การทดสอบเปรียบเทียบผลิตภัณฑ์ค้นหาช่องโหว่ด้านความปลอดภัยระบบ (OpenVAS, Nessus, Nexpose)

Comparative testing for system vulnerability assessment product (OpenVAS, Nessus, Nexpose)

นายนิติพัฒน์ อานน้อย

โครงงานสหกิจศึกษานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิทยาศาสตร์บัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีไทย – ญี่ปุ่น
พ.ศ. 2558

การทดสอบเปรียบเทียบผลิตภัณฑ์ค้นหาช่องโหว่ด้านความปลอดภัยระบบ (OpenVAS, Nessus, Nexpose)

Comparative testing for system vulnerability assessment product (OpenVAS, Nessus, Nexpose)

นายนิติพัฒน์ อานน้อย

โครงงานสหกิจศึกษานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิทยาศาสตร์บัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีไทย – ญี่ปุ่น
พ.ศ. 2558

คณะกรรมการสอบ

..... ประธานกรรมการสอบ
(ผศ.นรังสรรค์ วิไลสกุลยง)

..... กรรมการสอบ
(ดร.ธงชัย แก้วกิริยา)

..... อาจารย์ที่ปรึกษา
(อาจารย์ปราณิสา อิศรเสนา)

..... ประธานสหกิจศึกษาสาขาวิชา
(อาจารย์อมรพันธ์ ชมกลิ่น)

ชื่อโครงงาน	การทดสอบเปรียบเทียบผลิตภัณฑ์ค้นหาช่องโหว่ด้านความปลอดภัยระบบ (Nessus , Nexpose , OpenVAS)
ผู้เขียน	นายนิติพัฒน์ อานน้อย
คณะวิชา	เทคโนโลยีสารสนเทศ สาขาวิชาเทคโนโลยีสารสนเทศ
อาจารย์ที่ปรึกษา	อาจารย์ปราณิสา อิศรเสนา
พนักงานที่ปรึกษา	คุณพุทธิมงคล บำรุงพิพัฒนพร
ชื่อบริษัท	บริษัท เอส-เจเนเรชัน จำกัด
ประเภทธุรกิจ / สินค้า	ให้คำปรึกษาและจัดจำหน่ายผลิตภัณฑ์รักษาความปลอดภัยเครือข่าย

บทสรุป

ปัจจุบันความปลอดภัยทางเทคโนโลยีสารสนเทศเป็นปัจจัยสำคัญอย่างหนึ่งในการดำเนินธุรกิจ เพราะว่าข้อมูลสำคัญนั้นย่อมเป็นความลับและมีค่า จึงเป็นไม่ได้เลยที่จะยอมให้ข้อมูลเหล่านั้นตกไปอยู่ในมือของผู้ไม่หวังดี

โครงงานนี้คือการทดสอบเปรียบเทียบคุณสมบัติผลิตภัณฑ์ค้นหาช่องโหว่ด้านความปลอดภัย 3 ผลิตภัณฑ์ (Nessus , Nexpose ,OpenVAS) เพื่อนำมาใช้ในการตัดสินใจของลูกค้าในการซื้อผลิตภัณฑ์ค้นหาช่องโหว่ที่จะนำผลิตภัณฑ์ดังกล่าวไปใช้ค้นหาช่องโหว่ภายในบริษัทของตนเอง เพื่อที่จะได้ทำการป้องกันและแก้ไขระบบได้อย่างสมบูรณ์ โครงงานนี้ทำได้รับประสบการณ์ในการปฏิบัติงานจริงในบริษัท ซึ่งในระหว่างปฏิบัติงานได้มีโอกาสร่วมกับพนักงานภายในบริษัท ทำให้ได้รับความรู้ที่กว้างขวางเกี่ยวกับด้านความปลอดภัยทางสารสนเทศ ล้วนแล้วแต่มีประโยชน์ในการปฏิบัติงานในอนาคต จากผลการทดสอบเป็นที่น่าพอใจต่อลูกค้าเป็นอย่างมาก อีกทั้งยังสามารถเพิ่มยอดขายของทางบริษัทได้อีกด้วย

กิตติกรรมประกาศ

ในการปฏิบัติงานสหกิจศึกษาที่บริษัท เอส-เจเนเรชัน จำกัด เป็นระยะเวลาทั้งสิ้น 4 เดือน นั้น ได้รับความกรุณาและการดูแลจากบุคคลหลายๆท่าน, ได้รับเรียนรู้การทำงานจริง, และได้รับความรู้ต่างๆมากมาย ทำให้การปฏิบัติงานครั้งนี้สำเร็จลุล่วงไปได้ด้วยดี

ขอขอบคุณ คุณพุทธิมงคล บำรุงพิพัฒนพร พนักงานที่ปรึกษา ซึ่งให้การดูแลและให้คำปรึกษาต่างๆ ในการทำงาน รวมถึงตอบข้อสงสัยต่างๆอย่างกระจ่าง พร้อมทั้งแนะนำเทคนิคในการทำงาน ซึ่งสามารถนำไปใช้ได้จริง รวมไปถึงพนักงานท่านอื่นๆ ที่ให้การดูแลและตอบข้อสงสัย รวมถึงเป็นที่ปรึกษาและคอยให้ข้อมูลในด้านต่างๆในการทำงาน ทำให้การปฏิบัติงานสหกิจศึกษาตลอด 4 เดือน ที่ผ่านมาเป็นความทรงจำที่น่าประทับใจ ขอขอบพระคุณทุกท่านไว้ ณ โอกาสนี้ด้วย

นิติพัฒน์ อานน้อย

สารบัญ

หน้า

บทสรุป ก

กิตติกรรมประกาศ ข

สารบัญ ค

สารบัญตาราง ฉ

สารบัญภาพประกอบ ช

บทที่

1. บทนำ

1.1 ชื่อและที่ตั้งของสถานประกอบการ 1

1.2 ลักษณะธุรกิจของสถานประกอบการ หรือการให้บริการหลักขององค์กร 2

1.3 รูปแบบการจัดการองค์กรและการบริหารองค์กร 4

1.4 ตำแหน่งและหน้าที่งานที่นักศึกษาได้รับมอบหมาย 5

1.5 พนักงานที่ปรึกษาและตำแหน่งของพนักงานที่ปรึกษา 5

1.6 ระยะเวลาที่ปฏิบัติงาน 5

1.7 ที่มาและความสำคัญของปัญหา 5

1.8 วัตถุประสงค์หรือจุดมุ่งหมายของโครงงาน 6

1.9 ผลที่คาดว่าจะได้รับจากการปฏิบัติงานหรือโครงงานที่ได้รับมอบหมาย 6

2. ทฤษฎีและเทคโนโลยีที่ใช้ในการปฏิบัติงาน

2.1 ทฤษฎีที่ใช้ในการปฏิบัติงาน 7

2.1.1 ความหมายของ Penetration Test และ Vulnerability Assessment 7

2.1.1.1. การทำ Penetration Test จากภายนอกระบบเครือข่ายองค์กร (Black Box) 7

2.1.1.2. การทำ Penetration test ภายในองค์กรเชิงลึก (White Box) 10

2.1.2 มาตรฐานOWASP (Open Web Application Security Project) 13

2.1.3 มาตรฐานการกำหนดชื่อช่องโหว่ด้วย CVE (Common Vulnerabilities and

Exposures) 15

2.2 เทคโนโลยีที่ใช้ในการปฏิบัติงาน 16

2.2.1 Nessus vulnerability scanner 16

2.2.2 Nexpose 18

2.2.3 OpenVAS (Open Vulnerability Assessment System) 19

2.2.4 Metasploitable 20

3. แผนงานการปฏิบัติงานและขั้นตอนการดำเนินงาน

3.1 แผนการปฏิบัติงาน 21

3.2 รายละเอียดงาน 22

3.3 ขั้นตอนการดำเนินงาน 23

3.3.1 ขั้นตอนการศึกษาค้นคว้า 23

3.3.1.1 การศึกษาค้นคว้าเกี่ยวกับช่องโหว่ต่างๆ 23

3.3.1.1.1 OWASP (Open Web Application Security Project) 23

3.3.1.1.2 CVE (Common Vulnerabilities and Exposures) 26

3.3.2 ขั้นตอนการเตรียมการ 27

3.3.2.1 ติดตั้งระบบปฏิบัติการ Linux Kali Sana ลงบน VMware Workstation 27

3.3.2.2 ติดตั้ง Metasploitable ลงบน VMware Workstation 34

3.3.2.3 ติดตั้ง OpenVAS 36

3.3.2.4 ติดตั้ง Nexpose 38

3.3.2.5 ติดตั้ง Nessus 41

4. สรุปผลการดำเนินงาน การวิเคราะห์และสรุปผลต่างๆ

4.1 ขั้นตอนและผลการดำเนินงาน 43

4.1.1 ผลการดำเนินงานการพัฒนาเว็บแอปพลิเคชันสืบค้นและจัดเก็บฐานข้อมูลภายในบริษัท 43

4.1.2 ผลการดำเนินงานทดสอบแอปพลิเคชัน Nessus 44

4.1.3 ผลการดำเนินงานทดสอบแอปพลิเคชัน Nexpose 48

4.1.4 ผลการดำเนินงานทดสอบแอปพลิเคชัน OpenVAS 51

4.2 ผลการวิเคราะห์ข้อมูล 53

4.2.1 ผลการวิเคราะห์เปรียบเทียบ 53

4.3 วิจารณ์ข้อมูลโดยเปรียบเทียบผลที่ได้รับกับวัตถุประสงค์และจุดมุ่งหมายการปฏิบัติงานหรือการจัดทำโครงการ 55

5. บทสรุปและข้อเสนอแนะ

5.1 สรุปผลการดำเนินโครงงาน 56

5.2 แนวทางแก้ไขปัญหา 56

5.3 ข้อเสนอแนะจากการดำเนินงาน 56

เอกสารอ้างอิง 58

ประวัติผู้จัดทำโครงการ 59

สารบัญตาราง

ตารางที่ **หน้า**

3.1 แผนการปฏิบัติงาน 21

3.2 แสดงรายละเอียดงาน และลักษณะงานที่ปฏิบัติ 22

4.1 ตารางเปรียบเทียบผลิตภัณฑ์ 53

4.2 ตารางเปรียบเทียบผลิตภัณฑ์ (ต่อ) 54

4.3 ตารางเปรียบเทียบผลที่ได้รับกับวัตถุประสงค์ในการปฏิบัติงาน 55

สารบัญภาพประกอบ

ภาพที่ **หน้า**

1.1 สัญลักษณ์ S-Generation 1

1.2 แผนที่ S-Generation 1

1.3 ผังองค์กร S-Generation Co., Ltd. 4

1.4ผังองค์กร S-Forensics International Co., Ltd. 4

2.1 สัญลักษณ์ Nessus 16

2.2 หน้าจอแสดงรูปแบบการค้นหาช่องโหว่ Nessus 17

2.3 สัญลักษณ์ Nexpose 17

2.4 หน้าจอหลักของ Nexpose 18

2.5 สัญลักษณ์ OpenVAS 18

2.6 หน้าจอหลักของ OpenVAS 19

2.7 หน้าจอของ Metasploitable 20

3.1 ภาพโปรแกรม VMware Workstation รุ่นที่ 11 27

3.2 ไอคอน Create a New Virtual Machine 27

3.3 หน้าต่าง New Virtual Machine Wizard 28

3.4 หน้าต่างเลือกวิธีการในการติดตั้ง 28

3.5 หน้าต่างเลือกระบบปฏิบัติการ 29

3.6 หน้าต่างเลือก Directory ของ Virtual Machine 29

3.7 หน้าต่างเลือกขนาดและวิธีการเก็บ 30

3.8 หน้าต่างสรุปการติดตั้ง 30

3.9 หน้าจอขณะกำลังติดตั้ง Ubuntu Server 31

3.10 หน้าจอขณะทำการติดตั้ง Apache 31

3.11 การตรวจสอบการเปิดพอร์ท TCP HTTP 32

3.12 หน้าจอขณะกำลังแก้ไขไฟล์ด้วย CLI command 32

3.13 หน้าจอแสดงรายละเอียดของ PHP 33
3.14 หน้าจอตั้งรหัสผ่าน MySQL 34
3.15 การตรวจสอบการเปิดพอร์ท TCP MySQL 34
3.16 ภาพโปรแกรม VMware Workstation รุ่นที่ 11 34
3.17 ไอคอน Open a Virtual Machine 35
3.18 หน้าต่าง Metasploitable 35
3.19 หน้าต่างตั้งค่า Virtual Machine 36
3.20 หน้าจอเลือกโปรแกรม openvas initial setup 36
3.21 หน้าจอขณะติดตั้ง OpenVAS Initial Setup 37
3.22 หน้าจอหลังจากติดตั้ง OpenVAS Initial Setup (ต่อ) 37
3.23 ภาพโปรแกรม OpenVAS Start 38
3.24 หน้าจอแสดงการเริ่มต้นการทำงาน 38
3.25 หน้าต่างแรกของการติดตั้ง Nexpose 38
3.26 หน้าต่างแสดงความต้องการของโปรแกรม 39
3.27 หน้าต่างเลือกแฟ้มเพื่อสร้างทางลัด 39
3.28 หน้าต่างแสดงสถานการณ์ติดตั้ง 40
3.29 หน้าต่างเสร็จสิ้นการติดตั้ง 40
3.30 หน้าต่างเริ่มต้นการติดตั้ง Nessus 41
3.31 หน้าต่างยืนยันข้อตกลงทางลิขสิทธิ์ 41
3.32 หน้าต่างยืนยันการติดตั้ง 42
3.33 หน้าต่างเสร็จสิ้นการติดตั้ง 42
4.1 หน้าแรกของเว็บแอปพลิเคชัน 44
4.2 หน้าจอการเลือกรูปแบบการค้นหาช่องโหว่ Nessus 44
4.3 หน้าจอการกรอกรายละเอียดของการค้นหาช่องโหว่ Nessus 45
4.4 หน้าจอการกรอกรายละเอียดของการค้นหาช่องโหว่ Nessus (ต่อ) 45
4.5 หน้าจอการกรอกรายละเอียดของการค้นหาช่องโหว่ Nessus (ต่อ) 46

4.6 หน้าจอขณะกำลังสแกนค้นหาช่องโหว่ Nessus 46
4.7 หน้าจอแสดงสรุปผลการค้นหาช่องโหว่ Nessus 47
4.8 หน้าจอรายงานการค้นหาช่องโหว่ Nessus 47
4.9 หน้าจอกรอกรายละเอียดการค้นหาช่องโหว่ Nexpose 48
4.10 หน้าจอกรอกรายละเอียดการค้นหาช่องโหว่ Nexpose (ต่อ) 48
4.11 หน้าจอเลือกรูปแบบของการค้นหาช่องโหว่ Nexpose 49
4.12 หน้าจอขณะกำลังสแกนค้นหาช่องโหว่ Nexpose 49
4.13 หน้าจอขณะกำลังสแกนค้นหาช่องโหว่ Nexpose (ต่อ) 49
4.14 หน้าจอเลือกรูปแบบการออกรายงาน Nexpose 50
4.15 หน้าจอรายงานการค้นหาช่องโหว่ Nexpose 50
4.16 หน้าจอรายงานการค้นหาช่องโหว่ Nexpose (ต่อ) 51
4.17 หน้าจอกรอกรายละเอียดการค้นหาช่องโหว่ OpenVAS 51
4.18 หน้าจอระหว่างการค้นหาช่องโหว่ OpenVAS 52
4.16 หน้าจอรายงานการค้นหาช่องโหว่ OpenVAS 52

บทที่1

บทนำ

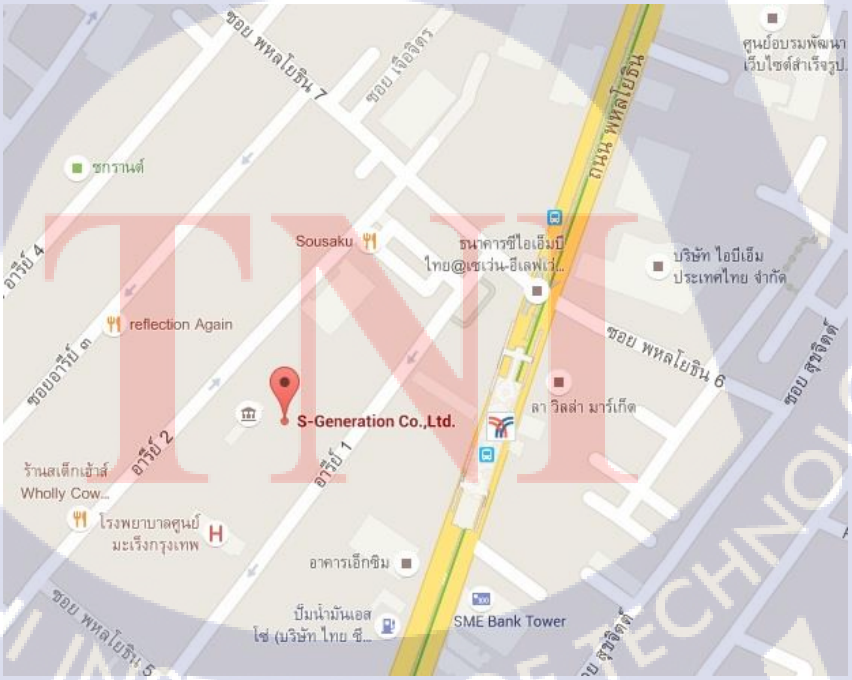
1.1 ชื่อและที่ตั้งของสถานประกอบการ

ภาษาไทย : บริษัท เอส-เจเนเรชัน จำกัด

ภาษาอังกฤษ : S-Generation Co., Ltd.

ที่อยู่ : เลขที่32/13-14 ชั้น6 อาคารThe Bliss Condo ซอยพหลโยธิน7 (อารีย์1) แขวงสามเสนใน เขตพญาไท จังหวัดกรุงเทพมหานคร 10400

ภาพที่ 1.1 สัญลักษณ์ S-Generation



ภาพที่ 1.2 แผนที่ S-Generation

1.2 ลักษณะธุรกิจของสถานประกอบการ หรือการให้การบริการหลักขององค์กร

บริษัท เอส-เจเนเรชัน จำกัด เป็นผู้นำตัวแทนจัดจำหน่าย Cybersecurity Solution ในประเทศไทย และกลุ่มประเทศในภูมิภาคอาเซียน อีกทั้งยังรับรองการเปิดเผยผลิตภัณฑ์สู่บริษัทชั้นนำ, รัฐวิสาหกิจและหน่วยงานรัฐบาล

บริษัท เอส-ฟอเรนสิกส์ อินเตอเนชันแนล จำกัด เป็นบริษัทสาขาของบริษัทเอส-เจเนเรชัน ให้บริการเกี่ยวกับกระบวนการสืบสวนสอบสวนความปลอดภัยข้อมูลด้านดิจิตอล, บริการให้ด้านการทำลายสื่อเก็บข้อมูลดิจิตอลต่างๆ

บริษัท เอส-เจเนเรชัน จำกัด มีการให้บริการหลัก 2 ประเภท ดังนี้

1) ผลิตภัณฑ์

1.1) Business Enterprise Solution เช่น Microsoft Share Point ,Microsoft Exchange, Oracle

1.2) Security เช่น Firewall, Monitoring, Rapid7, Acunetic, Checkmark, AppScan

2) บริการ

2.1) Training

2.2) Vulnerability Assessment (Penetration Test)

2.3) Implementations and Product

2.4) Consultant Service

บริษัท เอส-ฟอเรนสิกส์ อินเตอเนชันแนล จำกัด มีบริการ ดังนี้

DMSS (Digital Media Sanitation Service) การทำลายสื่อเก็บข้อมูลดิจิตอลต่างๆ เช่น ฮาร์ดดิสก์ไดร์ฟ, ซีดี, ดีวีดี, มีเดียการ์ดต่างๆ

1.2.1 ประวัติและพันธกิจ

1.) THE COMPANY

S-Generation เป็นรู้จักในประเทศไทยเป็นครั้งแรกในนามของ Quantiq International เมื่อปี พ.ศ.2548 ต่อมาได้รับเป็นที่ยอมรับอย่างเป็นทางการอีกครั้งในนาม S-Generation ในเดือนเมษายน พ.ศ.2554 ด้วยวิสัยทัศน์ที่จะเป็นผู้นำตัวแทนจัดจำหน่าย Cybersecurity Solutionในประเทศไทย และกลุ่มประเทศภูมิภาคอาเซียน ด้วยความร่วมมือพิเศษจากผู้จัดจำหน่ายระดับแนวหน้าด้าน Security and Digital Forensics เราประสบความสำเร็จในการให้บริการจดทะเบียนกับบริษัทขนาดกลางและหน่วยงานราชการ เราทำงานอย่างใกล้ชิดเพื่อสนับสนุนในการผลักดันธุรกิจของลูกค้าและผู้จัดจำหน่าย

2.) THE MARKET

ในขณะที่กระแสของโลกและความท้าทายของโลกมีความซับซ้อนมากขึ้นและความต้องการวิธีการแก้ไขปัญหาที่ถูกต้อง, มีความสามารถระดับสูงกำลังเป็นที่ต้องการเป็นอย่างมาก เรามีความมั่นใจเป็นอย่างมากว่าเราอยู่ในตำแหน่งที่ดีที่มีประโยชน์ในการรับรู้ความต้องการและมีความมีอิทธิพลในตลาดจะช่วยให้กระจายสินค้าและสร้างความสำเร็จร่วมกันในประเทศไทยและภูมิภาคอาเซียน

