรวมทั้งหมด	432			

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา / ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1771/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-761-2750 Fax: 0-2763-2600 ต่อ 2755 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่ 11

ชื่อ-สกุลนักศึกษา ศิรวิศ เกษจันทร์ รหัสนักศึกษา 58121012-2
คณะวิชา เทคโนโลยีวิศวกรรม สาขาวิชา เทคโนโลยีวิศวกรรมเครือข่าย

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้ ทักษะที่ได้รับ	ปัญหาและอุปสรรค
จันทร์		-		
อังคาร 14 ส.ค. 61	9	สร้าง vm workstation	vmware workstation	-
พุธ 15 ส.ค. 61	9	สร้าง vm mikrotik	mikrotik	-
พฤหัสบดี 16 ส.ค. 61	9	สร้าง vm snort	snort	-
ศุกร์ 17 ส.ค. 61	9	สร้าง vm honeypot	honeynet	-
เสาร์				
อาทิตย์				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	36	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	
จำนวนชั่วโมงในรายงานฉบับก่อน	432	ลงชื่อ ศิรวิศ (ศิรวิศ เกษจันทร์) วัน/เดือน/ปี 17/08/61 นักศึกษา	ลงชื่อ (ภาคิน โตวิมลกุล) ตำแหน่ง Pentester วัน/เดือน/ปี 17/08/61 ผู้ควบคุมการปฏิบัติงาน	
จำนวนชั่วโมงรวมทั้งหมด	468			

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา / ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1773 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์ 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่ 13

ชื่อ-สกุลนักศึกษา ณัฐวุฒ เกษจันทร์ รหัสนักศึกษา 6212101127
คณะวิชา เทคโนโลยีวิศวกรรม สาขาวิชา เทคโนโลยีสารสนเทศ

วัน-เดือน-ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 27 ส.ค. 61	9	ฝึกงาน Snort	Snort	-
อังคาร 28 ส.ค. 61	9	ฝึกงาน Snort	Snort	-
พุธ 29 ส.ค. 61	9	ฝึกงาน Snort	Snort	-
พฤหัสบดี 30 ส.ค. 61	9	ฝึกงาน Splunk	Splunk	-
ศุกร์ 31 ส.ค. 61	9	ฝึกงาน Splunk	Splunk	-
เสาร์				
อาทิตย์				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	45	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	
จำนวนชั่วโมงในรายงานฉบับก่อน	513	ลงชื่อ..... (ณัฐวุฒ เกษจันทร์) วัน/เดือน/ปี 31/08/61	ลงชื่อ..... (พงศกร ธนสิทธิกุล) ตำแหน่ง Pentester วัน/เดือน/ปี 31/08/61	
จำนวนชั่วโมงรวมทั้งหมด	558	นักศึกษา	ผู้ควบคุมการปฏิบัติงาน	

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา/ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1771/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์
สัปดาห์ที่ 12

ชื่อ-สกุลนักศึกษา กฤษวรา ทายันหนู รหัสนักศึกษา 58121012-4
คณะวิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 20 ส.ค. 61	9	ลง vm splunk	Splunk	-
อังคาร 21 ส.ค. 61	9	สร้างเว็บ honeypot	... ฟังก์ชัน	-
พุธ 22 ส.ค. 61	9	สร้างเว็บ honeypot	ฟังก์ชันต่างๆ	-
พฤหัสบดี 23 ส.ค. 61	9	ลง mikrotik ใหม่	mikrotik	-
ศุกร์ 24 ส.ค. 61	9	ลง mikrotik	mikrotik	-
เสาร์...../...../.....				
อาทิตย์...../...../.....				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	45	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ ลงชื่อ..... (กฤษวรา เกษจันทร์) วัน/เดือน/ปี 24/08/61 นักศึกษา	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ ลงชื่อ..... (.....) ตำแหน่ง pentester วัน/เดือน/ปี 24/08/61 ผู้ควบคุมการปฏิบัติงาน
จำนวนชั่วโมงในรายงานฉบับก่อน	468			
จำนวนชั่วโมงรวมทั้งหมด	513			

