

การพัฒนาและการปรับปรุงระบบ Clientless Remote Desktop Gateway และ VNC สำหรับระบบ Cyber RANGE DEVELOPMENT AND IMPLEMENTATION CLIENTLESS REMOTE DESKTOP GATEWAY SYSTEM AND VNC SERVICE FOR CYBER RANGE

SYSTEM

นายศุภณัฐ ไวยานิกรณ์

(

โครงงานสหกิจศึกษานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร ปริญญาวิทยาศาสตรบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยี ไทย-ญี่ปุ่น

W.A. 2560

การพัฒนาและการปรับปรุงระบบ Clientless Remote Desktop Gateway และ VNC สำหรับระบบ Cyber RANGE DEVELOPMENT AND IMPLEMENTATION CLIENTLESS REMOTE DESKTOP GATEWAY SYSTEM AND VNC SERVICE FOR CYBER RANGE SYSTEM

นายศุภณัฐ ไวยานิกรณ์

โครงงานสหกิจศึกษานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร วิทยาศาสตรบัณฑิต สาขาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีไทย - ญี่ปุ่น ปีการศึกษา 2560

คณะกรรมการสอบ

.....ประธานกรรมการสอบ

(ผศ<mark>. ตรีรัตน เมตต์กา</mark>รุณ์จิ<mark>ต)</mark>

.....<mark>.</mark> กรรม<mark>การส</mark>อบ

(อ. สลิลา <mark>ชีวกิด</mark>าการ)

......อาจาร<mark>ย์ที่ป</mark>รึกษา

(อ. ดร. ปร<mark>าณิส</mark>า อิศรเสนา)

.....ประธานสหกิจศึกษาสาขาวิชา

(อ. อมรพันธ์ ชมกลิ่น)

STITUTE (ลิขสิทธิ์ของสถาบันเทคโนโลยีไทย – ญี่ปุ่น

สื่อโดรงงาน การพัฒนาและการปรับปรุงระบบ Clientless Remote Desktop Gateway และ VNC สำหรับระบบ Cyber RANGE DEVELOPMENT AND IMPLEMENTATION CLIENTLESS REMOTE DESKTOP GATEWAY SYSTEM AND VNC SERVICE FOR CYBER RANGE SYSTEM นายศุภณัฐ ไวยานิกรณ์ ผู้เขียน คณะวิหา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ อาจารย์ที่ปรึกษา ดร ปราณิสา อิศรเสนา พนักงานที่ปรึกษา นายใกรสร โพธิ์แฉล้ม ชื่อบรินัท าเริ่ษัท ใหมาอร์ตรอบ จำกัด ประเภทธุรกิจ/สินค้า บริการแก้ไขปัญหาภัยคุกคามและความเสี่ยงทาง IT

บทสรุป

ในปัจจุบัน เทคโนโลยีสารสนเทสมีความก้าวหน้าอย่างมากทั้งในค้านการเชื่อมต่อ ระยะไกลระหว่างกันด้วยบริการ Remote Desktop Service ที่มีความก้าวหน้าขึ้นในส่วนของ ความเร็วของการประมวลผลและการแสดงผลและเทคโนโลยีที่นำมาใช้ร่วมด้วยนั้นสามารถปรับตัว ตามสภาพแวคล้อมของระบบได้ซึ่งส่งผลให้การเชื่อมต่อระยะไกลนั้นมีสภาพคล่องตัวมากยิ่งขึ้น โครงการนี้จึงได้พัฒนาและปรับปรุงระบบ Clientless Remote Desktop Gateway และ VNC สำหรับ ระบบ Cyber RANGE ที่เป็นระบบ CTF ในรูปแบบของ Web Application ที่เป็นระบบ production ที่ถูกพัฒนาและปรับปรุงภายในบริษัทมาอย่างยาวนาน โดยในการคำเนินงานได้มีการสร้างและ พัฒนาระบบ Clientless Remote Desktop Gateway ที่มีรูปแบบตอบสนองกวามต้องการอย่างชัดเจน รวมถึงนำ VNC ที่เป็นบริการอย่างหนึ่งจัดอยู่ในบริการของ Remote Desktop Service มาใช้ร่วมงาน กับระบบ Clientless Remote Desktop Gateway

หลังจากคำเนินงานนั้นผลลัพธ์ของการปฏิบัติงานนั้นสามารถแก้ไขปัญหาที่มีอยู่ในระบบ Cyber RANGE ของบริษัทให้สามารถทำงานได้อย่างถูกต้อง รวมถึงการแสดงผลและความเร็ว เพิ่มขึ้น ส่งผลให้การพัฒนาและปรับปรุงระบบ Cyber RANGE มีความคล่องตัวมากยิ่งขึ้น **Project's name**

Writer

Faculty

Faculty Advisor Job Supervisor

Company's name

Business Type / Product

DEVELOPMENT AND IMPLEMENTATION CLIENTLESS REMOTE DESKTOP GATEWAY SYSTEM AND VNC SERVICE FOR CYBER RANGE SYSTEM Mr.Supanut Vaiyanikorn Information Technology, Information Technology Dr. Pranisa Isarasena Mr.Kaisorn Pochalam Cybertron Co., Ltd.

Summary

Currently, the technology has made great strides in terms of remote connectivity. With Remote Desktop Service, the advances in processing and displaying speed and the technologies that are used together. It can adapt to the environment of the system, which results in a more streamlined remote connection. Development and Implementation Clientless Remote Desktop Gateway System and VNC Service for Cyber RANGE system as CTF web-based characteristics which is the production system has been developed and improved in the company for a long time. In operation, the Clientless Remote Desktop Gateway has been created and developed to meet the needs of the customers. VNC is a service that is included in the service of Remote Desktop Service to work with Clientless. Remote Desktop Gateway

After the operation, the result of the operation is to solve the problems that exist in the company's Cyber RANGE system to work properly, including the display and speed increase. As a result, the development and improvement of the Cyber RANGE system is more agile.

กิตติกรรมประกาศ

ขอขอบคุณบริษัท ไซเบอร์ตรอน จำกัด ที่มอบโอกาสให้ข้าพเจ้าได้มาเป็นส่วนหนึ่งในการ ปฏิบัติงานซึ่งส่งผลให้ข้าพเจ้าได้รับประสบการณ์ในการทำงานจริง อีกทั้งยังได้รับองก์ความรู้ต่าง ๆ มากมายทั้งในทางด้านทฤษฎีและทางด้านปฏิบัติ เพื่อฝึกให้เรียนรู้ด้วยตนเองตลอดจนช่วยชี้แนะหนทาง ที่ถูกต้องในการแก้ไขปัญหาในสภาพแวดล้อมของการทำงาน ส่งผลให้ข้าพเจ้าสามารถปฏิบัติตนได้ อย่างเหมาะสมในบริษัท ตลอดจนให้ความอนุเกราะห์ อนุญาตให้นักศึกษาสหกิจได้เข้าร่วมกิจกรรม ต่าง ๆ อาทิ การแบ่งปันองก์ความรู้ระหว่างแผนก การฝึกสอนที่ได้รับองก์ความรู้ เป็นต้น ซึ่ง ประสบการณ์ที่ข้าพเจ้าได้รับเหล่านี้ไม่สามารถหาได้ในห้องเรียน

งองอบคุณพนักงานทุกคนที่คอยให้ความช่วยเถอะ และคำปรึกษา ตลอดจนคำสอนและ กำตักเตือนในเรื่องที่ข้าพเจ้าผิดพลาดในระยะเวลา 18 สัปดาห์ที่ผ่านมา ข้าพเจ้ารู้สึกผูกพัน และรู้สึก ปราบปลึ้มสำหรับสิ่งที่ข้าพเจ้าได้รับ รวมถึงได้เป็นส่วนหนึ่งของงานในการปฏิบัติงานที่นี่ รวมถึง อาจารย์ ปราณิสา อิศรเสนา และพนักงานที่ปรึกษานายไกรสร โพธิ์แฉล้ม ที่คอยช่วยแหละให้คำแนะนำ และให้กำปรึกษาปัญหา เกี่ยวกับโครงงานสหกิจมาโดยตลอด ทำให้ข้าพเจ้าผ่านสหกิจศึกษาลุล่วงไปได้ ด้วยดี และสุดท้ายนี้ข้าพเจ้าขอขอบคุณคณะเทคโนโลยีสารสนเทศ และสถาบันเทคโนโลยีไทย-ญี่ปุ่นที่

> ศุภณัฐ ไวยานิกรณ์ ผู้จัดทำโครงงาน





บทที่

1. บทนำ

(🐂

1.1 ชื่อและที่ตั้งของสถานประกอบการ
1.2 ลักษณะธุรกิจของสถานประกอบการ หรือการให้บริการหลักขององค์กร
1.3 รูปแบบการจัดองค์กรและการบริหารองค์กร
1.4 ตำแหน่งและหน้าทึ่งานที่นักศึกษาใด้รับมอบหมาย
1.5 พนักงานที่ปรึกษา และ ตำแหน่งของพนักงานที่ปรึกษา
1.6 ระขะเวลาที่ปฏิบัติงาน
1.7 ที่มาและความสำคัญของปัญหา
1.8 วัตถุประสงค์หรือจุดมุ่งหมายของโครงงาน
1.9 ผลที่คาคว่าจะใด้รับจากการปฏิบัติงานหรือโครงงานที่ได้รับมอบหมาย

หน้า

ก

າເ

ค

٩

Ա

ល្អ

1

1

2

3

3

4

4

4

4

5

1.10 นิยามศัพท์เฉพาะ	5
2. ทฤษฎีและเทคโนโลยีที่ใช้ในการปฏิบัติงาน	7
2.1 ทฤษฎีที่ใช้ในการปฏิบัติงาน	8
2.1.1 ระบบเสมือน	8
2.11 รูปแบบของระบบเสมือน	9
2.12 ประโยชน์ของระบบเสมือน	10
2.1.2 ภาษา JAVA	11
2.1.2.1 รูปแบบพัฒนาโปรแกรมด้วยภาษา JAVA	11
2.1.2.2 ข้อคีของภาษา JAVA	11
2.1.3 พร็อกซีเซิร์ฟเวอร์ย้อนกลับ (Reverse Proxy)	12
2.1.4 ภาษา SQL	13
2.1.5 ภาษายูนิกซ์ (Unix System)	14
2.1.5.1 ลักษณะการทำงานของยูนิกซ์	15
2.1.5.2 <mark>การใช้งานยูนิกซ์</mark>	15
2.1.6 เทคโนโลยี VNC	15
2.1.6.1 การท <mark>ำงาน</mark> ของเทคโนโลยี VNC	16
2.1.6.2 ประโยชน์ของเทคโนโลยี VNC	17
2.2 เทคโนโลยีที่ใช้ในการปฏิบัติงาน	17
2.2.1 โปรแกรม VMware Workstation	17

2.2.2 โปรแกรม VMware ESXi	19
2.2.3 โปรแกรม VMware vSphere	20
2.2.4 ระบบปฏิบัติการ Ubuntu	21
2.2.4.1 ประเภทของระบบปฏิบัติการ Ubuntu	22
2.2.5 ระบบปฏิบัติการ Kali Linux 2	23
2.2.6 โปรแกรม Apache Tomcat	23
2.2.7 โปรแกรม MySQL	24
3. แผนงานการปฏิบัติงานและขั้นตอนการดำเนินงาน	27
3.1 แผนงานการปฏิบัติงาน	27
3.2 รายละเอียด โครงงาน	29
3.2.1 รายละเอียด VM ระบบ Clientless Remote Desktop Gateway บน	29
ระบบปฏิบัติการ Ubuntu 14.04 (VM เกรื่องที่ 1)	
3.2.1.1 รายละเอียดการทำงานของส่วนประกอบ Guacamole-Server	30
3.2.1.2 รายละเอียดการทำงานของส่วนประกอบ Guacamole-Client	30
3.2.2 รายละเอียด VM บริการ VNC บนระบบปฏิบัติการ Kali Linux 2	30
(VM เครื่องที่ 2)	
3.2.3 รายละเอียดแ <mark>ละก</mark> ารทำงานขอ <mark>ง</mark> ระบบ Cyber RANGE	31
3.3 ขั้นตอนการดำเนินงานที่นักศึกษาปฏิบัติงาน	31
3.3.1 ขั้นตอนการดำเนิน โครงการ	32
NSTITUTE OF THE	

4. สรุปผลการดำเนินงาน การวิเคราะห์และสรุปผลต่างๆ	65
4.1 ขั้นตอนและผลการคำเนินงาน	65
4.1.1 ผลของการทำโครงงาน	65
4.1.1.1 ระบบ Clientless Remote Desktop Gateway (VM เครื่องที่ 1)	65
4.1.1.2 ระบบปฏิบัติการ Kali Linux 2 (VM เครื่องที่ 2)	68
4.2 วิเคราะห์และวิจารณ์ข้อมูลเปรียบเทียบผลที่ได้รับกับวัตถุประสงค์และจุด มุ่งหมายในการปฏิบัติงานหรือการจัดทำโครงงาน	71
5. บทสรุปและข้อเสนอแนะ	72
5.1 สรุปผลการดำเนินงาน	72
5.2 แนวทางการแก้ไขปัญหา	73
5.3 ข้อเสนอแนะจากการคำเนินงาน	C 73
เอกสารอ้างอิง	74
ประวัติผู้จัดทำโครงงาน	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
VSTITUTE OF TECHT	

¥

รายการตาราง

ตาราง	หน้า
3.1 แสดงการปฏิบัติงานดำเนินงานโครงการตลอดทั้ง 18 สัปดาห์	27
3.1 แสดงการปฏิบัติงานดำเนินงานโครงการตลอดทั้ง 18 สัปดาห์ (ต่อ)	28
3.2 แสดงรายชื่อบริการของ VNC ที่คาดว่ามีแนวโน้มสามารถทำงานร่วมกับระบบ	35
3.3 แสดงรายการโปรแกรมและ Libraries ต่างๆที่จำเป็นสำหรับในการลงชุดโปรแกรม	43
Apache Guacamole 0.9.12-incubating	
3.3 แสดงรายการโปรแกรมและ Libraries ต่างๆที่จำเป็นสำหรับในการลงชุดโปรแกรม	44
Apache Guacamole 0.9.12-incubating (ต่อ)	
3.4 แสดงให้เห็นรายการการ download package ชุดโปรแกรม Apache Guacamole 0.9.12-	46
incubating	
3.5 แสดงรายการเตรียมความพร้อมของ environment สำหรับการติดตั้ง Apache Guacamole 0.9.12-incubating ภายในระบบปฏิบัติการ Ubuntu Server 14.04	4 8
3.6 แสดงรายการกำสั่งขั้นตอนการติดตั้ง ชุดโปรแกรม Apache Guacamole 0.9.12- incubating	48
3.7 แสดงถึงการจัดเต <mark>รี</mark> ยม w <mark>eb a</mark> pplication <mark>สำหรับ</mark> ส่วนปร <mark>ะ</mark> กอบ Apache-Guacamole-Client	49
3.8 แสดงรายละเอียดการกำ <mark>หนด</mark> ฐานข้อมูล และ import schema ต่ <mark>าง ๆ</mark> สำหรับการ	0 50
authentication ด้วย database ร่วมกับ Apache Guacamole 0.9.12-incubating	
3.9 แสดงรายการการ configure ระบบของ directory /etc/guacamole/guacamole.properties	51
3.10 แสดงกำสั่งการ restart service ทั้งหมดที่ใช้ในระบบ Apache Guacamole 0.9.12-	52
incubating	
3.11 แสดงรายการการติดตั้ง Nginx	54

Ŭ

3.12 แสดงรายการ การทำ testing tun	ing ของโปรแกรม 1	Vginx	56
4.1 แสดงรายชื่อของบริการต่าง ๆ ขอ	ง VNC ที่ใช้ในการ	ทคสอบร่วมกับระบบ	70
4.1 แสดงรายชื่อของบริการต่าง ๆ ขอ	ง VNC ที่ใช้ในการ	ทคสอบร่วมกับระบบ (ต่อ)	71



รายการภาพประกอบ

	ภาพ	หน้า	
	1.1 สัญลักษณ์ของบริษัท	1	
	1.2 แผนที่แสดงตำแหน่งของบริษัท	1	
	1.3 แผนผังรูปแบบการจัดและการบริหารองก์กร	3	
	2.1 องค์ประกอบของระบบ Virtualization ภายในทรัพยากร 1 เครื่อง	8	
	2.2 Logo ของบริการ VNC ที่มีชื่อว่า RealVNC	15	
	2.3 Diagram การทำงานของ VNC	17	
	2.4 Logo ของโปรแกรม VMware Workstation	17	
	2.5 ตัวอย่างหน้าต่างขณะใช้งานของโปรแกรม VMware Workstation 12 PRO	19	
	2.6 โครงสร้างของ VMware ESXi	20	
	2.7 Logo ของโปรแกรม VMware vSphere	20	
	2.8 Logo ของระบบปฏิบัติการ Ubuntu	22	
	2.9 Logo ของระบบปฏิบัติการ Kali Linux	23	
	2.10 Logo VON Apache Tomcat	24	
5	2.11 Logo ของโปรแกรม MySQL	26	
	3.1 หน้าจอการจำลอง ระบ <mark>บปฏิ</mark> บัติการ Kal <mark>i</mark> Linux ที่ใช้ tight VNC แบบ XFCE	34	
	3.2 Diagram ของ Reverse Proxy ที่ออกแบบ	36	
	3.3 การกำหนครายละเอียด Virtual Hardware สำหรับระบบปฏิบัติการ Ubuntu Server 14.04	38	
	3.4 การติดตั้งระบบปฏิบัติการ Ubuntu 14.04 (1)	39	

	3.5 การติดตั้งระบบปฏิบัติการ Ubuntu 14.04 (2)	39
	3.6 การติดตั้งระบบปฏิบัติการ Ubuntu 14.04 (3)	40
	3.7 การติดตั้งระบบปฏิบัติการ Ubuntu 14.04 (4)	41
	3.8 การติดตั้งระบบปฏิบัติการ Ubuntu 14.04 (5)	41
	3.9 การติดตั้งระบบปฏิบัติการ Ubuntu 14.04 (6)	42
	3.10 แสดงให้เห็นการติดตั้งโปรแกรมและ Libraries ในก่อนติดตั้งชุดโปรแกรม	45
	3.11 การแสดงรายละเอียด network adaptor ของ VM เกรื่องที่ 1	52
	3.12 แสดงการเข้าระบบ Apache Guacamole 0.9.12-incubatin ผ่าน Firefox Browser	53
	3.13 แสดงรายละเอียด Virtual Hardware ของระบบปฏิบัติการ Kali Linux 2	57
	3.14 การติดตั้งระบบปฏิบัติการ Kali Linux 2 (1)	57
	3.15 การติดตั้งระบบปฏิบัติการ Kali Linux 2 (2)	58
	3.16 การติดตั้งระบบปฏิบัติการ Kali Linux 2 (3)	58
	3.17 การติดตั้งระบบปฏิบัติการ Kali Linux 2 (4)	59
	3.18 การติดตั้งระบบปฏิบัติการ Kali Linux 2 (5)	59
	3.19 หน้า Login หลั <mark>งจ</mark> าก R <mark>estar</mark> t บนระบบปฏิบัติการ Kali Linux	60
	3.20 หน้าจอ desktop ของร <mark>ะบบ</mark> ปฏิบัติการ Kali Linux 2	60
Ż	3.21 หน้าเว็บ download Real VNC Connect 6.2	61
	3.22 การติดตั้ง Real VNC Connect 6.2 ผ่าน Command Line	62
	3.23 หน้าจอโปรแกรม Real VNC Connect 6.2	63
	4.1 แสดงระบบ Clientless Remote Desktop Gateway ในส่วนของ User Access Control (1)	66

Ŋ

4.2 แสดงระบบ Clientless Remote Desktop Gateway ในส่วนของ User Access Control (2)	66
4.3 แสดงระบบ Clientless Remote Desktop Gateway ในส่วนของ User Access Control (3)	67
4.4 รายละเอียด function การ record vdo ของระบบ	68
4.5 หน้าจอขณะใช้งาน OWASP Mantra Browser ผ่าน Apache Guacamole ที่ remote เข้าไป	69
ยัง Kali Linux 2	

4.6 หน้าจอขณะใช้งาน Wireshark ผ่าน Apache Guacamole ที่ remote เข้าไปยัง Kali Linux 2 70

T

a

Ż



1.1 ชื่อและที่ตั้งของสถานประกอบการ



ภาพที่ 1.1 สัญลักษณ์ของบริษัท ที่มา: goo.gl/FRg22s

ชื่อ ที่ตั้ง

T

บริษัทไซเบอร์ตรอน จำกัด 93/1 อาการจีพีเอฟวิทยุ ทาวเวอร์ บี, ห้อง 805 ชั้นที่ 8 ถนนวิทยุ แขวงลุมพินี เขตปทุมวัน กรุงเทพฯ 10330



ภาพที่ 1.2 แผนที่แสดงตำหน่งของบริษัท ที่มา: https://goo.gl/36n4q1

1.2 ลักษณะธุรกิจของสถานประกอบการ หรือการให้บริการหลักขององค์กร

บริษัท ไซเบอร์ตรอน จำกัด (Cybertron Co., Ltd.) เป็นบริษัทเกิดจากการร่วมลงทุนระหว่าง บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด และ บริษัท เจนเนอรัล อิเลคทรอนิค คอมเมอร์ซ เซอร์วิสเซส จำกัด คำเนินธุรกิจทางด้าน IT Security solution service ที่มุ่งเน้นเฝ้าระวังภัยคุกคาม ทางโลกออนไลน์และสร้างความตะหนักถึงความเสี่ยงของภัยคุกคามนั้น ๆ เพื่อสร้างมาตราการการ ป้องกันความเสี่ยงที่อาจจะเกิดขึ้นในอนาคตรวมถึงสร้างระบบจำลองที่สามารถวัดผลการทดสอบ ได้เพื่อให้ผู้ที่เข้ามาใช้งานสามารถตะหนักถึงความเสี่ยงในรูปแบบต่าง ๆ เพื่อนำเข้ารู้ที่ได้ไป ประยุกต์ใช้ได้ในอนาคตเพื่อประโยชน์อันสูงสุดและมีประสิทธิภาพ

บริการ Cyber Drill เป็นบริการสร้างสถานการณ์เพื่อให้ผู้ใช้งานคุ้นเคยกับภัยคุกคามและ ฝ่ายเทคโนโลยีสารสนเทศขององค์กรสามารถตอบสนองต่อเหตุการณ์ภัยคุกคามได้อย่างเร็ว ซึ่งจะมี การจำลองสถานการณ์การโจมตีด้วยรูปแบบภัยคุกคามและเทคนิควิธีการต่าง ๆ (CYBER DRILL EXERCISE) โดยการจำลองสถานการณ์การโจมตีจะสามารถวัดผลความตระหนักด้านความมั่นคง ปลอดภัยของผู้ใช้งานและช่วยลดจำนวนปัญหาด้านความมั่นคงขององก์กรได้อย่างมีประสิทธิภาพ

บริการ Cyber W.A.R เป็นแนวคิดใหม่ที่ถูกออกแบบมาเพื่อให้สามารถพัฒนาบุคลากรด้าน ใซเบอร์ได้อย่างรวดเร็ว ด้วยระบบจำลองยุทธ์ที่เรียกว่า Cyber RANGE ที่มีคุณสมบัติพร้อมในการ ฝึ ก ทุ ก ด้ า น ดี อ OFFENSIVE, DEFENSIVE, FORENSICS, SECURITY AUDIT แ ล ะ INTELLIGENCE โดยทำงานโดยอัตโนมัติ ซึ่งจะทำให้ผู้ใช้งานสามารถจำลองโจทย์สำหรับการฝึก หรือจัดแข่งขันได้โดยง่าย พร้อมทั้งสามารถวัดผลการฝึกได้เป็นระยะ และมีระบบการให้คะแนนที่ ยึดหยุ่น สามารถปรับเปลี่ยนได้ตามความต้องการ สอดกล้องกับมาตรฐานของ NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

10

บริการ Cyber 911 เป็นแนวคิดใหม่ที่ถูกออกแบบมาเพื่อให้การเฝ้าระวังภัยคุกคามมี ประสิทธิภาพสูงสุด ซึ่งเริ่มต้นโดยการวิเคราะห์สภาพแวดล้อม ลักษณะและโครงสร้างการ ปฏิบัติงานรวมถึงรูปแบบความเสี่ยงและภัยคุกคามที่แต่ละองค์กรมีแตกต่างกัน และจัดทำแผนและ ขั้นตอนการตอบสนองต่อภัยคุกคามเพื่อให้สามารถจัดการกับภัยคุกคามได้อย่างรวดเร็วเพื่อ ตอบสนองความต้องการขององค์กรนั้น ๆ ให้ได้รับความพึงพอใจสูงสุด

NSTITUTE OF

1.3 รูปแบบการจัดองค์กรและการบริหารองค์กร



ภาพที่ 1.3 แผนผังรูปแบบการจัดองค์กรและการบริหารองค์กร

คือแผนกที่นักศึกษาประจำอยู่

IC

จากภาพที่ 1.3 เป็นการแสดงแผนผังรูปแบบการจัดและการบริหารองค์กรมีจำนวน พนักงานในแผนกที่นักศึกษาประจำอยู่ทั้งหมด 8 คน (VP Innovation and Engineering 1 คน, Assistant VP Innovation 1 คน, Security Engineering Supervisor 1 คน, Production Development Manager 1 คน, Senior Developer 2 คน, Researcher & Developer 2 คน)

1.4 ตำแหน่งและหน้าที่งานที่นักศึกษาได้รับมอบหมาย

ตำแหน่ง Developer & Researcher หน้าที่งาน พัฒนาและปรับปรุงระบบ Cyber RANGE ของบริษัท