3.) THE VALUE

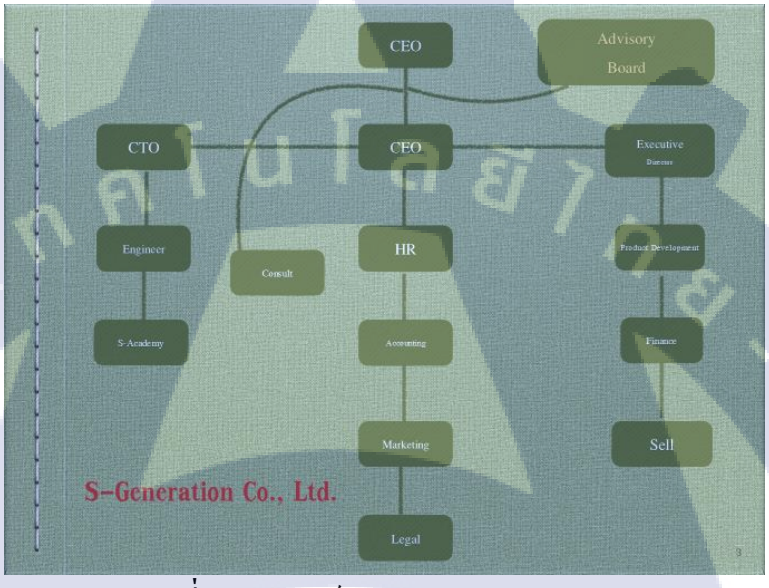
S-Generation และพันธมิตร รับรองการเปิดเผยผลิตภัณฑ์สู่บริษัทชั้นนำ,รัฐวิสาหกิจ และหน่วยงานรัฐบาล ร่วมด้วยกันกับความเชื่อถือและรายละเอียดขั้นสูง ทีมงานช่วยเหลือผลักดันธุรกิจ และเพิ่มมูลค่าที่แท้จริงให้กับสินค้าที่มีความต้องการเฉพาะ ด้วยวิธีการนี้เรามีความมั่นใจมากด้วยความร่วมมือของเราจะสร้างธุรกิจที่ดีและเพิ่มมูลค่าให้กับทุกฝ่าย

1.2.2 เป้าหมาย

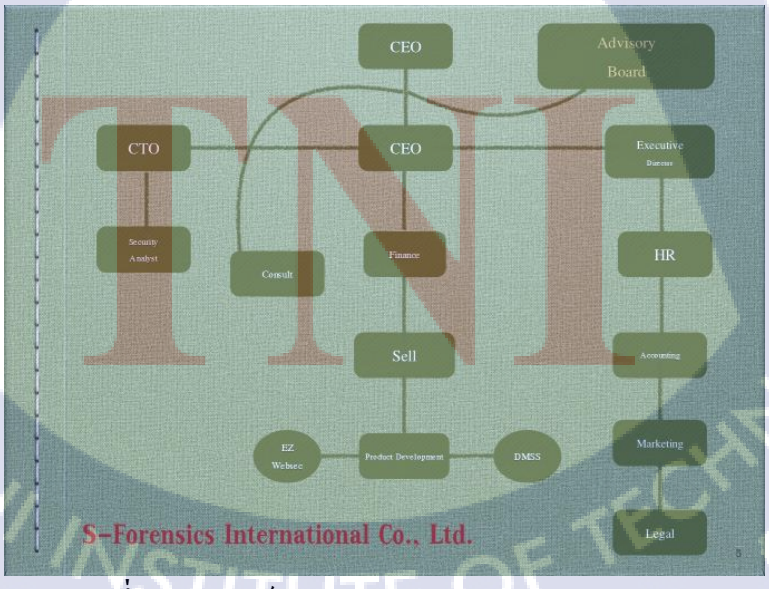
เป้าหมายของ S-Generation คือการกำหนดเป้าหมายและพัฒนาคอนเซ็ป “Generation-After-Next” และความสามารถในการสนับสนุนและป้องกันโลกไซเบอร์ S-Generation ได้ติดตามเป้าหมาย วิจัยและพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการสกัดกั้นภัยคุกคามและการโจมตีในโครงสร้างพื้นฐานด้านดิจิตอล S-Generation มุ่งเน้นไปที่การพัฒนาเทคโนโลยีที่สนับสนุนกฎระเบียบของการดำเนินการข้อมูล Information Operations (IO), สัญญาณข่าวกรอง Signals

Intelligence (SIGINT) และทุกขั้นตอนของการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ Computer Network Operations (CNO)

1.3 รูปแบบการจัดองค์กรและการบริหารองค์กร



ภาพที่ 1.3 ผังองค์กร S-Generation Co., Ltd.



ภาพที่ 1.4 ผังองค์กร S-Forensics International Co., Ltd.

1.4 ตำแหน่งงานและหน้าที่ที่นักศึกษาได้รับมอบหมาย

ตำแหน่งงาน : Developer, Asst. System Engineer

หน้าที่ที่ได้รับมอบหมาย : ออกแบบและพัฒนา Web Application, ออกแบบ Network Diagram, จัดทำแบบทดสอบเปรียบเทียบคุณสมบัติของผลิตภัณฑ์ค้นหาช่องโหว่

1.5 พนักงานที่ปรึกษา และ ตำแหน่งของพนักงานที่ปรึกษา

ชื่อพนักงาน : พุทธิมงคล บำรุงพิพัฒนพร

ตำแหน่ง : IT Security Analyst

E-mail : putthimongkol.b@s-generation.com

1.6 ระยะเวลาที่ปฏิบัติงาน

วันที่เริ่ม : 2 มิถุนายน พ.ศ. 2558

วันที่สิ้นสุด : 30 กันยายน พ.ศ. 2558

รวมทั้งสิ้น : 4 เดือน (18 สัปดาห์)

1.7 ที่มาและความสำคัญของปัญหา

- เนื่องจากลูกค้านั้นต้องการที่จะซื้อผลิตภัณฑ์ค้นหาช่องโหว่เพื่อที่จะนำไปใช้ในการทำ Vulnerability Assessment ภายในบริษัทของตนเอง แต่ต้องการผลิตภัณฑ์ที่มีประสิทธิภาพสูงสุดคุ้มค่าต่อการลงทุนด้านความปลอดภัย

- ลูกค้าไม่ทราบว่าผลิตภัณฑ์แต่ละผลิตภัณฑ์ที่มีทั้งOpen Source, Licenses นั้นมีคุณสมบัติและประสิทธิภาพต่างกันอย่างไร

1.8 วัตถุประสงค์หรือจุดมุ่งหมายของโครงงาน

- เพื่อศึกษาและพัฒนาความรู้การทำงานจากสถานปฏิบัติงานจริง
- เพื่อศึกษากระบวนการวิเคราะห์และประเมินช่องโหว่ของระบบสารสนเทศ
- เพื่อทดสอบการทำงานของ Vulnerability Tools ต่างๆ
- เพื่อเปรียบเทียบคุณสมบัติและผลลัพธ์ของ Vulnerability Tools ต่างๆ
- เพื่อนำผลลัพธ์ที่ได้จากการทำงาน นำไปเป็นข้อมูลส่วนหนึ่งในที่จะช่วยให้ลูกค้าของบริษัทสามารถตัดสินใจซื้อในผลิตภัณฑ์และบริการของบริษัท

1.9 ผลที่คาดว่าจะได้รับจากการปฏิบัติงานหรือโครงงานที่ได้รับมอบหมาย

- สามารถทำการแก้ไขและป้องกันช่องโหว่ในระบบสารสนเทศได้
- ได้รับประสบการณ์จากการทำงานในสถานประกอบการจริง สามารถทำไปใช้ในการทำงานจริงต่อไปในอนาคตได้
- เพื่อนำผลการดำเนินการไปใช้ในการตัดสินใจของลูกค้าที่ต้องการพัฒนาความปลอดภัยของระบบ

บทที่2
ทฤษฎีและเทคโนโลยีที่ใช้ในการปฏิบัติงาน

2.1 ทฤษฎีที่ใช้ในการปฏิบัติงาน

2.1.1 ความหมายของ Penetration Test และ Vulnerability Assessment

Penetration Test (Pen-Test) คือการทดสอบเพื่อหาช่องทางในการเข้าถึงระบบ (Exploit) ซึ่งการเข้าถึงระบบโดยผ่านช่องโหว่ที่พบอาจเป็น zero-day ที่ยังไม่พบการแจ้งเตือนจากผู้ผลิต (Vendor) และการกระทำใดๆที่อาจทำให้ผู้ว่าจ้างได้ทราบถึงความเสี่ยง เสมือนปฏิบัติการจริงเป็น Hacker!เพื่อเจาะระบบ

Vulnerability Assessment (VA) คือการประเมินหาความเสี่ยงที่เกิดจากช่องโหว่ที่ค้นพบตามช่องโหว่ที่มีความเสี่ยง ซึ่งส่วนใหญ่แล้วเป็นความเสี่ยงที่ปรากฏต่อสาธารณะแล้วตาม CVE (Common Vulnerabilities and Exposures)

การทำ Penetration test (การทดสอบเจาะระบบในเชิงลึก) ทั้งที่เกิดจากภายนอกระบบและภายในระบบเครือข่ายองค์กร ซึ่งการทำงานประเภทนี้ควรได้รับการอนุญาตจากบริษัท,องค์กรที่ว่าจ้างและมีการทำสัญญาการไม่เผยแพร่ความลับ ซึ่งต้องมีการเตรียมการกับผู้ดูแลระบบบริษัท, องค์กรให้ทราบถึงช่วงเวลาในการปฏิบัติงานที่แน่นอน เพื่อจะได้ระบุได้ว่าการโจมตีเกิดจากการทดสอบเจาะระบบจากทีมงานไม่ใช่นักโจมตีระบบอื่นที่ไม่เกี่ยวข้องในงาน ซึ่งส่วนนี้หากองค์กรมีระบบตรวจจับผู้บุกรุก IDS (Intrusion Detection System) ไม่ว่าเป็นระดับ Network หรือ Host base ก็จะเห็นความผิดปกติที่เกิดจากการทำการประเมินความเสี่ยงได้จาก Log ที่เกิดขึ้นบนอุปกรณ์

การทำ Penetration test และ Vulnerability Assessment มีขั้นตอนเป็นดังนี้

2.1.1.1. การทำ Penetration Test จากภายนอกระบบเครือข่ายองค์กร (Black Box)

การใช้เครื่องคอมพิวเตอร์จำลองเป็นนักโจมตีระบบเพื่อหาทางเข้าสู่ระบบเครือข่ายองค์กรที่ให้ทำการประเมินความเสี่ยง โดยมีขั้นตอนดังนี้

1. สำรวจ

ตรวจหาเครือข่ายเป้าหมายในการปฏิบัติงาน เช่นบริษัท XYZ ต้องการทำ Penetration Test เพื่อดูว่าเครือข่ายองค์กรบริษัทมีช่องทางใดที่เป็นช่องโหว่และมีโอกาสที่ถูกโจมตีจากภายนอกได้

การค้นหาข้อมูลบริษัท XYZ กับช่องทางการเชื่อมต่ออินเตอร์เน็ต โดยใช้เครื่องสาธารณะและซอฟต์แวร์ในการค้นหาข้อมูล ซึ่งประกอบด้วยการค้นหาช่องทางสาธารณะได้แก่การทำ whois ชื่อ Domain name ของบริษัท XYZ ที่ทำการเปิดข้อมูลในสาธารณะเช่น เว็บไซต์บริษัท อีเมล์บริษัท เป็นต้น สิ่งที่ได้ตรงนี้คือเราจะทราบถึง รายชื่อผู้จดทะเบียนชื่อเว็บไซต์ของบริษัท ที่อยู่ เบอร์โทรศัพท์ที่ใช้ในการติดต่อ วันหมดอายุของ domain เว็บไซต์บริษัทนั้นได้ วิธีอาจจะไม่ได้รับข้อมูลทั้งหมดเนื่องจากปัจจุบันได้มีการปิดข้อมูลชื่อผู้จดทะเบียนเว็บไซต์และข้อมูลอีเมล์ในการติดต่อได้

ผลลัพธ์ที่ได้จากการค้นหาข้อมูลสาธารณะนั้น คือ รายชื่ออีเมล์ของผู้จดทะเบียนเว็บไซต์เพื่อใช้ในการค้นหาข้อมูลบริษัท XYZ ยังสามารถใช้เครื่องมือในการเรียกใช้บริการ DNS ที่ผู้จดทะเบียนเว็บไซต์นั้นได้เช่น DNS เชื่อมโยงไปยังที่ใด ฝากไว้กับ ISP หรือตั้ง DNS Server เอง ซึ่งส่วนนี้จะสามารถค้นหาช่องโหว่ที่เกี่ยวข้องกับการใช้บริการ DNS Server ได้โดยตรวจสอบหา Zone Transfer เพื่อดูความสัมพันธ์อื่นจากชื่อ domain อื่นที่พบ เช่น www.xyz.com พบว่ามี DNS ที่เกี่ยวข้องคือ mail.xyz.com , ns1.xyz.com , ns2.xyz.com เป็นต้น ก็จะทำให้เครื่องเป้าหมายที่เราจะทำการ Penetration Test เพิ่มช่องทางการเข้าถึงได้ถึง 3 เครื่องจากในตัวอย่างนี้

- ในการใช้ข้อมูลสาธารณะนั้นยังมีอีกหลายวิธี เช่นตรวจสอบสถานะ Link ของเว็บไซต์เพื่อดูความสัมพันธ์ของข้อมูล , ตรวจสอบหา e-mail ของ domain จากเครื่องมือค้นหา (search engine) เพื่อดูพฤติกรรมการใช้ข้อมูลองค์กร ในกรณีก็ค้นหาคำว่า @xzy.com เพื่อว่าจะเข้าถึงระบบจาก e-mail พนักงานในองค์กรได้อีกทาง ซึ่งหากทำ Penetration Test ควรจะแจ้งให้บริษัทรับทราบถึงวิธีการดังกล่าวด้วย ไม่เช่นนั้นอาจผิดตามกฎหมายคอมพิวเตอร์ฯได้หากมีการตรวจสอบพบ

สำรวจช่องทางการเข้าถึงเครือข่ายองค์กร โดยวิธีการนี้ต่อยอดจากการแบบแรก ซึ่งเน้นไปทางการค้นหาเส้นทางการเดินทางของข้อมูล (Route) ของบริษัท XYZ เพื่อออกสู่อินเตอร์เน็ตภายนอก หากพบว่าช่วง IP Address ที่เป็น Public IP ของบริษัทนั้นที่ค่ามาจาก ISP ก็จะทำให้มีช่องทางการเข้าถึงมากขึ้นจากเดิม ซึ่งจะทำให้นักโจมตีระบบสามารถใช้เทคนิคการตรวจสอบได้มากขึ้นเช่นการทำ DDoS/DoS กับช่วง IP ที่บริษัทได้รับมา เป็นต้น

2. ตรวจสอบ

เมื่อทำการรวบรวมข้อมูลที่ได้มาจากขั้นตอนสำรวจนั้น ก็จะทำการวาดรูปความสัมพันธ์เครือข่ายองค์กรออกมาพร้อมกำหนดจุดที่ทำการตรวจสอบขึ้น การตรวจสอบจะใช้ check list ตามมาตรฐาน หรือใช้เครื่องมือในการตรวจสอบ ในกรณีนี้เป็นการทำ Penetration test จากภายนอก สิ่งที่ตรวจสอบได้แก่

1.) Information leak จากขั้นตอนที่หนึ่ง เช่น รายชื่อผู้จดทะเบียนเว็บไซต์, e-mail, รายชื่อ DNS ที่มีความสัมพันธ์กับบริษัท, ข้อมูลรั่วจากการใช้งานอินเตอร์เน็ตได้แก่ e-mail พนักงานในการโพสข้อมูล, Link ของเว็บไซต์บริษัทที่ทำให้ได้ข้อมูลอื่นๆ เป็นต้น

2.) Web Application checklist ตรวจสอบช่องโหว่ที่พบจากเว็บไซต์ www.xyz.com ว่ามีช่องโหว่ในการเข้าถึงระบบผ่าน Web application จากมาตรฐาน OWASP เป็นต้น

3.) DNS server checklist ตรวจสอบค่า Domain name server ที่แสดงข้อมูลสาธารณะ

4.) E-mail Server checklist ตรวจสอบค่าการใช้งาน E-mail server ที่แสดงข้อมูลสาธารณะ เช่นกรณีที่ บริษัท XYZ จัดทำ Mail server เองขึ้นการตรวจสอบจะตรวจว่า Mail server ของบริษัทนั้นจะมีโอกาสจดหมายขยะจะเข้าถึงได้หรือไม่ เป็นต้น

5.) Network Topology checklist ตรวจสอบการเชื่อมต่ออินเตอร์เน็ตบริษัท เส้นทางการ Route ของข้อมูล , จำนวน Link ของ ISP ที่บริษัท XYZ ใช้บริการ ส่วนนี้จะเน้นไปที่การทดสอบ DDoS/DoS ว่าทางบริษัท XYZ มีการควบคุมการโจมตีชนิดนี้ได้หรือไม่ ซึ่งจะแสดงให้เห็นถึงความพร้อมโครงสร้างเครือข่าย (Network) ของบริษัทว่าได้มีการจัดเตรียมเทคโนโลยีด้านความปลอดภัยครบถ้วนในส่วน Perimeter network เช่นได้มีการจัดทำ ACL (Access Control List) ค่า Blacklist ในอุปกรณ์ Router หรือ Firewall , มีอุปกรณ์ Firewall ที่ป้องกันทางเครือข่ายในระดับ stateful inspection หรือไม่ เป็นต้น

6.) ตรวจสอบ Port services จากข้อมูลในขั้นตอนสำรวจ เช่น พบว่า IP Address ของเว็บไซต์บริษัท , e-mail , DNS server, Router ก็ทำการตรวจสอบว่ามี Port services อะไรที่ทำการเปิดไว้เพื่อจะทำการขยายผลต่อในขั้นตอนต่อไป

3. วิเคราะห์

เมื่อทำการตรวจสอบจากการสำรวจและตรวจสอบ ภายนอกเครือข่ายองค์กรแล้วนำข้อมูลเหล่านั้นมาทำการวิเคราะห์เพื่อศึกษาว่าพบช่องโหว่และการเข้าถึงข้อมูล เช่น จากการตรวจสอบ Port services พบว่ามีการเปิด Port ที่มีช่องโหว่และสามารถเข้าถึงระบบจากภายนอกได้ ผ่านการให้บริการ Web server port 80 ช่องโหว่ที่พบคือ มีการใช้ Web server version เก่าและมี tools ในการเข้าถึงระบบ (Exploit) ผ่านช่องโหว่นี้ได้ หรือ ใน Web server เปิด port 1433 เป็นการเปิด port SQL server เป็น Data base บนเครื่อง Web server และมี exploit ที่เข้าถึงระบบได้ เป็นต้น ในขั้นตอนวิเคราะห์จะลงรายละเอียดถึงการเข้าถึงระบบจากภายนอก เป็นส่วนๆจากขั้นตอนสำรวจและตรวจสอบ เช่น ส่วนของ Web server , ส่วนของ E-mail Server , ส่วนของ DNS server และส่วนของ Router เป็นต้น

4. ประเมิน

หรือเรียกว่า Vulnerability Assessment เมื่อทำการวิเคราะห์ถึงช่องโหว่ที่พบแล้ว ถึงขั้นตอนสุดท้ายคือการประเมิน ว่าช่องโหว่ที่พบนั้นมีความเสี่ยงและมีผลกระทบต่อธุรกิจองค์กรอย่างไร ส่วนใหญ่เป็นเอกสารการแนะนำและการปิดช่องโหว่ที่พบ

สูตรการหาค่าความเสี่ยงต่อธุรกิจองค์กร Risk = Vulnerability x Threat หรือบ้างครั้งอาจจะเห็นเป็นสูตร Risk = Vulnerability x Threat x cost

การประเมินความเสี่ยง (Risk Assessment) สามารถมองได้ 2 แบบคือ

-ด้านมหาภาคภาพรวมองค์กร ที่ต้องดูถึง 3P คือ Vulnerability คน กระบวนการ และเทคโนโลยี Threat จากคน กระบวนการและเทคโนโลยี

-ด้านจุลภาคคือทางด้านเทคนิคอย่างเดียว คือมอง Vulnerability และ Threat เฉพาะทางเทคโนโลยี ไม่มองแบบครบ 3P คือการประเมินหาความเสี่ยงจาก ค่าความเสี่ยง (Risk)ที่พบ จะเกิดจาก ช่องโหว่ที่พบ (Vulnerability) คูณกับค่าภัยคุกคาม (Threat) ลักษณะภัยคุกคามที่พบก็มีความเสี่ยงสูง กลาง และต่ำ ซึ่งส่วนนี้ขึ้นอยู่รูปแบบผู้ทำเอกสารว่าจะจัดทำค่าการประเมินความเสี่ยงจากอุปกรณ์หรือเครื่องมือในตรวจวิเคราะห์ (Tools) มาสรุปความเสี่ยง สูง กลาง และต่ำ ก็ได้ และ จัดทำค่าดัชนีชี้วัดความเสี่ยงที่มีผลกระทบต่อธุรกิจทางด้านเทคนิค ซึ่งเอกสารในผลลัพธ์ของแต่ละบริษัทที่จัดทำอาจจะมีรูปแบบที่แตกต่างกันได้เช่นกัน

2.1.1.2. การทำ Penetration test ภายในองค์กรเชิงลึก (White Box)

เป้าหมายในการทำ Penetration Test ภายในคือการทดสอบหาช่องโหว่ที่พบจากการใช้งานไอซีทีในองค์กรเพื่อประเมินช่องโหว่และทำการปิดกั้นช่องโหว่ที่ค้นพบขึ้นเพื่อไม่เกิดปัญหาขึ้นในระยะยาว มีขั้นตอนการทำงานดังนี้

1. สำรวจ

สำรวจผังโครงสร้างงานได้ไอซีทีขององค์กร, แผนผังระบบเครือข่าย, ประเภทอุปกรณ์ประกอบด้วย

1.) Network Device ได้แก่ จำนวนอุปกรณ์ Router , อุปกรณ์ Switch, อุปกรณ์ Firewall, Network Load balacing, Network VPN, Bandwidth management, อุปกรณ์ NetworkIDS/IP ซึ่งต้องบอกตำแหน่ง (Perimeter zone , DMZ zone) และค่า IP Address เป็นต้น