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา/ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1773 3 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่ 14

ชื่อ-สกุลนักศึกษา [illegible] รหัสนักศึกษา 58121012-4

คณะวิชา [illegible] สาขาวิชา [illegible]

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 3 ก.ย. 61	9	[illegible] Splunk	Splunk	-
อังคาร 4 ก.ย. 61	9	[illegible] honeypot	honeypot	-
พุธ 5 ก.ย. 61	9	[illegible] Splunk	Splunk	-
พฤหัสบดี 6 ก.ย. 61	9	[illegible] Splunk	Splunk	-
ศุกร์ 7 ก.ย. 61	9	[illegible] Splunk	Splunk	-
เสาร์				
อาทิตย์				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	45	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	
จำนวนชั่วโมงในรายงานฉบับก่อน	558	ลงชื่อ [illegible]	ลงชื่อ [illegible]	
จำนวนชั่วโมงรวมทั้งหมด	603	([illegible])	([illegible])	
		วัน/เดือน/ปี 7/09/61	ตำแหน่ง Pentester	
		นักศึกษา	วัน/เดือน/ปี 7/09/61	
			ผู้ควบคุมการปฏิบัติงาน	

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา/ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1771/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่ 15

ชื่อ-สกุลนักศึกษา ณัฐวรา เกษจินดา รหัสนักศึกษา 58121012-4
คณะวิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 10/09/61	9	Test งาน	Honeypot	-
อังคาร 11/09/61	9	ทำเล่มรายงาน	word	-
พุธ 12/09/61	9	ทำเล่มรายงาน	word	-
พฤหัสบดี 13/09/61	9	ทำเล่มรายงาน	word	-
ศุกร์ 14/09/61	9	ทำเล่มรายงาน	word	-
เสาร์ ../../..				
อาทิตย์ ../../..				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	45	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	
จำนวนชั่วโมงในรายงานฉบับก่อน	603	ลงชื่อ ณัฐวรา เกษจินดา	ลงชื่อ [illegible]	
จำนวนชั่วโมงรวมทั้งหมด	648	วัน/เดือน/ปี 14/09/61 นักศึกษา	ตำแหน่ง Pentester วัน/เดือน/ปี 14/09/61 ผู้ควบคุมการปฏิบัติงาน	

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา/ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1771/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2666 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่ 16

ชื่อ-สกุลนักศึกษา นิฐวรา เกษจินดา รหัสนักศึกษา 5811210177-7

คณะวิชา เทคโนโลยีการจัดการ สาขาวิชา เทคโนโลยีวิศวกรรม

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 13 ก.ย. 61	9	ทำงานตามปกติ	ความรู้	-
อังคาร 14 ก.ย. 61	9	ทำงานตามปกติ	ความรู้	-
พุธ 15 ก.ย. 61	9	ทำงานตามปกติ	ความรู้	-
พฤหัสบดี 16 ก.ย. 61	9	ทำงานตามปกติ	ความรู้	-
ศุกร์ 17 ก.ย. 61	9	ทำงานตามปกติ	ความรู้	-
เสาร์				
อาทิตย์				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	45	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ ลงชื่อ นิฐวรา (นิฐวรา เกษจินดา) วันเดือนปี 21/09/61 นักศึกษา	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ ลงชื่อ (ชนกร เอกวิจิตรกุล) ตำแหน่ง Penkster วันเดือนปี 21/09/61 ผู้ควบคุมการปฏิบัติงาน
จำนวนชั่วโมงในรายงานฉบับก่อน	648			
จำนวนชั่วโมงรวมทั้งหมด	693			

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา/ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1771/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่ 14