1.5 พนักงานที่ปรึกษา และ ตำแหน่งของพนักงานที่ปรึกษา

ชื่อ นายใกรสร โพธิ์แฉล้ม

ตำแหน่ง Security Engineering Supervisor

1.6 ระยะเวลาที่ปฏิบัติงาน

29 พฤษภาคม 2560 – 29 กันยายน 2560 (รวมทั้งสิ้น 4 เคือน)

1.7 ที่มาและความสำคัญของปัญหา

ในปัจจุบันเทคโนโลยีสารสนเทศมีความก้ำวหน้ามากยิ่งขึ้นในทุก ๆ วัน โดยเฉพาะ เทคโนโลยี Remote Desktop Service ที่ถูกพัฒนาให้สามารถใช้บริการที่เรียกว่า remote desktop เพื่อที่จะสามารถเข้าถึงและใช้งานหรือควบคุมคอมพิวเตอร์เครื่องอื่นได้ จากระยะไกลผ่านสื่อกลาง เช่น เครือข่ายอินเทอร์เน็ตหรืออินทราเน็ต ได้อย่างมีประสิทธิภาพและมีความเร็วอย่างเหมาะสม สภาวะของของการเชื่อมต่อระหว่างกันในขณะนั้น

บริษัท ไซเบอร์ตรอน จำกัด ในส่วนของแผนก Cyber W.A.R นั้นได้มีการพัฒนา ปรับปรุง และแก้ไขระบบ Cyber RANGE ที่เป็น production หลักมาโดยตลอด แต่ก็ยังมีจุดบกพร่องบางอย่าง ที่ทำให้การใช้งานระบบฯ นั้นไม่สามารถใช้ได้ได้อย่างไม่เต็มประสิทธิภาพ ทำให้ทางบริษัทฯ มี กวามต้องการในการปรับปรุง และแก้ไขระบบฯ เพื่อแก้ไขปัญหาในด้านต่าง ๆ ที่เกิดขึ้นของตัว ระบบฯ เพื่อตอบสนองกวามต้องการของผู้ใช้งานให้ได้รับกวามพึงพอใจสูงสูด

1.8 วัตถุประสงค์หรือจุดมุ่งหมายของโครงงาน

เพื่อพัฒนาระบบ Cyber RANGE ให้สามารถแก้ไขปัญหาในเรื่องการแสดงผลหรือการ วัดผลได้ตรงตามความต้อ<mark>งการ</mark>ดังนี้

- เพื่อให้การremote ไปยังระบบปฏิบัติการ Kali Linux 2 สามารถเปิด Mantra browser ได้ อย่างสมบูรณ์
- เพื่อให้การremoteไปยังระบบปฏิบัติการ Kali Linux 2 สามารถเปิด โปรแกรม Wireshark ได้อย่างสมบูรณ์
- 3) เพื่อให้การremoteไปยังระบบปฏิบัติการ Kali Linux 2 มีความเร็วมากขึ้น

4) เพื่อให้ระบบ Clientless Remote Desktop สามารถวัดผลได้จาก Remote Desktop Service

1.9 ผลที่คาดว่าจะได้รับจากการปฏิบัติงานหรือโครงงานที่ได้รับมอบหมาย

- สามารถพัฒนาและปรับปรุงระบบ Cyber RANGE ที่เกิดปัญหาในแต่ละด้านให้ แสดงผลหรือสามารถแก้ไขปัญหาตรงตามความต้องการได้
- สามารถพัฒนาและปรับปรุงระบบ Cyber RANGE เพื่อที่สามารถต่อยอดการทำงาน ของแผนกได้มากยิ่งขึ้น

นโลยั

1.10 นิยามศัพท์เฉพาะ

1) VM(s)

VM(s) ย่อมาจาก Virtualization คือการจำลองเครื่องคอมพิวเตอร์เสมือนบน คอมพิวเตอร์หลักที่สามารถจำลองเครื่องคอมพิวเตอร์เสมือนได้ได้มากกว่า 1 เครื่อง ในเครื่องคอมพิวเตอร์หลัก 1 เครื่อง

2) Kali Linux 2

คือ ระบบปฏิบัติการรูปแบบนึงที่พัฒนามาจาก Linux ตะกูล Debian และนำเอา เครื่องมือ Hacking Methodology ระดับพื้นฐานมาติดตั้งเอาไว้

3) Apache Guacamole

คือ ระบบ Clientless Remote Desktop Gateway แบบ Open source ของ Apache ที เปรียบเสมือนเป็น gateway ในการเข้าถึง Remote Desktop service ต่าง ๆ ผ่านรูปแบบ web-based

4) VNC Service

ย่อมาจาก Virtual Network Computing คือ บริการ remote desktop service รูป แบบนึง ที่ทำงานคล้ายกับ RDP ปัจจุบันมีผู้ให้บริการเช่น RealVNC, TighVNC, TigerVNC เป็นต้น

5) VMware

คือชื่อของโปรแกรมประเภทการจำลองระบบเสมือน โดย VMware แบ่ง product ออกเป็นหลาย ๆ ส่วนเช่น VMware ESXi เป็นต้น 6) Infrastructure

คือโครงสร้างพื้นฐานของระบบ

7) Production Policy

้ คือข้อกำหนดหรือกฎเกณฑ์ ของ product แต่ละประเภทที่ถูกกำหนดโดยผู้บริหาร

8) Remote Desktop Service

้คือบริการในการเข้าถึงเครื่องคอมพิวเตอร์ระยะไกลมีลักษณะแบบ GUI

9) Desktop Environment

พื้นที่ desktop ต่าง ๆ โดยในระบบ Linux distro นั้นไม่ได้มี desktop ที่คงที่ เนื่องจากเป็น open source OS ทำให้จำเป็นต้องนำ Desktop Environment ชนิดต่าง ๆ มาใช้เพื่อให้สามารถใช้งานสะดวกมากยิ่ง

10) Mantra Browser

คือ browser ชนิดหนึ่ง ที่นำ engine ของ Firefox มาพัฒนาต่อโดยจะนำเกรื่องมือ Web Penetration Testing tools เพิ่มลงไป

11) load balance

คือ กระบวนการการแบ่งกระจายของการใหลเวียนของข้อมูลหรือ traffic ให้ environment มีสภาพกล่องตัวมากยิ่งขึ้น

12) environment

ความหมายที่หมายถึงในรายงานเล่มนี้หมายถึง สภาพแวคล้อมของระบบต่าง ๆ ใน แต่ละสถานการณ์ที่เกิดขึ้นซึ่งมีความแตกต่างกัน

13) CTF

คือระบบ จำลองแบบฝึกหัดเกี่ยวกับ องค์กวามรู้ทางด้าน Security โดยมีรุปแบบ การใช้งานโดยจะกำหนด ระบบที่เกิดช่องโหว่ขึ้นมาที่อางกำหนดมาในรุปแบบระบบ เสมือนหรือ VM โดยในช่องโหว่นั้นจะทำการใส่ ข้อกวามที่เรียกว่า Flag เมื่อผู้ใช้งาน มาใช้งานจะต้องหา Flag ให้พบจากช่องโหว่ชนิดต่าง ๆ เพื่อจบแบบฝึกหัด

14) Virtual Hardware

การจำลอง Hardware เสมือน เพื่อใช้ระสำหรับระบบเสมือน

15) IP address

เลขรหัสประจำคอมพิวเตอร์ที่ต่ออยู่บนเครือข่าย ซึ่งประกอบด้วยตัวเลข 4 ชุดและ มีเครื่องหมายจุดขั้นระหว่างชุด ยกตัวอย่างเช่น 192.168.1.1 เป็นต้นหรือนิยมเรียกสั้นๆ ว่า IP



บทที่ 2 ทฤษฎีและเทคโนโลยีที่ใช้ในการปฏิบัติงาน

องค์ประกอบของบทที่ 2 มีดังนี้

2.1 ทฤษฎีที่ใช้ในการปฏิบัติงาน

- 2.1.1 ระบบเสมือน
 - 2.1.1.1 รูปแบบของระบบเสมือน
 - 2.1.1.2 ประโยชน์ของระบบเสมือน
- 2.1.2 ภาษา JAVA
 - 2.1.2.1 รูปแบบการพัฒนาโปรแกรมด้วยภาษา JAVA
 - 2.1.2.2 ข้อดีของภาษา JAVA
- 2.1.3 พร๊อกซีเซิร์ฟเวอร์ย้อนกลับ (Reverse Proxy)
- 2.1.4 ภาษา SQL
- 2.1.5 ระบบยูนิกซ์ (Unix System)
 - 2.1.5.1 ลักษณะการทำงานของยูนิกซ์
 - 2.1.5.2 การใช้งานยูนิกซ์
- 2.1.6 เทคโนโลยี VNC

10

- 2.1.6.1 การทำงานของเทคโนโลยี VNC
- 2.1.6.2 ประโยชน์ของเทคโนโลยี VNC
- 2.2 เทคโนโลยีที่ใช้ในการปฏิบัติงาน
 - 2.2.1 โปรแกรม VMware Workstation
 - 2.2.2 โปรแ<mark>ก</mark>รม V<mark>Mwa</mark>re ES<mark>X</mark>i
 - 2.2.3 โปรแกรม V<mark>Mwa</mark>re vSphere
 - 2.2.4 ระบบปฏิบัติ<mark>การ U</mark>buntu
 - 2.2.4.1 ประ<mark>เภทข</mark>องระบบปฏิบัติการ Ubuntu
 - 2.2.5 ระบบปฏิบัติการ Kali Linux 2
 - 2.2.6 โปรแกรม Apache Tomcat
 - 2.2.7 โปรแกรม MySQL

2.1 ทฤษฎีที่ใช้ในการปฏิบัติงาน

2.1.1 ระบบเสมือน (Virtualization)



ภาพที่ 2.1 องค์ประกอบของระบบ Virtualization ภายในทรัพยากรณ์ 1 เครื่อง

Virtualization Technology [1] หากแปลความหมายตรงตัวให้เข้าใจง่ายๆ ก็คือ เทคโนโลยี ที่ช่วยให้สามารถใช้ Resource เช่น ซีพียู, หน่วยความจำ, ฮาร์คคิสก์ เป็นค้น ของคอมพิวเตอร์ 1 เครื่องหรือมากกว่านั้น เพื่อให้สามารถรันซอฟต์แวร์ หรือ application ในปริมาณมากๆ หรือรัน ระบบปฏิบัติการหลาย ๆ ตัว ให้สามารถทำงานพร้อมกันหลาย ๆ อย่างได้ ถึงแม้ว่าจะต่าง platform ก็ตาม โดยในแต่ละระบบปฏิบัติการที่รันอยู่นั้นจะไม่มีการขึ้นตรงต่อกันหรือแยกส่วนกันอย่าง ชัดเจนในส่วนของระบบปฏิบัติ แต่สามารถเชื่อมต่อถึงกันได้ในส่วนของระบบเครือข่าย ขึ้นอยู่กับ ความต้องการของผู้ใข้งาน

เมื่อกล่าวถึงเทคโนโลยี Virtualization Technology ซึ่งปัจจุบันเริ่มเป็นที่รู้จักกันอย่าง แพร่หลายนั้น ไม่ได้เป็นเทคโนโลยีใหม่เลย ในอดีตนั้นมีการใช้งานบนระบบขนาดใหญ่อยู่แล้ว แต่ เมื่อมีผู้นำมาใช้งานบนระบบที่มีขนาดเล็กลง ก็เริ่มมีการใช้งานอย่างแพร่หลายมากขึ้นเนื่องมาจาก รูปภาพของการใช้งานที่มีรูปแบบไม่ซับซ้อนและคล่องตัว รวมถึงหลาย ๆ บริษัทต่างพัฒนา ผลิตภัณฑ์ของตัวเองออกมาแข่งขันกันในตลาด โดยบริษัทที่มีชื่อเสียงมากก็คือ VMware Workstation อีกตัวที่พอจะรู้จักก็คือ Virtual PC ซึ่งไมโครซอฟต์ได้นำไปพัฒนาต่อจนกลายเป็น Hyper V และอีกค่ายได้แก่ Citrix ซึ่งการทำงานหลักโดยรวมของแต่ผลิตภัณฑ์ก็คือ สามารถจำลอง การทำงานของคอมพิวเตอร์ขึ้นมาหลายๆ เครื่อง โดยไม่ได้จำลองเฉพาะซีพียูเท่านั้น ทำการรัน ระบบปฏิบัติการหลายระบบได้พร้อมกัน บนเครื่องจริงๆ เพียงเกรื่องเดียว

2.1.1.1 รูปแบบของระบบเสมือน

ระบบเสมือนต่าง ๆ สามารถจำแนกประเภทออกเป็นรูปแบบต่าง ๆ ได้ดังนี้

- 1) Application Virtualization
- 2) Desktop Virtualization
- 3) Server Virtualization

Application Virtualization เป็นเทคโนโลยีที่เริ่มคิดก้นโดย Citrix Systems Inc. ซึ่งเป็นผู้นำ ตลาดค้าน Application Virtualization และเป็นผู้กิดก้น Terminal Server ให้กับ Microsoft จนเกิด เป็น Microsoft Terminal Server บน Windows Server2000, 2003 และ 2008 โดยใช้ Remote Desktop Protocol (RDP) ช่วยในการส่งหน้าจอการทำงานจากระยะไกล จาก Windows Server ไปยัง Wyse Thin Client ซึ่งทำหน้าที่เพียงรับหน้าจอ และส่งการกดปุ่มคีย์บอร์ดและเมาส์กลับไปเท่านั้น การ ประมวลผลการทำงานทำที่ Server ทั้งหมด ดังนั้น Thin Client จึงไม่ต้องการทรัพยากรมากเลย

Desktop Virtualization เป็นเทคโนโลยีที่ช่วยให้สามารถส่งหน้าจอการทำงานของ Windows XP Pro, Windows Vista ไปยังเครื่องปลายทาง สามารถทำงานเป็นแบบ Desktop ของแต่ ละคนแยกออกจากกัน หรือจะเป็น Pool ก็ได้ เช่นกำหนด Pool ไว้ 5 Desktop ใครมาก่อนก็จะเข้า Desktop แรก เข้ามาลำดับถัดไปก็ได้ Desktop ถัดไป เป็นต้น ปัจจุบันมีผู้นำตลาดค้านนี้อยู่ 2 ค่าย คือ VMware Workstation VDM ซึ่งใช้ RDP ส่วนค่าย Citrix XenDesktop ใช้ ICA Protocol ซึ่งทั้งคู่ จำเป็นต้องมี Server คือ VMware Workstation ESX หรือ Citrix XenServer ซึ่งต้องมีระบบปฏิบัติการ Windows XP หรือ Windows Vista ไว้ตามจำนวนผู้ใช้งานจริง ตามจำนวนที่ต้องใช้งาน และ มี Broker Server กลาง ให้เครื่อง Client ปลายทางเรียกเข้ามาใช้งาน เพื่อตรวจสอบผู้ใช้งานก่อน จะส่ง ให้เครื่อง Client เข้าไปใช้ Windows XP ต่อไป

Server Virtualization เป็นเทคโนโลยี Server Virtualization หรือการทำรวมศูนย์เครื่องแม่ ข่าย โดยการรวมเอา Server ที่มีอยู่ทั้งหมดเข้ามาอยู่กลายเป็น Server ขนาดใหญ่ยักษ์เพียงตัวเดียว แทนที่จะปล่อยแต่ละ Server ซึ่งมีขนาดเล็ก แยกกันอยู่ การนำเทคโนโลยี Virtualization มาช่วยรวม Server เข้าด้วยกัน สามารถร่วมใช้งานทรัพยากร เช่น CPU, Memory, Hard disk และอื่นๆ บนเครื่อง คอมพิวเตอร์แม่ข่ายให้สามารถรันระบบปฏิบัติการหลายๆ ตัว ได้พร้อมกันหลายๆ อย่าง ทำให้มี การใช้งานอุปกรณ์ต่างๆ ร่วมกัน มีผลทำให้ก่าใช้ง่ายลดลง ช่วยลดจำนวนเครื่องฮาร์ดแวร์ได้อย่าง มาก ยังทำให้มีความซับซ้อนน้อยลง รวมไปถึงสามารถดูข้อมูลและบริหารจัดการ Server ทั้งหมด ได้ในหน้าจอเดียว ผู้นำตลาดด้าน Server Virtualization เช่น VMware Workstation ESXi, Citrix XenServer และ Microsoft Hyper-V

2.1.1.2 ประโยชน์ของระบบเสมือน

เมื่อนำระบบ Virtualization มาใช้สามารถตอบสนองความต้องการขององค์กรและภาค ธุรกิจได้หลากหลากหลายรูปแบบมากมายโดยสามารถแบ่งประโยชน์ได้ดังต่อไปนี้ [2]

- ได้ ผลลัพธ์ที่เพิ่มขึ้นจากทรัพยากรที่มีอยู่แล้ว โดยการนำทรัพยากรในโครงสร้างพื้นฐานที่ มีอยู่มารวมกัน และเลิกกฎเก่าๆ ของการที่ต้องใช้งาน 1 Application 1 Server โดยการนำ งานของ หลายๆ Server มาทำงานร่วมกัน ทำให้เกิดและ Utilization ที่ดีขึ้น เช่น การรวม งานของ Server 2 เครื่องที่ทำงานไม่เคยเกิน 40% ของ CPU มารวมกันทำงานในเครื่องเดียว และทำให้ระบบสามารถเกิดเครื่อง Server ว่างสำหรับงานสำรอง หรืองานอื่นๆ ที่ต้องการ Hardware ใหม่เพื่อรองรับได้ Processing Power
- 2) ลดค่าใช้จ่ายของ Datacenter โดยลดจำนวนของโครงสร้างพื้นฐาน ซึ่งคือ การลดจำนวน ของ Server ลง ทำให้ต้องการพื้นที่น้อยลง ลดความจำเป็นในการใช้ไฟฟ้า และการทำความ เย็น บริหารจัดการได้ง่ายขึ้นเนื่องจากมีจำนวนน้อย และไม่จำเป็นต้องเพิ่มจำนวนของ ผู้ดูแลระบบ โดยที่ผู้ดูแลระบบสามารถดูแลจัดการได้อย่างใกล้ชิดมากขึ้น
- 3) เพิ่ม Availability ของ Hardware และ Application ซึ่งส่งผลให้ปรับปรุงความต่อเนื่องใน การคำเนินธุรกิจ นอกจากนี้ยังสามารถทำการสำรองข้อมูล หรือย้าย Virtual Machine ทั้ง ระบบไปยัง Hardware ใหม่ ได้ โดยไม่มีการติดขัดของการให้บริการ ตัดปัญหาการ บำรุงรักษาที่ไม่ได้วางแผนไว้ และต้องปิดระบบ รวมถึงสามารถกู้กืนระบบได้อย่างรวดเร็ว ในกรณีเกิดเหตุสุดวิสัยใดๆ ก็ตาม
- 4) ได้ความยืดหยุ่นในการปฏิบัติงาน สามารถตอบสนองต่อความต้องการของธุรกิจได้อย่าง dynamic โดย การปรับเปลี่ยนการบริหารจัดการทรัพยากรที่ยืดหยุ่น สามารถเพิ่มหรือลด ทรัพยากรให้กับระบบงานที่ต้องการเฉพาะช่วงบางช่วงเวลา นอกจากนี้การติดตั้งหรือนำ ระบบเข้าใช้งานก็ทำได้อย่างรวดเร็ว

2.1.2 ภาษา JAVA

ภาษา JAVA [3] จัดเป็นภาษาโปรแกรมที่ได้รับความนิยมมากอีกภาษาหนึ่งสามารถนำไป ประยุกต์ใช้งานไดมากมายหลากหลายด้าน จนติดอันดับโปรแกรมยอดนิยม โดยถูกพัฒนามาจาก บริษัทที่ชื่อว่า Sun Microsystems ซึ่งเป็นบริษัทคอมพิวเตอร์ชั้นนำของโลก โดยมีหัวหน้าทีมพัฒนา โปรแกรมชื่อว่า James Gosling ซึ่งโปรแกรมเมอร์ทั่วโลกยกย่องเขาว่าเป็นบิดาของ JAVA โดยชื่อ เดิมของภาษา JAVA ก็คือ Oak ซึ่งเป็นชื่อที่ทีมงานของ James Gosling ตั้งไว้เมื่อปี 1991 โดยมีความ ตั้งใจที่ว่าต้องการพัฒนาภาษาเขียนโปรแกรมที่มีความไม่ซับซ้อนแต่มีประสิทธิภาพพอสำหรับ หน่วยความจำภายในน้อย ๆ เนื่องมาจากยุคนั้นภาษา C จัดเป็นภาษาที่มีการควบคุมฮาร์ดแวร์ได้ดี แต่มีข้อเสียคือใช้หน่วยความจำมากจึงส่งผลให้มีการแจ้งเกิดของภาษา JAVA

ในส่วนของการทำงานของโปรแกรมภาษา JAVAกระบวนการพัฒนาโปรแกรมภาษา JAVA เราจะได้ไฟล์ Source code ที่มีนามสกุลเป็น .java แล้วนำ Source code ไปคอมไพล์ให้กลายเป็น Java Byte Code (.class) เมื่อถึงเวลาที่ด้องทำงานจริงในคอมพิวเตอร์หรืออุปกรณ์ต่าง ๆ Java Byte Code (.class) จะถูกคอมไพล์อีกครั้งให้เป็นภาษาเครื่องเฉพาะของอุปกรณ์นั้น ๆ จะเรียกการ คอมไพล์นี้ว่า Java Virtual Machine

2.1.2.1 รูปแบบการพัฒนาโปรแกรมด้วยภาษา JAVA

เนื่องจากภาษาจาวาสามารถพัฒนาโปรแกรมได้หลากหลายรูปแบบ ดังนั้นจึงมีชุด พัฒนาโปรแกรมที่เหมาะสมในแต่ละด้านแตกต่างกันดังนี้

- Java ME: ย่อมาจาก Java Micro Edition เป็นชุดพัฒนาสำหรับพัฒนาโปรแกรมที่ทำงานบน อุปกรณ์ขนาดเล็กเช่น โทรศัพท์มือถือ
- Java SE: ย่อมาจาก Java Standard Edition เป็นชุดพัฒนาสำหรับพัฒนาโปรแกรมที่ทำงาน บนคอมพิวเตอร์ทั่วไป
- 3) Java EE: ย่อมาจ<mark>าก Ja</mark>va Enterprise Edition เป็นชุดพัฒ<mark>นาสำ</mark>หรับพัฒนาระบบงานขนาด ใหญ่รองรับการทำงานแบบ Multi-user

2.1.2.2 ข้อดีของภาษา Java

หลังจากที่เราทราบหลักการทำงานของภาษาจาวามาบ้างแล้ว ต่อไปก็จะกล่าวถึงข้อคีของ ภาษา Java ที่หลายคนก็คงอยากทราบดังนี้

- ภาษาจาวาเป็นภาษาเชิงวัตถุ (ทำให้เรามองภาพเป็นวัตถุ เพื่อทำงานได้ง่าย)
- สามารถทำงานบนเครื่องคอมพิวเตอร์ต่างระบบได้
- ไวยากรณ์ของภาษาจาวาได้รับการออกแบบมาอย่างดีเยี่ยม
- มีระบบจัดลืนพื้นที่ให้หน่วยความจำอัติโนมัติ
- 5) มีความหลากหลายของคลาสจำนวนมากให้ใช้
- 6) ทำงานบนเว็บเบราเซอร์ได้ คือมีจาวาแอปเพล็ต (Java Applet)
- สนับสนุนงานหลากหลายระดับ ระดับเซิร์ฟเวอร์ ระดับคอมพิวเตอร์ส่วน บุคคล ไปจนถึงอุปกรณ์พกพา

2.1.3 พร็อกซีเซิร์ฟเวอร์ย้อนกลับ (Reverse Proxy)

พร็อกซีเซิร์ฟเวอร์ย้อนกลับคือ [4] อุปกรณ์รักษาความปลอดภัยที่โดยปกติ แล้วปรับใช้ใน DMZ เครือข่ายเพื่อป้องกันเซิร์ฟเวอร์ HTTP (หรือเซิร์ฟเวอร์ IBM® Sametime) บนอินทราเน็ต องค์กรโดยการดำเนินฟังก์ชันการรักษาความปลอดภัยที่ช่วยป้องกันเซิร์ฟเวอร์ ภายในจากการโจมตี โดยผู้ใช้บนอินเทอร์เน็ต

พร็อกซีเซิร์ฟเวอร์ย้อนกลับป้องกันเซิร์ฟเวอร์ HTTP ภายในโดยการจัดให้มีจุดเข้าถึง เครือข่ายภายในจุดเดียว การระบุจุดเข้าถึงเซิร์ฟเวอร์ HTTP ทั้งหมดบนเครือข่ายภายใน เพียงจุด เดียว จะทำให้เกิดข้อดีต่อการรักษากวามปลอดภัยที่เจาะจง และคุณสมบัติการเข้าถึง เครือข่าย

ผู้ดูแลระบบ สามารถใช้คุณลักษณะ การพิสูจน์ตัวตน และการควบคุมการเข้าถึงของพรีอก ซีเซิร์ฟเวอร์ข้อนกลับเพื่อควบคุม ว่าใครบ้างที่สามารถเข้าถึงเซิร์ฟเวอร์ภายใน และควบคุมว่า เซิร์ฟเวอร์ใดที่ผู้ใช้ แต่ละคนสามารถเข้าถึงได้ เมื่อปรับใช้พรีอกซีข้อนกลับ anระบวนการพิสูจน์ ตัวตนและสิทธิ์การเข้าถึงหลายเซิร์ฟเวอร์ภายใน สามารถควบคุมจากเครื่องเดียว ซึ่งทำให้การ กำหนดค่าการรักษากวาม<mark>ปลอ</mark>ดภัย ทำได้ง่าย ทราฟฟิกทั้งหมดไปยังอินทราเน็ต เซิร์ฟเวอร์ภายใน จะถูก กำหนดปลายทางสำ<mark>หรับ</mark>แอดเดรสเครือข่ายเดียว (แอดเดรสของ</mark>พรีอกซีเซิร์ฟเวอร์ ข้อนกลับ)