2.) เครื่องแม่ข่าย (Server) ได้แก่ Web Server, Mail Server , DNS Server ภายใน, Proxy Server, Authentication Server, ERP Server ซึ่งต้องบอกตำแหน่ง (DMZ zone) และค่า IP Address เป็นต้น

3.) เครื่องลูกข่าย (Client) ได้แก่ ระบบปฏิบัติการที่ใช้งานได้แก่ Window XP , Linux อื่นๆ ต้องบอกตำแหน่ง (VLAN) และค่า IP Address เป็นต้น

2. ตรวจสอบ

ตรวจสอบตามมาตรฐาน Security Checklist ดังนี้

1.) ตรวจสอบความมั่นคงปลอดภัยตามมาตรฐานของ อุปกรณ์ Network Devices ได้แก่ Security Checklist Router , Firewall , IDS/IPS เป็นต้น

2.) ตรวจสอบความมั่นคงปลอดภัยตามมาตรฐานของ เครื่องแม่ข่าย (Server) ได้แก่ Security Checklist Windows 2000 server , 2003 server , Linux Server เป็นต้น

3.) ตรวจสอบความมั่นคงปลอดภัยตามมาตรฐานของ เครื่องลูกข่าย (Client) ได้แก่ Security Checklist การใช้งานเครื่องคอมพิวเตอร์ในองค์กรตามมาตรฐาน ISO27001 เป็นต้น

ซึ่งในส่วน security checklist นั้นผู้ปฏิบัติงานสามารถนำข้อมูลจาก NIST , NSA หรือ Thai-cert ในเอกสารตรวจสอบในแต่ละส่วนได้

3. วิเคราะห์

การวิเคราะห์ช่องโหว่ที่พบจากการสำรวจและตรวจสอบในการวิเคราะห์นี้สามารถใช้อุปกรณ์ หรือ เครื่องมือในการประเมินความเสี่ยงเพื่อตรวจหาความผิดปกติและช่องโหว่ที่พบตามอุปกรณ์เครือข่าย (Network Devices) และเครื่องแม่ข่าย (Server) ที่สำคัญได้ การใช้เครื่องมือในการประเมินความเสี่ยง สิ่งที่ควรตรวจสอบให้มากขึ้นได้แก่

1.) การวิเคราะห์ในระดับเครือข่ายคอมพิวเตอร์ (Network Analysis)

- ปริมาณการใช้งาน Bandwidth ของระบบเครือข่าย ทั้งข้อมูลขาเข้าและขาออก
- ปริมาณ Throughput ของระบบเครือข่ายทั้งขาเข้าและขาออก แยกตาม Application Protocol ที่สำคัญ ด้วยเนื่องจากจะช่วยตรวจสอบถึงการใช้งานอันไม่พึงประสงค์ของ User ในองค์กร ว่ามีการแพร่ระบาดไวรัสคอมพิวเตอร์ , เครื่อง User เป็น Botnet , การส่งข้อมูลขยะ (spam) หรือมีพฤติกรรมที่ผิดต่อนโยบายบริษัทหรือไม่อีกด้วย ซึ่งในส่วนนี้จะสามารถนำไปวิเคราะห์เป็นค่าภัยคุกคามในองค์กร ที่ใช้ประกอบกับขั้นตอนสุดท้ายคือการประเมินได้ต่อไป

2.) การวิเคราะห์ในระดับอุปกรณ์เครือข่ายและเครื่องแม่ข่ายที่สำคัญ

- ทำการใช้เครื่องมือประเมินความเสี่ยงเพื่อตรวจดู Port Services ที่อุปกรณ์เครือข่าย และ เครื่องแม่ข่ายที่สำคัญเปิดอยู่

- วิเคราะห์ช่องโหว่จากการใช้เครื่องมือหลังจากตรวจ Port Services แล้วจะพบว่า Services ที่ทำการใช้งานอยู่บนอุปกรณ์เครือข่ายและเครื่องแม่ข่ายที่สำคัญ นั้นมีการเปิดใช้งานอยู่ นั้นมีความช่องโหว่ที่เป็นภัยรุนแรงหรือไม่ เช่น เปิด Port services 80 TCP เป็น Application Protocol ของ HTTP ซึ่งในนี้ประกอบด้วย Web Server ที่ใช้งานอยู่ที่เป็น IIS , Apache , หรืออื่นๆ ซึ่งหากเป็น Version ที่มีช่องโหว่ หรือมี code exploit ที่สามารถส่ง command หรือ script จากทางไกลและสามารถยึดครองเครื่องนั้นได้ก็จะถือว่าเป็นระดับภัยคุกคามที่รุนแรง เป็นต้น

- วิเคราะห์หา Security Patch ที่อัพเดทล่าสุดเพื่อเสริมสร้างความมั่นคงปลอดภัยให้กับอุปกรณ์เครือข่าย และ แม่ข่ายที่สำคัญ โดยทั้งนี้ควรทำการเตรียมแผนทดสอบถึงผลกระทบก่อนการอัพเดท Security Patch ก่อน

4. ประเมิน

ขั้นตอนนี้จะเป็นการสรุปผลความเสี่ยงที่พบจากขั้นตอนที่ผ่านมา โดยทำเป็นค่าดัชนีชี้วัดความเสี่ยง และผลการปฏิบัติงาน รวมถึงแนวทางในการปิดกั้นส่วนที่เป็นช่องโหว่ (Hardening) และป้องกันในระยะยาว ซึ่งในส่วนนี้จะเน้นไปทางการทำรายงานผลในรูปแบบเอกสาร ขยายความค่าดัชนีชี้วัดความเสี่ยงเกิดจาก Risk = Vulnerability x Threat ค่าความเสี่ยงที่ประเมินได้ ขึ้นอยู่กับนโยบายขององค์กรด้วย หากดูแล้วไม่กระทบกับธุรกิจมากค่าความเสี่ยงนั้นก็จะแปรผันไปกับการประเมินความเสี่ยงของผู้ปฏิบัติงาน (Penetration Tester) ซึ่งในแต่ละที่อาจมีค่าการประเมินไม่ที่เหมือนกัน เช่น ในกรณีที่พบว่า พบช่องโหว่ Web Server ที่ระบบ IIS 6.0 ที่ยังไม่ได้อัพเดท Patch security เมื่อประเมินแล้วว่า Web Server นั้นไม่สามารถเข้าถึงได้จากอินเตอร์เน็ต และเป็นเครื่องเฉพาะในแผนกใดแผนกหนึ่งดังนั้นระดับความสำคัญที่เป็นภัยคุกคามที่รุนแรงก็จะน้อยกว่าเครื่อง Web Server ที่เผยแพร่ข้อมูลสาธารณะ (Public IP)ได้ เป็นต้น ซึ่งค่าดัชนีชี้วัดส่วนนี้ขึ้นกับผู้ปฏิบัติงานในการทำ Penetration Test และประสบการณ์ รวมถึงความเชี่ยวชาญของบุคคลนั้นในการประเมิน บางครั้งการให้บริษัทต่างที่กันมาประเมินหาความเสี่ยง อาจมีค่ารายงานผลไม่เท่ากันขึ้นอยู่กับทีมปฏิบัติงาน

2.1.2 มาตรฐานOWASP (Open Web Application Security Project)

ความรู้เกี่ยวกับความปลอดภัยของ Web Application

OWASP TOP 10 ปรับปรุงทุกๆ 3 ปี ปรับปรุงล่าสุด ปี 2013

1.) Injection

โจมตีโดยใช้วิธีการส่งข้อมูลผ่านแอปพลิเคชั่น โดยข้อมูลที่ใช้นั้นเป็นการแทรกแซงการประมวลต่างๆ ภายในแอปพลิเคชั่น ไม่ว่าจะด้วยการใช้คำสั่ง SQL เพื่อขโมยข้อมูลหรือก่อให้เกิดความเสียหายของข้อมูล วิธีการป้องกันเบื้องต้น

SQL Injection – ป้องกันโดยหลีกเลี่ยงการประมวลผลโดยใช้คำสั่ง SQL ที่มาจากการต่อคำสั่งกับพารามิเตอร์ต่างๆ (string concatenation)

2.) Broken Authentication and Session Management

ฟังก์ชันแอปพลิเคชันเกี่ยวข้องกับการตรวจสอบสิทธิและการจัดการ session ที่พัฒนามาอย่างไม่ถูกต้อง จะทำให้ผู้โจมตีสามารถยึดรหัสผ่าน คีย์ หรือ session tokens หรือหลอกระบบมีข้อมูลส่วนตัวของผู้ใช้คนอื่น การป้องกันข้อมูลที่ใช้ระบุตัวตนของผู้ใช้งาน และการจัดการหรือเข้าถึงข้อมูล Session ที่ไม่ถูกต้อง นำมาซึ่งช่องโหว่ได้ วิธีป้องกันเบื้องต้น

ทำการเข้ารหัส และกำหนดรูปแบบที่คาดเดาได้ยากกับข้อมูลที่มีความสำคัญ เช่น รหัสผ่าน, เลขที่บัญชี เป็นต้น

ห้ามแสดง Session ID ให้ผู้ใช้เห็น ไม่ว่ากรณีใดๆ และควรมีการกำหนด Timeout ของ Session ID ด้วย

3.) Cross-Site Scripting (XSS)

การเปิดช่องโหว่ให้แฮกเกอร์บันทึกข้อมูลที่แทรกแซงการทำงานของ Browser เข้าสู่ระบบได้ ไม่ว่าจะเป็นข้อมูลในรูปแบบแท็ก script ต่างๆ และเมื่อมีการนำไปแสดงผลบน Browser ของผู้ใช้งาน อาจจะถูกขโมยข้อมูลระบุตัวตนที่สำคัญต่างๆ ได้ วิธีป้องกันเบื้องต้น

- ให้มีการตรวจสอบข้อมูลที่บันทึกผ่านเว็บไซต์ทุกครั้ง เช่นไม่อนุญาตให้ใช้แท็กที่เป็นอันตราย เช่น script tag เป็นต้น
- ตรวจสอบลักษณะของข้อมูลต่างๆ ว่าเป็นไปตามรูปแบบที่กำหนด
- หากเลี่ยงอักขระพิเศษบางอย่างไม่ได้ ให้ใช้ HTML Encoding ก่อนนำไปเก็บหรือใช้งาน

4.) Insecure Direct Object References

ช่องโหว่ในเรื่องของการปล่อยให้เข้าถึงทรัพยากรของระบบต่างๆ เช่นไฟล์ โฟลเดอร์ รวมถึงไปถึงข้อมูลบนฐานข้อมูลที่ผู้ใช้ไม่มีสิทธิ์เข้าถึงได้ วิธีป้องกันเบื้องต้น

- การพัฒนาแอพพลิเคชั่น จำเป็นต้องคำนึงถึงเรื่องการกำหนดสิทธิ์ในการเข้าถึงทรัพยากรที่สำคัญ

5.) Security Misconfiguration

ช่องโหว่ที่เกิดจากการตั้งค่าของระบบปฏิบัติการ แอพพลิเคชั่น ฐานข้อมูล รวมถึงนโยบายในการใช้งานที่หละหลวม วิธีการป้องกันเบื้องต้น

- หมั่นอัพเดท patch ของซอฟต์แวร์ที่ใช้อย่างสม่ำเสมอ
- กำหนดสิทธิ์การใช้งานของทรัพยากรต่างๆ บนเครื่องเซิร์ฟเวอร์ เปิดพอร์ตที่จำเป็นสำหรับแอพพลิเคชั่นเท่านั้น
- ไม่แสดงข้อผิดพลาดในการทำงานของระบบให้ผู้ใช้งานทราบ โดยตั้งค่าที่แอพพลิเคชั่น
- กำหนดให้มีการเปลี่ยนรหัสผ่านอยู่เสมอ

6.) Sensitive Data Expose

ช่องโหว่จากการป้องกันข้อมูลสำคัญต่างๆ ไม่เพียงพอ เช่นรหัสผ่าน เลขประจำตัวประชาชน หมายเลขบัตรเครดิต เป็นต้น วิธีการป้องกันเบื้องต้น

- เข้ารหัสในการจัดเก็บข้อมูลที่มีความสำคัญทั้งหมด
- ให้อัลกอริทึมและคีย์ในการเข้ารหัสที่แข็งแรง
- ปิดการใช้งาน Auto Complete กับข้อมูลที่มีความสำคัญ
- ติดตั้ง SSL กับเว็บไซต์ เพื่อป้องกันการแฮกข้อมูลผ่าน Network Traffic

7.) Missing Function Level Access Control

ช่องโหว่ที่เกิดการควบคุมสิทธิ์การใช้งานฟังก์ชัน หรือฟีเจอร์ของระบบ เฉพาะการแสดงผลหรือซ่อนบน UI เท่านั้น วิธีการป้องกันเบื้องต้น

- ตรวจสอบการเข้าถึงฟังก์ชัน หรือฟีเจอร์ จากการประมวลผลบนเซิร์ฟเวอร์ด้วย
- จัดเก็บ Audit log การเข้าถึงฟังก์ชัน หรือฟีเจอร์ที่ผิดปกติ เพื่อใช้ตรวจสอบย้อนหลังได้

8.) Cross-Site Request Forgery (CSRF)

เป็นวิธีการหลอกผู้ใช้งานหรือเหยื่อเข้าเว็บไซต์ของแฮกเกอร์ หากผู้ใช้งานมีการ login ไปยังเว็บไซต์สำหรับทำธุรกรรมต่างๆ ไว้ เช่น บริการทางอิเลคทรอนิคส์ของธนาคาร เว็บไซต์ของแฮกเกอร์จะส่ง Request ไปยังเว็บไซต์ปลายทางเพื่อทำธุรกรรมหรือประมวลผลต่างๆ โดยเว็บไซต์ปลายทางเข้าใจว่าเป็นผู้ใช้งานจริง วิธีการป้องกันเบื้องต้น

- ควรแทรกค่า token ต่างๆ ใน Hidden Field ใน Body ไปกับ HTTP Request โดยห้ามแสดงสิ่งเหล่านี้บน URL

- ควรมีการป้องกัน HTTP Request จาก URL หรือ Domain อื่น

- อาจมีการให้ระบุ CAPTCHA เพื่อตรวจสอบซ้ำอีกครั้ง

9.) Using Components with Known Vulnerabilities

การนำ Components หรือ Libraries ที่มีช่องโหว่มาใช้กับแอพพลิเคชั่นของเรา ก็จะส่งผลให้แอพพลิเคชั่นมีช่องโหว่ตามไปด้วย วิธีการป้องกันเบื้องต้น

- หมั่นตรวจสอบเวอร์ชันของ Components หรือ Libraries ที่นำมาใช้ และมีการตรวจสอบความปลอดภัยให้ครบถ้วนทุกครั้งที่ต้องการนำมาใช้งาน

10.) Unvalidated Redirects and Forwards

เว็บแอพพลิเคชั่นมีการ redirect หรือ forward ไปยังเว็บไซต์อื่น โดยไม่มีการตรวจสอบเสียก่อน ซึ่งอาจถูกโจมตีโดยพาผู้ใช้งานไปยังเว็บไซต์ที่มัลแวร์ หรือส่งไปยังหน้าเว็บไซต์ที่ไม่อนุญาตให้เข้าถึงได้ วิธีการป้องกันเบื้องต้น

- หลีกเลี่ยงการ redirect หรือ forward ไปยังเว็บไซต์ที่ไม่เกี่ยวข้องกับแอพพลิเคชั่น

- หากเลี่ยงไม่ได้ ให้กำหนดและควบคุมเว็บไซต์ที่อนุญาตให้ redirect หรือ forward ไปได้เท่านั้น

2.1.3 มาตราฐานการกำหนดชื่อช่องโหว่ด้วย CVE (Common Vulnerabilities and Exposures)

รายชื่อของช่องโหว่ที่เป็นมาตรฐานสากลที่ใช้สำหรับอ้างอิงถึงช่องโหว่แต่ละชนิด เพื่อให้ข้อมูลด้านช่องโหว่ , เจ้าของผลิตภัณฑ์ และผู้ใช้งานโปรแกรมสามารถเข้าใจได้ตรงกัน

องค์ประกอบของ CVE

1. ชื่อและหมายเลข CVE ประกอบด้วย ปีที่พบช่องโหว่ และลำดับของช่องโหว่ที่ได้รับ CVE ในปีนั้น “CVE-2014-7187 bash: off-by-one error in deeply nested flow control construct”

2. รายละเอียดโดยย่อของช่องโหว่

“Description : Off-by-one error in the read_token_word function in parse.y in GNU Bash through 4.3 bash43-026 allows remote attackers to cause a denial of service (out-of-bounds array access and application crash) or possibly have unspecified other impact via deeply nested for loops, aka the "word_lineno" issue.”

3. แหล่งข้อมูลอ้างอิง

“http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7187”

กระบวนการออกหมายเลข CVE เริ่มต้นเมื่อมีข่าวการค้นพบช่องโหว่ใหม่เกิดขึ้น จะมีการให้หมายเลข CAN (CVE candidates) เพื่อรอการเห็นชอบจากกรรมการ Editorial Board Members หลังจากผ่านกรรมการนี้แล้วจะได้รับหมายเลข CVE ต่อไป

2.2 เทคโนโลยีที่ใช้ในการปฏิบัติงาน

2.2.1 Nessus vulnerability scanner

ภาพที่ 2.1 สัญลักษณ์ Nessus

Nessus เป็นเครื่องมือค้นหาช่องโหว่ที่ได้รับความนิยมมากที่สุดในโลกที่ใช้ในกว่า 75,000 องค์กรทั่วโลก ตั้งขึ้นโดย Renaud Deraison ในปี 1998 เป็นเครื่องมือค้นหาช่องโหว่ฟรี เพื่อให้ชุมชนอินเตอร์เน็ตมีประสิทธิภาพในการรักษาความปลอดภัยจากระยะไกล Nessusได้รับการจัดอันดับอยู่ในระดับชั้นนำของผลิตภัณฑ์ในอุตสาหกรรมการรักษาความปลอดภัยและได้รับการรับรองโดยองค์กรรักษาความปลอดภัยข้อมูลมืออาชีพเช่นสถาบัน ในปี 2002 Renaud Deraison ได้ร่วมมือกับ Ron Gula และ Jack Huffard ในการก่อตั้งบริษัท Tenable Network Security ในปี 2005 Nessus ได้เปลี่ยนจาก Open Source เป็น Closed Source

คุณสมบัติของ Nessus Vulnerability scanner

1.) ค้นหาอุปกรณ์ต่างๆซึ่งอยู่ในระบบเครือข่าย

2.) ค้นหาว่าอุปกรณ์แต่ละชนิดเป็นประเภทใด หรือ Footprinting เช่น ระบุ IP Address , ระบุระบบปฏิบัติการ เป็นต้น

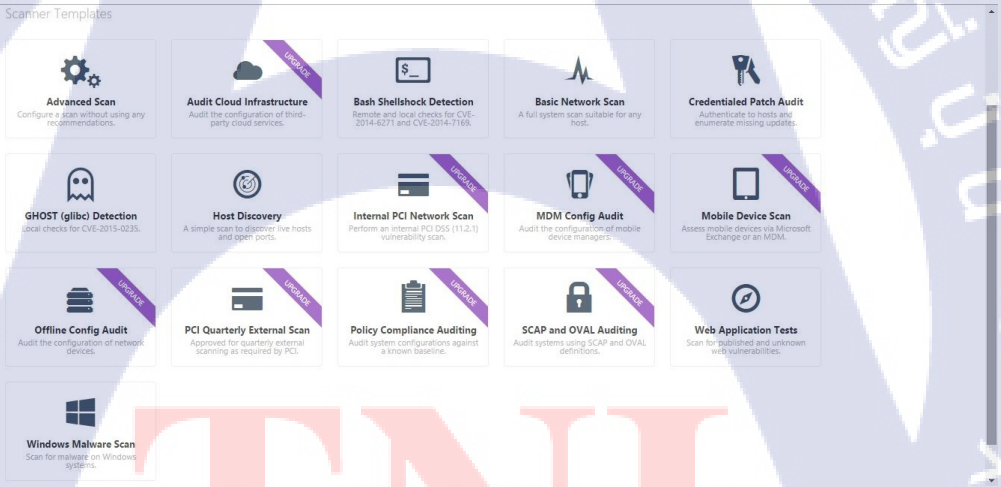
3.) ค้นหาว่าอุปกรณ์ต่างๆมีการใช้งานบริการอะไรบ้าง เช่น Mail, Web, Proxy หรือ FTP เป็นต้น

4.) ค้นหาว่าอุปกรณ์ต่างๆเปิดใช้งาน port อะไรบ้าง

5). ค้นหาว่าอุปกรณ์ต่างๆมีช่องโหว่อะไรบ้างที่เสี่ยงต่อการโจมตี โดยช่องโหว่เหล่านี้อ้างอิงจากมาตรฐานสากล เช่น CVE (Common Vulnerabilities and Exposures)