ชื่อ-สกุลนักศึกษา นิ่งนาท เกษจันทร์ รหัสนักศึกษา 58121012-7

คณะวิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีคอมพิวเตอร์

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 24/09/61	9	ทำ Slide	Power Point	
อังคาร 25/09/61	9	ทำ Slide	Power Point	
พุธ 26/09/61	9	ทำ Slide	Power Point	
พฤหัสบดี 27/09/61	9	ทำ Slide	Power Point	
ศุกร์ 28/09/61	9	ทำ Slide	Power Point	
เสาร์...../...../.....				
อาทิตย์...../...../.....				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	45	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	
จำนวนชั่วโมงในรายงานฉบับก่อน	693	ลงชื่อ..... (นิ่งนาท เกษจันทร์)	ลงชื่อ..... (ดลชัย เอกวิสารกุล)	
จำนวนชั่วโมงรวมทั้งหมด	738	วัน/เดือน/ปี 28/09/61 นักศึกษา	ตำแหน่ง Pentester วัน/เดือน/ปี 28/09/61 ผู้ควบคุมการปฏิบัติงาน	

<u>หมายเหตุ</u> นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา / ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ภาคผนวก ข

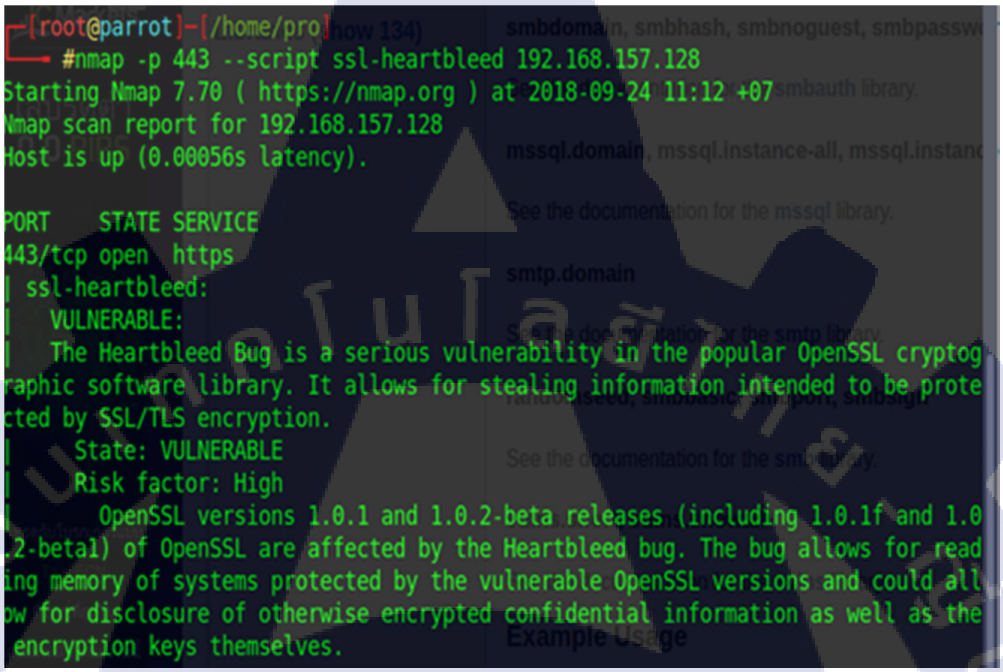
คู่มือการใช้งาน ระบบฮันนีพอตและล็อกไฟล์

ระบบนี้สร้างขึ้นเพื่อใช้สำหรับการโจมตีและเก็บล็อก ส่งล็อกและไปวิเคราะห์ที่ splunk