เมื่อพร็อกซีเซิร์ฟเวอร์ย้อนกลับ ถูกปรับใช้ URLs ที่เชื่อมต่อกับพรีอกซีเซิร์ฟเวอร์ย้อนกลับ เท่านั้น ที่จะทำให้เป็นพับลิกสำหรับผู้ใช้เว็บเบราว์เซอร์ ผู้ใช้จากอินเทอร์เน็ตใช้ URLs เหล่านี้เพื่อ เข้าถึงพร็อกซีเซิร์ฟเวอร์ย้อนกลับ พร็อกซีเซิร์ฟเวอร์ย้อนกลับ จัดการการร้องขอจากผู้ใช้ อินเทอร์เน็ตเหล่านี้ และเปลี่ยนทิศทางการร้องขอเหล่านี้ ไปยังเซิร์ฟเวอร์ HTTP ภายในที่เหมาะสม ผู้ดูแลระบบ ดำเนินการกำหนดค่าการแม็พ URL บนพร็อกซีเซิร์ฟเวอร์ ย้อนกลับที่ทำให้ การเปลี่ยนทิศทางนี้เป็นไปได้ เมื่อกำหนดค่าพร็อกซีเซิร์ฟเวอร์ ย้อนกลับ ผู้ดูแลระบบแม็พ URLs ที่ ใช้เพื่อเข้าถึง พร็อกซีเซิร์ฟเวอร์ย้อนกลับไปยัง URLs จริงของเซิร์ฟเวอร์ HTTP ภายใน เมื่อผู้ใช้ อินเทอร์เน็ตส่ง URL ไปยังพร็อกซีเซิร์ฟเวอร์ย้อนกลับ พร็อกซีเซิร์ฟเวอร์ย้อนกลับจะตรวจสอบ URL และใช้การกำหนดค่าการแม็พเหล่านี้ (หรือกฏ) เพื่อเขียน URL ใหม่

พร็อกซีเซิร์ฟเวอร์ ย้อนกลับเขียน URL ใหม่โดยการแทนเซิร์ฟเวอร์แอดเดรสที่ระบุ โดย ผู้ใช้อินเทอร์เน็ต (พร็อกซีเซิร์ฟเวอร์ย้อนกลับ) ด้วยแอดเดรสจริง ของผู้ใช้ภายใน จากนั้นการร้อง ขอ HTTP จะถูกส่งบนเครือข่าย ภายในจากพร็อกซีเซิร์ฟเวอร์ย้อนกลับไปยังเซิร์ฟเวอร์ภายในทราฟ ฟิกทั้งหมดที่ส่งไปยังผู้ใช้อินเทอร์เน็ตจากเซิร์ฟเวอร์ ภายในของคุณจะแสดงเป็นว่ามีจุดเริ่มต้นจาก แอดเดรสเครือข่ายเดียว

เมื่อเซิร์ฟเวอร์ HTTP ภายใน (หรือเซิร์ฟเวอร์ Sametime) ตอบกลับการร้องขอจาก ผู้ใช้ อินเทอร์เน็ต เซิร์ฟเวอร์ภายในจะส่งการตอบกลับไปยังพรีอกซีเซิร์ฟเวอร์ ย้อนกลับ และพรีอกซี เซิร์ฟเวอร์ย้อนกลับส่งการตอบกลับไปยัง ผู้ใช้อินเทอร์เน็ต การตอบกลับที่ส่งบนอินเทอร์เน็ตไปยัง ผู้ใช้อินเทอร์เน็ต จะมีแอดเดรสของพร็อกซีเซิร์ฟเวอร์ย้อนกลับ ไม่ใช่แอดเดรส ของเซิร์ฟเวอร์ HTTP ภายใน

2.1.4 ภาษา SQL

SQL [5] อ่านใด้ 2 แบบคือแอสคิวแอล และซิควอล มาจากคำว่า Structured Query Language คิดค้นโดยบริษัท IBM ภาษา SQL เป็นภาษาที่ใช้ร่วมกับการเขียนโปรแกรมคอมพิวเตอร์ ซึ่งใช้ในการจัดการ เรียกดูฐานข้อมูล โดยเฉพาะ และเป็นองค์ประกอบหนึ่งของระบบฐานข้อมูล แบบรีเลชั่นเนล (Relational Database) ซึ่งในปัจจุบันเป็นที่นิยมอย่างมาก เนื่องจากเป็นระบบ ฐานข้อมูลที่ไม่ซับซ้อน ง่ายต่อการเข้าใจ มีประสิทธิภาพการทำงานสูง สามารถทำงานที่ซับซ้อนได้ โดยใช้คำสั่งเพียงไม่กี่กำสั่<mark>ง แต่</mark>จะอยู่ในรูปแบบภาษาอังกฤษซึ่งเป็นภาษาสากล

ภาษา SQL แบ่งออกเป็น 2 ส่วน คือ

- Data Definition Language หรือ DDL เป็นภาษาสำหรับการนิยามข้อมูล
- 2) Data Manipulation Language หรือ DML เป็นภาษาสำหรับการจัดการข้อมูลล
- 3) ภาษาสำหรับควบคุมข้อมูล (Control Language)
- 4) ภาษาสำหรับเรียกดูข้อมูล (Data Query Language)

คำสั่ง SQL สำหรับเรียกดูข้อมูลที่ต้องการแบบทันที (Interactive SQL) เป็นการเรียกใช้ คำสั่ง SQL สั่งงานที่จอภาพ สำหรับเรียกดูข้อมูลขณะที่ยังทำงานอยู่ได้ทันที เช่น SELECT PRODUCT_NAME FROM M_PRODUCT WHERE PRODUCT_ID = 'PD01';

คำสั่ง SQL ที่จะต้องเขียนร่วมกันโปรแกรมอื่น ๆ (Embedded SQL) ใช้ร่วมกับคำสั่งของ โปรแกรมภาษาอื่น ๆ อย่างเช่น PL/I PASCAL เป็นต้น หรือแม้แต่กับคำสั่งในโปรแกรมที่ระบบ จัดการฐานข้อมูลนั้นที่มีใช้เฉพาะ เช่น ORACLE มี PL/SQL (Procedural Language /SQL) ตัวอย่างการใช้คำสั่ง SQL ในภาษา PL/I EXEC SQL SELECT PRODUCT_NAME INTO :X PRODUCT_NAME FROM M_PRODUCT WHERE PRODUCT_ID = 'PD01';

2.1.5 ระบบยูนิกซ์ (Unix System)

(0

Unix System [6] เป็นระบบปฏิบัติการที่เคยพัฒนาในห้องแล็บ Bellสร้างขึ้นเพื่อใช้กับ เครื่องมินิคอมพิวเตอร์ และเมนเฟรม ใช้ในการควบคุมการทำงานของศูนย์คอมพิวเตอร์ที่มีการ เชื่อมลูกข่ายคอมพิวเตอร์ หรืออุปกรณ์ต่อพ่วงเป็นจำนวนมาก ดังนั้นยูนิกซ์ จึงมักใช้ในระบบ เครือข่ายคอมพิวเตอร์ที่มีขนาดใหญ่ และมีการเชื่อมต่อเครือข่ายระยะไกลต่อมาได้มีการพัฒนาให้ สามารถนำยูนิกซ์มาใช้กับ<mark>เครื่อ</mark>งคอมพิวเตอ<mark></mark>ร์ได้

ยูนิกซ์เป็นระบบ<mark>ปฏิบั</mark>ติการประเภทหนึ่ง ที่เป็นเทคโนโ<mark>ลยีแ</mark>บบเปิด (open system)ซึ่งเป็น แนวคิดที่ผู้ใช้ไม่ต้อง ผูกติด กับระบบใดระบบหนึ่งหรืออุปกรณ์ยี่ห้อเดียวกัน นอกจากนี้ยูนิกซ์ยังถูก ออกแบบมาเพื่อตอบสนองการใช้งานใน ลักษณะให้มีผู้ใช้ได้หลายคน ในเวลาเดียวกัน เรียกว่า มัลติ ยูสเซอร์ (multiusers)และสามารถทำงานได้หลายๆงานใน เวลาเดียว กันในลักษณะที่เรียกว่ามัลติ ทาสกิ้ง (multitasking)

2.1.5.1 ลักษณะการทำงานของยูนิกซ์

ลักษณะการทำงาน ยูนิกซ์ ติดต่อกับผู้ใช้ได้โดยการพิมพ์กำสั่งลงบนเครื่องหมาย Prompt Sign แต่ในปัจจุบัน สามารถจำลองจอภาพการทำงานของยูนิกซ์ ให้อยู่ในสภาพแวคล้อมของ วินโดวส์ได้แล้ว ทำให้สามารถทำงานติดต่อกับผู้ใช้ได้สะดวกมากยิ่งขึ้น โดยคุณสมบัติพิเศษของ ยูนิกซ์ คือ เรื่องของการรักษาความปลอดภัยในระบบเครือข่ายกอมพิวเตอร์ รวมทั้งมีความสามารถ สูงในด้านการติดต่อสื่อสารระยะไกลระหว่างกอมพิวเตอร์ ทำให้ยูนิกซ์ถูกนำมาใช้เป็น ระบบปฏิบัติการสำหรับเครือข่ายของโลกที่เรียกว่า อินเทอร์เน็ต ดังนั้นก่อนที่ผู้ใช้จะเข้าสู่ระบบ ยูนิกซ์ ได้จะต้องทำการพิมพ์ Login Name และ (Password)

2.1.5.2 การใช้งานของยูนิกซ์

การที่ผู้ใช้จะขอใช้บริการบนระบบยูนิกซ์ได้นั้นจะต้องได้รับอนุญาตจากผู้ดูแลระบบหรือที่ เรียกว่าซิสเตมแอดมินิสเตรเตอร์ (System Administrator) ก่อน หลังจากนั้นผู้ใช้จะได้รับรายชื่อผู้ใช้ หรือล๊อกอินเนม (login name) และรหัสผ่าน (password) มา แต่บางระบบ จะมีรายชื่ออิสระเพื่อให้ ผู้ใช้ชั่วคราว โดยอาจมีล๊อกอินเนมเป็น guest, demo หรือ fieldซึ่งจะไม่ต้องใช้รหัสผ่าน การเข้าใช้ ระบบเราเรินกว่า ล๊อกอิน (login) โดยทั่วไปเมื่อระบบพร้อมที่จะให้บริการจะปรากฏข้อความว่า login:หรือข้อความใน ลักษณะที่คล้ายๆ กันรวมเรียกว่า พรอมต์ล๊อกอิน (Prompt log in)เมื่อปรากฏ หรอมต์แล้วก็ให้พิมพ์ล๊อกอินเนมของผู้ใช ตามด้วย การกดปุ่มจากนั้นระบบจะสอบถามรหัสผ่าน กึ พิมพ์รหัสที่ถูกต้องลงไปตามด้วยปุ่มซึ่งรหัสผ่านที่พิมพ์ลงไปจะไม่ถูกแสดงผลออก ทางจอภาพเมื่อ รหัสผ่านถูกต้องก็จะปรากฏเครื่องหมาย \$ ซึ่งเป็นเครื่องหมายเตรียมพร้อมของระบบ

2.1.6 เทคโนโลยี VNC

10

ภาพที่ 2.2 Logo ของบริการ VNC ที่มีชื่อว่า RealVNC

FΑ

VNC [7] ย่อมาจาก Virtual Network Computing เป็นโปรแกรมประเภท Remote Control จากคอมพิวเตอร์เครื่องหนึ่งไปยังคอมพิวเตอร์อีกเครื่องหนึ่ง หรือระหว่างเครื่อง Client ไปยังเครื่อง Server พูดง่ายๆ VNC คือระบบแบ่งปั้นทรัพยากรหน้าจอคอมพิวเตอร์ร่วมกัน รวมถึง Input Device เช่น Mouse และ Keyboard สำหรับทำการ Remote Control คอมพิวเตอร์เครื่องอื่นๆ และยังสามารถ ทำงานร่วมกันได้หลายเครื่องพร้อมๆ กันรวมทั้งมือถือ เช่น IPhone หรืออุปกรณ์ อิเลคทรอนิคส์ อื่นๆ ได้อีกด้วย

VNC เป็นโปรแกรมประเภทฟรีแวร์และมีหลายเวอร์ชั่น ในการติดตั้งโปรแกรม VNC เพื่อ ใช้งานนั้น จะต้องดูว่าเครื่องที่เราจะทำการติดตั้งเป็นระบบปฏิบัติการประเภทไหนเราจะต้อง Download เวอร์ชั่นเฉพาะของระบบปฏิบัติการนั้นๆมาติดตั้งถึงจะสามารถใช้งานได้เช่น ถ้า ระบบปฏิบัติการของ Windows ก็สามารถติดตั้ง Real VNC หรือ Ultra VNC เป็นต้น และในการ ติดตั้งต้องดูด้วยว่าเครื่องที่เราจะทำการติดตั้งเป็นเครื่อง Client หรือเครื่อง Server ถ้าเป็นเครื่อง Client เราก็ทำการติดตั้งเป็น VNC Viewer แต่ถ้าเป็นเครื่อง Server ให้เราทำการติดตั้งเป็น VNC Server

2.1.6.1 การทำงานของเทคโนโลยี VNC

10

ถ้าท่านเป็นอีกคนหนึ่งที่มีสำนักงานตั้งอยู่ในหลายๆ พื้นที่ หรือท่านเป็นคนที่ชอบเดินทาง บ่อย หรือในขณะที่ท่านเองกำลังพักผ่อนอยู่กับบ้าน แต่มีงานที่จะต้องทำที่อยู่ในเครื่องคอมพิวเตอร์ ที่สำนักงานของท่าน และท่านเองก็ไม่สามารถที่จะเดินทางเข้าไปในสำนักงาน ได้ในขณะนั้น VNC สามารถช่วยพวกท่านได้ ท่านสามารถนั่งอยู่ที่บ้าน หรือที่ไหนๆก็ได้ในโลกนี้ ที่มีเครือข่าย อินเตอร์เน็ต แล้วใช้ VNC ช่วยในการติดต่อสื่อสารจากเครื่องคอมพิวเตอร์ของท่านที่บ้าน (หรือที่ที่ อยู่ ณ ขณะนั้น) ไปยังเครื่องคอมพิวเตอร์ที่สำนักงานของท่าน (หรือที่ใหนก็ได้) เพื่อทำงาน

โดยหลักการทำงานของ VNC จะเป็นการเชื่อมต่อกอมพิวเตอร์จากระยะไกล โดยใช้เมาส์ และกีย์บอร์คในการกวบคุมเกรื่องซึ่งเป็นการรี โมทกอมพิวเตอร์ในลักษณะ User Support โดยที่ไม่ ต้องเดินไปยังเกรื่องของ User VNC ได้ถูกพัฒนามาหลายเวอร์ชั่นด้วยกัน จากหลายค่ายผู้ผลิต Software เช่น Real VNC, Ultra VNC หรือ Tight VNC เป็นต้น แต่ไม่ว่าจะมีการพัฒนามาจาก หลากหลายค่ายหลากหลายผู้ผลิต แต่ VNC ก็ถูกพัฒนาโดยภาษาเดียวกัน คือภาษา JAVA และ เนื่องจากมันถูกพัฒนาโดยภาษา JAVA ดังนั้นจึงทำให้มันมีจุดเด่นอยู่พอสมควรคือ สามารถที่จะใช้ งานได้บนหลายๆ Platform (โดยการ Install Version ที่พัฒนาสำหรับ OS นั้นๆ) ไม่ว่าจะเป็น Windows UNIX LINUX หรืออื่นๆ



ภาพที่ 2.3 Diagram การทำงานของ VNC

2.1.6.2 ประโยชน์ของเทคโนโลยี VNC

ประโยชน์ของ VNC สามารถนำมาใช้ได้หลากหลายในงานไอที ดังนี้

- File-Transfer คือ การรับ ส่งไฟล์ต่างๆ
- 2) Text Chat คือ การสนทนาผ่านเครือข่าย
- 3) MS Log-on คือ การเข้าใช้งานคอมพิวเตอร์อีกเครื่องหนึ่ง
- 4) Multi Monitor Support คือ การดูแลคอมพิวเตอร์หลายๆเครื่องจากจอเดียว
- 5) Auto Reconnect คือ การเชื่อมต่อใหม่โดยอัตโนมัติ

2.2 เทคโนโลยีที่ใช้ในการปฏิบัติงาน

(0

2.2.1 โปรแกรม VMware Workstation

ภาพที่ 2.4 Logo โปรแกรม VMware Workstation ที่มา: goo.gl/TG6KG9

VMware Workstation Workstation [8] เป็นโปรแกรมซึ่งใช้ในการสร้าง Virtual Machine(VM) หรือเครื่องคอมพิวเตอร์เสมือน เป็นการสร้างเครื่องคอมพิวเตอร์ขึ้นมาอีกเครื่อง ภายในเครื่องของเราเอง ดังนั้นจึงทำให้เราสามารถทำลองใช้งาน OS หรือโปรแกรมอื่น ๆ ที่ต้องการ ใด้โดยไม่ต้องทำการ format เครื่องหรือใช้ PC อีกเครื่องหนึ่งมาเพื่อทดสอบ และ VM ที่กำลังมีการ ใช้ง้านอยู่บน VMware Workstation สามารถที่นำมาใช้งานภายนอกได้จริงในทันที(โดยใช้การ Bridge(Default) หรือ NAT ออกมาที่ Host ที่ได้ทำการ Run VMware Workstation อยู่) ดังนั้น ประโยชน์อีกอย่างหนึ่งของ VMware Workstation คือสามารถทำการจำลองการทำงานของระบบ Network ได้โดยใช้คอมพิวเตอร์เพียงเครื่องเดียว

นักพัฒนา Software และผู้ทำการทดสอบ software ซึ่งสามารถทำการทดสอบและ integration ของ multi-tier-application ไม่ว่าจะทำงานบน O/S เดียวกันหรือต่าง O/S กันบนเครื่องๆ เดียวกัน และ VMware Workstation สามารถที่จะเก็บ environment เริ่มต้นเพื่อนำกลับมาใช้ได้ โดยง่าย> ผู้ที่มีความจำเป็นต้องใช้ legacy application สามารถใช้ VMware Workstation Workstation เพื่อให้เครื่อง desktop ของท่านสามารถ run O/S เก่าๆเช่น DOS ในการใช้งาน legacy application ในขณะที่ run O/S ใหม่ๆเพื่อทดสอบความพร้อมในการทำ migrationสำหรับห้อง demo หรือ ห้องเรียน ด้วยความสามารถในการเก็บ environment เริ่มต้น VMware Workstation จะประหยัดเวลา ในการเตรียมการเรียนการสอนได้เป็นอย่างมาก> เพิ่มประสิทธิภาพในการ support ของ help desk หรือ technical service team ด้วยการทำ replication ของ configuration เครื่องที่มีปัญหาเพื่อทำการ ทดสอบโดยไม่ต้องใช้เครื่องที่ทาง user ต้องใช้งาน

ในการทดสอบการลงโปรแกรมใหม่ๆ เพราะการทำงานจะทำงานเสมือนเป็นคอมพิวเตอร์ อีกตัวหนึ่ง ซึ่งถ้าเกิดความผิดพลาดใดๆ ก็จะไม่มีผลต่อตัวระบบปฏิบัติการกอมพิวเตอร์ระบบหลัก และอีกตัวอย่างหนึ่งก็เช่น มีคอมพิวเตอร์อยู่เครื่องนึงที่มีระบบปฏิบัติการ (OS) อยู่แล้วแล้วเราทำ การลงโปรแกรมที่มีชื่อว่า VMware Workstation Vsphere Client โปรแกรมนี้สามารถติดตั้ง OS ได้ หลายตัวที่สำคัญสามารถรัน OS พร้อมกันได้ด้วย สรุป OS ที่ลงในโปรแกรม VMware Workstation Vsphere Client หลายๆตัว<mark>ก็กือ</mark> Virtual Machine

10



ภาพที่ 2.5 ตัวอย่างหน้าต่างขณะใช้งานของโปรแกรม VMware Workstation 12 PRO ที่มา: goo.gl/FKTw1n

2.2.2 โปรแกรม VMware ESXi

16

VMware ESXi [9] แรกเริ่มเดิมที VMware มีแต่ ESX และเมื่อ ESX ติดตลาดและทำตัว เปรียบเสมือนระบบปฏิบัติการตัวหนึ่งจึงนำไปจำหน่ายพ่วงกับ เซิร์ฟเวอร์หลายค่าย บางทีถูกโหลด ไว้ในฮาร์ดดิสก์ บางทีมาเป็นไดร์ฟ USB แล้วแต่ว่าก่ายไหนจะรังสรรค์ผลงานออกมายังไง ส่วน VMware ESX ที่จำหน่ายพร้อมกับเซิร์ฟเวอร์นี้จึงได้ชื่อเป็น ESXi โดย i ก็คือ Integrated จะจำหน่าย มาพร้อมกับเซิร์ฟเวอร์เท่านั้น ช่วงเวลาหลัง กิดว่าน่าจะเป็นที่ ESXi แบบเดิม รองรับเซิร์ฟเวอร์ได้ ในวงจำกัด และการงายผ่านเซิร์ฟเวอร์ลูกก้าไม่สามารถทดลองก่อนได้ เจ้า ESXi แบบมากับ เซิร์ฟเวอร์จึงได้ชื่อใหม่เป็น ESXi Embedded โดยวีเอีมแวร์ออก ESXi Installable มาอีกหนึ่งตัว ESXi Installable สามารถ<mark>ดาวน์</mark>โหลดมาติด<mark>ต้</mark>้งได้โดยง่ายไม่ต้องรอซื้อ</mark>พ่วงกับเซิร์ฟเวอร์



ภาพที่ 2.6 โครงสร้างของ VMware ESXi ที่มา: goo.gl/Egvoyw

2.2.3 โปรแกรม VMware vSphere



ภาพที่ 2.7 Logo ของโปรแกรม VMware vSphere ที่มา: goo.gl/VTaEbY

VMware vSphere [10] คือ Product ของ VMware ตัวหนึ่ง เป็นตัวแปรสำคัญในการทำ ระบบ Server Virtualization ซึ่งถือเป็นส่วนหนึ่งใน SDDC (Software-Defined Data Center) ประกอบด้วย 3 ระบบหลักๆ ก็คือ Server Virtualized, Network Virtualized, Storage Virtualized โดยมีประโยชน์ในการทำดังนี้

- ถดค่าใช้จ่ายในการซื้อเครื่อง Server เป็นที่ทราบกันว่า ราคาของเครื่อง Server ค่อนข้าง สูงและด้วยการทำ Server เสมือน (Server Virtualization) จะสามารถสร้าง Server เสมือน ได้จำนวนมากเช่นเดียวกับเรามี Server หลายๆ เครื่อง อยู่ใน Server จริงเพียงเครื่องเดียว
- ลดค่าไฟ การทำ Server Virtualization นอกจากสามารถตัดค่าเครื่อง Server ได้แล้ว ค่าใช้จ่ายจำนวนมหาศาลที่จะถูกตัดไปโดยปริยายเลยคือ "ค่าไฟ" เป็นที่ทราบกันว่า เครื่อง

Server นั้นต้องใช้งานอยู่ตลอด 24 ชั่วโมง และการรวม Server (Server Consolidation) จะ เป็น Solution

- ลดภาระการทำงานของทางด้านไอทีที่ต้องดูแล Server ภาระในการดูแลเครื่อง Server หลายๆเครื่อง เป็นเรื่องที่สำบาก และน่าปวดหัวเป็นอย่างมาก ซึ่งการทำ Server เสมือน จะ สามารถทำให้คุณดูแลเกรื่อง Server หลายๆเครื่องได้ในเกรื่องเดียว
- ลดค่าดูแลรักษา การที่เรามีเครื่อง Server ในความดูแลหลายๆเครื่อง ค่าดูแลรักษาก็ต้องสูง ตามอย่างเลี่ยงไม่ได้ เพราะอุปกรณ์ทุกอุปกรณ์จะมีค่าดูแลรักษาทั้งสิ้น ไม่ว่าจะเป็นความ สูญเสียเพราะการทำงานที่ผิดพลาดหรือกวามสูญเสียของอุปกรณ์ที่เสื่อมไปตามกาลเวลา
- สามารถโอนข้ายข้อมูลได้สะดวก หมดบัญหาเรื่องการโอนข้ายข้อมูลจากเครื่องหนึ่ง ไปอีก เครื่องที่น่าปวดหัวด้วย Solution จากเรา เพราะการทำ Vmware Server Vitualization มี ฟังก์ชั่น ที่สามารถโอนถ่ายข้อมูล อย่างรวดเร็ว และสะดวกสบาย
- 6. ลดพื้นที่ ที่ต้องใช้ในการจัดวาง Server จริง (Physical Server) หลายๆองก์กร ประสบปัญหา มีความจำเป็นต้องใช้ Server หลายๆ เครื่อง แต่พื้นที่จัดวางไม่เอื้ออำนวย
- ถงระบบปฏิบัติการได้หลากหลาย Vmware vSphere สามารถสร้าง Server เสมือน ที่ใช้ ระบบปฏิบัติการที่ต่างกันได้ ทั้งยังสามารถรองรับระบบปฏิบัติการเก่า ได้มากกว่าการใช้ Physical Server