6.) บ่งบอกถึงระดับความเสี่ยงของแต่ละอุปกรณ์

7.) บอกวิธีป้องกันหรือแก้ไขช่องโหว่ของความเสี่ยงที่เกิดขึ้น

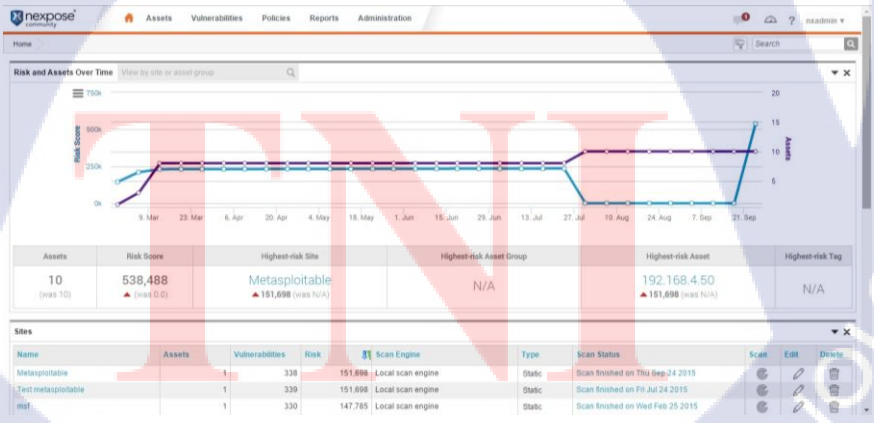


ภาพที่ 2.2 หน้าจอแสดงรูปแบบการค้นหาช่องโหว่ Nessus

2.2.2 Nexpose

ภาพที่ 2.3 สัญลักษณ์ Nexpose

Nexpose จะทำการสแกนช่องโหว่ต่าง ๆ และเครือข่ายในระบบที่ใช้งาน จะดำเนินการตรวจสอบช่องโหว่ของเครือข่ายจากภายนอก เพื่อตรวจสอบเครือข่ายและเว็บแอพพลิเคชั่นยึดตาม IP Address ที่เชื่อมต่อกับอินเทอร์เน็ตของผู้ค้าหรือผู้ให้บริการ โดยตรวจสอบช่องโหว่ในระบบ-ปฏิบัติการ, Service, ช่องทางการสื่อสารของอุปกรณ์ที่แฮกเกอร์อาจใช้เป็นเป้าโจมตีไปยังเครือข่ายส่วนตัวขององค์กรได้ สำหรับการป้องกัน ควรที่จะอัพเดทข้อมูลเพื่อป้องกันช่องโหว่ให้เป็นปัจจุบัน ซึ่ง Nexpose จะทดสอบตามมาตรฐานของ PCI DSS (มาตรฐานที่มีความจำเป็นต่อสถาบันการเงิน) เพื่อตรวจสอบข้อบกพร่องที่มีอยู่ในระบบได้อย่างรวดเร็ว และให้คำแนะนำโดยละเอียดสำหรับการแก้ไข เพื่อป้องกันการโจมตีผ่านทองช่องโหว่ หรือภัยคุกคามต่าง ๆ



ภาพที่ 2.4 หน้าจอหลักของ Nexpose

2.2.3 OpenVAS (Open Vulnerability Assessment System)

ภาพที่ 2.5 สัญลักษณ์ OpenVAS

แพลทฟอร์มสำหรับสแกนช่องโหว่บนระบบเครือข่ายฟรี โดยองค์ประกอบหลักเป็นแพ็คเก็จ Linux หรือสามารถดาวน์โหลดมาใช้งานได้ในรูปแบบ Virtual Appliance สำหรับทดสอบและประเมินผลระบบ OpenVAS มีการอัพเดทฐานข้อมูลการค้นหาช่องโหว่ทุกวันจาก Network Vulnerability Tests (NVT) ซึ่งปัจจุบันมีฐานข้อมูลช่องโหว่มากกว่า 33,000 รูปแบบ

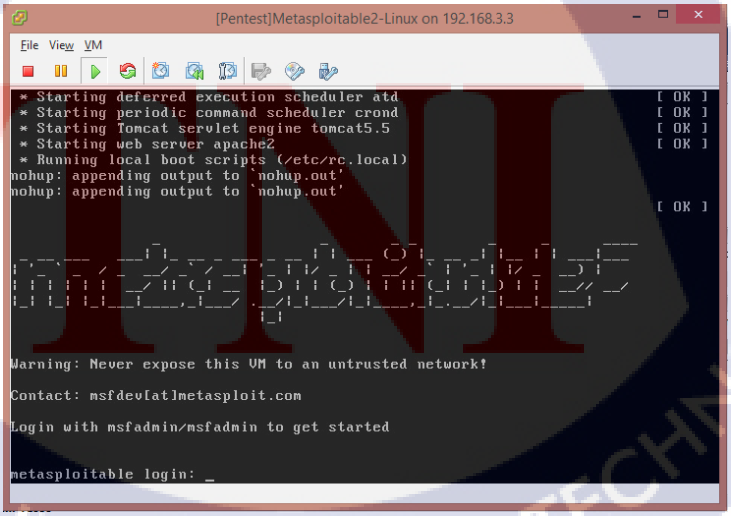
ผู้ใช้งานสามารถควบคุม OpenVAS ผ่านทาง GUI และ CLI ได้ เช่น Greenbone Security Assistant (GSA) เป็น GUI ผ่านหน้าเว็บเบราเซอร์, Greenbone Security Desktop (GSD) เป็นแบบ Qt-based Desktop Client ที่รันได้บนทั้ง Linux และ Windows และ OpenVAS CLI สำหรับการรันคำสั่งผ่าน Command Line

OpenVAS ไม่ใช่ตัวสแกนที่ง่ายและเร็วที่สุด แต่เป็นเครื่องมือที่มีฟังก์ชันให้เลือกใช้ได้หลากหลาย เช่น รองรับการสแกนหลายระบบพร้อมกัน สามารถสแกนตามกำหนดเวลาได้ เป็นต้น

ภาพที่ 2.6 หน้าจอหลักของ OpenVAS

2.2.4 Metasploitable

Metasploitable เป็นระบบปฏิบัติการมีช่องโหว่ของระบบปฏิบัติการ Linux สร้างขึ้นโดย Rapid7 ระบบปฏิบัติการนี้ถูกสร้างขึ้นเพื่อตรวจสอบความปลอดภัยของข้อมูล มีเป้าหมายที่จะทำการตรวจสอบ, การสแกนและใช้ประโยชน์จากระบบปฏิบัติการนี้ได้อย่างถูกต้องตามกฎหมาย



ภาพที่ 2.7 หน้าจอของ Metasploitable

บทที่ 3
แผนงานการปฏิบัติงาน และขั้นตอนการดำเนินงาน

3.1 แผนการปฏิบัติงาน

จากการที่ข้าพเจ้าได้เข้าปฏิบัติสหกิจศึกษาที่บริษัท เอส-เจเนเรชั่น จำกัด ได้รับมอบหมายให้จัดทำการเปรียบเทียบ Report ของ Tool Vulnerabilityเป็นงานหลัก รวบทั้งได้รับมอบหมายงานเพิ่มเติม ยกตัวอย่างเช่น ออกปฏิบัติงานนอกสถานที่กับDMSS ออกแบบโครงสร้างระบบเน็ตเวิร์ค และจัดทำเว็บแอปพลิเคชั่นที่ใช้งานภายในบริษัท เป็นต้น

ตารางที่ 3.1 แผนการปฏิบัติงาน

หัวข้องาน	เดือนที่ 1				เดือนที่ 2				เดือนที่ 3				เดือนที่ 4			
Web Application																
-Gather requirement																
-Design																
-Backend Coding																
-Database Coding																
-Testing and Maintenance																
DMSS																
-On site																
Network Design Diagram																
-Gather requirement																
-Design																
-Present & proof																
-Revise																
Vulnerability Assessment																
-Support CVE																
-Vulnerability Scan																

3.2 รายละเอียดงาน

ตารางที่ 3.2 แสดงรายละเอียดงาน และลักษณะงานที่ปฏิบัติ

ลำดับ	งานที่ปฏิบัติ	ลักษณะงานที่ปฏิบัติ
1	ออกแบบเว็บแอปพลิเคชั่น	รับความต้องการระบบจากแผนกต่างๆ ศึกษาและออกแบบเว็บแอปพลิเคชั่น
2	ปฏิบัติงานนอกสถานที่ DMSS	ทำลายสื่อเก็บข้อมูล เช่น ฮาร์ดดิสก์ไดร์ฟ, ซีดี, ซีดี-รอม, ดีวีดี, ดีวีดี-รอม
3	ออกแบบระบบเครือข่ายภายใน	รวบรวมความต้องการระบบต่างๆ และศึกษาความเป็นไปได้ในการออกแบบระบบเครือข่าย
4	ศึกษารวบรวมข้อมูลช่องโหว่	รวบรวมและจัดทำข้อมูลช่องโหว่ต่างๆ
5	ปฏิบัติงานที่ได้รับมอบหมายอื่นๆ	ปฏิบัติงานตามที่ได้รับมอบหมายจากรุ่นพี่ เช่น สืบค้นข้อมูลผลิตภัณฑ์ความปลอดภัยต่างๆ

3.3 ขั้นตอนการดำเนินงาน

3.3.1 ขั้นตอนการศึกษาค้นคว้า

3.3.1.1 การศึกษาค้นคว้าเกี่ยวกับช่องโหว่ต่างๆ

ศึกษาวิธีการใช้งานช่องโหว่ต่างที่นิยมในปัจจุบัน จากนั้นนำข้อมูลมารวบรวมและสังเคราะห์ช่องโหว่ที่จะสามารถใช้งานได้จริง เช่น OWASP, CVE

3.3.1.1.1 OWASP (Open Web Application Security Project)

1.) Injection

โจมตีโดยใช้วิธีการส่งข้อมูลผ่านแอปพลิเคชั่น โดยข้อมูลที่ใช้นั้นเป็นการแทรกแซงการประมวลต่างๆ ภายในแอปพลิเคชั่น ไม่ว่าจะด้วยการใช้คำสั่ง SQL เพื่อขโมยข้อมูลหรือก่อให้เกิดความเสียหายของข้อมูล วิธีการป้องกันเบื้องต้น

SQL Injection – ป้องกันโดยหลีกเลี่ยงการประมวลผลโดยใช้คำสั่ง SQL ที่มาจากการต่อคำสั่งกับพารามิเตอร์ต่างๆ (string concatenation)

2.) Broken Authentication and Session Management

ฟังก์ชันแอปพลิเคชันเกี่ยวข้องกับการตรวจสอบสิทธิและการจัดการ session ที่พัฒนามาอย่างไม่ถูกต้อง จะทำให้ผู้โจมตีสามารถยึดรหัสผ่าน คีย์ หรือ session tokens หรือหลอกระบบมีข้อมูลส่วนตัวของผู้ใช้คนอื่น การป้องกันข้อมูลที่ใช้ระบุตัวตนของผู้ใช้งาน และการจัดการหรือเข้าถึงข้อมูล Session ที่ไม่ถูกต้องนำมาซึ่งช่องโหว่ได้ วิธีป้องกันเบื้องต้น

ทำการเข้ารหัสและกำหนดรูปแบบที่คาดเดาได้ยากกับข้อมูลที่มีความสำคัญ เช่น รหัสผ่าน, เลขที่บัญชี เป็นต้น

ห้ามแสดง Session ID ให้ผู้ใช้เห็น ไม่ว่ากรณีใดๆ และควรมีการกำหนด Timeout ของ Session ID ด้วย

3.) Cross-Site Scripting (XSS)

การเปิดช่องโหว่ให้แฮกเกอร์บันทึกข้อมูลที่แทรกแซงการทำงานของ Browser เข้าสู่ระบบได้ ไม่ว่าจะเป็นข้อมูลในรูปแบบแท็ก script ต่างๆ และเมื่อมีการนำไปแสดงผลบน Browser ของผู้ใช้งาน อาจจะถูกขโมยข้อมูลระบุตัวตนที่สำคัญต่างๆ ได้ วิธีป้องกันเบื้องต้น

- ให้มีการตรวจสอบข้อมูลที่บันทึกผ่านเว็บไซต์ทุกครั้ง เช่นไม่อนุญาตให้ใช้แท็กที่เป็นอันตราย เช่น script tag เป็นต้น

- ตรวจสอบลักษณะของข้อมูลต่างๆ ว่าเป็นไปตามรูปแบบที่กำหนด

- หากเลี่ยงอักขระพิเศษบางอย่างไม่ได้ ให้ใช้ HTML Encoding ก่อนนำไปจัดเก็บหรือใช้งาน

4.) Insecure Direct Object References

ช่องโหว่ในเรื่องของการปล่อยให้เข้าถึงทรัพยากรของระบบต่างๆ เช่น ไฟล์, โฟลเดอร์รวมถึงไปถึงข้อมูลบนฐานข้อมูลที่ผู้ใช้ไม่มีสิทธิ์เข้าถึงได้ วิธีป้องกันเบื้องต้น

- การพัฒนาแอพพลิเคชั่น จำเป็นต้องคำนึงถึงเรื่องการกำหนดสิทธิ์ในการเข้าถึงทรัพยากรที่สำคัญ

5.) Security Misconfiguration

ช่องโหว่ที่เกิดจากการตั้งค่าของระบบปฏิบัติการ แอพพลิเคชั่น ฐานข้อมูล รวมถึงนโยบายในการใช้งานที่หละหลวม วิธีการป้องกันเบื้องต้น

- หมั่นอัพเดท Patch ของซอฟต์แวร์ที่ใช้อย่างสม่ำเสมอ

- กำหนดสิทธิ์การใช้งานของทรัพยากรต่างๆ บนเครื่องเซิร์ฟเวอร์ เปิดพอร์ตที่จำเป็นสำหรับแอพพลิเคชั่นเท่านั้น

- ไม่แสดงข้อผิดพลาดในการทำงานของระบบให้ผู้ใช้งานทราบ โดยตั้งค่าที่แอพพลิเคชั่น

- กำหนดให้มีการเปลี่ยนรหัสผ่านอยู่เสมอ

6.) Sensitive Data Expose

ช่องโหว่จากการป้องกันข้อมูลสำคัญต่างๆ ไม่เพียงพอ เช่นรหัสผ่าน เลขประจำตัวประชาชน หมายเลขบัตรเครดิต เป็นต้น วิธีการป้องกันเบื้องต้น

- เข้ารหัสในการจัดเก็บข้อมูลที่มีความสำคัญทั้งหมด
- ให้อัลกอริทึมและคีย์ในการเข้ารหัสที่แข็งแรง
- ปิดการใช้งาน Auto Complete กับข้อมูลที่มีความสำคัญ
- ติดตั้ง SSL กับเว็บไซต์ เพื่อป้องกันการแฮกข้อมูลผ่าน Network Traffic

7.) Missing Function Level Access Control

ช่องโหว่ที่เกิดการควบคุมสิทธิ์การใช้งานฟังก์ชัน หรือฟีเจอร์ของระบบเฉพาะการแสดงผลหรือซ่อนบน UI เท่านั้น วิธีการป้องกันเบื้องต้น

- ตรวจสอบการเข้าถึงฟังก์ชัน หรือฟีเจอร์ จากการประมวลผลบนเซิร์ฟเวอร์ด้วย
- จัดเก็บ Audit log การเข้าถึงฟังก์ชัน หรือฟีเจอร์ที่ผิดปกติ เพื่อใช้ตรวจสอบย้อนหลังได้

8.) Cross-Site Request Forgery (CSRF)

เป็นวิธีการหลอกผู้ใช้งานหรือเหยื่อเข้าเว็บไซต์ของแฮกเกอร์ หากผู้ใช้งานมีการ login ไปยังเว็บไซต์สำหรับทำธุรกรรมต่างๆ ไว้ เช่น บริการทางอิเลคทรอนิคส์ของธนาคาร เว็บไซต์ของแฮกเกอร์จะส่ง Request ไปยังเว็บไซต์ปลายทางเพื่อทำธุรกรรมหรือประมวลผลต่างๆ โดยเว็บไซต์ปลายทางเข้าใจว่าเป็นผู้ใช้งานจริง วิธีการป้องกันเบื้องต้น

- ควรแทรกค่า token ต่างๆ ใน Hidden Field ใน Body ไปกับ HTTP Request โดยห้ามแสดงสิ่งเหล่านี้บน URL
- ควรมีการป้องกัน HTTP Request จาก URL หรือ Domain อื่น
- อาจมีการให้ระบุ CAPTCHA เพื่อตรวจสอบซ้ำอีกครั้ง

9.) Using Components with Known Vulnerabilities

การนำ Components หรือ Libraries ที่มีช่องโหว่มาใช้กับแอพพลิเคชั่นของเรา ก็จะส่งผลให้แอพพลิเคชั่นมีช่องโหว่ตามไปด้วย วิธีการป้องกันเบื้องต้น

- หมั่นตรวจสอบเวอร์ชันของ Components หรือ Libraries ที่นำมาใช้ และมีการตรวจสอบความปลอดภัยให้ครบถ้วนทุกครั้งที่ต้องการนำมาใช้งาน

10.) Unvalidated Redirects and Forwards

เว็บแอพพลิเคชั่นมีการ Redirect หรือ Forward ไปยังเว็บไซต์อื่น โดยไม่มีการตรวจสอบเสียก่อน ซึ่งอาจถูกโจมตีโดยพาผู้ใช้งานไปยังเว็บไซต์ที่มัลแวร์หรือส่งไปยังหน้าเว็บไซต์ที่ไม่อนุญาตให้เข้าถึงได้ วิธีการป้องกันเบื้องต้น

- หลีกเลี่ยงการ Redirect หรือ Forward ไปยังเว็บไซต์ที่ไม่เกี่ยวข้องกับแอพพลิเคชั่น

- หากเลี่ยงไม่ได้ ให้กำหนดและควบคุมเว็บไซต์ที่อนุญาตให้ Redirect หรือ Forward ไปได้เท่านั้น

3.3.1.1.2 CVE (Common Vulnerabilities and Exposures)

รายชื่อของช่องโหว่ที่เป็นมาตรฐานเดียวกันสำหรับอ้างอิงถึงช่องโหว่แต่ละชนิด เพื่อให้แหล่งข้อมูลด้านช่องโหว่, เจ้าของผลิตภัณฑ์ และผู้ใช้งานโปรแกรมสามารถเข้าใจได้ตรงกัน

ชื่อของ CVE ประกอบด้วย ปีที่พบช่องโหว่ และลำดับของช่องโหว่ที่ได้รับ CVE ในปีนั้น เช่น CVE-1999-0065 เป็นต้น

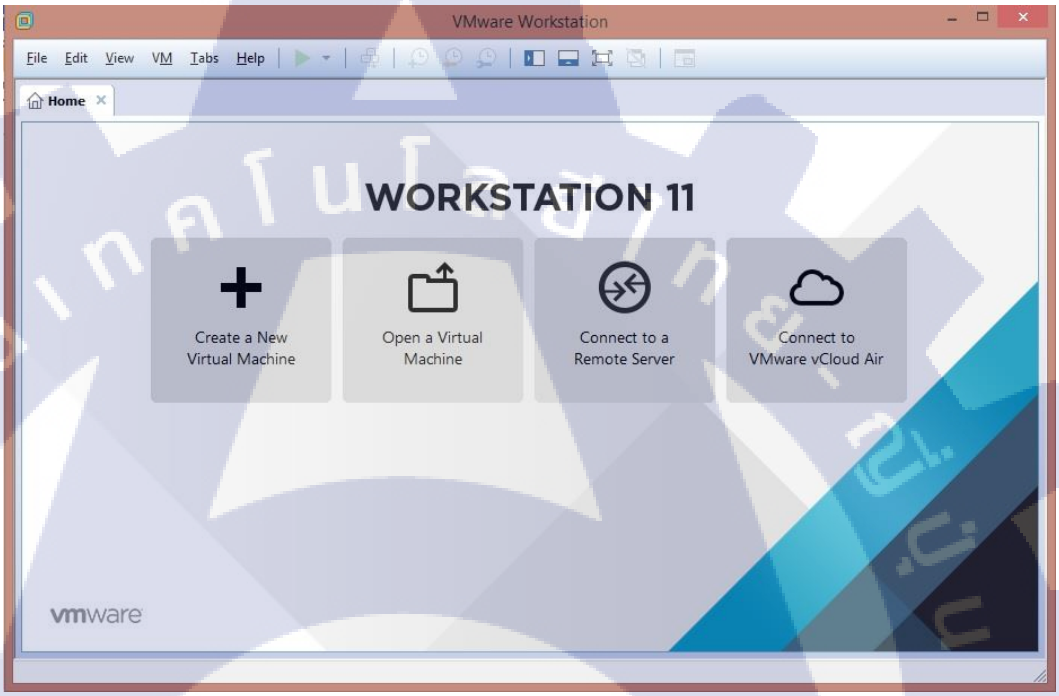
องค์ประกอบของ CVE

* ชื่อและหมายเลข CVE
* รายละเอียดโดยย่อของช่องโหว่
* แหล่งข้อมูลอ้างอิง

3.3.2 ขั้นตอนการเตรียมการ

3.3.2.1 ติดตั้งระบบปฏิบัติการ Linux Kali Sana ลงบน VMware Workstation

1.) เปิดโปรแกรม VMware Workstation

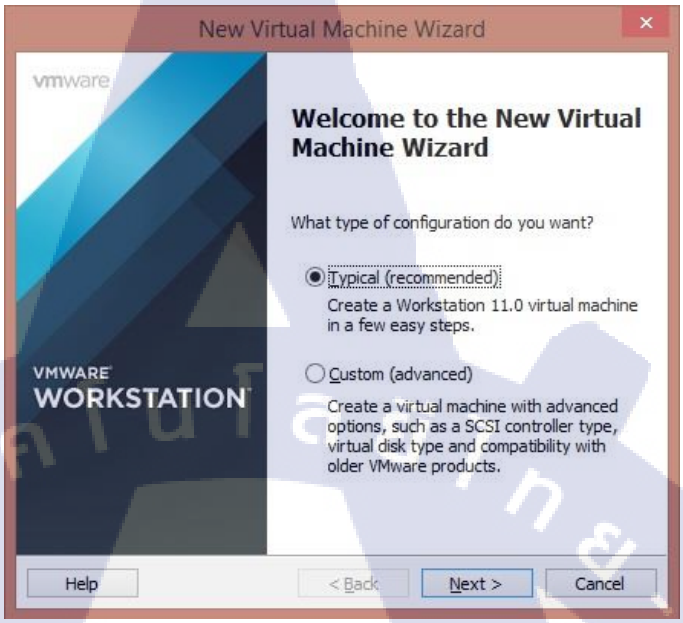


ภาพที่ 3.1 ภาพโปรแกรม VMware Workstation รุ่นที่ 11

2.) กดไอคอน Create a New Virtual Machine

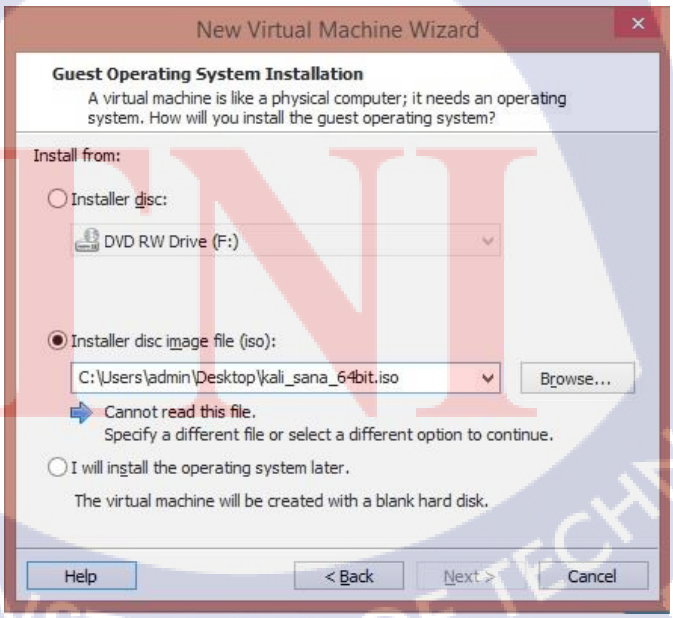
ภาพที่ 3.2 ไอคอน Create a New Virtual Machine