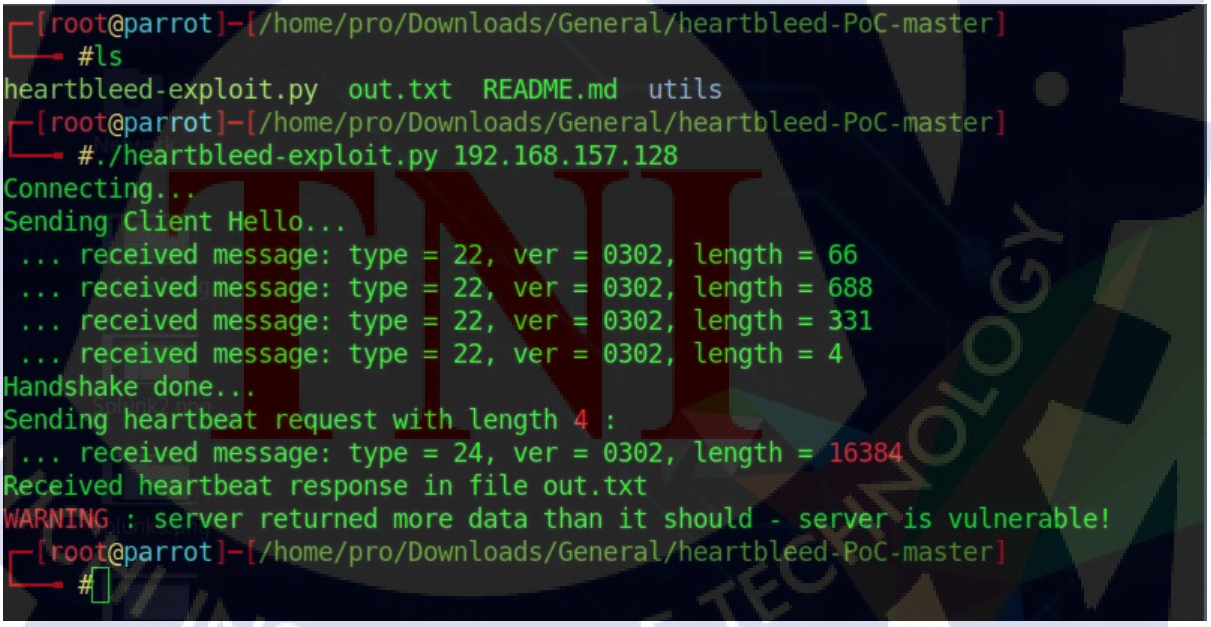
1.เริ่มจากการแสกนหาช่องโหว่ โดยใช้ software Nmap

Nmap –sV iptarget

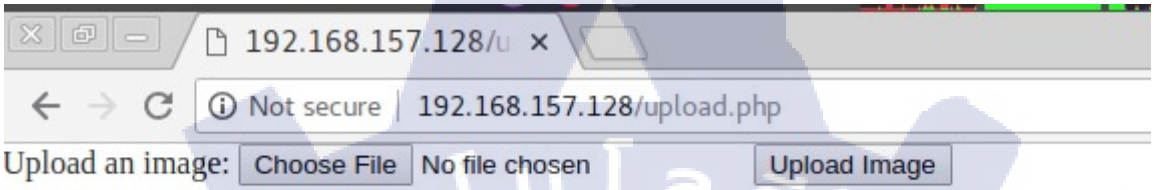
2.จากข้อ 1 service SSL เปิดอยู่ แสกนช่องโหว่ heartbeat