2.2.4 ระบบปฏิบัติการ Ubuntu

[11] สำหรับผู้ที่ไม่รู้จัก Linux Ubuntu ว่าคืออะไรนั้น จริงๆมันคือระบบปฏิบัติการ Linux ชนิดหนึงซึ่ง ลีนุกซ์ (Linux) ก็เป็นระบบปฏิบัติการเช่นเดียวกับ Dos, Window หรือ Unix โดยลื นุกซ์นั้นจัดว่าเป็นระบบปฏิบัติการขูนิกซ์ประเภทหนึ่ง การที่ลีนุกซ์เป็นที่กล่าวงานกันมากงณะนี้ เนื่องจากความสามารถงองตัวระบบปฏิบัติการและโปรแกรมประยุกต์ที่ทำงานบนระบบลีนุกซ์ โดยเฉพาะอย่างยิ่งโปรแกรมในตระกูลงอง GNU (GNU's Not UNIX) และสิ่งที่สำคัญที่สุดก็คือ ระบบลีนุกซ์เป็นระบบปฏิบัติการประเภทฟรีแวร์ (Free Ware) และเป็นที่นิยมเอามาทำเป็น server เพื่อทำเป็น webserver หรือ LAMP

ลินุกซ์ ถือเป็นส่วนสำคัญของซอฟต์แวร์เซิร์ฟเวอร์ที่เรียกว่า LAMP ย่อมาจาก Linux, Apache, MySQL, Perl/PHP/Python ซึ่งเป็นที่นิยมใช้เป็นเว็บเซิร์ฟเวอร์ และพบมากสุดระบบหนึ่ง ตัวอย่างซอฟต์แวร์ซึ่งพัฒนาสำหรับระบบนี้กือ มีเดียวิกิ ซอฟต์แวร์สำหรับวิกิพีเดีย เนื่องจากราคาที่ ต่ำและการปรับแต่งได้หลากหลาย ลินุกซ์ถูกนำมาใช้ในระบบฝังตัว เช่นเครื่องรับสัญญาณ โทรทัศน์
โทรศัพท์มือถือ และอุปกรณ์พกพาต่าง ๆ ลินุกซ์เป็นคู่แข่งที่สำคัญของ ซิมเบียนโอเอส ซึ่งใช้ใน โทรศัพท์มือถือจำนวนมาก และใช้แทนวินโควส์ซีอี และปาล์มโอเอส บนเครื่องคอมพิวเตอร์พกพา เครื่องบันทึกวิดีโอก็ใช้ลินุกซ์ที่คัดแปลงเป็นพิเศษ ไฟร์วอลล์และเราเตอร์หลายรุ่น เช่นของ Linksys ใช้ลินุกซ์และขีดความสามารถเรื่องทางเครือข่ายของมัน

โครงการ Ubuntu มีการออกรุ่นของระบบปฏิบัติการทุก 6 เดือน แต่ละรุ่นใช้เรียกโดยโค้ด เนม และเลขกำกับรุ่น ตามการพัฒนา ซึ่งใช้ตามเลขปีคริสต์ศักราชและเดือนที่ออก เช่น การออกใน เดือนตุลาคม ค.ศ. 2004 จะมีเลขรุ่นเป็น 4.10 ใช้เป็นหมายเลขรุ่นไปด้วยการเปิดตัวทุกเวอร์ชันจะ ออกช้ากว่า GNOME ประมาณ 1 เดือน, และออกตามหลัง 1 เดือน เมื่อ X.org ออกเวอร์ชันใหม่. ดังนั้นทุกๆการเปิดตัว จะประกอบด้วยเวอร์ชันใหม่ของทั้งGNOME และ X สำหรับเวอร์ชัน 6.06 และ 8.04 จะมีการติดป้ายชื่อ Long Term Support (LTS) เป็นการบอกว่ามันจะได้รับการสนับสนุน และการปรับปรุงเป็นเวลา 3 ปีสำหรับเครื่องเคสทีอปและ 5 ปี สำหรับเครื่องแม่ข่าย, ด้วยการจ่ายค่า สนับสนุนทางเทคนิคของบริษัท Canonical



ภาพที่ 2.8 Logo ของระบบปฏิบัติการ Ubuntu

2.2.4.1 ประเภทขอ<mark>งระบบปฏิบัติการ</mark> Ubu<mark>ntu</mark>

ในส่วนนี้มีด้วยกัน 2 แบบคือ desktop และ server ซึ่งโดยหลักการแล้วทั้ง 2 แบบทำงานได้ ไม่ต่างกัน แต่ถ้าคุณใช้งานบน PC หรือ notebook ก็ควรเลือกแบบ desktop เพราะเราจะสามารถ console ด้วยหน้า GUI ได้ สำหรับผู้ที่ต้องการ install เพื่อใช้งานเป็น server ที่เปิดใช้งานตลอดเวลา และ console ด้วยผ่าน remote ssh ไม่ต้องอาศัย GUI ก็เลือกแบบ Server เช่นเดียวกันคือมีด้วยกัน 2 version คือ 32bit และ 64bit ซึ่งขึ้นอยู่กับเครื่องที่เรา install ด้วยว่า support 64bit หรือไม่ (ถ้าเป็น Intel คือ Core 2 duo ขึ้นไป) เราแนะนำให้ใช้ 64bit ถ้าเครื่องรองรับ

2.2.5 ระบบปฏิบัติการ Kali Linux 2

Kali Linux [12] คือระบบปฏิบัติการชนิดนึงที่พัฒนาต่อยอดมาจาก ระบบปฏิบัติการที่ชื่อ ว่า Black Track โดย Kali Linux เป็นระบบปฏิบัติการที่เป็น Linux Distribution ของระบบปฏิบัติการ Debian โดยนำ Repository ทั้งหมดของ Debian มาใช้เป็น โครงสร้างพื้นฐานและภายในตัว ระบบปฏิบัติการนั้นจะประกอบไปด้วยเครื่องมือและ โปรแกรมที่ใช้สำหรับการทำ Penetration Testing เป็นระบบปฏิบัติการเฉพาะทาง เพื่อใช้สำหรับการทำงานสายเฉพาะ อีกทั้งประเภทของ Kali Linux นั้นในปัจจุบันได้ใช้ Desktop Environment ของ GNOME เป็นค้า Default ถึงอย่างไรก็ ตาม Desktop Environment ก็ได้แตกแขยงออกมาหลากหลายรูปแบบให้สามารถ เลือกใช้ได้เช่น Cinnamon และอื่น ๆ เป็นต้น

Kali Linux 2.0 หรือโค้คเนม "Kali Sana" เป็นแพลทฟอร์มรันบนระบบปฏิบัติการ Debian Jesse สำหรับใช้เจาะระบบคอมพิวเตอร์เพื่อตรวจหาช่องโหว่โดยเฉพาะ ซึ่งมาพร้อมกับชุดทดสอบ เจาะระบบมากกว่า 100 รายการ รวมทั้งมีระบบการวิเคราะห์เชิงสถิติ การแฮ็ค และวิศวกรรม ย้อนกลับ (Reverse Engineering) ในเวอร์ชัน 2.0 ล่าสุดนี้ ได้ทำการออกแบบอินเตอร์เฟสใหม่ จัด กลุ่มเครื่องมือ และเมนูแสดงผลต่างๆเพื่อให้ใช้งานได้สะดวกกล่องตัวมากยิ่งขึ้น



<mark>ภาพที่ 2.9</mark> Logo <mark>ข</mark>องระบบปฏิบัตการ Kali Linux ที่มา: goo.gl/HjDnDN

2.2.6 โปรแกรม Apache Tomcat

Apache Tomcat [13] คือ web server และ servlet container ที่เอามาใช้สำหรับ software ที่ ใช้ภาษา JAVA โดย Tomcat นั้นเป็น web server แบบ Open source ที่นำพวกเทคโนโลยี Java Servlet และ Java Server มปรับปรุงจนกลายเป็น Tomcat อีกที่และถูกพัฒนาโดยกลุ่ม Apache Software Foundation

อีกทั้งเป็นโปรแกรมบรรจุเว็บ (web container) ที่พัฒนาโคยมูลนิธิซอฟต์แวร์ Apache Tomcatใช้ ข้อกำหนดของเซิร์ฟเลตและเจเอสพีจากซันไมโครซิสเต็มส์มาเป็นต้นแบบในการทำงาน ซึ่งกำหนด สภาพแวคล้อมสำหรับโค้ดจาวาเพื่อทำงานบนเว็บเซิร์ฟเวอร์ นอกจากนั้นTomcatได้เพิ่มเครื่องมือ สำหรับการจัดการการตั้งค่าที่เก็บในรูปแบบแฟ้มเอกซ์เอ็มแอล และมีโปรแกรม HTTP เซิร์ฟเวอร์ อยู่ในตัวเอง

Apache Tomcat เคยเป็นโครงการย่อยของโครงการจาการ์ตา แต่ปัจจุบันได้แยกตัวออกมา เป็นโครงการหลักของมูลนิธิซอฟต์แวร์อะแพชี โดย Tomcatเป็นเว็บเซิร์ฟเวอร์ที่รองรับเซิร์ฟเลต และเจเอสพี โดยทำงานร่วมกับตัวแปลโปรแกรมชื่อ Tomcat แจสเปอร์ (Tomcat Jasper) ในการ แปลงเจเอสพีให้กลายเป็นเซิร์ฟเลตก่อนนำไปประมวลผล

เอนจินเซิร์ฟเลตของTomcatนั้นมักทำงานร่วมกับ อะแพชี เว็บเซิร์ฟเวอร์ (Apache HTTP Server) หรือโปรแกรมเว็บเซิร์ฟเวอร์อื่นๆ หรือสามารถตั้งตัวเป็นเซิร์ฟเวอร์เอกเทศก็ได้ ซึ่งในการ พัฒนาก่อนหน้านี้มีแนวความกิดว่า เมื่อTomcatทำงานเป็นโปรแกรมที่ทำงานโดดเดี่ยว (standalone) จะเหมาะกัสภาแวดล้อมที่ไม่ต้องการความรวดเร็วและการดูแลธุรกรรม (transaction) มากนัก อย่างไรก็ตามแนวความกิดดังกล่าวไม่มีอีกต่อไป เนื่องจากTomcatได้เพิ่มประสิทธิภาพเป็น เซิร์ฟเวอร์ที่รองรับสภาพแวดล้อมที่มีการจราจรหนาแน่นสูงTomcatสามารถทำงานได้ข้าม ระบบปฏิบัติการ เพียงแก่ต้องการจาวารันไทม์เอนไวรอนเมนต์ (Java Runtime Environment) เท่านั้น



ภาพที่ 2.10 Logo ของ Apache Tomcat ที่มา: goo.gl/DDZku5

2.2.7 โปรแกรม MySQL

MySQL [14] คือ โปรแกรมระบบจัคการฐานข้อมูล ที่พัฒนาโคยบริษัท MySQL AB มี หน้าที่เก็บข้อมูลอย่างเป็นระบบ รองรับคำสั่ง SQL เป็นเครื่องมือสำหรับเก็บข้อมูล ที่ต้องใช้ร่วมกับ เครื่องมือหรือโปรแกรมอื่นอย่างบูรณาการ เพื่อให้ได้ระบบงานที่รองรับ ความต้องการของผู้ใช้ เช่น ทำงานร่วมกับเครื่องบริการเว็บ (Web Server) เพื่อให้บริการแก่ภาษาสคริปต์ที่ทำงานฝั่งเครื่อง บริการ (Server-Side Script) เช่น ภาษา php ภาษา aps.net หรือภาษาเจเอสพี เป็นต้น หรือทำงาน ร่วมกับโปรแกรมประยุกต์ (Application Program) เช่น ภาษาวิชวลเบสิกดอทเน็ต ภาษาจาวา หรือ ภาษาซีชาร์ป เป็นต้น โปรแกรมถูกออกแบบให้สามารถทำงานได้บนระบบปฏิบัติการที่หลากหลาย และเป็นระบบฐานข้อมูลโอเพนทซอร์ท (Open Source)ที่ถูกนำไปใช้งานมากที่สุด

MySQL: มายเอสคิวแอล เป็นระบบจัคการฐานข้อมูล โดยใช้ภาษา SQL. แม้ว่า MySQL เป็นซอฟต์แวร์ โอเพนซอร์ส แต่แตกต่างจากซอฟต์แวร์ โอเพนซอร์สทั่วไป โดยมีการพัฒนาภายใต้ บริษัท MySQL AB ในประเทศสวีเดน โดยจัคการ MySQL ทั้งในแบบที่ให้ใช้ฟรี และแบบที่ใช้ใน เชิงธุรกิจ MySQL สร้างขึ้น โดยชาวสวีเดน 2 คน และชาวฟินแลนด์ ชื่อ David Axmark, Allan Larsson และ Michael "Monty" Widenius. ปัจจุบันบริษัทซันไม โครซิสเต็มส์ (Sun Microsystems, Inc.) เข้าซื้อกิจการของ MySQL AB เรียบร้อยแล้ว ฉะนั้นผลิตภัณฑ์ภายใต้ MySQL AB ทั้งหมดจะ ตกเป็นของซัน ชื่อ "MySQL" อ่านออกเสียงว่า "มายเอสคิวเอล" หรือ "มายเอสคิวแอล" (ในการอ่าน อักษร L ในภาษาไทย) ซึ่งทางซอฟต์แวร์ไม่ได้อ่าน มายซีเควล หรือ มายซีควล เหมือนกับซอฟต์แวร์ จัดการฐานข้อมูลตัวอื่น

ในระบบปฏิบัติการ Red Hat Linux นั้น มีโปรแกรมที่สามารถใช้งานเป็นฐานข้อมูลให้ ผู้ดูแลระบบสามารถเลือกใช้งานได้ หลายโปรแกรม เช่น MySQL และ PostgreSQL ผู้ดูแลระบบ สามารถเลือกติดตั้งได้ทั้งในขณะที่ติดตั้งระบบปฏิบัติการ Red Hat Linux หรือจะติดตั้งภายหลังจาก ที่ติดตั้งระบบปฏิบัติการก็ได้ อย่างไรก็ตาม สาเหตุที่ผู้ใช้งานจำนวนมากนิยมใช้งานโปรแกรม MySQL คือ MySQL สามารถทำงานได้อย่างรวดเร็ว น่าเชื่อถือและใช้งานได้ง่าย เมื่อเปรียบเทียบ ประสิทธิภาพในการทำงานระหว่างโปรแกรม MySQL และ PostgreSQL โดยพิจารณาจากการ ประมวลผลแต่ละกำสั่งได้ผลลัพธ์ดังรูปที่ 1 นอกจากนั้น MySQL ถูกออกแบบและพัฒนาขึ้นมาเพื่อ ทำหน้าเป็นเครื่องให้บริการรองรับการจัดการกับ ฐานข้อมูลขนาดใหญ่ ซึ่งการพัฒนายังคงคำเนิน อยู่อย่างต่อเนื่อง ส่งผลให้มีฟังก์ชันการทำงานใหม่ๆ ที่อำนวยความสะดวกแก่ผู้ใช้งานเพิ่มขึ้นอยู่ ตลอดเวลา รวมไปถึงการปรับปรุงด้านความต่อเนื่อง ความเร็วในการทำงาน และความปลอดภัย ทำ ให้ MySQL เหมาะสมต่อการนำไปใช้งานเพื่อเข้าถึงฐานข้อมูลบนเครือข่ายอินเทอร์เน็ต

10-

MySQL ถือเป็นระบบจัดการฐานข้อมูล (Database Management System (DBMS) ฐานข้อมูลมีลักษณะเป็นโครงสร้างของการเก็บรวบรวมข้อมูล การที่จะเพิ่มเติม เข้าถึงหรือ ประมวลผลข้อมูลที่เก็บในฐานข้อมูลจำเป็นจะต้องอาศัยระบบจัดการ ฐานข้อมูล ซึ่งจะทำหน้าที่ เป็นตัวกลางในการจัดการกับข้อมูลในฐานข้อมูลทั้งสำหรับการ ใช้งานเฉพาะ และรองรับการ ทำงานของแอพลิเคชันอื่นๆ ที่ต้องการใช้งานข้อมูลในฐานข้อมูล เพื่อให้ได้รับความสะดวกในการ จัดการกับข้อมูลจำนวนมาก MySQL ทำหน้าที่เป็นทั้งตัวฐานข้อมูลและระบบจัดการฐานข้อมูล

MySQL เป็นระบบจัดการฐานข้อมูลแบบ relational ฐานข้อมูลแบบ relational จะทำการ เก็บข้อมูลทั้งหมดในรูปแบบของตารางแทนการเก็บข้อมูลทั้งหมดลงในไฟล์ เพียงไฟล์เดียว ทำให้ ทำงานได้รวดเร็วและมีความยืดหยุ่น นอกจากนั้น แต่ละตารางที่เก็บข้อมูลสามารถเชื่อมโยงเข้าหา กันทำให้สามารถรวมหรือจัด กลุ่มข้อมูลได้ตามต้องการ โดยอาศัยภาษา SQL ที่เป็นส่วนหนึ่งของ โปรแกรม MySQL ซึ่งเป็นภาษามาตรฐานในการเข้าถึงฐานข้อมูล

MySQL แจกจ่ายให้ใช้งานแบบ Open Source นั่นกือ ผู้ใช้งาน MySQL ทุกคนสามารถใช้ งานและปรับแต่งการทำงานได้ตามต้องการ สามารถคาวน์โหลคโปรแกรม MySQL ได้จาก อินเทอร์เน็ตและนำมาใช้งานโดยไม่มีก่าใช้จ่ายใดๆ

> **ภาพที่ 2.11** Logo ของโปรแกรม MySQL ที่มา: goo.gl/aVUFJ7

(

R

บทที่ 3

แผนงานการปฏิบัติงานและขั้นตอนการดำเนินงาน

องค์ประกอบของบทที่ 3 มีดังนี้

- 3.1 แผนการปฏิบัติงาน
- 3.2 รายละเอียดโครงงาน
 - 3.2.1 รายละเอียด VM ระบบ Clientless Remote Desktop Gateway บนระบบปฏิบัติการ
 Ubuntu 14.04 (VM เครื่องที่ 1)
 - 3.2.1.1 รายละเอียดและการทำงานของส่วนประกอบ Guacamole-Server
 - 3.2.1.2 รายละเอียดและการทำงานของส่วนประกอบ Guacamole-Client
 - 3.2.2 รายละเอียด VM บริการ VNC บนระบบปฏิบัติการ Kali Linux 2 (VM เครื่องที่ 2)
 - 3.2.3 รายละเอียดและการทำงานของระบบ Cyber RANGE
- 3.3 ขั้นตอนการคำเนินงานที่นักศึกษาปฏิบัติงาน
 - 3.3.1 ขั้นตอนการดำเนินงานโครงการ

3.1 แผนงานการปฏิบัติงาน

ตารางที่ 3.1 แสดงการปฏิบัติงานดำเนินงานโครงการตลอดทั้ง 18 สัปดาห์

ซึ่งรายละเอียดการปฏิบัติงานทั้งหมดนั้นจะกล่าวถึงในหัวข้อ 3.3 "ขั้นตอนการดำเนินงาน" จากตารางที่ 3.1 แสดงให้เห็นถึงการสรุปการปฏิบัติงานของการดำเนินงานโครงการจริงที่บริษัทฯ

รายละเอียด			ģ	ມີຄ <mark>ຸ</mark> น	เายเ	ĩ	ſ	ទេកវ្	ງາຄາ	L	ĺ	สิงห	าคม		
រ ខេព	<u>ະເດຄ</u>	61		1	2	3	4	1	2	3	4	1	2	3	4
1) ศึกษาการทำงานข	องเท	คโนโลยี V	NC										0		/
และบริการต่าง ๆ ที่เก	กี่ยวข้	, 0\											\leq		
2) ศึกษาการทำงานข	องระ	บบ Clientl	ess						<	1	Y	~			
Remote Desktop Gar	teway	/ และระบบ	ต่าง						3		1		^		
ๆ ที่เกี่ยวข้องกับเทค	โนโล	ปี remote					Y								
						-			_	-					

หมายถึง ร<mark>ะ</mark>ยะเว<mark>ลาปฏิ</mark>บัติงา<mark>น</mark>จริง

รายละเอียด		มิถุนายน			กรกฎาคม			สิงหาคม			1	
3 10110100M	1	2	3	4	1	2	3	4	1	2	3	4
3) ติดตั้งระบบปฏิบัติการ Kali Linux 2												
และ Ubuntu server 14.04 บน VMware												
Workstation												
4) ติดตั้งระบบ Clientless Remote												
Desktop Gateway ที่มีชื่อว่า Apache												
Guacamole 0.9.12-incubating บน												
ระบบปฏิบัติการ Ubuntu server 14.04												
5) ทคลองและตรวจสอบความถูกต้องใน			Ġ		7						-	
การใช้งานของ Apache Guacamole						1	7	-				
0.9.12-incubating								Ŷ				
6) ทคสอบ VNC ที่สามารถใช้งานร่วมกับ												
ระบบปฏิบัติการ Kali Linux 2											2	\$
7) ติดตั้ง reverse proxy บน VM Ubuntu												-
server 14.04 ที่มีชื่อว่า Nginx											2	
8) ทดสอบ RealVNC และ Nginx ให้												S
ทำงานร่วมกับ Apache Guacamole 0.9.12-												
incubating												
9) นำระบบที่ผ่านการทคสอบบน												
VMware Workstation deploy کا VMware											1	
ESXi												1
10) พัฒนาระบบที่ผ่า <mark>นการ</mark> ทดสอบแล้ <mark>ว</mark> ให้												X
ทำงานร่วมกับและ m <mark>igrat</mark> ion ร่วมกับ												2
ระบบ Cyber RANGE				-						(
11) ทดสอบระบบ Cyber RANGE									2	2		
เวอร์ชัน10.8							(

ตารางที่ 3.1 แสดงการปฏิบัติงานดำเนินงาน โครงการตลอดทั้ง 18 สัปดาห์ (ต่อ)

จากตารางที่ 3.1 แสดงการปฏิบัติงานของการคำเนินงานโครงการ ตามการปฏิบัติงานจริงที่ บริษัท ไซเบอร์ตรอน จำกัด โดยมีช่วงเวลาคำเนินงานทั้งหมด ตั้งแต่เดือน มิถุนายน จนถึงเดือน สิงหากม ระยะเวลาที่ใช้ในการคำเนินงานทั้งสิ้น 3 เดือน ในระหว่างสหกิจศึกษาพบว่า การ ปฏิบัติงานข้อที่ 6 "ทคสอบ VNC ที่สามารถใช้งานร่วมกับระบบปฏิบัติการ Kali Linux 2" เป็น ขั้นตอนที่ใช้เวลาขาวนานและเป็นปัญหามากที่สุด อันเนื่องมาจากนักศึกษาได้ปฏิบัติงานของบริษัท ควบคู่กับดำเนินงาน โครงการสหกิจศึกษา ไปด้วย เป็นเหตุผลทำให้ระยะเวลาดำเนินงาน โครงการ ภาพรวมมีระยะเวลาขาวนาน รวมถึงการปฏิบัติงานข้อที่ 13 "ติดต่อและปรึกษาขอบเขตของการ ดำเนินงานร่วมกับพนักงานของบริษัทฯ" คือการติดต่อประสานงานตลอดเวลาร่วมกับพนักงานของ ที่บริษัทฯ ซึ่งเป็นสาเหตุที่ใช้เวลานานเช่นกัน

3.2 รายละเอียดโครงงาน

การพัฒนาและปรับปรุงระบบ Clientless Remote Desktop Gateway และ VNC สำหรับ ระบบ Cyber RANGE นั้นได้มีการขั้นตอนการปฏิบัติงานและการคำเนินงานต่าง ๆ ทั้งหมดตาม ตารางที่ 3.1 โดยรายละเอียดของโครงการนั้นได้มีการปฏิบัติบนเทคโนโลยี VM โดยมีการกำหนด VM ทั้งหมด 2 VMs ซึ่งก็คือ VM สำหรับระบบ Clientless Remote Desktop Gateway บน ระบบปฏิบัติการ Ubuntu Server 14.04 และอีก VM สำหรับบริการ VNC บนระบบปฏิบัติ Kali Linux หลังจากนั้น ได้ทำการ Mapping ระหว่าง VM ตามที่ได้ตั้งสมมุติฐานและได้วางแผนเอาไว้ที่ ขึ้นตรงตามวัตถุประสงค์ที่กล่าวไว้ใน บทที่ 1 โดยลักษณะการทำงานต่าง ๆ รวมถึงรายละเอียด ปลีกย่อย ของ VM ของหมดของขอบเขตในโครงการ จะมีทั้งสิ้น 2 VM และจะอธิบายในส่วน หัวข้อย่อยถัดไป

3.2.1 รายละเอียด VM ระบบ Clientless Remote Desktop Gateway บนระบบปฏิบัติการ Ubuntu server 14.04 (VM เครื่องที่ 1)

ในส่วนของรายละเอียดของ VM เครื่องนี้นั้นคือระบบ Clientless Remote Desktop Gateway ที่ติดตั้งบนระบบปฏิบัติการ Ubuntu Server 14.04 หลังจากนั้นจะติดตั้ง ชุดโปรแกรมที่มี ชื่อว่า Apache Guacamole 0.9.12-incubating ซึ่งเป็นระบบ Clientless Remote Desktop Gateway โดยเป็นชุดโปรแกรม ที่มีองค์ประกอบแบ่งออกเป็นสองส่วนคือ Guacamole-Client และ Guacamole-Server มีลักษณะ web-based ที่คอยจัดหา Remote Desktop Service ต่าง ๆ ให้กับ Host หรือลูกข่ายที่เข้ามา connect ร่วมกัน