3.) เลือกTypical กดปุ่ม Next



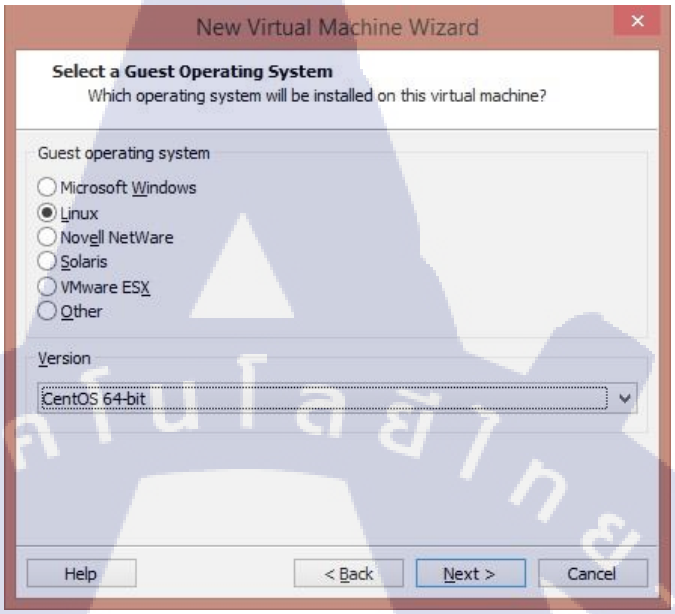
ภาพที่ 3.3 หน้าต่าง New Virtual Machine Wizard

4.) เลือก Installer disc image file (iso) และ Browse ไฟล์ image ของ Kali sana



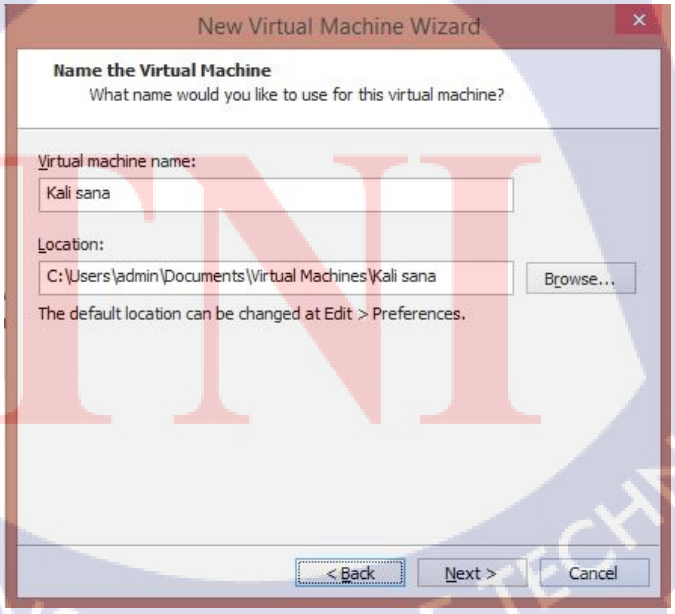
ภาพที่ 3.4 หน้าต่างเลือกวิธีการในการติดตั้ง

5.) เลือกระบบปฏิบัติการ Linux Version ContOS 64-bit



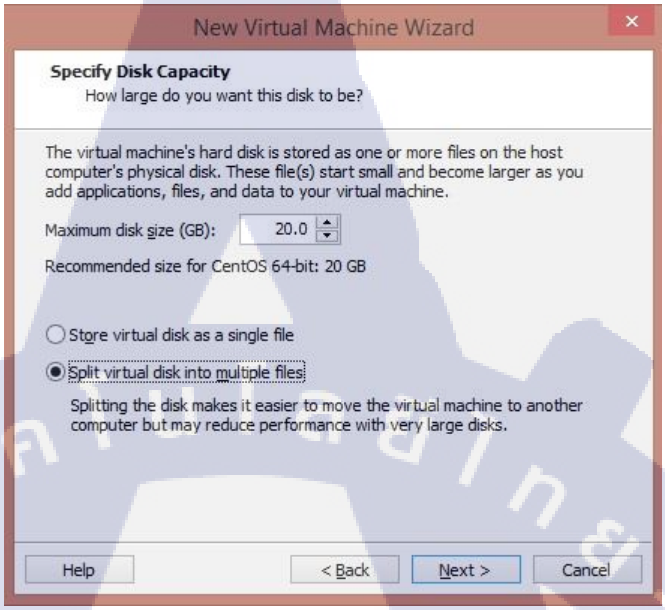
ภาพที่ 3.5 หน้าต่างเลือกระบบปฏิบัติการ

6.) กด Next เพื่อสร้าง Directory ของ Virtual Machine



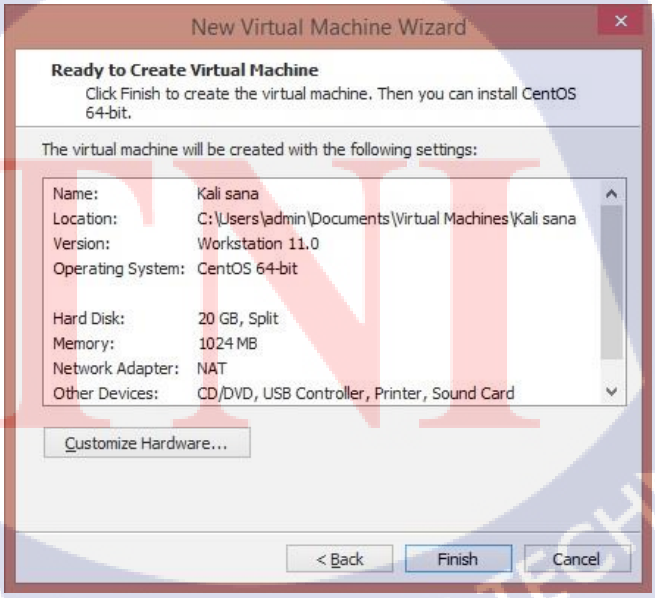
ภาพที่ 3.6 หน้าต่างเลือก Directory ของ Virtual Machine