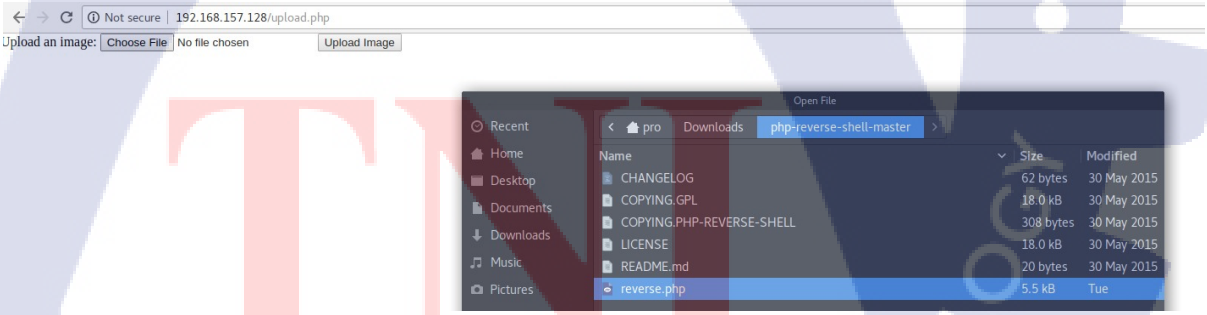
3.ใช้สคริปต์ในการโจมตี



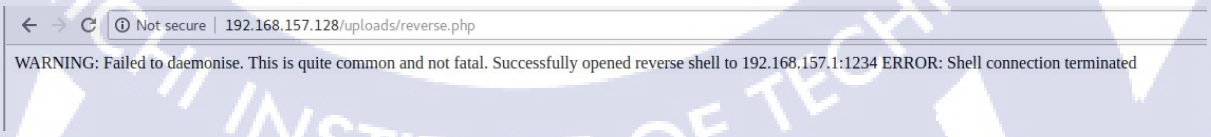
4.เปิดดูพอร์ต 80 พบหน้าเว็บอัพโหลด



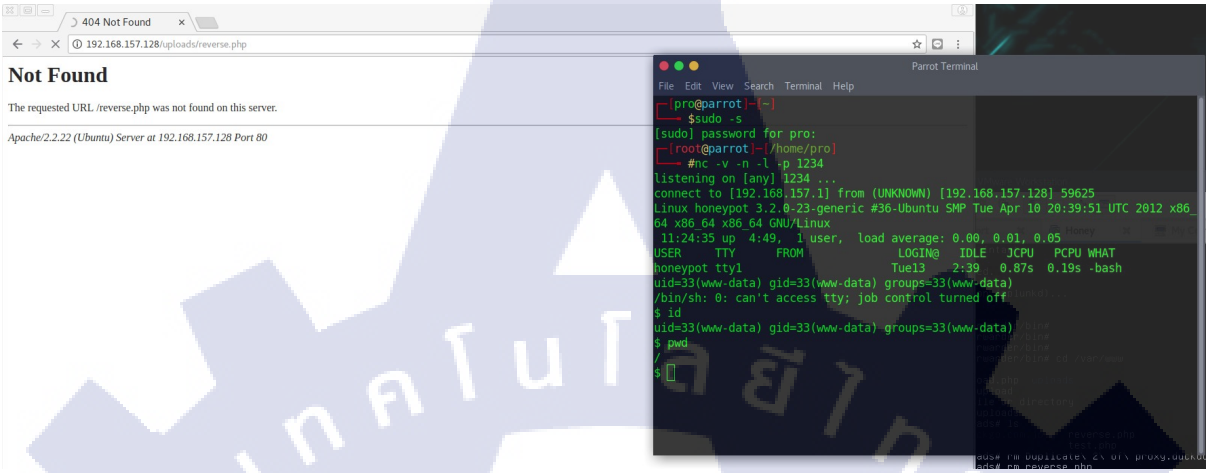
5.upload reverse shell



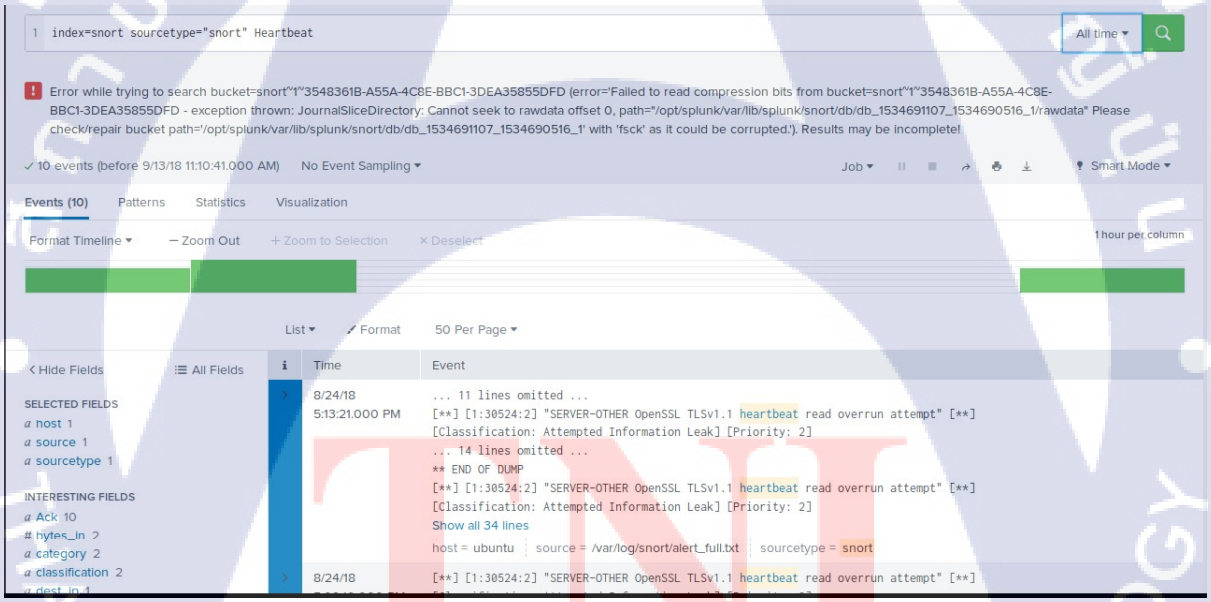
6.run reverse shell อีกฝั่งเปิดคำสั่ง nc ไว้

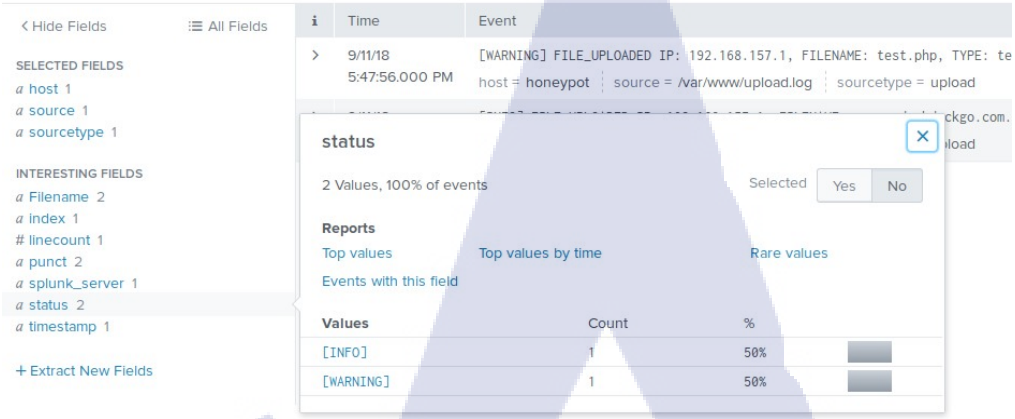


7.ผลลัพธ์



8. ผลลัพธ์ Log on Splunk




Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a Filename 2
a index 1
linecount 1
a punct 2
a splunk_server 1
a status 2
a timestamp 1
+ Extract New Fields
Time
Event
9/11/18
5:47:56.000 PM
[WARNING] FILE_UPLOADED IP: 192.168.157.1, FILENAME: test.php, TYPE: te
host = honeypot
source = /var/www/upload.log
sourcetype = upload
status
2 Values, 100% of events
Selected
Yes
No
Reports
Top values
Top values by time
Rare values
Events with this field
Values
Count
%
[INFO]
1
50%
[WARNING]
1
50%

ประวัติผู้จัดทำโครงงาน

ชื่อ – สกุล นางสาว ณัฐวรา เกษจันทร์

วัน เดือน ปีเกิด 9 เมษายน 2540

ประวัติการศึกษา

ระดับประถมศึกษา โรงเรียนช่างอากาศอำรุง พ.ศ. 2546

ระดับมัธยมศึกษา โรงเรียนราชินีบน พ.ศ. 2552

ระดับอุดมศึกษา สถาบันเทคโนโลยีไทย-ญี่ปุ่น พ.ศ. 2558

ทุนการศึกษา - ไม่มี -