3.2.1.1 รายละเอียดและการทำงานของส่วนประกอบ Guacamole-Server

เป็นส่วนที่ทำหน้าที่ควบคุมและประมวลผล ของชุดโปรแกรม Apache Guacamole โดยมี การทำงานหลัก ๆ คือ การจัดหา Remote Desktop Service ต่าง ๆ ให้กับ host ที่เข้ามา connect โดย Remote desktop service ต่าง ๆ นั้นจะครอบคลุมตามนี้คือ RDP หรือ Remote Desktop Protocol, VNC หรือ Virtual Network Computing, SSH หรือ Secure Shell รวมถึงจะประมวลผลในส่วนของ ระบบเครือข่าย และ ฟีเจอร์อื่น ๆ เช่น ระบบ VDO recorder เป็นต้น ซึ่งจะทำงานร่วมกับ ส่วนประกอบ Guacamole-Client ที่มีการทำงานตามที่กล่าวไปในหัวข้อ 3.2.1.2 ตลอดเวลา บน โปรโตคอลส่วนตัวที่มีชื่อว่า guacamole protocol และมี guacad เป็น command หลักในการควบคุม ส่วนของ Guacamole-Server ผ่าน UNIX command

3.2.1.2 รายละเอียดและการทำงานของส่วนประกอบ Guacamole-Client

10

เป็นส่วนที่รับค่าการตั้งค่าและการใช้งานตัวชุดโปรแกรมฯ ผ่านผู้ใช้งานในรูปแบบของ web-based โดยมีการทำงานหลัก ๆ คือ การรับค่าการตั้งค่าตัวชุดโปรแกรมฯ ผ่านหน้าเว็บ โดยหน้า เว็บนั้นจะมี tomcat เป็นโปรแกรมที่ทำหน้าที่เป็น web server เนื่องมาจากชุดโปรแกรม Apache Guacamole มีการใช้ภาษา JAVAในการประมวลผล และในการจัดเก็บข้อมูลต่าง ๆ ที่ใช้ในระบบฯ นั้นจะเชื่อมโยงกับ MySQL ที่เป็นฐานข้อมูลในการเก็บค่าการตั้งค่าของผู้ใช้งานรวมถึงข้อมูลที่ใช้ ประมวลผล ซึ่งจะทำงานควบคู่กับ Guacamole-Server

3.2.2 รายละเอียด VM บริการ VNC บนระบบปฏิบัติการ Kali Linux 2 (VM เครื่องที่ 2)

ในส่วนของรายละเอียดของ VM เครื่องนี้นั้นคือระบบปฏิบัติที่ถูกลงบริการ VNCเอาไว้ ตามที่วางแผนไว้ตาม สมมุติฐานและปัญหาที่พบ ตามที่กล่าวไว้ในบทที่ 1 โดย VM เครื่องนี้มีจุด ประสงรค์เพื่อเป็น host เอาไว้สำหรับเชื่อมต่อกับ VM เครื่องที่ 1 ที่เป็นระบบปฏิบัติการ Ubuntu Server 14.04 ที่ได้ลงระบบ Clientless Remote Desktop Gateway ที่มีชื่อว่า Apache Guacamole เอาไว้ บนระบบ เครื่อข่ายของ VMware Workstation โดยบริการ VNC ที่ได้ติดตั้งบน ระบบปฏิบัติการ Kali Linux 2 นั้นคือบริการ VNC ที่มีชื่อว่า Real VNC โดยชื่อรุ่นโปรแกรมคือ Real VNC Connect 6.2 สำหรับระบบปฏิบัติการ Linux

3.2.3 รายละเอียดและการทำงานของระบบ Cyber RANGE

เป็นระบบที่ให้บริการ CTF หรือ Capture The Flag ที่มีรูปแบบเป็น web-based โดยระบบ จะจำลองเหตุการณ์ปัญหาต่าง ๆ ทาง Cyber Security ซึ่งจะถูกแจกแจงมาในรูปแบบของ Scenario ลักษณะระบบเสมือน หรือ VM เพื่อให้ผู้ใช้งานสามารถเข้ามาแก้ไขปัญหาต่าง ๆ เพื่อบรรลุ วัตถุประสงก์ของ Scenario ต่าง ๆ เพื่อให้รับความรู้ทาง Offensive Security และ Defensive Security รวมถึง IT Auditing โดยในส่วนของ Offensive Security นั้นจะมีการจำลอง VM ทั้งหมด 2 ตัว โดย จะแบ่งออกตามนี้กือ VM เครื่องที่ 1 คือ เครื่องเป้าหมายที่มีช่องโหว่ชนิดต่าง ๆ ฝังเอาไว้ และ VM เครื่องที่ 2 คือเครื่องที่เป็นระบบปฏิบัติการ Kali Linux 2 เอาไว้ใช้สำหรับ ทำการ Hacking เพื่อหา ช่องโหว่ของ VM เครื่องที่ 1 ที่ได้กล่าวไป โดยในการเข้าถึงช่องโหว่ของเครื่องเป้าหมายนั้นจะ ได้รับ Flag ที่เป็นกำตอบของScenario นั้น ๆ จะมาในรูปแบบของข้อความเป็นหลัก และในส่วน ของ Defensive Security นั้น จะเป็นการจำลองเครื่อง VM ที่มีช่องโหว่เกิดขึ้น โดยผู้ใช้จะต้องหา ช่องโหว่ดังกล่าวให้เออและแก้ไขมันให้ถูกต้องตรงตามวัตถุประสงก์ของ Scenario ที่กำหนด และ ในส่วนของ IT Auditing นั้น ลือการตรวจสอบระบบ จะมีรูปแบบคือ การให้ผู้ใช้งาน ทำการ Checking Environment ทาง Security list ของ เครื่องเป้าหมาย ตาม รายการที่ให้มาว่าตรงตาม รายการที่กำลังทำการ Auditing หรือไม่

3.3 ขั้นตอนการดำเนินงานที่นักศึกษาปฏิบัติงาน

งานที่ได้รับมอบหมายจากบริษัท ไซเบอร์ตรอน จำกัด ในช่วงสหกิจศึกษาเป็นระยะเวลา 18 สัปหาด์นั้น งานส่วนมากเป็นงานพัฒนาและปรับระบบ Cyber RANGE เป็นหลักและงานอื่น ๆ จะ เป็นงานทางด้าน Incident Response ของห้องปฏิบัติการ Security Operation Center ของแผนก Cyber 911

โดยในหัวข้อ 3.3 จะขอกล่าวเพียงแก่ขั้นตอนการคำเนินงานโครงการเท่านั้นนั้นอัน เนื่องมาจาก งานที่ได้รับมอบหมายชิ้นอื่น ๆ ทางบริษัทฯ ที่ไปสหกิจศึกษาไม่อนุญาตให้นำมาใส่ใน รายงานสหกิจศึกษา ดังนั้นส่วนของขั้นตอนการคำเนินงานโครงการนั้นจะกล่าวเพิ่มเติมในหัวข้อ 3.3.1 โดยจะครอบกลุมในส่วนของขั้นตอนการคำเนินงานโครงการภายใต้ระบบเสมือน หรือ VM ผ่านโปรแกรม VMware Workstation เพียงนั้น ในส่วนของการอธิบายการนำระบบที่ทดสอบเสร็จ สิ้น deploy ขึ้น VMware ESXi ของทางบริษัทนั้นจะขอกล่าวเพียง กระบวนการและขั้นตอนการ ปฏิบัติ

3.3.1 ขั้นตอนการดำเนินงานโครงการ

ในการพัฒนาและปรับปรุงระบบ Clientless Remote Desktop Gateway และ VNC สำหรับ ระบบ Cyber RANGE นั้นจะมีกระบวนการอธิบายขั้นตอนการคำเนินงานต่าง ๆ ดังนี้ โดยจะอธิบาย แจกจงเป็นรูปแบบของการทฤษฎี SDLC เป็นหลัก

1) วิเคราะห์ความต้องการ (Requirement Analysis)

เนื่องมาจากระบบ Clientless Remote Desktop Gateway ของระบบ Cyber RANGE นั้นได้ มีการใช้งานอยู่แล้วแต่เป็นระบบที่เกิดปัญหาก่อนข้างเยอะอย่างเช่น ไม่สามารถรองรับจำนวน host ได้มากเพียงพอ โดยถ้าเกิดเหตุการที่ ผู้เข้าที่เป็น host เข้ามาใช้งานระบบ จะเกิดปัญหาด้าน traffic ของระบบเครือข่ายทำให้ ระบบ Clientless Remote Desktop Gateway เกิดอาการค้างหรือใช้งาน ไม่ได้ ชั่วคราว เป็นเหตุทำให้ส่งผลต่อการใช้งานระบบของผู้เล่น

นอกจากนี้ยังมีปัญหาในส่วนของการ remote เข้าไปยังระบบปฏิบัติการ Kali Linux 2 ใน ระบบซึ่งจะพบปัญหาว่าไม่สามารถเปิดใช้งาน โปรแกรมดังต่อไปนี้

- 1) Browser Mantra ไม่สามารถเปิดใช้งานได้
- 2) Wireshark ไม่สามารถเปิดใช้งานได้
- 3) OpenVAS ไม่สามารถเปิดใช้งานได้

ในส่วนของปัญหาที่กล่าวไปในบทที่ 1 และกล่าวเพิ่มเติมเมื่อข้างต้นนั้น ได้นำปัญหา ดังกล่าวมาปรึกษาร่วมกับพนักงานในแผนกและส่งปัญหาเข้าที่ประชุมของแผนก ซึ่งผลสรุปของ การประชุมนั้นได้ข้อสรุปว่า ระบบ Cyber RANGE นั้นมีปัญหาหลาย ๆ อย่าง ซึ่งได้แจกแจงข้อสรุป ทั้งหมดดังนี้

1) ปัญหาโปร<mark>แกร</mark>มไม่สาม<mark>า</mark>รถแ<mark>สดงผล</mark>ได้ถูก<mark>ต้อง</mark>ขณะใช้งาน remote ไปยัง ระบบปฏิบัติการ <mark>Kali</mark>

Linux

- 2) ปัญหาในเรื่องการ limited convergent ของการใช้งานระบบ Cyber RANGE ผ่านระบบ
- Clientless Remote Desktop Gateway

 ปัญหาในเรื่อง Access Control ของระบบ Clientless Remote Desktop Gateway ที่ไม่ สามารถ

จัดการ หมวดหมู่และจัดทำระบบ Authority ได้

4) ปัญหาการ develop recorder function ของระบบ Clientless Remote Desktop Gateway จากข้อสรุปปัญหาจากการประชุมนั้น ได้มีแนวทางการวิเคราะห์ปัญหาโดยอ้างอิง security policy ของทางบริษัทนั้นทางฝ่ายพนักงานของแผนก มีวัตถุประสงค์ที่ในการอยากแก้ไขปัญหา พร้อมทั้งเสริมความปลอดภัยให้กับตัวระบบควบคู่ไปด้วย ดังนั้นในการออกแบบนั้นจะเสริมใน ส่วนของ ความปลอดภัยของระบบ

2) การออกแบบ (Design)

(

เมื่อสรุปบึญหาที่พบเจอในระบบ Cyber RANGE อย่างแน่ชัดแล้วตามในหัวข้อ การ วิเกราะห์ความต้องการ หลังจากนั้นจะนำปัญหาต่าง ๆ มาทำการแจกแจงเพื่อหาแนวทางการแก้ไขที่ มีความเป็นไปได้มากที่สุด

> การออกแบบแนวทางการแก้ไขปัญหาของโปรแกรมไม่สามารถแสดงผลได้ ถูกต้องขณะใช้งาน remote ไปยัง ระบบปฏิบัติการ Kali Linux

ในส่วนของการออกแบบวิธีแก้ไขปัญหาในข้อนี้ขั้นแรกได้มีการจัดการค้นคว้าแนวทางการ แก้ไขซึ่งได้มีรายละเอียดข้อมูลทางเทคนิคของปัญหาคือ ระบบปฏิบัติการ Kali Linux 2 ตัวเก่านั้น ได้มีการติดตั้งบริการ Tight VNC ที่มีการใช้งาน Desktop Environment ซึ่งชื่อว่า XFCE ไว้แล้ว ซึ่ง อ้างอิงจากสมมุติฐานได้ข้อสรุปว่า การที่เกิดปัญหาของโปรแกรม Browser OWASP Mantra และ Wireshark และ OpenVAS ไม่สามารถทำงานได้ตามปกตินั้นอาจจะเกิดสาเหตุ เพราะมีการใช้งาน Desktop Environment ที่มีชื่อว่า XFCE ซึ่งอาจเป็นสาเหตุของปัญหา ตามรูปภาพที่ 3.1 ที่แสดงการ ใช้งาน Tight VNC ด้วย Desktop Environment ที่มีชื่อว่า XFCE



ภาพที่ 3.1 หน้าจอการจำลอง ระบบปฏิบัติการ Kali Linux ที่ใช้ tight VNC แบบ XFCE

จากรูปภาพที่ 3.1 นั้น ได้มีการศึกษาการทำงานของ Tight VNC จนเกิดสมมุติฐานในเรื่อง ของการใช้งาน เนื่องจาก Tight VNC จำเป็นต้องใช้ Desktop Environment มาคอยประมวลผลใน การ remote แยกส่วนอีกที่ไม่ได้มีการนำ native desktop มาใช้งานโดยตรง ด้วยเหตุผลนี้อาจจะเป็น สาเหตุหลักทำให้เกิดปัญหาที่น่าจะเป็นไปได้มากที่สุด

10

ในการค้นหาแนวทางการแก้ไขปัญหานั้น โดยวางแผนไว้ว่าจะทดลองนำบริการ VNC ของ แต่ละผู้บริการมาทำการทดสอบร่วมกับระบบ Cyber RANGE ซึ่งกระบวนการนี้อาจจะใช้เวลานาน เนื่องจาก ผู้ให้บริการ VNC นั้นมีหลากหลายส่งผลให้ในการทดลองใช้บริการของแต่ละ ผู้ให้การ นั้นอาจจะใช้เวลาก่อนข้างนาน อย่างไรก็ตาม ถ้า environment ที่ใช้ทดลองร่วมด้วยนั้นมีลักษณะ ชัดเจน จะสามารถเลือกใช้ บริการ VNC ของผู้ให้บริการต่าง ๆ ได้เจาะจงมากยิ่งขึ้น

จากเหตุผลที่กล่า<mark>วไป</mark> ทำให้มีการกันกว้าหาบริการ VNC จากผู้ให้บริการต่าง ๆ โดยจะแจก แจงผู้ให้บริการ VNC ที่มีแนวโน้มสามารถทำงานร่วมกับระบบ Cyber RANGE ได้มากที่สุดตาม ตารางที่ 3.2

34

ลำคับ	ชื่อบริการ	จุดเด่น
1	UltraVNC	Open source และมีการ configuration ที่ไม่ซับซ้อน
2	Tiger VNC	Open source และมี performance ที่ดี
3	X11VNC	Open source
4	Vino	ติดตั้งและ configuration ง่ายเพราะเป็นของ GNOME
5	Real VNC	Commercial และมีระบบ Access Control และมีการ Configuration ที่หลากหลาย
6	NoMachine	Commercial และมีการ Configuration ที่หลากหลาย

ตารางที่ 3.2 แสดงรายชื่อบริการของ VNC ที่คาดว่ามีแนวโน้มสามารถทำงานร่วมกับระบบ

จากตารางที่ 3.2 สามารถบอกรายชื่อผู้ให้บริการ VNC จากหลาย ๆ ผู้ให้บริการที่มี แนวโน้มสามารถทำร่วมกับระบบ Cyber RANGE รวมถึงแสดงจุดเด่นของผู้ให้บริการนั้น ๆ เพื่อ นำมาตัดสินใจในการนำมาใช้ต่อไป

(2) การออกแบบแก้ไขปัญหาในเรื่องการ limited convergent ของการใช้งานระบบ
 Cyber RANGE ผ่านระบบ Clientless Remote Desktop Gateway

ในส่วนของการออกแบบวิธีแก้ไขปัญหาในข้อนี้ ขั้นแรกนั้นจากการที่วิเคราะห์ปัญหา พบว่า ระบบ Cyber RANGE ในส่วนของ การเข้า remote ผ่านระบบ Clientless Remote Desktop Gateway ของผู้ใช้งานหรือ host นั้นจากการทดสอบร่วมกับพนักงานในแผนกพบว่า เมื่อผู้ใช้งานใช้ งานเกิน 50 คนขึ้นไปนั่น ระบบ Clientless Remote Desktop Gateway จะเริ่มทำงานผิดพลาดและ แม่นยำน้อยลง เนื่องมาจาก จำนวน traffic ที่ไม่มีการทำกระบวนการ load balance ใด ๆ ใน flow control ของ Infrastructure

จากเหตุผลที่กล่าวไปก่อนหน้านั้น ได้กำหนดสมมุติฐานและข้อมุลที่ได้จากการค้นคว้า พบว่าเครื่องมือ reverse proxy มีแนวโน้มในการสามารถแก้ไขปัญหานี้ได้ เนื่องจากกระบวนการ ของ reverse proxy นั้นคือการทำกระบวนการ load balance traffic ซึ่งจะช่วยให้ traffic มีสภาพ คล่องตัวในการโยกย้ายมากยิ่งขึ้น อีกทั้งเครื่องมือ reverse proxy นั้นสามารถ ปรับแต่ง การทำงาน ได้โดยมีลักษณะค่อนข้างยืดหยุ่น ทำให้เหมาะสมกับระบบ Infrastructure ส่วนใหญ่

ดังนั้น จากผลลัพธ์ของการค้นคว้ารวมถึงได้ประชุมร่วมกับพนักงานในแผนกสรุปได้ว่า ผู้ ให้บริการเครื่องมือ reverse proxy พบว่า ผู้ให้บริการที่มี product ที่ชื่อว่า Nginx มีแนวโน้มความ เป็นไปได้ในการสามารถนำมาใช้ร่วมกับ Infrastructure ของระบบ Cyber RANGE มากที่สุด



ภาพที่ 3.2 Diagram ของ Reverse Proxy ที่ออกแบบ

จากภาพที่ 3.2 นั้นได้แสดงให้เห็นถึง diagram infrastructure ที่ออกแบบไว้โดยมีการนำ Nginx มาใช้ร่วมระหว่างการ remote ผ่าน Clientless Remote Desktop Gateway ผ่านไปยัง VM Kali Linux โดยจากสมมุติฐานที่ได้กล่าวไปนั้น nginx จะสามารถ ทำการ load balance traffic ทำให้ สภาพ traffic มีสภาพที่ยืดหยุ่นมากยิ่งขึ้น

> (3) การออกแบบการแก้ไขปัญหาในเรื่อง Access Control ของระบบ Clientless Remote Desktop Gateway ที่ไม่สามารถจัดการ หมวดหมู่และจัดทำระบบ Authority ได้

ในส่วนของการออกแบบวิธีแก้ไขปัญหาในข้อนี้ ขั้นแรกนั้นจากการที่วิเคราะห์ปัญหา พบว่า ระบบ Clientless Remote Desktop Gateway ที่ถูกนำมาใช้งานร่วมกับระบบ Cyber RANGE นั้นไม่ได้มีการจัดการส่วนของกระบวนการ User Access Control ทำให้ในการจัดการในส่วนของ User Management นั้นจะจัดการได้ก่อนข้างยากลำบาก เนื่องจากในการกำหนด หมวดหมู่หรือ role ของ user นั้น ในระบบเก่า ไม่มี function ในการจัดการส่วนนี้ทำให้ ไม่สามารถจัดหมวดหมู่ของ ผู้ใช้งานได้ รวมถึงใช้การระบบ role-based ก็ไม่สามารถใช้งานได้ ทำให้การพัฒนาระบบ Cyber RANGE เป็นไปอย่างลำบากเนื่องจากไม่สามารถ ยืนยันได้ว่าผู้ใช้งานระบบนั้น มีสิทธิสถานะอะไร เมื่อใช้งานระบบ Clientless Remote Desktop Gateway ตามเหตุผลที่กล่าวไปทำให้นั้น จากการค้นคว้าพบว่า Apache Guacamole 0.9.12-incubating นั้นมี ระบบ User Access Control เป็นแบบ RBAC หรือ Role-Based Access Control ทำให้สามารถจัดการ User Management ง่ายมากยิ่งขึ้น โดยอ้างอิงตามสมมุติฐานที่กิดไว้

(4) การออกแบบการแก้ไขปัญหาการ develop recorder function ของระบบ Clientless
 Remote Desktop Gateway

ในส่วนของการออกแบบวิชีแก้ไขปัญหาในหัวข้อนี้นั้น ขั้นแรกจากการที่วิเคราะห์ปัญหา พบว่า ระบบ Clientless Remote Desktop Gateway ที่ถูกนำมาใช้งานร่วมกับระบบ Cyber RANGE นั้นไม่ได้มีส่วนของการ recorder VDO ผ่าน Remote Desktop Service ใด ๆ จากการวิเคราะห์กวาม ต้องการที่กล่าวไปนั้นหัวหน้างานประจำแผนก มีความต้องการ function recorder VDO ผ่าน Remote Desktop Service ซึ่งจากการก้นคว้านั้น พบว่า Apache Guacamole 0.9.12-incubating นั้นมี function ในการ record VDO ผ่าน Remote Desktop Service เช่น RDP VNC รวมถึง SSH เป็นต้น หลังจากการนำเสนอหัวข้อปัญหานี้เข้าที่ประชุมนั้นได้ข้อสรุปการออกแบบการแก้ไขปัญหาใน หัวข้อนี้ว่า ควรนำ Apache Guacamole 0.9.12-incubating มาใช้งานร่วมกับระบบ Cyber RANGE โดยดำเนินงานตามเหตุผลที่อ้างอิงตาสมมุติฐานที่ได้วางไว

3) การพัฒนาและปรับปรุงระบบ (Development and Implementation)

10

งอบเงตการพัฒนาและปรับปรุงระบบโดยได้กำหนดงอบเงตงองการพัฒนาและปรับปรุง ระบบ ตามการออกแบบที่กล่าวไปข้างต้นโดยการพัฒนาและปรับปรุงบนระบบเสมือน (VM) ด้วย โปรแกรม VMware Workstation โดยมีการกำหนด VM ดังนี้

- VM เครื่องที่ 1 ระบบปฏิบัติการ Ubuntu Server 14.04 32 bit (LTS) โดยจะทำการถงขชุด โปรแกรม Apache Guacamole 0.9.12-incubating
- 2) VM เครื่องที่ 2 ระบบปฏิบัติการ Kali Linux 2 64bit (Rolling) โดยจะทำการถงโปรแกรมReal VNC Connect 6.2

หลังจากนั้นจะคำเนินการเชื่อมต่อระหว่างกันผ่านเครือข่าย VM network ภายใต้ VMware Workstation PRO 12 เพื่อทำการทคลองให้บรรลุวัตถุประสงค์และแก้ไขปัญหา ที่กำหนดไว้ในบท ที่ 1 ในส่วนของขั้นตอนการพัฒนาและปรับปรุงระบบในหัวข้อนี้จะแบ่งออกเป็น ขั้นตอนการ พัฒนาและปรับออกเป็น 2 ส่วนตามขอบเขตที่กำหนดเอาไว้ก่อนหน้านี้

ขั้นตอนการติดตั้งระบบ Clientless Remote Desktop Gateway (VM เครื่องที่ 1)

โดยในขั้นตอนแรกนั้นจะทำการติดตั้ง ระบบปฏิบัติการ Ubuntu Server 14.04 (Trusty Tahr) 32 bit เพื่อเอาไว้ใช้เป็นระบบปฏิบัติการในการรองรับ ชุดโปรแกรม Apache Guacamole 0.9.12-incubating กับ โปรแกรม Nginx ที่เป็น reverse proxy ขั้นตอนการติดตั้งระบบปฏิบัติการ Ubuntu Server 14.04 (Trusty Tahr) LTS 32bit

Name.	Obulitu 14.04_Cilentiess_Remote_Desktop_Gateway
Location	D:\\/Mc\CoonCuacamolo
Version:	Workstation 14 v
Operating S	ystem: Ubuntu
Hard Disk:	10 GB, Split
Memory:	102 <mark>4 MB</mark>
Network Ad	pter: NAT
Other Devic	es: 2 CPU cores, CD/DVD, USB Controller, Printer, Sound C

ภาพที่ 3.3 การกำหนดรายละเอียด Virtual Hardware สำหรับระบบปฏิบัติการ Ubuntu Server

< Back

Finish

Cancel

10

14.04

จากภาพที่ 3.3 จ<mark>ะทำก</mark>ารกำหนดรายละเอียด Virtual Hardw</mark>are เพื่อใช้สำหรับการสร้าง VM ก่อนติดตั้งระบบปฏิบ<mark>ัติกา</mark>ร Ubuntu Server 14.04 32 bit บน<mark>โปรเ</mark>เกรม VMware Workstation

🔟 Ubuntu 14.04	4_Clientless_Rem	ote_Desktop_Gateway	- VMware Workstation	- 🗆	×
Workstation 🔻					
ⓓ Home ×	🕞 Ubuntu 14.04	4_Clientless_Re ×			
		Lar	nguage		
	Amahic Anabic Asturianu Bengali Tibetan Bosanski Català Čeština Dansk Deutsch Dzongkha EXApruká English Esperanto Espeñol Espeñol Espeñol Suomi	rrangais Gaeilge Galego Gujarati חירlu Hindi Hrvatski Magyar Bahasa Indonesia Íslenska Italiano 日本語 うらのjeo Kasak Khmer 考えてえた 覚국어 Kurdí Lao Lietuviškai Latviski	Malayalam Malayalam Marathi Burmese Nepali Nederlands Norsk pynorsk Punjabi (Burmukhi) Polski Português do Brasil Português do Brasil Português Română Pyccxwû Sâmegilli Sâmegilli Samegilli Sovenšcina Slovenšcina Slovenšcina Slovenšcina Slovenšcina Slovenšcina Slovenšcina	Tail G [*] Oxix Thai Tagalog Türkçe Uyghur Ykpaïнcьka Tiếng Việt 中文(衛体) 中文(繁體)	