7.) กด Next เพื่อยืนยันการเลือกขนาดพื้นที่จัดเก็บและรูปแบบการจัดเก็บข้อมูล

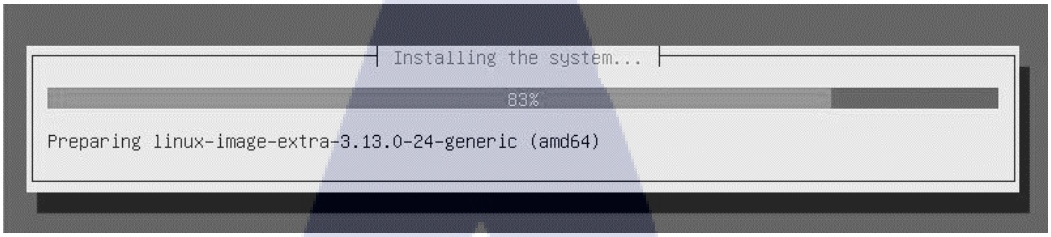


ภาพที่ 3.7 หน้าต่างเลือกขนาดและวิธีการเก็บ

8.) กด Finish เพื่อสิ้นสุดการติดตั้ง



ภาพที่ 3.8 หน้าต่างสรุปการติดตั้ง



ภาพที่ 3.9 หน้าจอขณะกำลังติดตั้ง Ubuntu Server

9.) ติดตั้ง Apache ลงบน Kali sana

9.1.) พิมพ์ “sudo apt-get install apache2” แล้วกดแป้น Enter

9.2.) กดแป้น y แล้วกดแป้น Enter

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  apache2-bin apache2-data libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap ssl-cert
Suggested packages:
  www-browser apache2-doc apache2-suexec-pristine apache2-suexec-custom apache2-utils
  openssl-blacklist
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
  ssl-cert
0 upgraded, 8 newly installed, 0 to remove and 31 not upgraded.
Need to get 1,284 kB of archives.
After this operation, 5,342 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu/ trusty/main libapr1 amd64 1.5.0-1 [85.1 kB]
Get:2 http://security.ubuntu.com/ubuntu/ trusty-security/main apache2-bin amd64 2.4.7-1ubuntu4.1 [83
9 kB]
Get:3 http://security.ubuntu.com/ubuntu/ trusty-security/main apache2-data all 2.4.7-1ubuntu4.1 [160
 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu/ trusty/main libaprutil1 amd64 1.5.3-1 [76.4 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu/ trusty/main libaprutil1-dbd-sqlite3 amd64 1.5.3-1 [10.5 k
B]
Get:6 http://security.ubuntu.com/ubuntu/ trusty-security/main apache2 amd64 2.4.7-1ubuntu4.1 [87.5 k
B]
Get:7 http://us.archive.ubuntu.com/ubuntu/ trusty/main libaprutil1-ldap amd64 1.5.3-1 [8,634 B]
Get:8 http://us.archive.ubuntu.com/ubuntu/ trusty/main ssl-cert all 1.0.33 [16.6 kB]
Fetched 1,284 kB in 13s (96.4 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libapr1:amd64.
(Reading database ... 51373 files and directories currently installed.)
Preparing to unpack .../libapr1_1.5.0-1_amd64.deb ...
Unpacking libapr1:amd64 (1.5.0-1) ...
Selecting previously unselected package libaprutil1:amd64.
Preparing to unpack .../libaprutil1_1.5.3-1_amd64.deb ...
Unpacking libaprutil1:amd64 (1.5.3-1) ...
```

ภาพที่ 3.10 หน้าจอขณะทำการติดตั้ง Apache

9.3.) ตรวจสอบการติดตั้ง apache ว่าทำงานได้หรือไม่โดยการพิมพ์คำสั่ง “netstat –l | grep http” หรือ “ /usr/sbin/lsof –i | grep –i httpd”

ภาพที่ 3.11 การตรวจสอบการเปิดพอร์ท TCP HTTP

10.) ติดตั้ง PHP

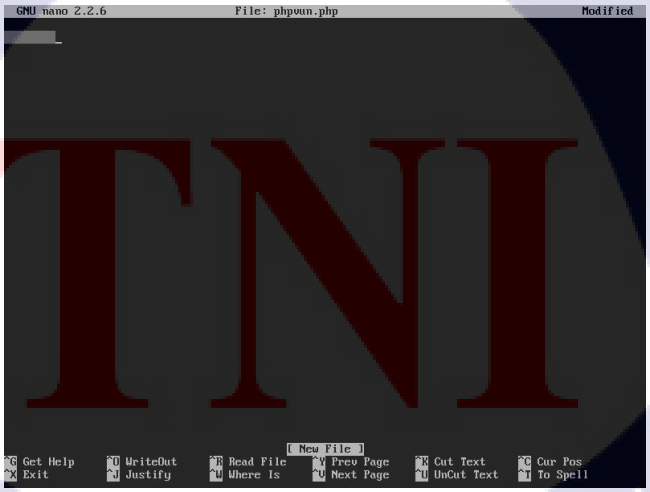
10.1.) พิมพ์คำสั่ง “sudo apt-get install php5”

10.2.) พิมพ์คำสั่ง “sudo apt-get install libapache2-mod-php5”

11.) ตรวจสอบการติดตั้ง PHP ว่าทำงานได้หรือไม่

11.1.) เข้าไปที่ Directory html โดยการพิมพ์คำสั่ง “cd /” และคำสั่ง “cd var/www/html/”

11.2.) สร้างไฟล์ที่ใช้ทดสอบโดยคำสั่ง “sudo nano test.php”



ภาพที่ 3.12 หน้าจอขณะกำลังแก้ไขไฟล์ด้วย CLI command

11.3.) พิมพ์ “<?php phpinfo(); ?>

11.4.) กดแป้น Ctrl + x

11.5.) กดแป้น y แล้วกดแป้น Enter

11.6.) กดแป้น Enter

11.7.) ใช้ Browser เข้าไปไฟล์ที่สร้างไว้

PHP Version 5.5.9-1ubuntu4.3

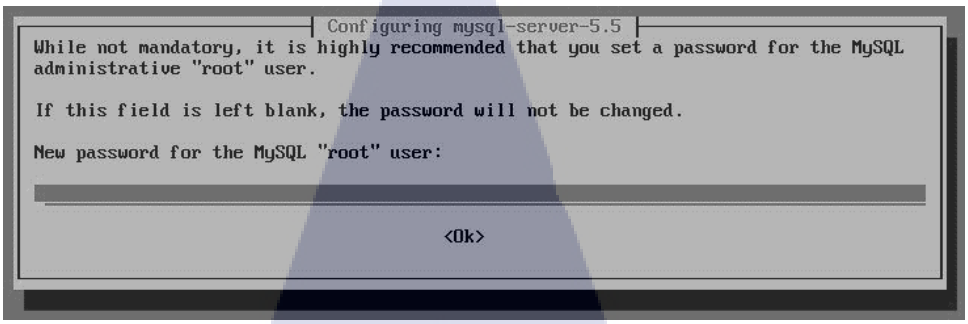
System	Linux ubuntu 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64
Build Date	Jul 7 2014 16:33:02
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/05-opcache.ini, /etc/php5/apache2/conf.d/10-pdo.ini, /etc/php5/apache2/conf.d/20-json.ini, /etc/php5/apache2/conf.d/20-readline.ini
PHP API	20121113
PHP Extension	20121212
Zend Extension	220121212
Zend Extension Build	API220121212,NTS
PHP Extension Build	API20121212,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	enabled
Registered PHP Streams	https, ftps, compress.zlib, compress.bzip2, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, tls
Registered Stream Filters	zlib.*, bzip2.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk

ภาพที่ 3.13 หน้าจอแสดงรายละเอียดของ PHP

18.) ติดตั้ง mysql

18.1.) พิมพ์คำสั่ง “sudo apt-get install mysql-server”

18.2.) ตั้งรหัสผ่าน



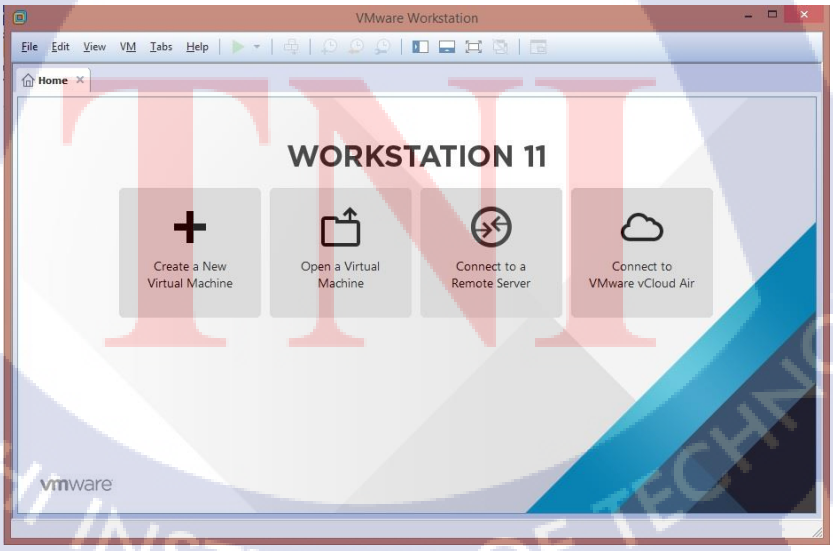
ภาพที่ 3.14 หน้าจอตั้งรหัสผ่าน MySQL

19.) ตรวจสอบการติดตั้ง apache ว่าทำงานได้หรือไม่โดยการพิมพ์คำสั่ง “netstat –tap | grep mysql”

ภาพที่ 3.15 การตรวจสอบการเปิดพอร์ท TCP MySQL

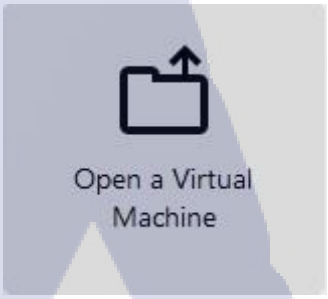
3.3.2.2 ติดตั้ง Metasploitable ลงบน VMware Workstation

1.) เปิดโปรแกรม VMware Workstation



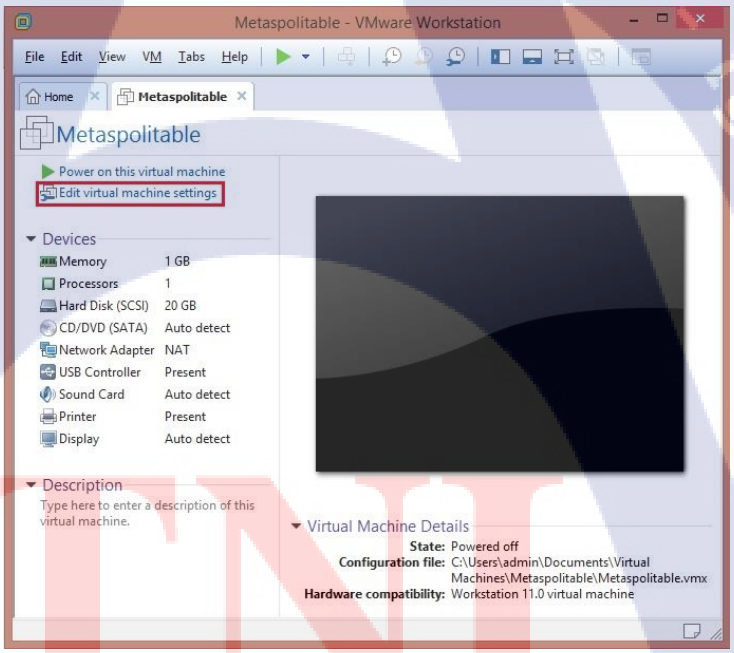
ภาพที่ 3.16 ภาพโปรแกรม VMware Workstation รุ่นที่ 11

2.) กดไอคอน Open a Virtual Machine



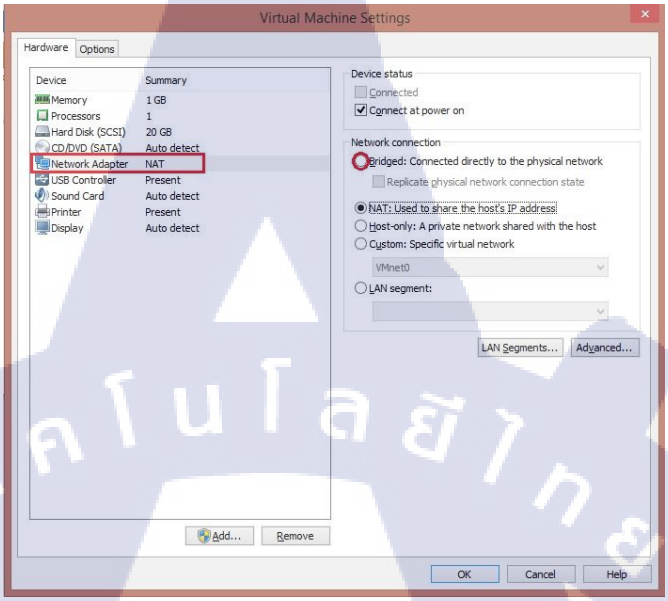
ภาพที่ 3.17 ไอคอน Open a Virtual Machine

3.) กด Edit virtual machine settings



ภาพที่ 3.18 หน้าต่าง Metasploitable

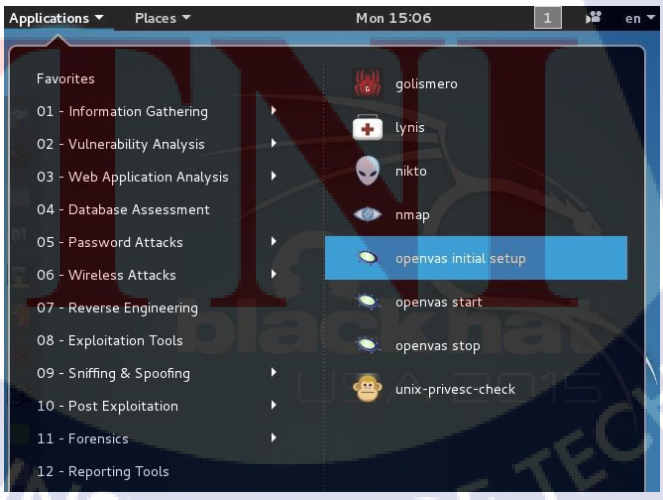
4.) กด Network Adapter แล้วเลือก Bridged



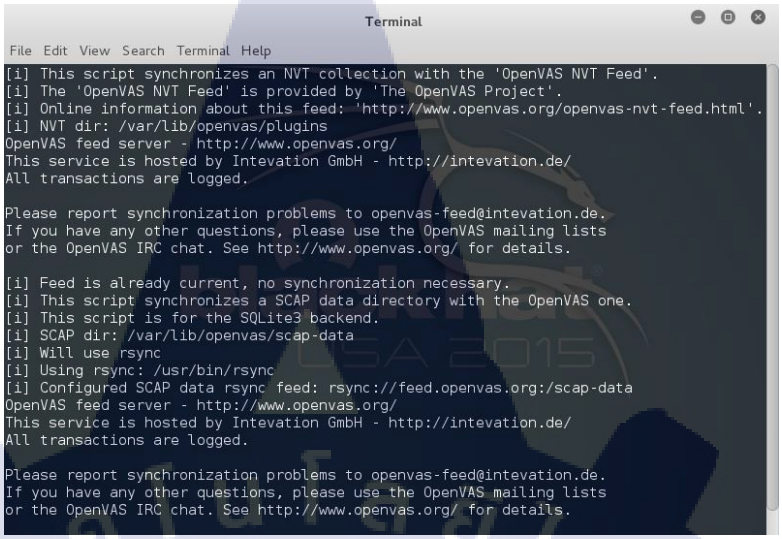
ภาพที่ 3.19 หน้าต่างตั้งค่า Virtual Machine

3.3.2.3 ติดตั้ง OpenVAS

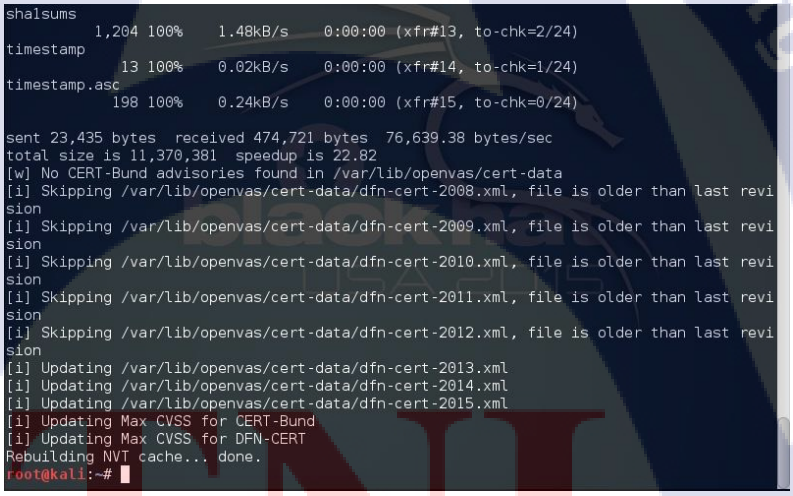
1.) เปิดโปรแกรม openvas initial setup



ภาพที่ 3.20 หน้าจอเลือกโปรแกรม openvas initial setup

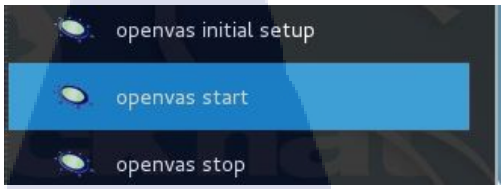


ภาพที่ 3.21 หน้าจอขณะติดตั้ง OpenVAS Initial Setup

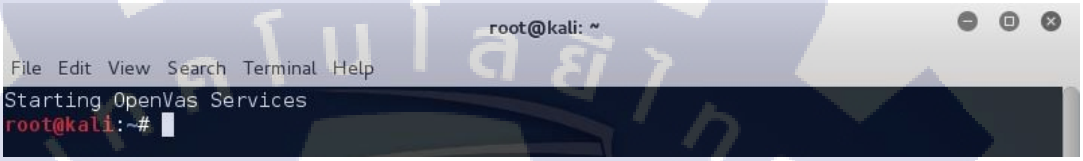


ภาพที่ 3.22 หน้าจอหลังจากติดตั้ง OpenVAS Initial Setup (ต่อ)

2.) เปิดโปรแกรม openvas start



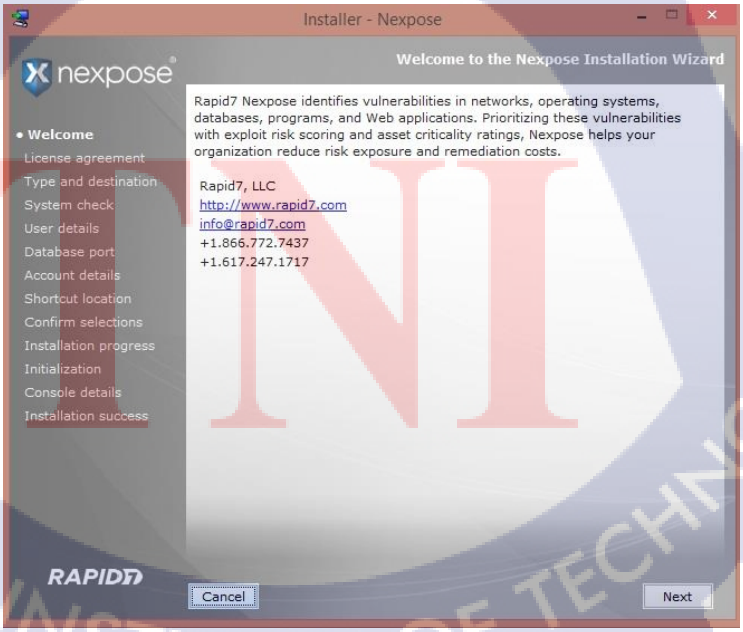
ภาพที่ 3.23 ภาพโปรแกรม OpenVAS Start



ภาพที่ 3.24 หน้าจอแสดงการเริ่มต้นการทำงาน

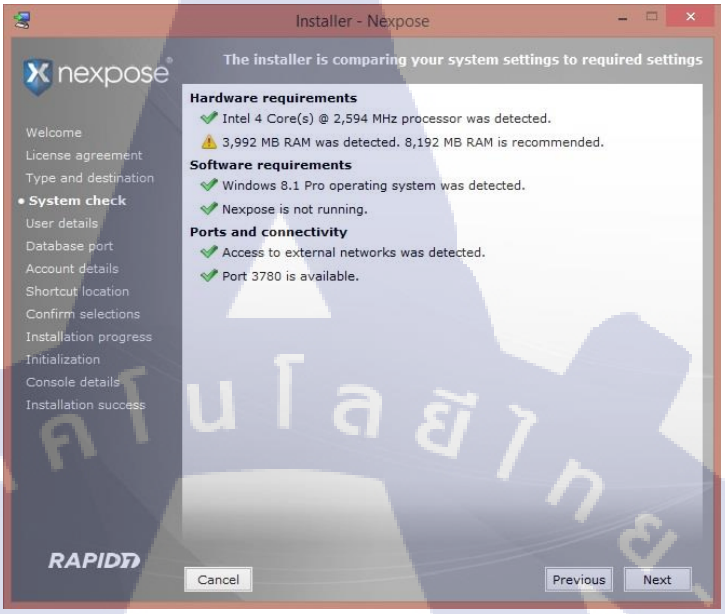
3.3.2.4 ติดตั้ง Nexpose

1.) กดปุ่ม Next



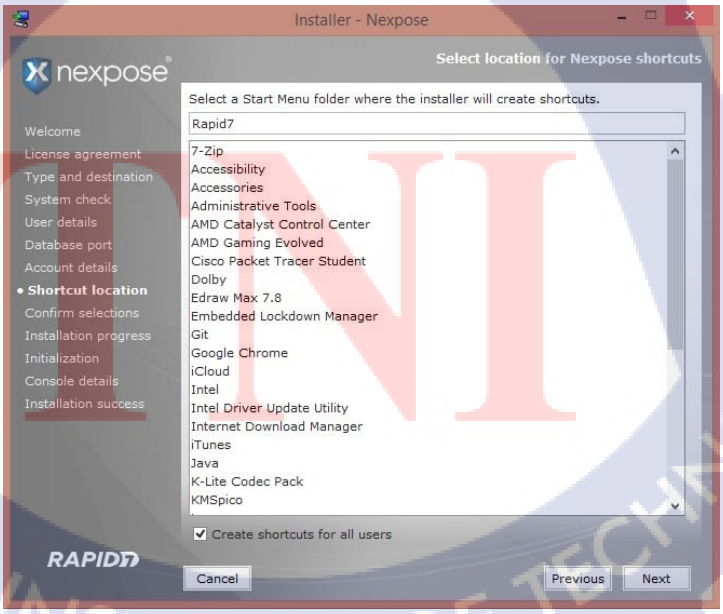
ภาพที่ 3.25 หน้าต่างแรกของการติดตั้ง Nexpose

2.) กดปุ่ม Next



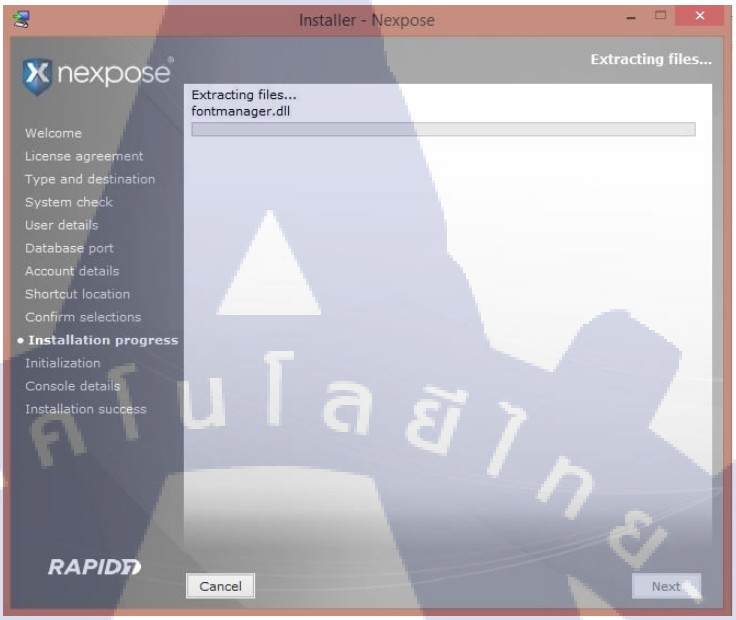
ภาพที่ 3.26 หน้าต่างแสดงความต้องการของโปรแกรม

3.) กดปุ่ม Next



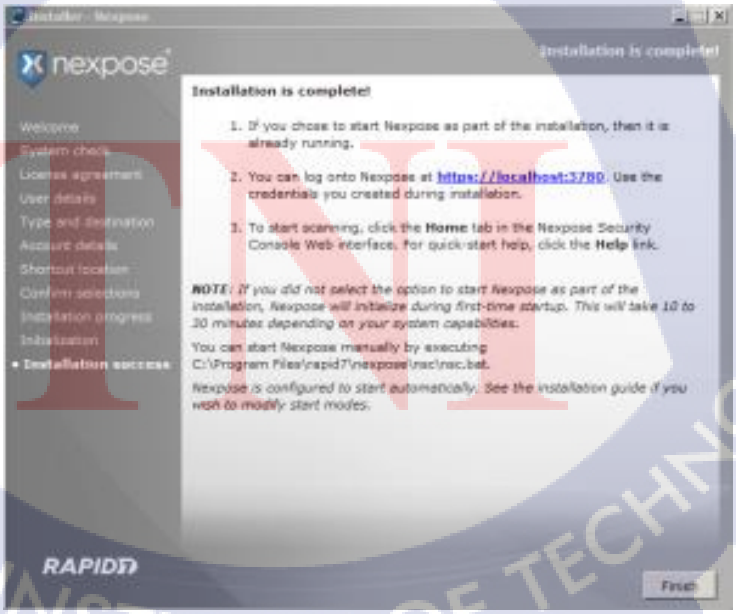
ภาพที่ 3.27 หน้าต่างเลือกแฟ้มเพื่อสร้างทางลัด

4.) กดปุ่ม Next



ภาพที่ 3.28 หน้าต่างแสดงสถานการณ์ติดตั้ง

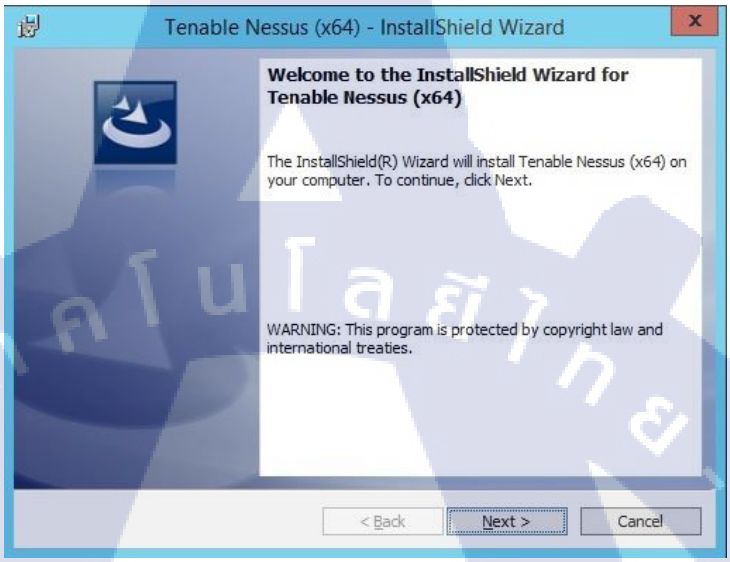
5.) กดปุ่ม Finish



ภาพที่ 3.29 หน้าต่างเสร็จสิ้นการติดตั้ง

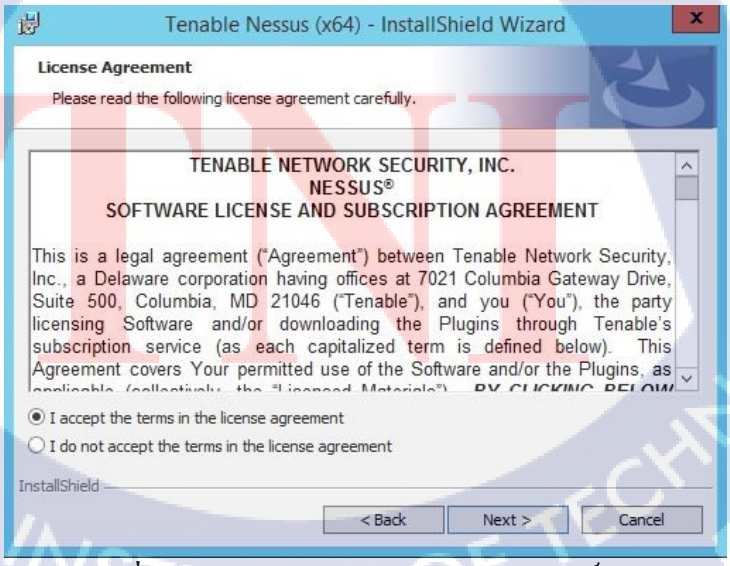
3.3.2.5 ติดตั้ง Nessus

1.) กดปุ่ม Next



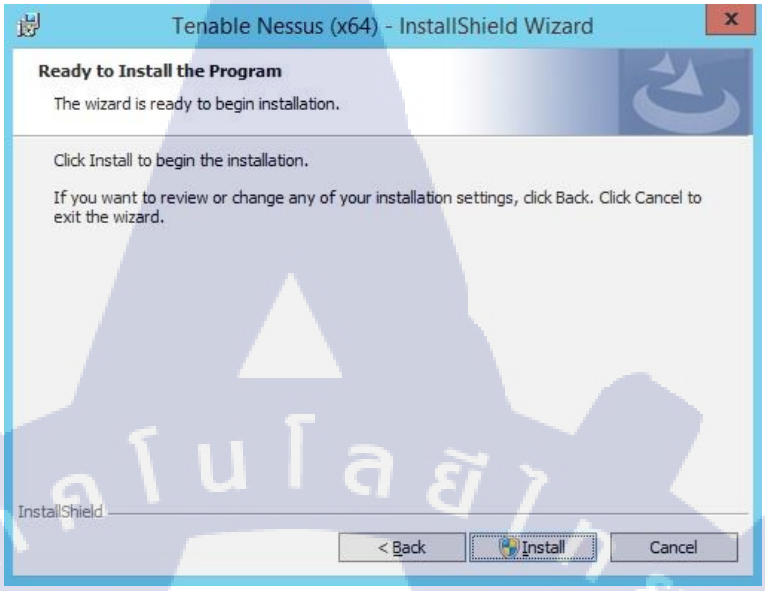
ภาพที่ 3.30 หน้าต่างเริ่มต้นการติดตั้ง Nessus

2.) กดปุ่ม Next



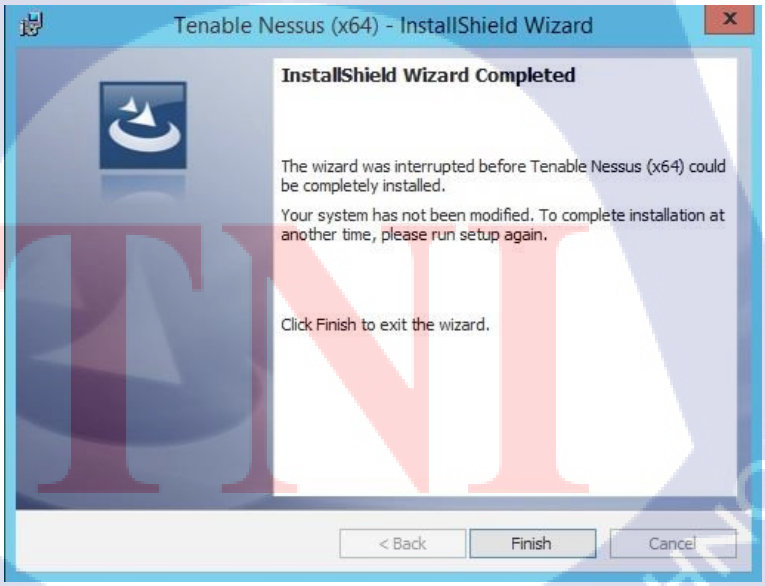
ภาพที่ 3.31 หน้าต่างยืนยันข้อตกลงทางลิขสิทธิ์

3.) กดปุ่ม Install



ภาพที่ 3.32 หน้าต่างยืนยันการติดตั้ง

4.) กดปุ่ม Install



ภาพที่ 3.33 หน้าต่างเสร็จสิ้นการติดตั้ง

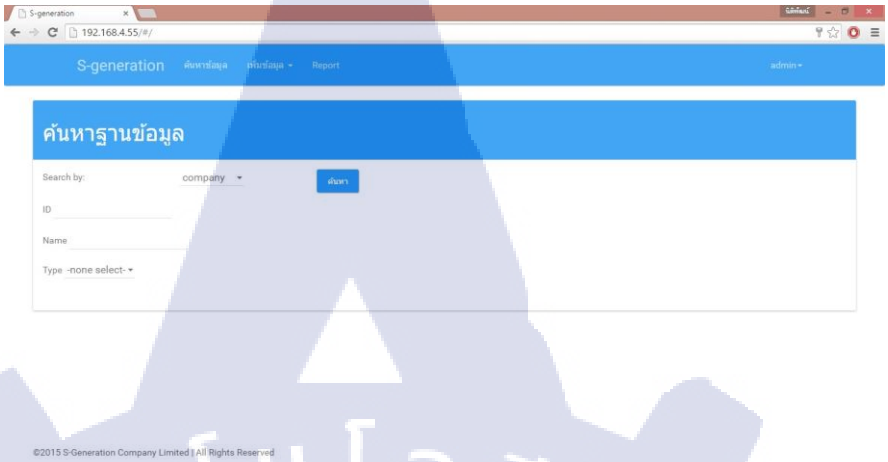
บทที่ 4
ผลการดำเนินงาน การวิเคราะห์ และสรุปผลต่างๆ

4.1 ขั้นตอนและผลการดำเนินงาน

จากการที่ได้ปฏิบัติงานสหกิจศึกษาที่บริษัท เอส-เจเนเรชัน จำกัด ในครั้งนี้ได้มีโอกาสเข้าร่วมเป็นส่วนหนึ่งในการออกปฏิบัติงานนอกสถานที่ในส่วนของบริการ DMSS (Digital Media Sanitization Service) การออกแบบและพัฒนาเว็บแอปพลิเคชันเพื่อใช้ในการสืบค้นและจัดเก็บฐานข้อมูล ออกแบบโครงสร้างระบบเครือข่ายผ่านในบริษัท และได้รับมอบหมายให้ทำโครงงานการทดสอบเปรียบเทียบแอปพลิเคชันค้นหาช่องโหว่ด้านความปลอดภัยระบบ 3 ผลิตภัณฑ์ (OpenVAS, Nessus, Nexpose) ทำได้รับประสบการณ์ในการปฏิบัติงานจริงในบริษัท ซึ่งในระหว่างปฏิบัติงานได้มีโอกาสร่วมกับพนักงานภายในบริษัท ทำให้ได้รับความรู้ที่กว้างขวางเกี่ยวกับด้านความปลอดภัยทางสารสนเทศ ล้วนแล้วแต่มีประโยชน์ในการปฏิบัติงานในอนาคต