ภาพที่ 3.4 การติดตั้งระบบปฏิบัติการ Ubuntu Server 14.04 (1)

จากรูปภาพทที่ 3.4 เป็นการเลือกภาษาที่ใช้ในการเตรียมพร้อมในการติดตั้ง ระบบปฏิบัติการ Ubuntu Server 14.04

10



ภาพที่ 3.5 การติดตั้งระบบปฏิบัติการ Ubuntu Server 14.04 (2)

Ubuntu 14.04_Clientless_Remote_Desktop_Gateway - VMware Workstation - 🗆 🗙
File Edit View VM Tabs Help 📕 🗸 🖶 💭 💭 💭 🖬 🗔 🛱 🔯 🛅
Home × Bubuntu 14.04_Clientless_Re ×
[1] Configure the network Please enter the hostname for this system. The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here. Hostname: Ubuntu <go back=""> <continue></continue></go>
<tab> moves; <space> selects; <enter> activates buttons</enter></space></tab>
To direct input to this VM, click inside or press Ctrl+G. 📮 🕤 🔄 🚽 🖉 📄 🥠 👌 📔 💭

40

ภาพที่ 3.6 การติดตั้งระบบปฏิบัติการ Ubuntu Server 14.04 (3)

TC

ภาพที่ 3.5 เลือก Install Ubuntu เพื่อเข้าสู่กระบวนการติดตั้ง หลังจากเลือกภาษาที่ใช้ในการ ติดตั้งเสร็จ โดย หลังจากนั้นจะมีการตั้งค่าเกี่ยวกับ keyboard ให้ตั้งค่าให้เป็นภาษา English ทั้งหมด หลังจากนั้นจะเข้าสู่การตั้งค่าชื่อเครื่องหรือ host name ตามรูปภาพที่ 3.6 หลังจากนั้นจะเข้าสู่ กระบวนการตั้ง password ตาม<mark>ลำดับ</mark>



ภาพที่ 3.7 การติดตั้งระบบปฏิบัติการ Ubuntu Server 14.04 (4)

หลังจากนั้นจะเป็นการ การเลือกที่จะเข้ารหัส home directory เนื่องจากเป็นเซิฟเวอร์ ที่ นำไปใช้งานร่วมกับ ระบบ Cyber RANGE ทำให้จำเป็นต้อง เข้ารหัส เพราะควรคำนึงถึงเรื่องความ ปลอดภัยเป็นหลัก

(0)



ภาพที่ 3.8 การติดตั้งระบบปฏิบัติการ Ubuntu Server 14.04 (5)

หลังจากนั้นจะเป็นการค่าเกี่ยวกับ การแบ่ง partition เนื่องจากได้มีการจัดสรรเรื่อง hardware ให้กับ VM ในเรื่องของ storage แค่ลุกเดียวทำให้ไม่เป็นปัญหากับการติดตั้ง ซึ่งสามารถ เลือกได้ตามปกติ



ภาพที่ 3.9 การติดตั้งระบบปฏิบัติการ Ubuntu Server 14.04 (6)

10

หลังจากนั้นจะเป็นการคำเนินการการตั้งค่า ของกระบวนการในภาพที่ 3.8 แล้วระบบจะเริ่ม กระบวนการ โดยจะเริ่มทำการแตก ไฟล์การติดตั้งและนำ repositories ต่าง ๆ จองพื้นที่ใน storage ของ VM เมื่อเสร็จสิ้นระบบจะทำการ restart แล้วจะขึ้นหน้าจอตามภาพที่ 3.9 หลังจากนั้นผู้ใช้ สามารถเริ่ม login ได้โดยรายละเอียดการ login เพื่อเข้าสู่ระบบนั้น account ในการ login นั้นจะ อ้างอิงตามที่ได้กำหนดไว้ตอนติดตั้งระบบปฏิบัติการเมื่อขั้นตอนก่อนหน้านี้ หลังจากนั้นโดยให้ใส่ username และ password ตามที่ได้ตั้งไว้ในขั้นตอนการติดตั้ง เมื่อใส่ username และ password เพื่อ login เข้าระบบ ก็สามารถใช้งานได้ตามปกติ

หมายเหตุ: เนื่องจากตอน login จะlogin เข้าระบบในสิทธิของ user ที่ตั้งไว้ซึ่ง ถ้าผู้ใช้งานต้องการใช้ งานสิทธิ root user ให้ เรียกใช้ command sudo -su จำทำการ ยกระดับสิทธิเป็น root user

WSTITUTE O

ขั้นตอนการติดตั้งชุดโปรแกรม Apache Guacamole 0.9.12-incubating

หลังจากคำเนินการติดตั้งระบบปฏิบัติการ Ubuntu Server 14.04 LTS 32 bit ในขั้นตอน ก่อนหน้านี้แล้วนั้น ในขั้นตอนการติดตั้ง ชุดโปรแกรม Apache Guacamole 0.9.12-incubating นั้น จะต้องมีการจัดเตรียมโปรแกรมต่าง ๆ รวมถึง library ที่จำเป็นต้องใช้ในการติดตั้งชุดโปรแกรม Apache Guacamole 0.9.12-incubating หลังจากนั้นจะทำการ download package ชุดโปรแกรมซึ่ง ประไปด้วยสองส่วนดังนี้

- 1) Apache-Guacamole-Server
- 2) Apache-Guacamole-Client

10

และ download package ในส่วนของการ authentication ที่ใช้ในส่วนของหน้าเว็บ ในส่วน ของ Apache-Guacamole-Client หลังจากนั้นก้จะจัดเตรียม environment ภายในระบบปฏิบัติการ ให้พร้อมสำหรับติดตั้งชุดโปรแกรม พอเสร็จขั้นตอนนี้ก็จะเริ่มขั้นตอนการติดตั้งชุดโปรแกรม ใน ส่วนของ Apacha-Guacamole-Server เพื่อลงสิ้นสิ้นจะเริ่มทำการ configuration ตัวชุดโปรแกรม ให้ เหมาะสมและสามารถทำงานร่วมกับ web server tomcat7 และระบบเครือข่ายได้ หลังจากนั้นจะ ดำเนินการติดตั้ง Apache-Guacamole-Client ที่มีลักษณะ web-based ซึ่งในส่วนของขั้นตอนนี้นั้น สามารถ develop เองได้ทั้งหมดโดยจะกล่าวเพิ่มเติมในหัวข้อ หมายเหตุในส่วนถัดไป

หมายเหตุ: ในการติดตั้งชุดโปรแกรม ทั้งหมดนั้นจะเป็นการติดตั้งในรูปแบบของ Unix Command และในการติดตั้งชุดโปรแกรม Apache Guacamole 0.9.12-incubating ในส่วนของ Client ที่มี รูปแบบหน้าเว็บไซต์นั้นส่วนนี้ นักพัฒนาสามารถ develop หน้าเว็บต์ด้วยตนเองได้ทั้งหมด โดย สามารถหาข้อมูลเพิ่มเติมได้ในการพัฒนาให้หน้าเว็บขึ้นมาใหม่ให้เชื่อมโยงกับ ส่วน Apache-Guacamole-Server

ตารางที่ 3.3 แสดงรายกา<mark>ร โป</mark>รแกรมและ รายการ Libraries ต่าง ๆ ที่จำเป็นสำหรับในการลงชุด โปรแกรม Apache Guacamole 0.9.12-incubating

รายชื่อ dependencies ที่ต้องติดตั้ง	UNIX Command
รายชื่อ Libraries	
build-essential	apt-get install -y build-essential
libcairo2-dev	apt-get install -y libcairo2-dev
libjpeg-turbo8-dev	apt-get install -y libjpeg-turbo8-dev

รายชื่อ dependencies ที่ต้องติดตั้ง	UNIX Command
libossp-uuid-dev	apt-get install -y libossp-uuid-dev
libavcodec-dev	apt-get install -y libavcodec-dev
libavutil-dev	apt-get install -y libavutil-dev
libswscale-dev	apt-get install -y libswscale-dev
libfreerdp-dev	apt-get install -y libfreerdp-dev
libpango1.0-dev	apt-get install -y libpango1.0-dev
libssh2-1-dev	apt-get install -y libssh2-1-dev
libtelnet-dev	apt-get install -y libtelnet-dev
libvncserver-dev	apt-get install -y libvncserver-dev
libpulse-dev	apt-get install -y libpulse-dev
libssl-dev	apt-get install -y libssl-dev
libvorbis-dev	apt-get install -y libvorbis-dev
libwebp-dev	apt-get install -y libwebp-dev
รายชื่อ Programs	6
mysql-server	apt-get install -y mysql-server
mysql-client	apt-get install -y mysql-client
mysql-common	apt-get install -y mysql-common
mysql-utilities	apt-get install -y mysql-utilities
tomcat7	apt-get install -y tomcat7
freerdp	apt-g <mark>et</mark> instal <mark>l -y f</mark> reerdp
ghostscript	apt-get install -y ghostscript
jq	apt-get install -y jq
wget	apt <mark>-get</mark> instal <mark>l -y w</mark> get
curl	apt-get install -y curl
dpkg-dev	apt-get install -y dpkg-dev

ตารางที่ 3.3 แสดงรายการโปรแกรมและ รายการ Libraries ต่าง ๆ ที่จำเป็นสำหรับในการลงชุด โปรแกรม Apache Guacamole 0.9.12-incubating (ต่อ)

จากตารางที่ 3.3 นั้นแสดงรายละเอียดโปรแกรมและ Libraries ต่าง ๆ ที่จำเป็นในการติดตั้ง รวมถึง Unix Command ที่เป็นคำสั่งใช้ในการดำเนินการติดตั้ง โดยจะมีการแบ่งการติดตั้ง ออกเป็น สองส่วน โดยส่วนแรกคือ ส่วนของ Library ที่ครอบคลุม Remote Desktop Service เช่น VNC RDP ้เป็นต้น และหน้าเว็บไซต์ และส่วนที่สองคือ ส่วนของ Program ต่าง ๆ ที่เกี่ยวข้องกับเว็บไซต์เช่น Tomcat ที่เป็น webserver และ MySOL ที่เป็นฐานข้อมลไว้สำหรับเก็บข้อมลของเว็บไซต์ โดยใน การติดตั้ง MySQL นั้นจำเป็นต้องกำหนด account ในการ login เพื่อทำการ connection ไปยัง ฐานข้อมูล MySQL

หมายเหตุ: ในการติดตั้ง dependencies ที่จำเป็นนั้น ไม่จำเป็นต้องติดตั้งทั้งหมดเนื่องจาก การใช้งาน ของ Library ต่าง ๆ นั้นจะขึ้นตรงกับการออกแบบของผู้พัฒนาเป็นหลัก



To direct input to this VM, click inside or press Ctrl+G.

ภาพที่ 3.10 แสดงให้เห็นการติดตั้งโปรแกรมและ Libraries ในก่อนติดตั้งชุดโปรแกรม

เมื่อติดตั้ง โปรแกรมและ Libraries ต่าง ๆ ที่จำเป็นในการติดตั้งชุดโปรแกรมเสร็จสิน ใน ส่วนถัดไปจะเป็นขั้นตอนการติดตั้ง download ชุดโปรแกรม และทำการติดตั้ง

ตารางที่ 3.4 แสดงให้เห็นรายการการ download package ชุดโปรแกรม Apache Guacamole 0.9.12incubating เพื่อใช้สำหรับการติดตั้ง

รายชื่อ package ที่ต้อง download	UNIX Command
guacamole-client-0.9.12-incubating.tar.gz	wget
	http://apache.org/dyn/closer.cgi?action=download
	&filename=incubator/guacamole/0.9.12-
	incubating/source/guacamole-client-0.9.12-
	incubating.tar.gz
guacamole-server-0.9.12-incubating.tar.gz	wget http://apache.org/dyn/closer.cgi?action=download
	&filename=incubator/guacamole/0.9.12-
	incubating/source/guacamole-server-0.9.12-
	incubating.tar.gz
guacamole-0.9.12-incubating.war	wget
	http://apache.org/dyn/closer.cgi?action=download
	&filename=incubator/guacamole/0.9.12-
	incubating/binary/guacamole-0.9.12-
	incubating.war
guacamole-auth-jdbc-0.9.12-incubating.tar.gz	wget
	http://apache.org/dyn/closer.cgi?action=download
	&filename=incubator/guacamole/0.9.12-
	incubating/binary/guacamole-auth-jdbc-0.9.12-
	incubating.tar.gz
mysql-connector-java-5.1.43 <mark>.tar.g</mark> z	wget
	https://dev.mysql.com/get/Downloads/Connector-
	J/mysql-connector-java-5.1.43.tar.gz

จากตารางที่ 3.4 ได้อธิบายรายการการ download ชุดโปรแกรมเพื่อเตรียมพร้อมสำหรับ กระบวนการติดตั้งซึ่งมีลักษณะ zip file โดยรายละเอียด package ต่าง ๆ นั้นจะมีการอธิบายดังนี้ guacamole-client-0.9.12-incubating.tar.gz คือ package สำหรับ ติดตั้ง ส่วนของ Apache-Guacamole-Client ที่เป็นส่วนการรับค่าการตั้งค่าและควบคุมระบบฯ ผ่าน web-based โดยในส่วนนี้ นั้นนักพัฒนาสามารถ develop หน้าเว็บด้วยตนเองได้หรือจะเลือกใช้ หน้าเว็บสำเร็จรูปที่ทาง Apache ให้มาก็ได้

guacamole-server-0.9.12-incubating.tar.gz คือ package สำหรับการติดตั้งส่วนของ Apache-Guacamole-Server ที่เป็นส่วนของการประมวลผลและการจัดการ Remote Desktop Service ต่าง ๆ อาทิ VNC, RDP เป็นต้นโดยกวบคุมผ่าน โปรโตกอลส่วนตัวที่มีชื่อวา guacamole protocol และสั่งการผ่าน UNIX Command ที่มีชื่อว่า guacad

guacamole-0.9.12-incubating.war คือ package สำหรับการติดตั้ง หน้าเว็บสำเร็จรูปของทาง Apache ที่ถูกจัดเตรียมมาให้ โดยweb application นี้มีวัตถุประสงก์เพื่อ ควบกุมและจัดการการตั้งก่า ต่าง ๆ ผ่าน web-based ซึ่ง web application สำเร็จรูปนี้มีให้สำหรับ กรณีที่ นักพัฒนา มีความต้องการ ที่จะติดตั้ง Apache Guacamole แต่ไม่ต้องการที่จะพัฒนาหน้าเว็บสำหรับระบบ

guacamole-auth-jdbc-0.9.12-incubating.tar.gz คือ package สำหรับการติดตั้ง ระบบการ authentication รูปแบบหนึ่ง ที่จำเป็นต้องใช้งานร่วมกับ Apache-Guacamole-Client โดยในส่วนของ package นั้นมีการ authentication ในรูปแบบของ Database authentication โดยผู้พัฒนาสามารถ เลือกการ authentication รูปแบบอื่น ๆ โดยตัวเลือก authentication อื่นๆ คือ LDAP คือการ authentication แบบกระบวนการ LDAP, NoAuth คือการไม่มีการ Authentication ใด ๆ ในระบบ, Duo คือการใช้การ Authentication แบบชุด Key-Pair เป็นต้น เนื่องจากขอบเขตของเทคโนโลยีที่ได้ ปรึกษาร่วมกับพนักงานที่บริษัทนั้น ได้มีข้อสรุปว่าจะมีการเลือกใช้ การ authentication แบบ Database ดังนั้นจึงเลือกใช้ Package guacamole-auth-jdbc-0.9.12-incubating.tar.gz

10

mysql-connector-java-5.1.43.tar.gz คือ package มีลักษณะเป็น โปรแกรมที่ใช้สำหรับการ เชื่อมต่อระหว่าง Apache-Guacamole-Client กับฐานข้อมูล MySQL โดยจะทำหน้าที่ติดต่อสื่อสาร และสร้าง transaction ระห<mark>ว่างก</mark>ันเพื่อป้องกันการเกิดปัญห</mark>าต่าง ๆ

หมายเหตุ: หลังจาก download ชุดโปรแกรมต่าง ๆ เสร็จสินนั้น package ที่ถูก download จะมี รูปแบบ zip file นามสกุล .tar.gz เป็นหลัก ดังนั้นจำเป็นต้อง แกะไฟล์ด้วย UNIX Command #tar xzf package.tar.gz หลังจากเสร็จสิ้นการ download ก็จะเข้าสุ่กระบวนการการจัดการ environment ภายใน ระบบปฏิบัติการให้พร้อมสำหรับการติดตั้งชุดโปรแกรม Apache Guacamole 0.9.12-incubating โดยจะมีกำสั่ง UNIX Command ตามตารางที่ 3.5

ตารางที่ 3.5 แสดงรายการการเตรียมความพร้อมของ environment สำหรับการติดตั้ง Apache Guacamole 0.9.12-incubating ภายในระบบปฏิบัติการ Ubuntu Server 14.04

UNIX Command	ความหมาย
1) mkdir -p /etc/guacamole/lib	สร้างโฟลเคอร์ /etc/guacamole/lib โดยไม่
	ขึ้นข้อความแจ้งเตือนถ้าโฟลเดอร์ดังกล่าวมี
L L L	อยู่แล้ว
2) mkdir -p	สร้างโฟลเดอร์ /etc/guacamole/extensions
/etc/guacamole/extensions	โดยไม่ขึ้นข้อความแจ้งเตือนถ้าโฟลเดอร์
	ดังกล่าวมีอยู่แล้ว

จากตารางที่ 3.5 แสดงให้เห็นถึงการเตรียมความพร้อมของ environment สำหรับการติดตั้ง Apache Guacamole 0.9.12-incubating ภายในระบบปฏิบัติการ Ubuntu Server 14.04 ซึ่งจะมีการ สร้าง โฟลเดอร์ ด้วยกำสั่ง mkdir และ มี option คือ -p โดยหลังจากสร้างโฟลเดอเสร็จสิ้นแล้ว ขั้นตอนถัดไปจะเป็นการ ติดตั้งชุดโปรแกรมที่ download จากขั้นตอนก่อนหน้า โดยจะมี รายละเอียดการขั้นตอนติดตั้งดังนี้

ตารางที่ 3.6 แสดงรายการกำสั่งขั้นตอนการติดตั้ง ชุดโปรแกรม Apache Guacamole 0.9.12incubating

UNIX Command	<mark>ค</mark> วามหมาย
(optional) cd guacamole <mark>-serv</mark> er-0.9.12-	เข้าไ <mark>ป</mark> ยัง folder guacamole-server-0.9.12-
incubating	incubating
1) ./configurewi <mark>th-in</mark> it-dir=/etc/init.d	ก <mark>ารเต</mark> รียมคว <mark>ามพ</mark> ร้อมการตั้งค่าในพารามิเตอร์
	ini.d
2) make	compile package ที่เป็นภาษา JAVA
3) make install	การติดตั้ง package ที่เป็นภาษา JAVA
4) systemctl enable guacd	สั่งการให้ repository guacd ทำงานแบบ
	startup

จากตารางที่ 3.6 แสดงให้เห็นถึงขั้นตอนการติดตั้งชุดโปรแกรม โดยในส่วนของ optional นั้นคือ กรณีที่ root ไม่ได้อยู่ใน โฟลเดอร์ของตัวชุดโปรแกรม โดยถ้าอยู่ในโฟลเดอร์ถึงชุด โปรแกรมอยู่แล้ว ก็สามารถดำเนินการขั้นตอนการติดตั้งได้ตามปกติ หมายเหตุ: ในขั้นตอนการติดตั้ง ของตารางที่ 3.6 นั้น ในส่วนของการ ติดตั้ง ห้ามมีกระบวนการใด ใดในการ ประมวลผล package แสดงการเกิด error เด็ดขาด ถ้ากรณีที่เกิดการ error ในกระบวนการ ใด กวรตรวจสอบ file ชุดโปรแกรมเบื้องต้น เช่น เรื่องของกวามสมบุรณ์ของไฟล์ เป็นต้น

หลังจากติดตั้ง ชุดโปรแกรม Apache Guacamole 0.9.12-incubating เสร็จสิ้นแล้วนั้นใน กระบวนการถัดไปคือการจัดเตรียม web application สำหรับ Apache-Guacamole-Client โดยมี ขั้นตอนการเตรียมการดังนี้

enent	
UNIX Command	ความหมาย
1) mv guacamole-0.9.12-incubating.war	นำไฟล์ guacamole-0.9.12-incubating.war
/etc/guacamole/guacamole.war	ย้ายไปใน directory /etc/guacamole/ โดย
	เปลี่ยนชื่อใหม่เป็นชื่อว่า guacamole.war
2) ln -s /etc/guacamole/guacamole.war	สร้างลิ้งค์แบบ symbolic ระหว่าง
/var/lib/tomcat7/webapps/	/etc/guacamole/guacamole.war กับ
	/var/lib/tomcat7/webapps/
3) ln -s /usr/local/lib/freerdp/guac*.so	สร้างลิ้งค์แบบ symbolic ระหว่าง s
/usr/lib/dpkg- <mark>architecture</mark> -	/usr/ <mark>lo</mark> cal/lib/freerdp/guac*.so กับ so
qDEB_BUILD_GN <mark>U_T</mark> YPE/freerd <mark>p</mark> /	/usr/lib/dpkg <mark>- arc</mark> hitecture -
	qDEB_BUILD_GNU_TYPE/freerdp/
4) cp mysql-connector <mark>-java</mark> -5.1.43/my <mark>sq</mark> l-	<mark>คัดถอ</mark> กไฟล์ <mark>cp m</mark> ysql-connector-java-
connector-java-5.1.43-bin.jar	5.1.43/mysql-connector-java-5.1.43-bin.jar
/etc/guacamole/lib/	ใปยัง directory /etc/guacamole/lib/
5) cp guacamole-auth-jdbc-0.9.12-	คัดถอกไฟถ์ guacamole-auth-jdbc-0.9.12-
incubating/mysql/guacamole-auth-jdbc-	incubating/mysql/guacamole-auth-jdbc-
mysql-0.9.12-incubating.jar	mysql-0.9.12-incubating.jar ไปยัง directory
/etc/guacamole/extensions/	/etc/guacamole/extensions/

ตารางที่ 3.7	แสดงถึงการจัดเตรียม	web application	สำหรับส่วนประกอบ	Apache-Guacamole-
	Client			S /

จากตารางที่ 3.7 แสดงให้ถึงขั้นตอนการการจัดเตรียม web application โดยจะมีการอธิบาย โดยอ้างอิงตามหัวข้อของตาราง คือ ในหัวข้อแรกนั้น คือการนำเว็บสำเร็จรุปของทาง Apache ที่มี นามสกุล .war ย้ายไปส่วนของการประมวลผลของระบบ Apache Guacamole เพื่อให้เชื่อมต่อกับ ส่วนของการประมวลผล หลังจากนั้นในหัวข้อที่ 2 และ 3 นั้นคือการเชื่อมลิ้งระหว่าง directory เพื่อ เชื่อมต่อทำให้สามารถโยกย้ายการทำงานไฟล์ระหว่างกันได้ และในข้อที่ 4 จะเป็นการนำโปรแกรม connector ที่มีนามสกุล .jar ของ MySQL มาใช้ร่วมกับ web application โดยนำไปวางในโฟลเดอ lib ของชุด โปรแกรม guacamole และในขั้นตอนที่ 5 นั้นคือการนำ package authentication แบบ database ที่มีนามสกุล .jar โดยได้กำหนดไว้ในหัวข้อ ก่อนหน้านำไปเชื่อมต่อกับระบบ guacamole โดยเป็นนำไปวางในโฟลเดอ extension

กระบวนการถัดไปจะเป็นการกำหนด ชื่อฐานข้อมูลสำหรับประมวลผลของระบบ และนำ schema ต่าง ๆ จากไฟล์ guacamole-auth-jdbc-0.9.12-incubating ทำการ import เข้าไปยังฐานข้อมูล เพื่อกำหนดให้ฐานข้อมูลพร้อมใช้งานในส่วนของการ database authentication ที่กำหนดมาในวิธี ก่อนหน้านี้ โดยขั้นตอนการสร้างฐานข้อมูลนั้นมีตามตารางที่ 3.8

SQL Command	ความหมาย
1) create database guacamole_db;	สร้างฐานข้อมูลที่ชื่อว่า guacamole_db
2) create user	สร้างผุ้ใช้งานที่มีชื่อว่า guacamole_user
'guacamole_user'@'localhost'	โดยอ้างอิงร่วมกับ localhost โดยมี
identified by "P@ssw0rd";	ร <mark>หั</mark> สผ่าน <mark>คือ P</mark> @ssw0rd
3) GRANT	ใ <mark>ห้</mark> สิทธิ ก <mark>ารคว</mark> บคุม SELECT INSERT
SELECT,INSE <mark>RT,</mark> UPDATE,DELETE	บ <mark>P</mark> DATE <mark>DEL</mark> ETE กับผู้ใช้งานชื่อ
ON guacamole_db.* TO	guacamole_user ในฐานข้อมูล
'guacamole_u <mark>ser'@</mark> 'localhost <mark>';</mark>	guacamole_db
4) flush privileges;	Compile สิทธิ
5) cat guacamole-auth-jdbc-0.9.12-	นำค่า schema ทั้งหมด ใส่ใน ฐานข้อมูล
incubating/mysql/schema/*.sql	guacamole_db
mysql -u root -p\$mysqlrootpassword	Or
guacamole_db	
 SELECT,INSERT,UPDATE,DELETE ON guacamole_db.* TO 'guacamole_user'@'localhost'; 4) flush privileges; 5) cat guacamole-auth-jdbc-0.9.12- incubating/mysql/schema/*.sql mysql -u root -p\$mysqlrootpassword guacamole_db 	UPDATE DELETE กับผู้ใช้งานชื่อ guacamole_user ในฐานข้อมูล guacamole_db Compile สิทชิ นำค่า schema ทั้งหมด ใส่ใน ฐานข้อมูล guacamole_db

authentication ด้วย database ร่วมกับ Apache Guacamole 0.9.12-incubating

ตารางที่ 3.8 แสดงรายละเอียดการกำหนดฐานข้อมูลและ import schema ต่าง ๆ สำหรับการ

จากตารางที่ 3.8 นั้นคือการใช้ SQL Command ในการสั่งการ ฐานข้อมูลสำหรับการเตีรยม กวามพร้อมฐานข้อมูล MySQL ให้ทำงานร่วมกับ Apache Guacamole 0.9.12-incubating โดยสร้าง user เฉพาะสำหรับการจัดการฐานข้อมูล หมายเหตุ: ก่อนจะเริ่มกระบวนการนี้จะเป็นต้อง มีการสร้าง database ที่ชื่อว่า guacamole_db มา เรียบร้อยก่อนหน้านี้แล้ว