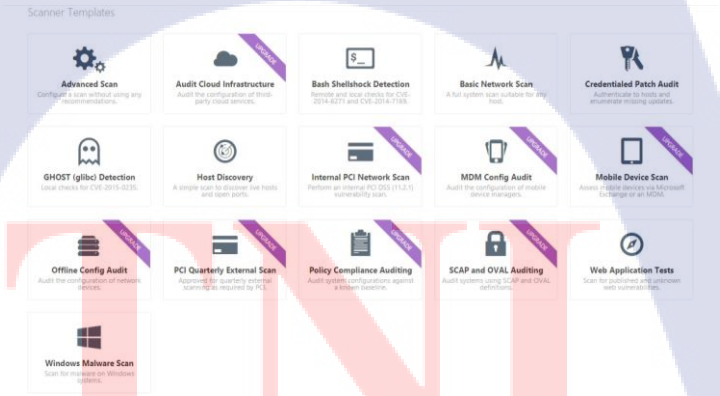
4.1.1 ผลการดำเนินงานการพัฒนาเว็บแอปพลิเคชันสืบค้นและจัดเก็บฐานข้อมูลภายในบริษัท

ในช่วงสัปดาห์แรก เป็นช่วงของการศึกษาทำความเข้าใจเกี่ยวกับการเขียนโปรแกรมที่จะนำมาใช้ในการพัฒนาระบบใหม่ และโครงสร้างการทำงานของฐานข้อมูลภายในเว็บแอปพลิเคชัน โดยงานหลักที่ได้รับมอบหมายคือ การพัฒนาเว็บแอปพลิเคชันเพื่อใช้ในการสืบค้นและจัดเก็บฐานข้อมูลภายในบริษัท

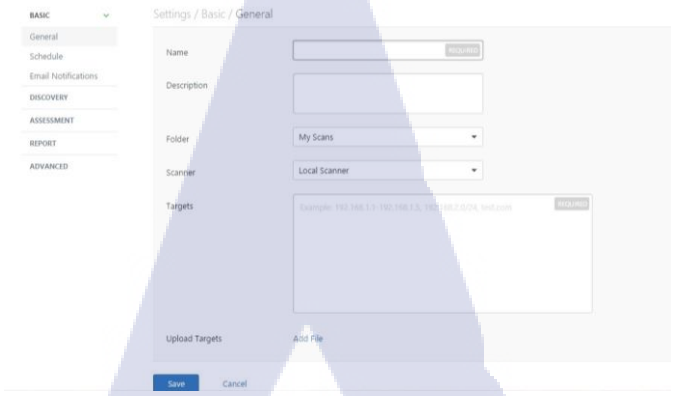


ภาพที่ 4.1 หน้าแรกของเว็บแอปพลิเคชัน

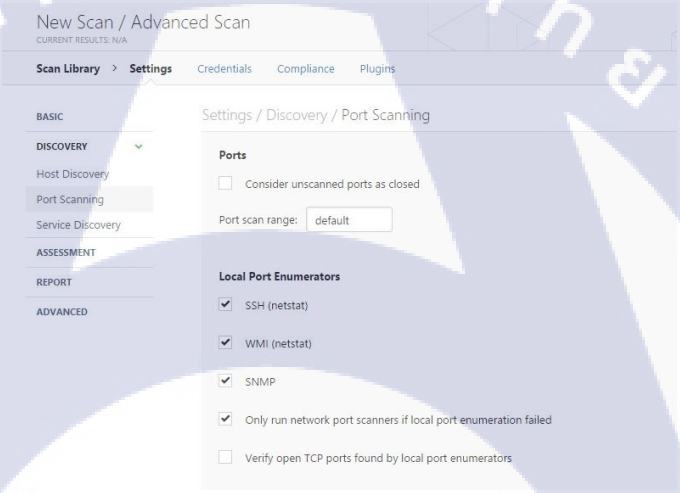
4.1.2 ผลการดำเนินงานทดสอบแอปพลิเคชัน Nessus



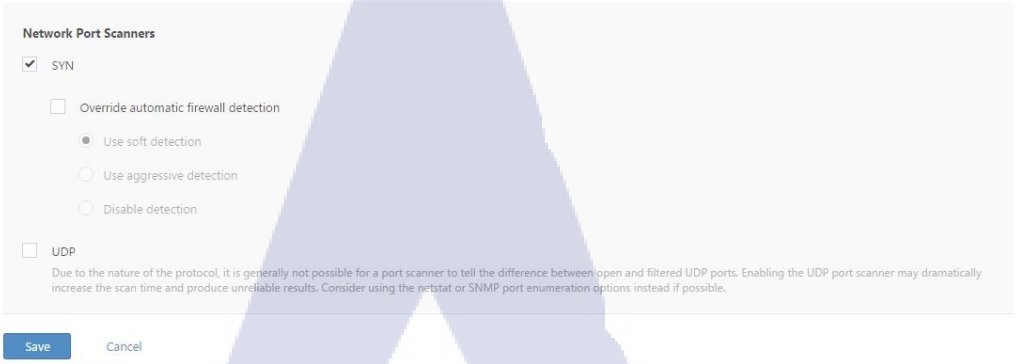
ภาพที่ 4.2 หน้าจอการเลือกรูปแบบการค้นหาช่องโหว่ Nessus



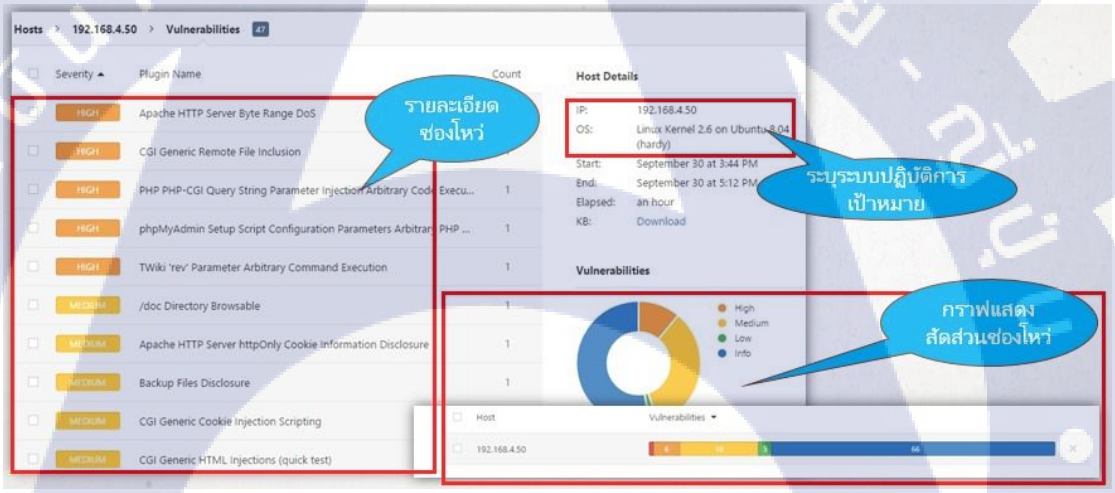
ภาพที่ 4.3 หน้าจอการกรอกรายละเอียดของการค้นหาช่องโหว่ Nessus



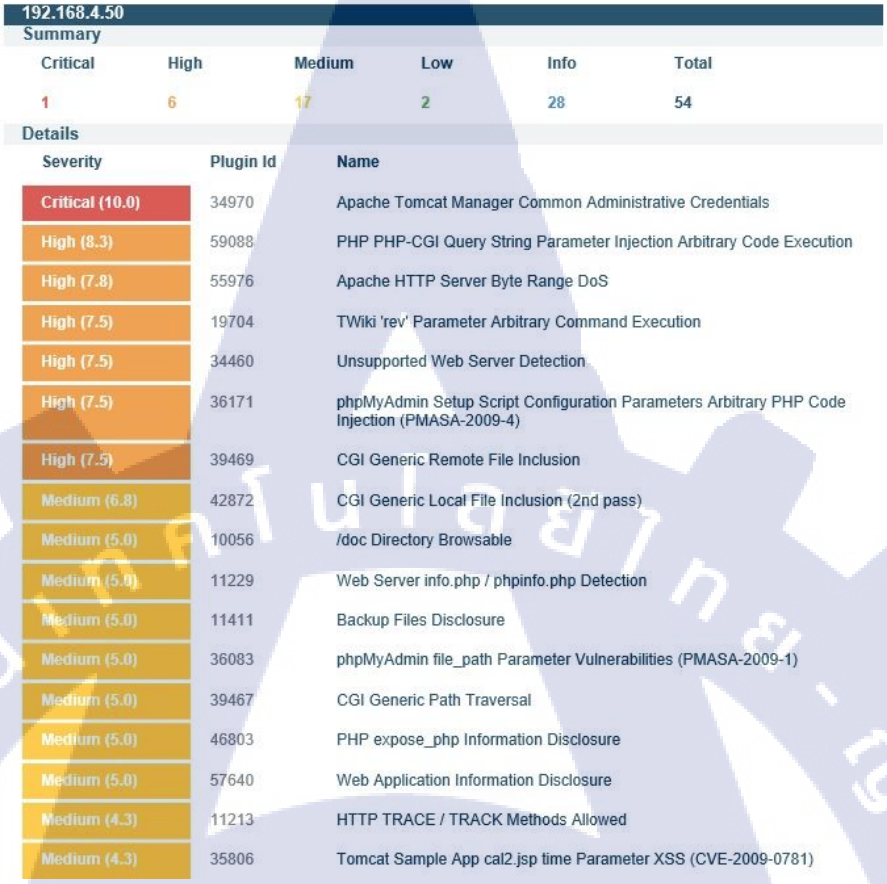
ภาพที่ 4.4 หน้าจอการกรอกรายละเอียดของการค้นหาช่องโหว่ Nessus (ต่อ)



ภาพที่ 4.5 หน้าจอการกรอกรายละเอียดของการค้นหาช่องโหว่ Nessus (ต่อ)



ภาพที่ 4.6 หน้าจอขณะกำลังสแกนค้นหาช่องโหว่ Nessus



192.168.4.50

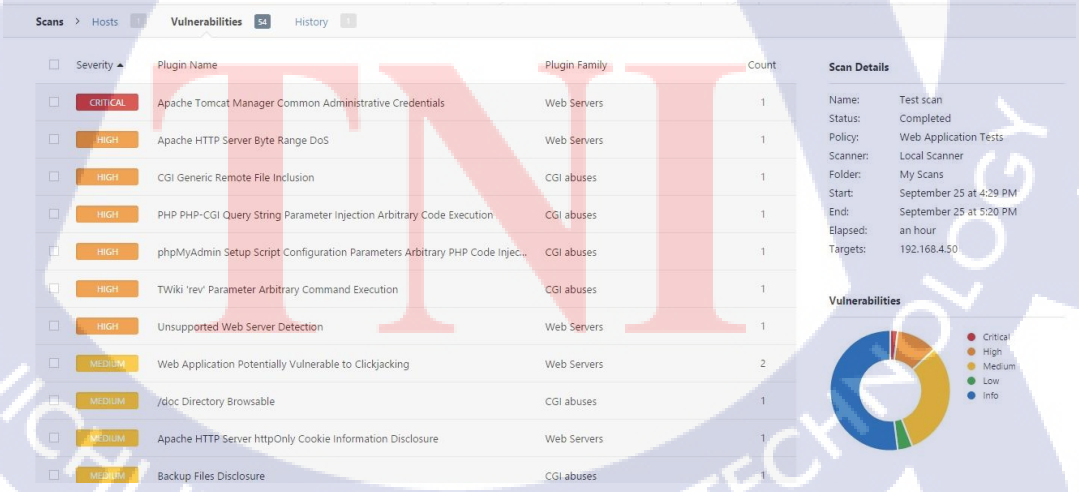
Summary

Critical	High	Medium	Low	Info	Total
1	6	17	2	28	54

Details

Severity	Plugin Id	Name
Critical (10.0)	34970	Apache Tomcat Manager Common Administrative Credentials
High (8.3)	59088	PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution
High (7.8)	55976	Apache HTTP Server Byte Range DoS
High (7.5)	19704	TWiki 'rev' Parameter Arbitrary Command Execution
High (7.5)	34460	Unsupported Web Server Detection
High (7.5)	36171	phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)
High (7.5)	39469	CGI Generic Remote File Inclusion
Medium (6.8)	42872	CGI Generic Local File Inclusion (2nd pass)
Medium (5.0)	10056	/doc Directory Browsable
Medium (5.0)	11229	Web Server info.php / phpinfo.php Detection
Medium (5.0)	11411	Backup Files Disclosure
Medium (5.0)	36083	phpMyAdmin file_path Parameter Vulnerabilities (PMASA-2009-1)
Medium (5.0)	39467	CGI Generic Path Traversal
Medium (5.0)	46803	PHP expose_php Information Disclosure
Medium (5.0)	57640	Web Application Information Disclosure
Medium (4.3)	11213	HTTP TRACE / TRACK Methods Allowed
Medium (4.3)	35806	Tomcat Sample App cal2.jsp time Parameter XSS (CVE-2009-0781)

ภาพที่ 4.7 หน้าจอแสดงสรุปผลการค้นหาช่องโหว่ Nessus



Scans › Hosts 1 Vulnerabilities 54 History 1

Severity	Plugin Name	Plugin Family	Count
CRITICAL	Apache Tomcat Manager Common Administrative Credentials	Web Servers	1
HIGH	Apache HTTP Server Byte Range DoS	Web Servers	1
HIGH	CGI Generic Remote File Inclusion	CGI abuses	1
HIGH	PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution	CGI abuses	1
HIGH	phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injec...	CGI abuses	1
HIGH	TWiki 'rev' Parameter Arbitrary Command Execution	CGI abuses	1
HIGH	Unsupported Web Server Detection	Web Servers	1
MEDIUM	Web Application Potentially Vulnerable to Clickjacking	Web Servers	2
MEDIUM	/doc Directory Browsable	CGI abuses	1
MEDIUM	Apache HTTP Server httpOnly Cookie Information Disclosure	Web Servers	1
MEDIUM	Backup Files Disclosure	CGI abuses	1

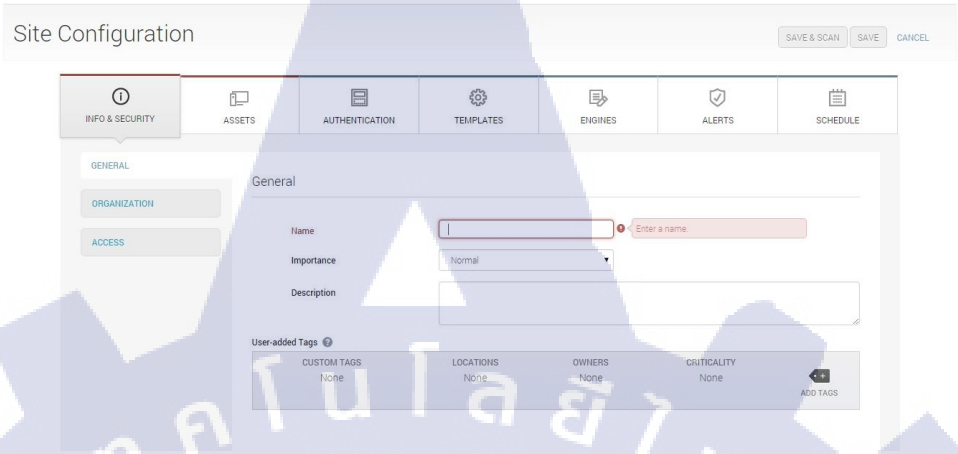
Scan Details

Name:	Test scan
Status:	Completed
Policy:	Web Application Tests
Scanner:	Local Scanner
Folder:	My Scans
Start:	September 25 at 4:29 PM
End:	September 25 at 5:20 PM
Elapsed:	an hour
Targets:	192.168.4.50

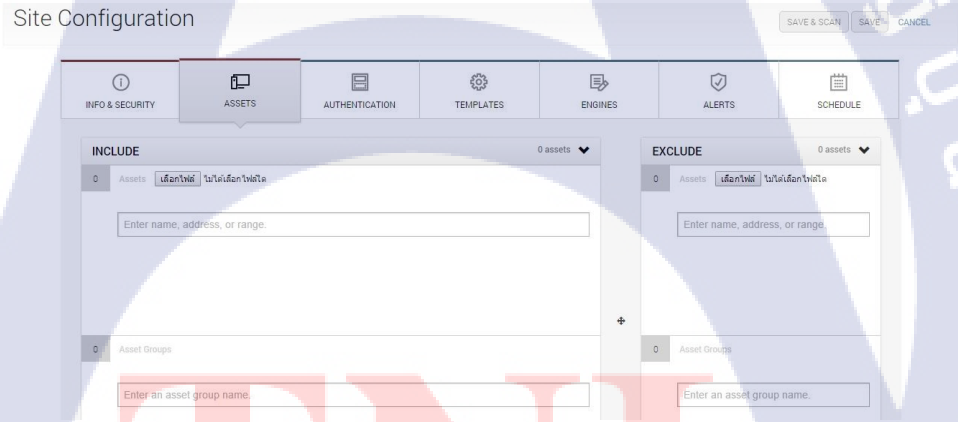
Vulnerabilities

ภาพที่ 4.8 หน้าจอรายงานการค้นหาช่องโหว่ Nessus

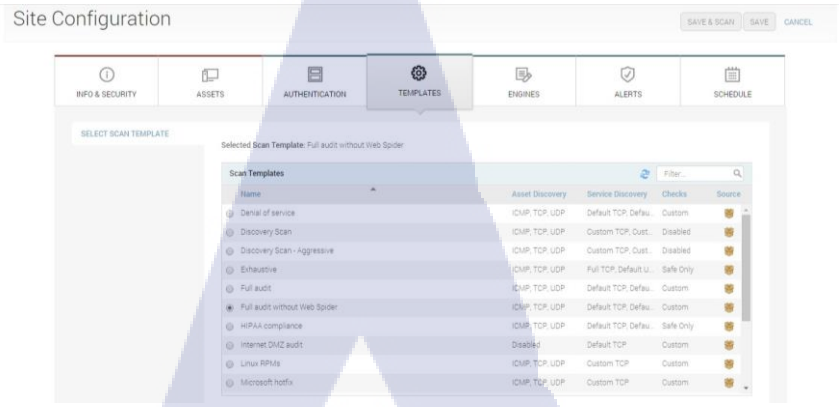
4.1.3 ผลการดำเนินงานทดสอบแอปพลิเคชัน Nexpose



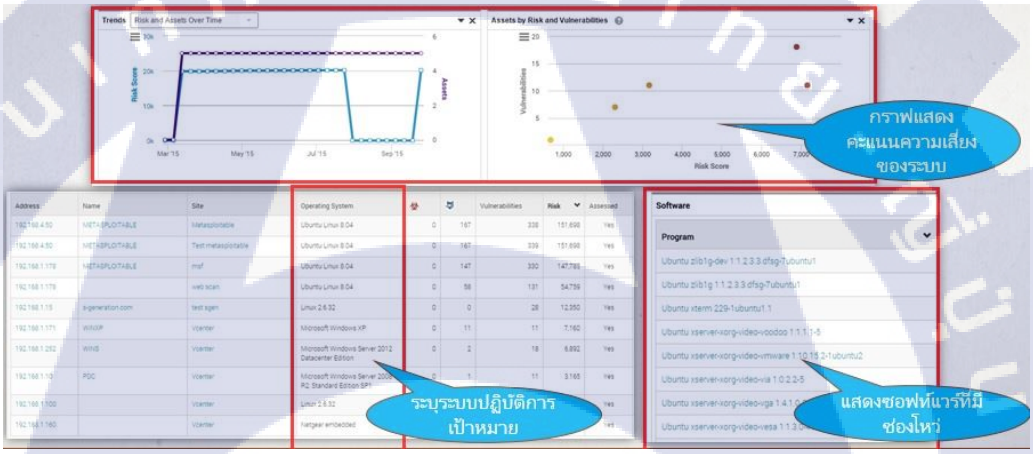
ภาพที่ 4.9 หน้าจอกรอกรายละเอียดการค้นหาช่องโหว่ Nexpose



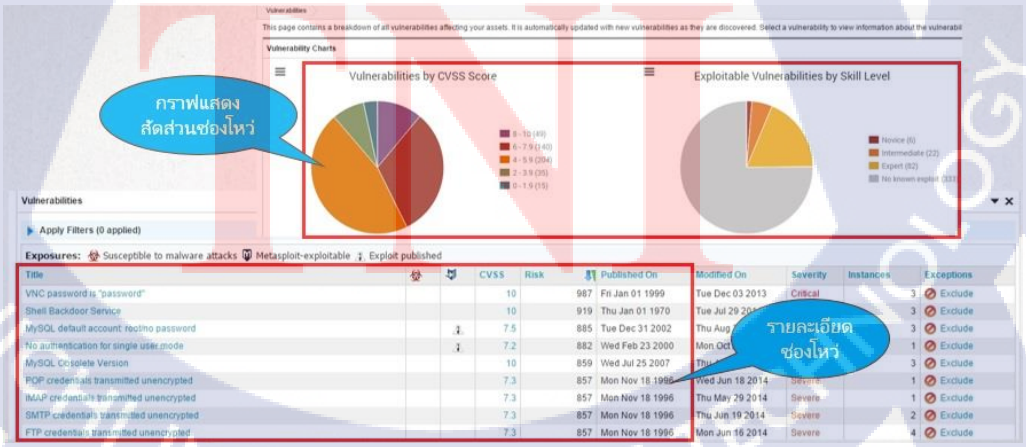
ภาพที่ 4.10 หน้าจอกรอกรายละเอียดการค้นหาช่องโหว่ Nexpose (ต่อ)



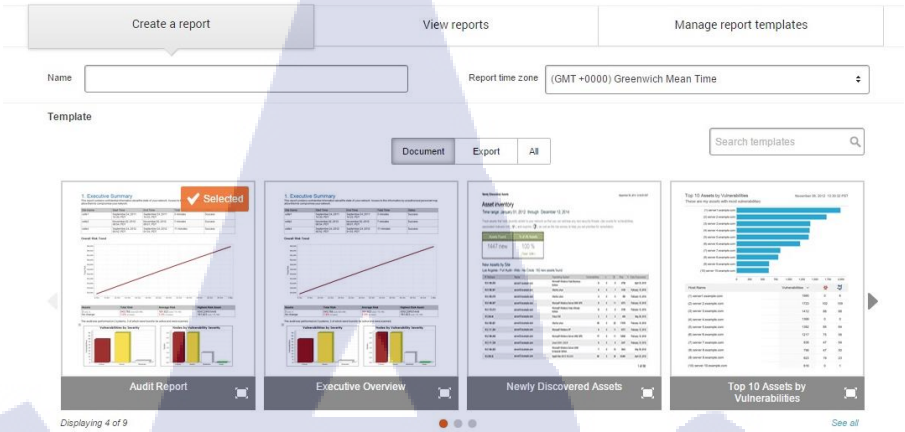
ภาพที่ 4.11 หน้าจอเลือกรูปแบบของการค้นหาช่องโหว่ Nexpose



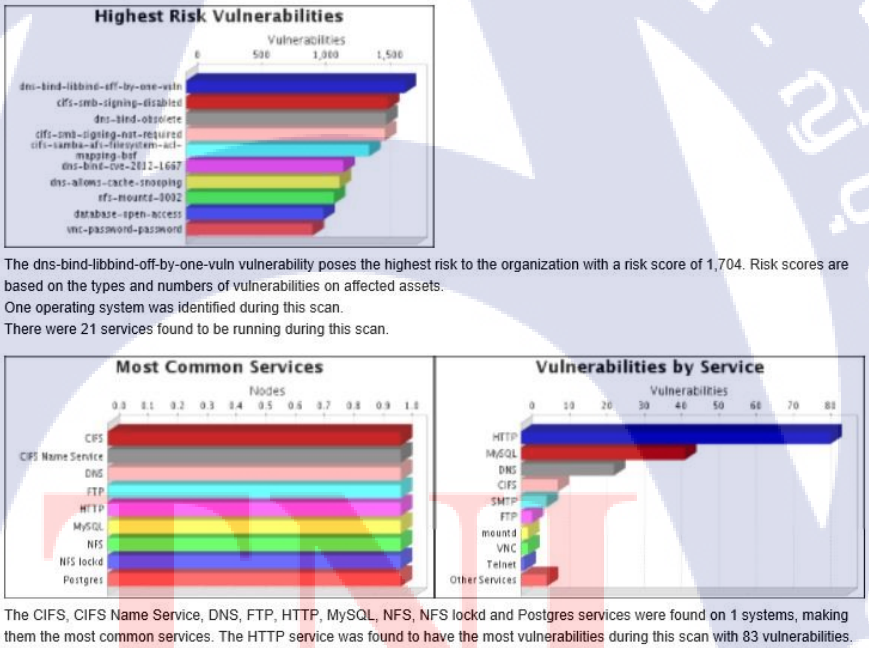
ภาพที่ 4.12 หน้าจอขณะกำลังสแกนค้นหาช่องโหว่ Nexpose



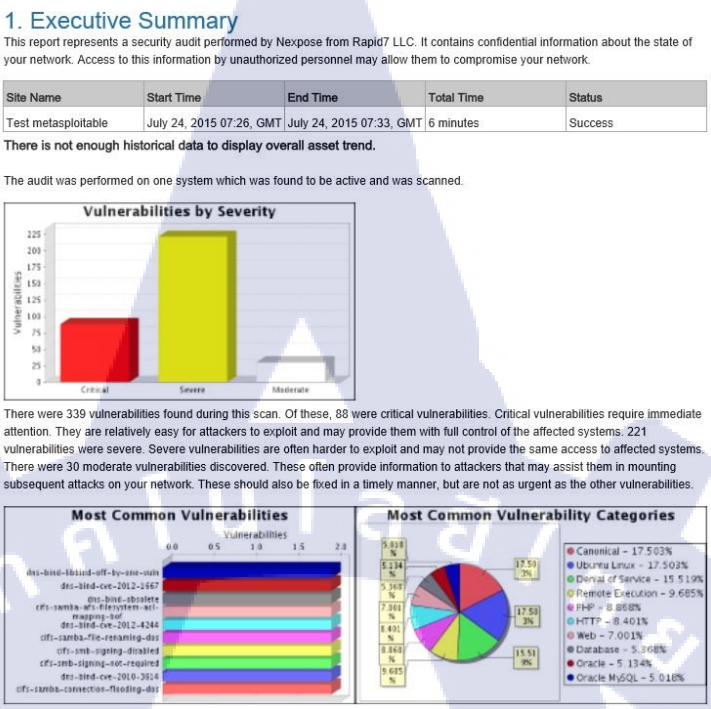
ภาพที่ 4.13 หน้าจอขณะกำลังสแกนค้นหาช่องโหว่ Nexpose (ต่อ)



ภาพที่ 4.14 หน้าจอเลือกรูปแบบการออกรายงาน Nexpose



ภาพที่ 4.15 หน้าจอรายงานการค้นหาช่องโหว่ Nexpose



1. Executive Summary

This report represents a security audit performed by Nexpose from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

Site Name	Start Time	End Time	Total Time	Status
Test metasploitable	July 24, 2015 07:26, GMT	July 24, 2015 07:33, GMT	6 minutes	Success

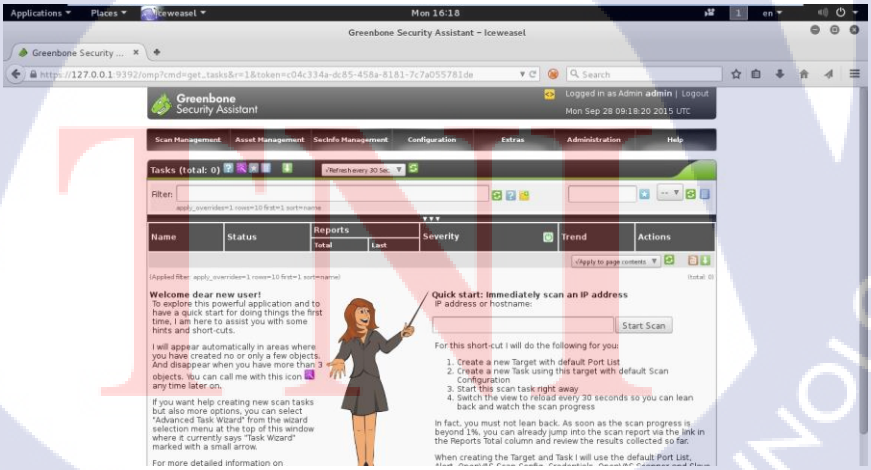
There is not enough historical data to display overall asset trend.

The audit was performed on one system which was found to be active and was scanned.

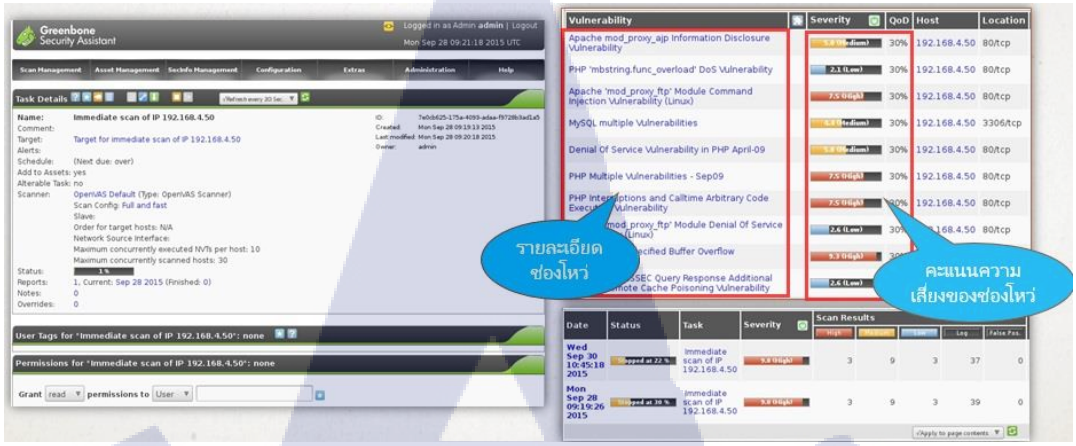
There were 339 vulnerabilities found during this scan. Of these, 88 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 221 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 30 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities.

ภาพที่ 4.16 หน้าจอรายงานการค้นหาช่องโหว่ Nexpose (ต่อ)

4.1.4 ผลการดำเนินงานทดสอบแอปพลิเคชัน OpenVAS



ภาพที่ 4.17 หน้าจอกรอกรายละเอียดการค้นหาช่องโหว่ OpenVAS



ภาพที่ 4.18 หน้าจอระหว่างการค้นหาช่องโหว่ OpenVAS

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.4.50	3	9	3	39	0
Total: 1	3	9	3	39	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.

This report contains all 54 results selected by the filtering described above. Before filtering there were 96 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.4.50	SMB	Success	Protocol SMB, Port 445, User

2 Results per Host

2.1 192.168.4.50

ภาพที่ 4.19 หน้าจอรายงานการค้นหาช่องโหว่ OpenVAS

4.2 ผลการณ์วิเคราะห์ข้อมูล

จากการปฏิบัติงานตั้งแต่เดือนมิถุนายน ถึงเดือนตุลาคม เป็นระยะเวลา 4 เดือน หรือ 18 สัปดาห์ ประสบความสำเร็จในระดับที่ดี เนื่องจากได้รับประสบการณ์ในการทำงานจริง และความรู้ต่างๆ ทั้งด้านการทำงาน จากการปฏิบัติงานตลอดระยะเวลา 18 สัปดาห์ ได้ทำการศึกษาและทดลองใช้งานแอปพลิเคชันค้นหาช่องโหว่ ครอบคลุมช่องโหว่ตาม OWASP Top 10, CVE

4.2.1 ผลการวิเคราะห์เปรียบเทียบ

ตาราง 4.1 ตารางเปรียบเทียบผลิตภัณฑ์

ผลิตภัณฑ์	คุณสมบัติ	การออกรายงาน	ราคา
OpenVAS	- ค้นหา Foot printing เช่น IP Address , ระบบปฏิบัติการ - ค้นหา Service เช่น Mail, Web , Proxy หรือ FTP - ค้นหา Port - ค้นหาช่องโหว่โดยอ้างอิงจากมาตรฐาน-สากล เช่น CVE (Common Vulnerabilities and Exposures) - บ่งบอกถึงระดับความเสี่ยงของแต่ละอุปกรณ์ - บอกวิธีป้องกันหรือแก้ไขช่องโหว่ของความเสี่ยงที่เกิดขึ้น - รองกันการแสกนหลายระบบพร้อมกัน - แสกนตามเวลาที่กำหนดได้	- แสดงรายงานสรุปในรูปแบบตาราง - แสดงชื่อช่องโหว่มาตรฐาน - แสดงจำนวนของ False Positive - แหล่งอ้างอิงช่องโหว่ CVE, CVSS, BID, OSVDB, OWASP	ฟรี

ตาราง 4.2 ตารางเปรียบเทียบผลิตภัณฑ์ (ต่อ)

ผลิตภัณฑ์	คุณสมบัติ	การออกรายงาน	ราคา