กระบวนการถัดไปจะเป็นขั้นตอนการ configure ระบบ Apache Guacamole ในเรื่องของ ระบบเครือข่าย และระบบ การ authentication แบบ database โดยมีขั้นตอนการ configure ดังนี้

guacamole.properties UNIX Command ความหมาย echo "mysql-hostname: localhost" >> น้ำข้อมูล mysql-hostname: localhost เขียน /etc/guacamole/guacamole.properties ลง /etc/guacamole/guacamole.properties echo "mysql-port: 3306" >> น้ำข้อมูล mysql-port: 3306 เขียนลง /etc/guacamole/guacamole.properties /etc/guacamole/guacamole.properties echo "mysql-database: guacamole db" น้ำข้อมูล mysql-database: guacamole db >> /etc/guacamole/guacamole.properties เขียนลง /etc/guacamole/guacamole.properties echo "mysql-username: guacamole_user" น้ำข้อมูล mysql-username: >> /etc/guacamole/guacamole.properties guacamole_user เขียนลง /etc/guacamole/guacamole.properties echo "mysql-password: P@ssw0rd" >> น้ำข้อ<mark>ม</mark>ูล my<mark>sql-p</mark>assword: P@ssw0rd /etc/guacamole/guacamole.properties เขียนลง /etc/guacamole/guacamole.properties

ตารางที่ 3.9 แสดงรายการการ configure ระบบของ directory /etc/guacamole/

จากตารางที่ 3.9 <mark>ได้มีกา</mark>รอธิบาย<mark>เกี่ย</mark>วกับการตั้ง<mark>ค่าของระบบ</mark> Apache Guacamole โดยจะ เป็นการตั้งค่าให้ระบบสามารถเชื่อมต่อกับฐานข้อมูล MySQL ในส่วนของการ Authentication ตามที่กำหนดไว้ในขั้นตอนก่อนหน้านี้

หมายเหตุ: ในการตั้งก่าระบบจากตารางที่ 3.9 นั้น ข้อมูลการตั้งก่าที่เกี่ยวกับฐานข้อมูลจำเป็นต้อง เป็นข้อมูลเดียวกับการสร้างฐานข้อมูลในตารางที่ 3.8 เท่านั้น หลังจากนั้นจะทำการ start และ restart service ทั้งหมดที่เกี่ยวข้อง ตามคำสั่งที่กำหนดใน ตารางที่ 3.10 เพื่อให้ระบบพร้อมใช้งาน

ตารางที่ 3.10 แสดงกำสั่งการ restart service ทั้งหมดที่ใช้ในระบบ Apache Guacamole 0.9.12-

incubating			
UNIX Command	1		ความหมาย
service mysql restart		ເรີ່ນກຳກາ	รทำงานของ service mysql ใหม่
service tomcat7 restart		ເรີ່ນຄາรทໍ	ำงานของ service tomcat7 ใหม่
Service guacd restart		ເรີ່ນการทໍ	างานของ service apache guacamole
	U	ใหม่	1 2

จากตารางที่ 3.10 นั้นได้ระบุการการใช้กำสั่ง เริ่มต้นการทำงานของ บริการที่เกี่ยวข้องกับ ระบบใหม่อีกครั้ง เมื่อดำเนินการขั้นตอนเหล่านี้สมบูรณ์ ระบบจะสามารถใช้งานได้ตามปกติ โดย สามารถเข้าใช้งานผ่าน browser โดยการระบุ domain name ที่ตั้งไว้สำหรับ website ในส่วนของ Apacje guacamole-Client

หมายเหตุ: ถ้าเกิดกรณีที่ไม่ได้มีการกำหนด domain name เอาไว้สามารถเข้าถึงหน้าเว็บได้ผ่าน IP address ของระบบปฏิบัติการ

ootQu	buntu:~#			
coorde	com text alder			
pootfilu	huntu:~# netstat -ntunln			
active	Internet connections (only ser	uers)		
Proto	Recu-O Send-O Local Address	Foreign Address	State	PID/Program name
Cn	A 127 A A 1:336	0 0 0 0 *	LISTEN	873/musmld
icn.	0 0 0 0 0 0 80	0.0.0.0.*	LISTEN	915/nginy -g daemor
Cn Cn	0 0 127 0 0 1:4822	0 0 0 0:*	LISTEN	894/macd
icn .	0 0 0 0 0 0:22	0.0.0.0:*	LISTEN	834/sshd
cn	0 0 0.0.0.0:443	0.0.0:*	LISTEN	915/nginx -g daemon
cn6	0 0 ::::8080	:::*	LISTEN	888/ java
:cn6	0 0 ::::80		LISTEN	915/nginx -g daemor
cv6	0 0 :::21	111*	LISTEN	841/usftpd
cp6	0 0 :::22	:::*	LISTEN	834/sshd
ıdp	0 0 0.0.0.0:68	0.0.0:*		801/dhclient
rootQu	buntu:~#			
rootQu	buntu:~# ifconf <mark>ig</mark>			
ens33	Link encap:Ethernet HWaddr	00:0c:29:8b:45:07		
	inet addr:1 <mark>92.168</mark> .153.128	Bcast:192.168.153.255 Masl	k:255.255.255.0	
	inet6 addr: fe80::20c:29ff:	fe8b:4507/64 Scope:Link		
	UP BROADCAST RUNNING MULTIC	AST MTU:1500 Metric:1		
	RX packets: <mark>166 er</mark> rors:0 dro	pped:0 overruns:0 frame:0		
	TX packets: <mark>48 err</mark> ors:0 drop	ped: <mark>0</mark> overruns:0 carrier:0		
	collisions: <mark>0 txqu</mark> euelen:100	0		
	RX bytes:19965 (19.9 KB) T	K bytes:5852 (5.8 KB)		
.0	Link encap:Local Loopback			
	inet addr:127.0.0.1 Mask:2	5.0.0.0		
	Ineth addr: ::1/128 Scope:H			
1000	DY packate:160 empere:0 days			
	TY mackets: 160 errors:0 dro	ppea.0 overruns.0 frame.0	0	
1.00	collisions:0 typuquelen:1	ppeu.o overruns.o carrier.o		
	RY butes: 11840 (11 8 KB) T	(butes:11840 (11 8 KB)		
	IN BUCS. HOIO (II.0 MD) I.	A bytes. 11010 (11.0 Kb)		
ootQu	huntu:"#			
00000				

ภาพที่ 3.11 การแสดรายละเอียด network adapter ของ VM เครื่องที่ 1

ในส่วนของการเข้าส่วนของ web application ของระบบ Apache Guacamole 0.9.12incubating นั้นเนื่องจาก ไม่ได้มีการกำหนด domain name เอาไว้สำหรับการเข้า ดังนั้นการเข้าถึงจะ มีการเข้าผ่าน IP address ตามรูปภาพที่ 3.11 นั้น IP address ของ VM เครื่อง ที่1 คือ 192.168.153.138

หลังจากนั้นจะทดสอบเข้าหน้าเว็บ ด้วย URL <u>http://192.168.153.138:8080/guacamole/</u> โดยผลพธ์นั้นจะแสดงตามภาพที่ 3.12 ที่แสดงถึง หน้าเว็บ ที่มี function login เพื่อเข้าสู่บบใน สถานฃะ admin เพื่อที่จะทำการ configuration ระบบ Apache Guacamole ต่อไป



ภาพที่ 3.12 แสดงการเข้าระบบ Apache Guacamole 0.9.12-incubatin ผ่าน Firefox browser หมายเหตุ: ในการ Login เข้าระบบ ของ Apache Guacamole นั้น โดยมี account default คือ username คือ guacadmin และ password คือ guacadmin

ขั้นตอนการติดตั้งโ<mark>ป</mark>รแกร<mark>มชนิ</mark>ด Rev</mark>erse Proxy

ในการติดตั้งโปรแกรมชนิด Reverse Proxy นั้นจากขอบเขตปัญหาที่ได้กล่าวไว้ในส่วน ของการออกแบบ ได้ข้อสรุปว่ามีการเลือกใช้โปรแกรมประเภท Reverse Proxy ที่มีชื่อว่า Nginx โดยในหัวข้อนี้จะกล่าวถึงการวิธีการติดตั้งโปรแกรม Nginx บนระบบปฏิบัติการ Ubuntu Server 14.04 LTS 32 bit และวิธีการ performance tuning หลังการติดตั้งให้เหมาะสมกับ environment ที่ นำไปใช้ให้เหมาะที่สุด

โดยมีขั้นตอนการติดตั้ง reverse proxy ที่ชื่อว่า Nginx ดังนี้

Download Repository ผ่าน UNIX Command ตามตารางที่ 3.11 โดยจะแสดงให้เห็น กระบวนการการติดตั้งด้วย Command บนระบบปฏิบัติการ Ubuntu Server 14.04

ตารางที่ 3.11 แสดงรายการการติดตั้ง Nginx

UNIX Command	ความหมาย
apt-get install nginx	ติดตั้งโปรแกรม nginx
service nginx restart	เริ่มต้นการทำงาน service nginx ใหม่อีกครั้ง
update-rc.d nginx defaults	น้ำ service nginx ให้้ทำงาน แบบ startup

จากตารางที่ 3.11 นั้นได้แสดงขั้นตอนการติดตั้ง reverse proxy ที่มีชื่อว่า nginx ไปเรียบร้อย แล้วนะ หลังจากนั้นจะทำการ configuration เพื่อปรับการตั้งค่าในส่วนของ performance ของ nginx เพื่อให้เหมาะสมกับ environment มากที่สุด โดยจากปัญหาที่กล่าวขึ้นในบทที่ 1 กับ ในส่วนของการ ออกแบบนั้น คือ การที่ระบบ Clientless Remote Desktop ไม่สามารถรองรับ traffic ปริมาณมากของ ผู้ใช้งานหรือ host ได้เกิน 50 คน ดังนั้นจากปัญหาหลังจากนำโปรแกรม nginx เข้ามาใช้ทำให้เรา สามารถ ปรับเปลี่ยนและตั้งค่า ในส่วนของ traffic ของ connection link ได้ โดยในการทำ performance tuning นั้นมีรายละเอียดการ tuning ดังนี้

หมายเหตุ: การตั้งค่าค่าต่าง ๆ ของการทำ performance tuning ของโปรแกรม nginx นั้นจะ เข้าไป แก้ไขจาก directory ดังนี้ /etc/nginx/nginx.conf

```
# you must set worker processes based on your CPU cores, nginx does not
benefit from setting more than that
worker processes auto; #some last versions calculate it automatically
# number of file descriptors used for nginx
# the limit for the maximum FDs on the server is usually set by the OS.
# if you don't set FD's then OS settings will be used which is by default
2000
worker_rlimit_nofile 100000;
# only log critical errors
error_log /var/log/nginx/error.log crit;
# provides the configuration file context in which the directives that
affect connection processing are specified.
events {
   # determines how much clients will be served per worker
   # max clients = worker_connections * worker_processes
   # max clients is also limited by the number of socket connections
available on the system (~64k)
   worker connections 4000;
   # optmized to serve many clients with each thread, essential for linux
-- for testing environment
   use epoll;
```

```
# accept as many connections as possible, may flood worker connections
if set too low -- for testing environment
    multi accept on;
}
# cache informations about FDs, frequently accessed files
# can boost performance, but you need to test those values
open file cache max=200000 inactive=20s;
open_file_cache_valid 30s;
open_file_cache_min_uses 2;
open_file_cache_errors on;
# to boost I/O on HDD we can disable access logs
access_log off;
# copies data between one FD and other from within the kernel
# faster then read() + write()
sendfile on;
# send headers in one peace, its better then sending them one by one
tcp nopush on;
# don't buffer data sent, good for small data bursts in real time
tcp_nodelay on;
# reduce the data that needs to be sent over network -- for testing
environment
gzip on;
gzip_min_length 10240;
gzip_proxied expired no-cache no-store private auth;
gzip_types text/plain text/css text/xml text/javascript application/x-
javascript application/json application/xml;
gzip disable msie6;
# allow the server to close connection on non responding client, this will
free up memory
reset_timedout_connection on;
# request timed out -- default 60
client_body_timeout 10;
# if client stop responding, free up memory -- default 60
send timeout 2;
# server will close connection after this time -- default 75
keepalive_timeout 30;
# number of requests client can make over keep-alive -- for testing
environment
keepalive requests 100000;
       จากข้อความต้นคือรายละเอียดการทำ best performance tuning โดยในส่วนของภาพรวม
้ ค่าต่าง ๆ ที่ถูกปรับเปลี่ยน ส่วนใหญ่ในการปรับเปลี่ยน จะเป็นในเรื่องของการปรับลด/เพิ่มขนาด
buffer หลังจากนั้นจะทำการ testing tuning เพื่อทำการวัดผมของการเปลี่ยนค่า configuration ตาม
```

```
ตารางที่ 3.12
```

ตารางที่ 3.12 แสดงรายการ การทำ testing tuning ของโปรแกรม ningx

UNIX Command	ความหมาย
nginx -s reload	เป็นคำสั่งใช้ในการ save configuration
service nginx restart	เริ่มต้นบริการ nginx ใหม่อีกครั้ง
nginx -t	เป็นคำสั่งใช้ในการ test configuration
/etc/init.d/nginx configtest	เป็นคำสั่งใช้ในการ test configuration

จากตารางที่ 3.12 นั้นแสดงให้เห็นการ ทำ testing tuning ของโปรแกรม nginx ซึ่งหลังจาก ดำเนินการเสร็จ ถ้าไม่มีการ return ข้อความ error ใด ๆ กลับมา จะสรุปได้ว่า การ tuning เสร็จ สมบูรณ์

ขั้นตอนการติดตั้งระบบปฏิบัติการ Kali Linux และบริการ VNC (VM เครื่องที่ 2)

10

การติดตั้งระบบปฏิบัติการ Kali Linux 2 นั้นเพื่อเป็นระบบปฏิบัติการเอาไว้รองรับสำหรับ บริการ Real VNC โดยในลำดับแรกนั้นจะเป็นการอธิบายขั้นตอนการติดตั้งระบบปฏิบัติการ Kali Linux 2 64 bit (Rolling) หลังจากนั้นจะทำการติดตั้งบริการ RealVNC ที่มีชื่อว่า Real VNC Connect 6.2 เพื่อเป็น VNC server ไว้ทำงานร่วมกับระบบ Clientless Remote Desktop Gateway หรือ Apache Guacamole 0.9.12-incubaing เพื่อแก้ไขปัญหาตามที่ได้วางเอาไว้ในบทที่ 1

ขั้นตอนการติดตั้งระบบปฏิบัติการ Kali Linux 2 64 bit (Rolling) นั้นในส่วนของขั้นตอน การติดตั้งนั้นมีขั้นตอนดังนี้

กำหนด Virtual Hardw<mark>are บ</mark>นโปรแกรม VMware Workstation เพื่อใว้ใช้ในการติดตั้ง ระบบปฏิบัติการ Kali Lin<mark>ux 2</mark> ตามภาพที่ <mark>3</mark>.13

The virtual machine	will be created with the following settings:	
Name:	Kali Linux 2 64bit	
Location:	D:\VMs\CoopKALINEW	
Version:	Workstation 14.x	
Operating System:	Debian 9.x 64-bit	
Hard Disk:	10 GB, Split	
Memory:	1024 MB	
Network Adapter:	NAT	
Other Devices:	2 CPU cores, CD/DVD, USB Controller, Prir	nter, Sound C
Customize Uprdu		
Customize Haruv	/die	

ภาพที่ 3.13 แสดงรายละเอียด Virtual Hardware ของระบบปฏิบัติการ Kali Linux 2

หลังจากนั้นในกระบวนการต่อไปนั้น จะเข้าสู่กระบวนการการติดตั้งระบบปฏิบัติการ Kali Linux 2 โดยตามภาพที่ 3.14 นั้น จะเป็นการเลือกหัวข้อ install เพื่อติดตั้ง เนื่องจากในการติดตั้ง ระบบปฏิบัติการ Kali Linux 2 นั้นสามารถดำเนินการ boot แบบ Live คือการที่สามารถใช้งาน Kali Linux 2 ได้โดยไม่ต้องผ่านกระบวนการ install แต่จะมีข้อจำกัดบางส่วนเช่นกัน



ภาพที่ 3.14 การติดตั้งระบบปฏิบัติการ Kali Linux 2 (1)
หลังจากนั้นจะเข้าสู่กระบวนการเลือกภาษาที่ใช้ในการติดตั้ง ตามภาพที่ 3.15 ได้มีการเลือก ภาษา English เป็นภาษาในการติดตั้ง



ภาพที่ 3.15 การติดตั้งระบบปฏิบัติการ Kali Linux 2 (2)

หลังจากนั้นภาพที่ 3.16 แสดงการตั้งชื่อ hostname ให้กับระบบปฏิบัติการซึ่งจากภาพได้ตั้ง ชื่อ hostname มีชื่อว่า Kali และหลังจะนั้นจะมีการตั้งก่า password ไว้สำหรับ ในการ login เข้าระบบ

(6



ภาพที่ 3.16 การติดตั้งระบบปฏิบัติการ Kali Linux 2 (3)

NSTITUTE OF

หลังจากนั้น ภาพที่ 3.17 จะเป็นการเลือก disk storage ที่ใช้ในการจองพื้นที่ให้สำหรับ repository ของ Kali Linux 2 ซึ่งจาก การกำหนด Virtual Hardware นั้นได้มีกำหนด disk ลูกเดียว ดังนั้นในขั้นตอนนี้ก็สามารถเลือกแบบ standard guide เพื่อให้ง่ายต่อการติดตั้งได้ หมายเหตุ: ในการติดตั้งสามารถแบ่ง partition ได้ในส่วนกระบวนการนี้

🕽 Kali Linux 2 64bit - VMwar	Workstation		- 0	×
ile <u>E</u> dit <u>V</u> iew V <u>M</u> ∏abs	Help 📕 🕶 🖶 💭 💭	9 🗖 🗖		
🕽 Kali Linux 2 64bit 🛛 🛛				
This is an overview of partition to modify is partitions, or a devic Conf Conf Conf	(ii) Partition disks your currently configured partitit s settings (file system, mount point to initialize its partition table d partitioning sure software RAID sure the Logical Volumes sure isons your escal yourses	ons and mount po. nt, etc.), a free e.	nts. Select a space to create	7
SCSI1 <u>Undo</u>	(0,0,0) (sda) – 10.7 GB VMware, VM #1 primary 9.7 GB f ext4 , #5 logical 1.1 GB f swap (changes to partitions	Mware Virtual S / swap		2
<go back=""></go>	h partitioning and write changes to	o disk		
			_	
1> for help; <tab> moves</tab>	; <space> selects; <enter> activate</enter></space>	es buttons		
direct input to this VM, click	inside or press Ctrl+G.			

ภาพที่ 3.17 การติดตั้งระบบปฏิบัติการ Kali Linux 2 (4)

หลังจากนั้นเมื่อตอบตกลงไปกระบวนการติดตั้งจะคำเนินการติดตั้ง จะใช้เวลาจำนวนนึ งตามภาพที่ 3.18 หลังจากนั้นระบบจะทำการ restart หลังจากการติดตั้งเสร็จสมบูรณ์ตามภาพที่ 3.20

IC



ภาพที่ 3.18 การติดตั้งระบบปฏิบัติการ Kali Linux 2 (5)



ภาพที่ 3.19 หน้า Login หลังจากการ restart บนระบบปฏิบัติการ Kali Linux

จากภาพที่ 3.19 เมื่อทำการ login ด้วย root user และ password ตามที่กำหนดไว้ในขั้นตอน การติดตั้งจะสามารถเข้าสู่ desktop ตามภาพที่ 3.20



10

ภาพที่ 3.20 หน้าจอ desktop ของระบบปฏิบัติการ Kali Linux 2

เมื่อดำเนินการติดตั้งจนถึงขั้นตอนตามภาพที่ 3.20 จะสามารถใช้งานระบบปฏิบัตการได้ อย่างปกติ จึงสรุปได้ว่าการติดตั้งระบบปฏิบัติการ Kali Linux 2 64 bit เสร็จสมบูรณ์ หลังจากนั้นจะอธิบายขั้นตอนการติดตั้งโปรแกรม Real VNC Connect 6.2 บน ระบบปฏิบัติการ Kali Linux 2 64bit โดยมีรายละเอียดดังนี้

ในการติดตั้ง RealVNC นั้น จะต้องมีการติดตั้ง VNC Server ซึ่งมีโปรแกรมในการติดตั้งชื่อ ว่า Real VNC Connect 6.2 โดยสามารถติดตั้งได้จากเว็บไซต์ official [15] ตามภาพที่ 3.21 ซึ่งในการ download เพื่อที่จะติดตั้งนั้น ตามภาพ ได้เลือกประเภทการ download บนระบบปฏิบัติการ Linux และเลือก package การติดตั้งแบบนามสกุล deb เพื่อง่ายต่อการติดตั้งตามภาพที่ 3.20



ภาพที่ 3.21 หน้าเว็บ download Real VNC Connect 6.2

หลังจากนั้นเมื่อผ่านกระบวนการ download package Real VNC Connect 6.2.deb เสร็จสิ้น ต่อไปจะเป็นกระบวนการติดตั้งด้วย UNIX Command คือ dpkg -i และตามด้วยชื่อ package เช่น dpkg -i VNC-Server-6.2.8-Linux-64bit.deb ตามภาพที่ 3.22



ภาพที่ 3.22 การติดตั้ง Real VNC Connect 6.2 ผ่าน Command Line

หมายเหตุ: ถ้าระบบปฏิบัติการได้ติดตั้ง VNC ของผู้ให้บริการอื่น ๆ เช่น TightVNC เอาไว้ก่อน ล่วงหน้า เมื่อติดตั้ง Real VNC Connect 6.2 นั้นจะเกิดปัญหาเนื่องจากตัวโปรแกรมจะไม่ยอมให้ install package เนื่องจาก repository ซ้ำ ดังนั้นจำเป็นต้องถอนการติดตั้ง VNC ของผู้ให้บริการอื่น ๆ ก่อน

(0)

หลังจากติดตั้งเรียบร้อยสามารถเรียกใช้งานโปรแกรมผ่าน UNIX Command คือ vnc-x11serviced หลังจากนั้นจะทำการฝังให้โปรแกรมทำงานแบบ startup โดยมีรายละเอียด UNIX Command คือ sysetmcel enable vncsever -virtuald.service หลังจากนั้นโปรแกรมจะแสดงขึ้นมา ตมภาพที่ 3.23

62



ภาพที่ 3.23 หน้าจอโปรแกรม Real VNC Connect 6.2

4) การทดสอบระบบ (Testing)

ในส่วนของการทคสอบนั้นจะมีการทคสอบ 2 ส่วนคังนี้

ทดสอบภายใน VMware Workstation PRO บนเครื่องพิมเวอตร์ของตัวเอง โดยในส่วนนี้ นั้นจะทดสอบให้แน่ชัดว่า ระบบเสมือนที่อ้างอิงตามที่ดำเนินการปฏิบัตินั้น สามารถแก้ไขปัญหา ของระบบ Cyber RANG ได้ชัดเจนเมื่อแน่ชัดพอควร จะเข้าสู้กระบวนการถัดไป ทดสอบภายใน ระบบ Cyber RANGE บนเครื่องเซิร์ฟเวอร์ของบริษัท โดยในส่วนนี้จะทดสอบให้สามารถใช้งาน จริงได้ ร่วมกับระบบ Cyber RANGE บนโปรแกรม VMware ESXi ที่เข้าถึงได้ผ่าน VM vSphere ระหว่าง VM เครื่องที่ 1 และ VM เครื่องที่ 2 โดยจะกำหนดสมมุติฐานคือ จะนำระบบ Apache Guacamole 0.9.12-incubating ใน VM เครื่องที่ 1 มาเชื่อมต่อ เพื่อ remote ไปยัง ระบบปฏบัติการ Kali Linux 2 และทำการเปิดโปรแกรม ดังนี้

- 1) Browser OWASP Mantra
- 2) Wireshark

10

จากหัวข้อที่กล่าวไปเพื่อทคสอบผลลัพธ์ สามารถเปิดใช้งานได้ตามปกติที่ได้วางแผนเอาไว้ หรือไม่ รวมถึงทคสอบการใช้งานจนผ่านการประเมินจนเสร็จสมบูรณ์ 5) ปรับปรุงรักษาและประเมินผล (Maintenance)

T

ในส่วนหัวข้อนี้ได้มีการปรับปรุงรักษาและประเมินผล ในการ CI workshop ครั้งที่ 2 โดยมี ผู้เข้าร่วมงานทั้งหมด 50 คน ที่ใช้ระบบ Cyber RANGE เวอชั่นหลังจาก ปรับปรุงเรื่องระบบ Clientless Remote Desktop Gateway และ VNC