Nessus	- ค้นหา Foot printing เช่น IP Address , ระบบปฏิบัติการ - ค้นหา Service เช่น Mail, Web , Proxy, FTP - ค้นหา Port - ค้นหาช่องโหว่โดยอ้างอิงจากมาตรฐาน-สากล เช่น CVE (Common Vulnerabilities and Exposures) - บ่งบอกถึงระดับความเสี่ยงของแต่ละอุปกรณ์ - บอกวิธีป้องกันหรือแก้ไขช่องโหว่ของความเสี่ยงที่เกิดขึ้น	- แสดงรายงานสรุปตามรูปแบบของPlugins ของแอปพลิเคชัน - แสดงชื่อช่องโหว่มาตรฐาน - แจ้งช่องโหว่ที่เป็น False Positive - แหล่งอ้างอิงช่องโหว่ CVE, CWE, CVSS, BID, CERT, OSVDB, OWASP	$2,000 / 1 ปี
Nexpose	- ค้นหา Foot printing เช่น IP Address , ระบบปฏิบัติการ - ค้นหา Service เช่น Mail, Web, Proxy, FTP - ค้นหา Port - ค้นหาช่องโหว่โดยอ้างอิงจากมาตรฐาน-สากล เช่น CVE (Common Vulnerabilities and Exposures) - บ่งบอกถึงระดับความเสี่ยงของแต่ละอุปกรณ์ - บอกวิธีป้องกันหรือแก้ไขช่องโหว่ของความเสี่ยงที่เกิดขึ้น - ทดสอบตามมาตรฐานของ PCI DSS (มาตรฐานที่มีความจำเป็นต่อสถาบันการเงิน)	- แสดงรายงานสรุปในรูปแบบแผนภูมิกราฟแท่ง, กราฟวงกลม - แสดงชื่อช่องโหว่มาตรฐาน - แสดงโค้ดที่ช่องโหว่ - แจ้งช่องโหว่ที่เป็น False Positive - เลือกรูปแบบของรายงานได้หลายรูปแบบ - แหล่งอ้างอิงช่องโหว่ Apple, CVE, BID, CERT, CWE, OVAL, REDHAT, OSVDB, OWASP, XF, Debian	$2,000 / 1 ปี

4.3 วิเคราะห์และวิจารณ์ข้อมูลโดยเปรียบเทียบผลที่ได้รับกับวัตถุประสงค์และจุดมุ่งหมายในการปฏิบัติงานหรือการจัดทำโครงการ

จากการปฏิบัติงานสหกิจศึกษาในครั้งนี้ ได้มีโอกาสเข้าร่วมเป็นส่วนหนึ่งในการออกปฏิบัติงานนอกสถานที่ในส่วนของบริการ DMSS การออกแบบและพัฒนาเว็บแอปพลิเคชันเพื่อใช้ในการสืบค้นและจัดเก็บฐานข้อมูล ออกแบบโครงสร้างระบบเครือข่ายผ่านในบริษัท ได้ประสบการณ์ในการทำงานจริงในบริษัทที่ไม่สามารถเรียนรู้ได้จากการเรียนในห้องเรียน สามารถปรับตัวให้ทำงานกับผู้อื่นได้ และสามารถรับผิดชอบงานที่ได้รับมอบหมายเสร็จได้ตามกำหนดที่วางแผนไว้ด้วยดี

ตาราง 4.3 ตารางเปรียบเทียบผลที่ได้รับกับวัตถุประสงค์ในการปฏิบัติงาน

วัตถุประสงค์	ผลที่ได้รับ
เพื่อศึกษาและพัฒนาความรู้การทำงานจากสถานปฏิบัติงานจริง	ได้รับประสบการณ์จากการทำงานในสถานประกอบการจริง สามารถทำไปใช้ในการทำงานจริงต่อไปในภายภาคหน้าได้
เพื่อศึกษากระบวนการวิเคราะห์และประเมินช่องโหว่ของระบบสารสนเทศ	สามารถนำผลที่ได้มาประเมินความเสี่ยงที่เกิดขึ้นบนระบบ
เพื่อทดสอบการทำงานของ Vulnerability Tools ต่างๆ	ทำให้รู้ถึงกระบวนการทำงานของเครื่องมือต่างๆของผลิตภัณฑ์
เพื่อเปรียบเทียบคุณสมบัติและผลลัพธ์ของ Vulnerability Tools ต่างๆ	ทำให้ได้เห็นถึงความแตกต่างของผลิตภัณฑ์ต่างๆได้อย่างชัดเจน
เพื่อนำผลลัพธ์ที่ได้จากการทำงาน นำไปเป็นข้อมูลส่วนหนึ่งในที่จะช่วยให้ลูกค้าของบริษัทสามารถตัดสินใจซื้อในผลิตภัณฑ์และบริการของบริษัท	จากรายงานที่ได้ ทำให้ลูกค้ามีแรงจูงใจตกลงที่จะซื้อผลิตภัณฑ์

จากวัตถุประสงค์ข้างต้น โครงงานการทดสอบเปรียบเทียบแอปพลิเคชันค้นหาช่องโหว่ 3 ผลิตภัณฑ์ (OpenVAS, Nessus, Nexpose) สามารถตอบสนองความต้องการของลูกค้าได้เป็นอย่างดี

บทที่ 5

บทสรุปและข้อเสนอแนะ

5.1 สรุปการดำเนินงาน

จากการปฏิบัติงานตั้งแต่เดือนมิถุนายน ถึงเดือนตุลาคม เป็นระยะเวลา 4 เดือน หรือ 18 สัปดาห์ ประสบความสำเร็จเป็นอย่างมาก เนื่องจากได้รับประสบการณ์ในการทำงานจริง และความรู้ต่างๆ ทั้งด้านการทำงาน ด้านการออกแบบระบบโครงสร้างเครือข่ายภายในบริษัท การออกแบบและสร้างเว็บแอพพลิเคชั่นที่ใช้งานสำหรับฐานข้อมูลบนระบบเครือข่ายภายใน ซึ่งสามารถนำไปพัฒนาให้สามารถใช้บนอินเตอร์เน็ตภายนอกได้ การเรียนรู้การทำงานอย่างเป็นระบบ การกำหนดเวลาในการทำงานแต่ละขั้นตอน การปรับตัวในการทำงานร่วมกับผู้อื่น การทำงานเป็นทีม การเรียนรู้การทำงานและการศึกษาค้นคว้าด้วยตนเอง และการแก้ไขปัญหาต่างๆที่เกิดขึ้น

5.2 แนวทางการแก้ไขปัญหา

การทำงานในโครงงาน ทดสอบเปรียบเทียบคุณสมบัติของผลิตภัณฑ์ค้นหาช่องโหว่ นั้นได้พบปัญหาในหลายๆรูปแบบ ไม่ว่าจะเป็นการรวบรวมข้อมูลช่องโหว่ต่างๆ ความไม่พร้อมของอุปกรณ์ที่จะใช้ในการทดสอบ ข้อมูลผลิตภัณฑ์ต่างๆที่จำเป็นต้องใช้ในการทดสอบ การใช้งานผลิตภัณฑ์ต่างๆ ซึ่งรุ่นพี่ได้ช่วยสอนและแนะนำให้มีความเข้าใจกับการใช้งานจริง หลังจากนั้นก็ไปศึกษาค้นคว้าด้วยตนเอง เมื่อไม่เข้าใจส่วนไหนก็สามารถไปขอคำแนะนำจากพนักงานที่ปรึกษาได้

5.3 ข้อเสนอแนะจากการดำเนินงาน

1. จากการดำเนินงานที่ผ่านมาทำให้ได้เรียนรู้การทำงานจริง การปรับตัวให้สามารถทำงานร่วมกับผู้อื่นได้ รวมถึงการทำงานร่วมกันเป็นทีมภายในองค์กร เมื่อเกิดปัญหาในการทำงานต้องหาทางแก้ไขและปรึกษากับพนักงานที่ปรึกษาในทันที

2. การทำงานกับผลิตภัณฑ์ใหม่ๆที่ไม่เคยศึกษามาก่อนเป็นการเรียนรู้ที่ดีจึงควรที่จะมีการเรียนการสอนเกี่ยวกับความรู้หรือแอปพลิเคชันที่ใช้ให้มีพื้นฐานที่เพียงพอ ก่อนจะเริ่มดำเนินงาน

3. หลังจากที่ได้ทำงานจริง การทำงานนั้นต้องมีการวางแผนอย่างเป็นระบบเป็นขั้นเป็นตอนเพื่อให้การทำงานนั้นไม่ยุ่งยากซับซ้อนและเข้าใจง่าย เมื่อเกิดความผิดพลาดก็จะสามารถแก้ไขปัญหาได้อย่างรวดเร็วและถูกต้อง

4. เนื่องจากได้รับโอกาสให้มีส่วนร่วมในการทดสอบเปรียบเทียบคุณสมบัติของผลิตภัณฑ์ค้นหาช่องโหว่ ที่ต้องนำมาใช้งานจริง จึงมีความจำเป็นจะต้องวางแผนให้สามารถพัฒนาได้ทันในระยะเวลาที่กำหนด

5.นักศึกษาที่ต้องการไปสหกิจศึกษาควรเตรียมความพร้อมในด้านที่จะไปทำงานสถานประกอบการแห่งนั้น ๆ ควรหาจุดเด่นของตนเองว่าถนัดอะไร เพื่อจะได้รู้ว่าเราเหมาะสมกับงานประเภทใด และเพื่อเป็นแนวทางในการลงวิชาเลือกสาขาต่อไป

เอกสารอ้างอิง

1. Matteo Meucci and Andrew Muller, **OWASP Testing Guide v4** [Online], Available : https://www.owasp.org/images/5/52/OWASP_Testing_Guide_v4.pdf [2015, August 30]
2. Council on Cyber Security, **The Critical Security Controls for Effective Cyber Defense** [Online], Available : https://www.sans.org/media/critical-security-controls/CSC-5.pdf [2015, September 5]
3. พุทธิมงคล บำรุงพิพัฒนพร, **Metasploit Training** [Offline]
4. นนทวรรธนะ สาระมาน, **การทำ Penetration Test แบบมืออาชีพ ตอนที่ 1** [Online], Available : http://nontawattalk.blogspot.com/2009/10/penetration-test-1.html [2015, September 7]
5. นนทวรรธนะ สาระมาน, **การทำ Penetration Test แบบมืออาชีพ ตอนที่ 2** [Online], Available : http://nontawattalk.blogspot.com/2009/10/penetration-test-2.html [2015, September 7]
6. Tenable Network Security, Inc., **Nessus Documentation** [Online], Available : http://tenable.com/documentation/nessus/content/docs.pdf [2015, September 15]
7. Amtsgericht Osnabrück, **OpenVAS Documentation** [Online], Available : http://docs.greenbone.net/index.html#user_documentation [2015, Septmber 16]
8. Mglinski**, Nexpose User's Guide Product version: 6.0 (English)** [Online], Avilable : https://community.rapid7.com/docs/DOC-1387 [2015, September 18]
9. University of Virginia, **How to read a Nessus Report** [Online], Available : http://its.virginia.edu/network/nessusreport.html [2015, September 20]

ประวัติผู้จัดทำโครงงาน

ชื่อ – สกุล นายนิติพัฒน์ อานน้อย

วัน เดือน ปีเกิด 31 ธันวาคม 2536

ประวัติการศึกษา

ระดับประถมศึกษา ประถมศึกษาตอนปลาย พ.ศ. 2548
โรงเรียนธัญญสิทธิศิลป์

ระดับมัธยมศึกษา มัธยมศึกษาตอนปลาย พ.ศ. 2554
โรงเรียนธัญรัตน์

ระดับอุดมศึกษา คณะเทคโนโลยีสารสนเทศ สาขาเทคโนโลยีมัลติมีเดีย พ.ศ. 2558
สถาบันเทคโนโลยีไทย – ญี่ปุ่น

ทุนการศึกษา กองทุนกู้ยืมเพื่อการศึกษา (กยศ.)

ประวัติการฝึกอบรม 1 รู้เท่าทันมารยาทและกฎหมายการใช้ Social Network ณ มหาวิทยาลัยเกษมบัณฑิต

2 ICSS:Skill standard for IT Professionals Information Technology Promotion Agency ณ สถาบันเทคโนโลยีไทย-ญี่ปุ่น

3 CITEC The Hacker Secret 2011 CITEC ณ สถาบันเทคโนโลยีไทย-ญี่ปุ่น

ผลงานที่ได้รับการตีพิมพ์ - ไม่มี -