> กุกโนโลฮั77 ง

> > VSTITUTE OF

บทที่ 4

สรุปผลการดำเนินงาน การวิเคราะห์และสรุปผลต่าง ๆ

องค์ประกอบของบทที่ 4 มีดังนี้

4.1 ขั้นตอนและผลการดำเนินงาน

- 4.1.1 ผลของการคำเนินโครงงาน
 - 4.1.1.1 ระบบ Clientless Remote Desktop Gateway (VM เครื่องที่ 1)
 - 4.1.1.2 ระบบปฏิบัติการ Kali Linux 2 (VM เครื่องที่ 2)
- 4.2 วิเคราะห์ผลของการทำโครงงานวิจารณ์ข้อมูลโดยเปรียบเทียบผลที่ได้รับกับวัตถุประสงค์และ จุดมุ่งหมายการปฏิบัติ

4.1 ขั้นตอนและผลการดำเนินงาน

จากการปฏิบัติงานตลอคระยะเวลา 18 สัปดาห์ สามารถสรุปผลการคำเนินงานได้ดังนี้

4.1.1 ผลของการดำเนินโครงงาน

รายละเอียดผลการดำเนินงานโครงงานนั้นสามารถจำแนกได้เป็น 4 ส่วน โดยอ้างอิง ปัญหา 4 หัวข้อ ในบทที่ 1 ได้ดังนี้

4.1.1.1 ระบบ Clientless Remote Desktop Gateway (VM เครื่องที่ 1)

ในส่วนของปัญหาของระบบ Clientless Remote Desktop Gateway จากปัญหาในบทที่ 1 และการออกแบบ ในบทที่ 3 ได้มีการจำแนกปัญหาทั้งหมดออกเป็น 2 ปัญหาในส่วนของ ระบบ Clientless Remote Desktop Gateway โดยแบ่งเป็นดังนี้

 ปัญหาการออกแบบการแก้ไขปัญหาในเรื่อง Access Control ของระบบ Clientless Remote Desktop Gateway ที่ไม่สามารถจัดการ หมวดหมู่และจัดทำระบบ Authority จากปัญหาที่กล่าวไปหลังจากดำเนินงานโครงการได้ปรับปรุงระบบ Clientless Remote Desktop Gateway ใหม่เป็นเวอชั่น 0.9.12-incubating ซึ่งหลังจากดำเนินการนั้น ระบบใหม่ได้มีการ จัดการ ผู้ใช้งานแบบ User Access Control ทั้ง Mandatory Access Control และ Role-based Access Control ส่งผลให้สามารถบริหาร User Management ที่เข้ามาใช้งานในระบบได้อย่างอืดหยุ่นและ ควบคุมได้ดีมากขึ้นทั้งในเรื่องความเร็ว ความเชื่อถือ และความปลอดภัย ตามตัวอย่างภาพที่ 4.1 และ 4.2 และ 4.3

S DRAVA S DRAVA S D DL AS DSCI 104 Appacht Gui283hiftitie M S SorgenStract M S	- 🗆 ×
← → ① # 192.168.153.128:8080/gu C O Q Search ☆ 自 ↓	^ ⊽ » ≡
SETTINGS	💄 guacadmin 👻
Active Sessions History Users Connections Preferences	
Click or tap on a user below to manage that user. Depending on your access level, use deleted, and their passwords can be changed.	rs can be added and
2 New User Rilter	
guacadmin test01	
alura ej	
	1 5

ภาพที่ 4.1 ระบบ Clientless Remote Desktop Gateway ในส่วนของ User Access Control (1)

10

7 S DSGUNJ 15 O PL // S DSGUN4 UNA S Apaché Guacamole	break; ase ga_screenshot: M_ScryenShot_D; gameaction = ga_noth;	ng:					-	
← 🛈 🔏 192.168.153.12	8:8080/guacan	୯ 📀	Q Search	☆自	+ 1			=
EDIT USER					2	guaca	dmin	- 1
Username: Password: Re-enter Password:								
PROFILE								
Full name:								
ACCOUNT RESTRICT	IONS							
Login disabled: Password expired:								

ภาพที่ 4.2 ระบบ Clientless Remote Desktop Gateway ในส่วนของ User Access Control (2)

rs Dsgung 15,0 pH // S Dsgund IN C Apaché Guacamole	break; case ga_screenshot: M_Scr_mShot_0;			aready horoged	□ ×
 i) <u>#</u> 192.168.153.1 	28:8080/guacan C	Search	☆自		» =
ACCOUNT RESTRIC	TIONS				^
Login disabled: Password expired: Allow access after: Do not allow access aft Enable account after: Disable account after: User time zone:	HH:MM:SS HH:MM:SS YYYY-MM-DD YYYY-MM-DD				
PERMISSIONS Administer system: Create new users: Create new connection Create new connection Create new sharing pro Change own password	ns: proups: pofiles: proups: proups	la a		Ś	

ภาพที่ 4.3 ระบบ Clientless Remote Desktop Gateway ในส่วนของ User Access Control (3)

จากภาพที่ 4.1 4.2 และ 4.3 นั้นแสดงรายละเอียดของการตั้งก่า User Access Control ใน ระบบ Clientless Remote Desktop Gateway โดยจะมี function ต่าง ๆที่ใช้ในการ จัดการ user เช่น การกำจัดสิทธิของ function Permissions ที่สามารถกำหนดสิทธิในการคำเนินงานปฏิบัติ ต่อ function ต่าง ๆ และไปส่วนของ function Account Restrict ที่สามารถกำหนด ระยะเวลา ของ account นั้น ๆ ได้ เพื่อป้องกันปัญหา account ที่ไม่จำเป็น

2) การออกแบบแก้ไขปัญหาในเรื่องการ limited convergent ของการใช้งานระบบ Cyber RANGE ผ่านระบบ Clientless Remote Desktop Gateway

จากปัญหาที่กล่า<mark>วไปนั้น</mark>หลักจา<mark>ก</mark>ดำเนินงานได้ทำการ<mark>ติดตั้</mark>งระบบ Reverse Proxy ที่มี ชื่อว่า Nginx บน VM เครื่องที่ 1 ระบบปฏิบัติการ Ubuntu Server 14.04 LTS 32 bit หลังจาก นั้นก็ได้ทำการ performance tuning โดยอ้างอิง environment ของระบบ Cyber RANGE เป็น หลัก และ policy ของบริษัทเพื่อเสริมสร้างความปลอดภัยให้กับ ระบบมากยิ่งขึ้น ซึ่งผลการ ดำเนินงานนั้น ส่งผลให้ ระบบ Cyber RANGE สามารถรองรับผู้เล่นที่มีจำนวนมากขึ้นมาใช้งาน ระบบพร้อมกัน โดยไม่มีผลกระทบต่อความเร็วในการใช้งาน ทำให้สามารถแก้ไขปัญหาได้ การออกแบบการแก้ไขปัญหาการ develop recorder function ของระบบ Clientless Remote Desktop Gateway

จากปัญหาที่กล่าวนั้นหลังการคำเนินงานการปรับปรุงและพัฒนาระบบ Clientless Remote Desktop Gateway 0.9.12-incubating ส่งผลให้มี function VDO recorder สำหรับ VNC และ RDP ตามภาพที่ 4.4 และ 4.5 เมื่อคำเนินงานใช้งานจะได้รับ raw file ซึ่งสามารถนำไป encode เพิ่มเติมได้ ส่งผลให้เป็น function ดังกล่าวเป็นประโยชน์มากต่อการพัฒนาต่อไปในอนาคต

Arona breas //s. Documu Apaché Guadamole M_Screenshot: apaché Guadamole gamesticine da no panac	ching;	see svalidount = validount	 ×
🕤 🛈 🔏 192.168.153.128.8080/guaca	C C Search	☆ 自 ♣	
Encoding: UTF-8 v			^
INC Repeater			
Destination host:			
Destination port:	 (\$)		
Screen Recording			
Recording nath:	[home]		1:5
Pocording pame			
Automotion llu arosto recording nath			
Automatically create recording path.			
SFTP			
Enable SFTP:]		
Hostname:			
Port:	.		
Username:			
Password:			~
			× .

4.1.1.2 ระบบปฏิบัติการ Kali Linux 2 (VM เครื่องที่ 2)

จากปัญหาในส่วนของ ระบบปฏิบัติการ Kali Linux 2 จากปัญหาที่กล่าวถึงในบทที่ 1 นั้น ปัญหาของ ระบบปฏิบัติการ Kali Linux 2 ใน ระบบ Cyber RANGE ได้เกิดปัญหาดังนี้ 1) การออกแบบแนวทางการแก้ไขปัญหาของโปรแกรมไม่สามารถแสดงผลได้ถูกต้อง ขณะใช้งาน remote ไปยัง ระบบปฏิบัติการ Kali Linux จากปัญหาที่กล่าวไปนั้นหลังจากการดำเนินงาน ได้มีการเปลี่ยนบริการ VNC โดยเดิมที่ใช้ Tight VNC ที่มี Desktop Environment ที่ชื่อว่า XFCE นั้นได้มาใช้ Real VNC แทนซึ่งผลลัพธ์ หลังจากการใช้ Real VNC นั้น พบว่า สามารถเปิด OWASP Mantra Browser และ Wireshark ได้ ขณะ remote ภายในรบบ Cyber RANGE ตามรูปภาพที่ 4.5 และ 4.6

S D 5,0 5	sguna 17 s os kali	SCUM // S_DSGUNS	case ga_screene M_ScreenShot gameaction = c	hot: D: a_nothing:			sep->valido	n; ouns = valideo	ont;	eq		×
4) (i) 💋	192.168.153.	128:8080/gua	san 🤤 🤁	0	Q Search		合自	♦ 🏫	♥	»	=
	Applic	ations 👻 🛛 Pla	aces 👻 🎯 Fir	efox 🔻	Mo	n 04:31		¥(1 /	((1))	७ -	
	Welcor	re to OWASP I /elcome to OWA III ▼ C Go	Mantra - Free an SP Mantra × to a Website	nd Open Sou	arce Brov	vser based S	Security Fran	Google	WASP Ma	C	□ ◎ ◎ ↑ ★	
	* *	Your installe uses an inte thus some s you update	ed version of Fl rnal IP address shown flags wil to the current	agfox is nov location dat l begin to go version.	v more tl tabase to et progre	han a few mo look up ser essively mor	onths old. Fl ver location e inaccurate	agfox and until	Don't show	this ag	gain ×	6
		ube	twitte		lost	.fm	(~	S.		~]	
		001			antra			וכ			3	
	5			2								
		(\mathbf{F})			_		_	_			12	
	Ģ	$\underline{\heartsuit}$								A		
	2	WAS	SP		f	ace	bo	ok		K	339	
	<	V2									CIL	

ภาพที่ 4.5 หน้าจอบณะใช้งาน OWASP Mantra Browser ผ่านApache Guacamole ที่ remote เข้า

10

ใ<mark>ปยัง Kali</mark> Linux 2

/ S_DSGUN3 95.0.01.7/.S_DSQUM	oreak; case da screenshot;		natarn:	// all eady fooded	×
	M_ScreenShot 11: gameaction - ga, noth	ing;		valideo.nt;	
🔶 🛈 🔏 192.168.153.1	28:8080/guacan	C 🕥 Q Se	arch 🗘	💼 🖡 🎓 🛡 »	=
Applications - Plac	ces 👻 🔝 Wireshar	rk ▼ Mon 04:32		⊯ 1 💉 🕬 🖒 ▾	
	1	The Wireshark Netwo	rk Analyzer	000	
<u>File</u> <u>Edit</u> <u>View</u> <u>Go</u>	<u>Capture</u> <u>Analyze</u>	Statistics Telephony	<u>Wireless</u> <u>T</u> ools <u>H</u>	lelp	
	ð 🗋 🕅 🖸 '	Q, ♦ ₱ .J №	* <u> </u>	ର୍ ଦ୍ 🎹	
Apply a display filter	<ctrl-></ctrl->			Expression +	
Welcome Capture using this f eth0	e to Wireshark ilter: 📕 Enter a capt			×	
Loopbaci nflog ofruieue Learn User's Guide You are runn	k: lo e · Wiki · Questic ing Wireshark 2.2.5 (ons and Answers · M	lailing Lists n unknown).		
	rantura		No Packets	Profile: Default	

ภาพที่ 4.6 หน้าจอขณะใช้งาน Wireshark ผ่านApache Guacamole ที่ remote เข้าไปยัง Kali Linux 2

ส่วนการวัดผลในการเลือกผู้บริการ Real VNC มาใช้งานนั้นได้มีการกำหนดขอบเขต โดย ได้มีการทดลองนำบริการ VNC ของแต่ละผู้บริการมาทำการทดสอบร่วมกับระบบ Cyber RANGE โดยมีละเอียดตารางตามตารางที่ 4.1ที่แสดงขอบเขตของผู้ให้บริการ VNC ที่เลือกมาใช้งานเพื่อทำ การทดสอบประสิทธิภาพ

ตารางที่ 4.1 แสดงรายชื่อบริการต่าง ๆ ของ VNC ที่ใช้ในการทดสอบ

IG

ถำดับ	ชื่อบริการ	ผลการ <mark>ทดส</mark> อบ
1	UltraVNC	ไม่สาม <mark>า</mark> รถใช้ง <mark>านร่วมก</mark> ับได้เนื่ <mark>องจ</mark> ากปัญหา performance
2	Tiger VNC	ไม่สาม <mark>าร</mark> ถใช้งานร่ว <mark>มก</mark> ันได้เ <mark>นื่องจ</mark> ากปัญหา maintenance
3	X11VNC	ไม่สามารถใช้งานร่วมกันเนื่องจากปัญหาของ service
4	Vino	ไม่สามารถใช้งานร่วมกันเนื่องจากปัญหาของ service
5	Real VNC	สามารถทำงานร่วมกันได้

ถำดับ	ชื่อบริการ	ผลการทดสอบ
6	NoMachine	สามารถทำงานร่วมกันได้แต่ redundancy ลำบาก

ตารางที่ 4.1 แสดงรายชื่อของบริการต่าง ๆ ของ VNC ที่ใช้ในการทดสอบร่วมกับระบบ (ต่อ)

จากตารางที่ 4.1 แบบว่า หมายเลข 5 และ 6 ที่สามารถใช้งานร่วมกับระบบ Cyber RANGE ใค้ดีที่สุดแต่เนื่องจากหมายเลข 6 นั้น ไม่รองรับกับ Apache Guacamole 0.9.12-incubating เพราะมี การใช้ protocol ส่วนตัวที่ไม่ได้มการใช้งาน โปรโตคอล VNC ทั่วไปทำให้ หมายเลข 5 คือ Real VNC เป็นตัวเลือกที่ดีที่สุด

4.2 วิเคราะห์และวิจารณ์ข้อมูลโดยเปรียบเทียบผลที่ได้รับกับวัตถุประสงค์และ จุดมุ่งหมายในการปฏิบัติงานหรือการจัดทำโครงงาน

ในส่วนนี้จะขอวิจารณ์ข้อมูลเฉพาะในในส่วนของโครงงานเท่านั้น เนื่องจากมีการกำหนด วัตถุประสงค์และจุดมุ่งหมายของการปฏิบัติงานที่ชัดเจน โดยการพัฒนาและปรับปรุงระบบ Clientless Remote Desktop Gateway และ VNC สำหรับระบบ Cyber RANGE โดยมีการเพิ่ม กุณสมบัติดังต่อไปนี้

- เพื่อให้การ remote ไปยังระบบปฏิบัติการ Kali Linux 2 สามารถเปิด Mantra browser ได้อย่างสมบูรณ์
- เพื่อให้การremote ใปยังระบบปฏิบัติการ Kali Linux 2 สามารถเปิด โปรแกรม Wireshark ได้อย่างสมบูรณ์
- 3) เพื่อให้การremoteไปยังระบบปฏิบัติการ Kali Linux 2 มีความเร็วมากขึ้น
- เพื่อให้ระบบ Clientless Remote Desktop สามารถวัดผลได้จาก Remote Desktop Service

โคยมีผลลัพธ์ดังนี้

- 1) สามารถเปิ<mark>คโปรแ</mark>กรม OWASP Mantra Browser แ<mark>ละใช้งา</mark>นได้อย่างปกติ remote
- 2) สามารถเปิดโปรแกรม Wireshark และใช้งานได้อย่างปกติขณะ remote
- มีการนำ nginx มาใช้ทำให้สามารถใช้กระบวนการ load balance และ เพิ่ม/ลด traffic ทำให้จัดการได้ง่ายขึ้นทำให้มีการ remote แล้วมีความเร็วเพิ่มขึ้น
- 4) มีfunction Screen Recorder ทำให้สามารถอัด video บน service VNC ได้

บทที่ 5 บทสรุปและข้อเสนอแนะ

5.1 สรุปผลการดำเนินงาน

(0

จากการดำเนินงานทั้งหมดใช้ระยะเวลาทั้งหมด 18 สัปดาห์ในการพัฒนาและปรับปรุง ระบบ Clientless Remote Desktop Gateway และ VNC สำหรับระบบ Cyber RANGE ในการติดตั้ง ทั้งหมดนั้นจะติดตั้งอยู่ในรูปแบบ VMs ซึ่งจะแบ่งแยกออกเป็นทั้งหมด 2 ส่วน VM ใน VM ส่วน แรกนั้นจะเป็น VM ของระบบปฏิบัติการ Ubuntu 14.04 ที่จะติดตั้งส่วนต่าง ๆ ทั้งหมดสองส่วน ส่วนแรกนั้นคือ Reverse Proxy ที่มีชื่อว่า Nginx และส่วนที่สองระบบ Clientless Remote Desktop Gateway ที่มีชื่อว่า Apache Guacamole ซึ่งองค์ประกอบของ Apache Guacamole จะถูกแบ่งออกเป็น สองส่วน ส่วนแรกนั้นคือส่วน Guacamole-Server ที่ใช้ควบคุมและประมวลผล Remote Desktop Service ต่าง ๆ และส่วนที่สองคือส่วน Guacamole-Client ที่เป็นรูปแบบ web-based ถูกประมวลผล โดย Tomcat 8 ผ่านภาษา JAVA และเก็บข้อมูลด้วย MySQL ส่วนนี้จะใช้สำหรับควบคุมการตั้งค่า ต่าง ๆ ของ Guacamole-Server หลังจากนั้นก้จะทำการติดตั้งส่วนของ Nginxเพื่อใช้งานร่วมกับ VNC service ในส่วน VM ที่สองนั้นจะเป็น VM ของ ระบบปฏิบัติการ Kali Linux 2 โดยจะติดตั้ง RealVNC Service ลงบนระบบปฏิบัติการ Kali Linux 2 เพื่อเอาไว้ใช้ทำงานควบคู่กับระบบ Apache Guacamole ที่ติดตั้งไปแล้วตามที่กล่าวไปก่อนหน้านั้น

เมื่อติดตั้งส่วนประกอบต่าง ๆ เสร็จเรียบร้อยแล้วก็จะทำการ Testing เพื่อเก็บข้อผิดพลาด ให้ได้มากที่สุดเมื่อเจอข้อผิดพลาดก็จะทำการแก้ไขให้เสร็จสิ้นเพื่อเข้าสู่กระบวนการต่อไปก็คือการ Migration เมื่อส่วน Testing เรียบร้อยแล้ว จะเข้าสู่การ Migration VMs ต่าง ๆ ที่ผ่านการ Testing แล้วโดยจะทำการ Migrate ร่วมกับระบบ Cyber RANGE และหลังจากนั้นจะทำการ Develop เพิ่มเติมเพื่อให้การ Migration เสร็จสิ้นสมบูรณ์พร้อมใช้งานมากที่สุด

ผลลัพธ์ของการ<mark>พัฒน</mark>าและการ<mark>ป</mark>รับปรุงในค<mark>รั้</mark>งนี้คือ ระบบ Clientless Remote Desktop Gateway และ VNC ที่ได้พัฒนาและปรับปรุงไปแล้วนั้นได้แก้ไขข้อผิดพลาดและเพิ่มความสามารถ ให้กับระบบ Cyber RANGE ได้ตรงตามจุดมุ่งหมายที่กำหนดเอาไว้

VSTITUTE O

5.2 แนวทางการแก้ไขปัญหา

จากการดำเนินงานระบบ Clientless Remote Desktop Gateway และ VNC สำหรับระบบ Cyber RANGE ไปแล้วนั้นได้พบเจอปัญหาต่าง ๆ ดังนี้

1) ปัญหา การประมวลผลของ Nginx ใน VM Ubuntu 14.04

สาเหตุของปัญหานี้มาจากการใช้ก่า Default Configuration ของตัว Nginx ที่มีมา ให้ แล้วนำมาทำงานร่วมกับ Apache Guacamole ที่ใช้ RealVNC จะเกิดปัญหาในเรื่องของ ความเร็ว ในการแสดงผลทำให้ใช้งานลำบาก แนวทางการแก้ไขปัญหาเบื้องต้นคือ การ Configuration ในด้าน Performance Tuning ของ Nginx จะทำให้การแสดงผลผ่าน Apache Guacamole ด้วย VNC มี ลักษณะรวดเร็วและราบรื่นมากขึ้นกว่าเดิม ทำให้ใช้งานได้สะดวกขึ้น

2) ปัญหา Misconfiguration ในการ Access เข้าถึงสิทธิ Admin ในส่วนของการ Configuration ใน RealVNC บน Kali Linux 2 ผ่าน Apache Guacamole

สาเหตุของปัญหานี้มาจากการไม่ได้ Configuration RealVNC บน Kali Linux 2 ตาม Policy ที่กำหนดไว้ ใน Environment ที่เหมาสมเช่นการใช้ค่า Default Configuration ของ RealVNC ส่งผลให้เมื่อนำไปใช้งาน ผู้ใช้งานที่ Access ที่เข้าถึง Kali Linux ได้นั้นสามารถได้สิทธิ Configuration ของ RealVNC ซึ่งการกระทำนี้จะส่งผลกระทบที่รุนแรงจนทำให้ระบบ Cyber RANGE เกิดปัญหาได้ในภายหลัง แนวทางแก้ไขปัญหาคือ Configuration ในส่วนของ User Access Control ให้เหมาะสมตาม Policy ของ Environment นั้น ๆ

5.3 ข้อเสนอแนะจากการดำเนินงาน

จากการคำเนินงานที่ผ่านมาการ configuration ในส่วนต่าง ๆ ไม่ว่าในส่วนของ Nginx หรือ ระบบ Apache Guacamole หรือ ในส่วนของ RealVNC บน Kali Linux 2 สำหรับการนำไปใช้งาน จริงนั้นควรมีการออกแบบในส่วนของ Infrastructure Design ให้ชัดเช่น เนื่องจากถ้าไม่เป็นเช่นนั้น ตัวระบบในส่วนของการส่งค่าและการรับค่ารวมถึงการประมวลผลอาจจะไม่สามารถแสดงผลได้ ตรงตามความต้องการของผู้พัฒนาได้อันเนื่องมาจาก Environment ที่ไม่เหมาะสม รวมถึงกวรมีการ กำหนด Production Policy ให้รัดกุมก่อนทำการ configuration ระบบ ถ้ามิเช่นนั้นในการใช้งาน ผู้ใช้งานระบบอาจเข้าถึงตัวระบบในสิทธิของ ผู้พัฒนาได้ ซึ่งการกระทำดังกล่าวเป็นผลทำให้ระบบ มีความเสี่ยงในเรื่องของความปลอดภัยเป็นอย่างมาก



เอกสารอ้างอิง

- Virtualizaion,2013,zplus[Online] Available: <u>http://www.zplus.co.th/virtualiz ion.html</u> [2017, June 16].
- ระบบเสมือน,2012,baycoms[Online] Available:
 http://www.baycoms.com/index.php/technology-upd-e/vm1.html [2017, June 16].
- 3) การใช้งาน Reverse Proxy, 2014,IBM[Online] Available: <u>goo.gl/nriEpb</u> [2017, June 19].
- 4) Reverse Proxy,2015,IBM[Online] Available: <u>goo.gl/nriEpb</u> [2017, June 19].
- 5) การใช้งานSQL,2015, blog.bossturteam[Online] Available: goo.gl/5n24F7 [2017, June 21].
- 6) Unix คืออะไร,2015,blog.gm[Online] Available: <u>goo.gl/ekLDrR</u> [2017, June 22].
- 7) Real VNC,2014,surawit555.myreadyweb[Online] Available:

http://surawit555.myreadyweb.com/page-24996.html [2017, June 23].

- Virtual-machine,2012,nitiponvirtualmachine[Online] Available: https://nitiponvirtualmachine.blogspot.com/2016/05/virtual-machine.html [2017, June 24].
- 9) VMware ESXi,2015,host4pro[Online] Available: <u>goo.gl/mvvoKs</u> [2017, June 24].
- 10) VMware vSphere,2015.host4pro[Online] Available: goo.gl/fYdnQf [2017, June 25].
- 11) Ubuntu,2014,saixii[Online] Available: https://saixiii.com/linux-ubuntu/ [2017, June 26].
- 12) Kali Linux 2.0,2015,techtalkthai[Online] Available: <u>https://www.techtalkthai.com/kali-linux-2-</u> <u>0-released/</u> [2017, June 26].
- 13) Apache Tomc ,2017, wikipedia[Online] Available: <u>https://goo.gl/nsy1ok</u> [2017, June 28].
- MySQL,2017,wikipedia[Online] Available: <u>http://th.easyhostdomain.com/dedic ed-servers/mysql.html</u> [2017, June 28]

15) วิธีติดตั้ง Ubuntu 14.04[Online] Available: <u>https://www.tecmint.com/ubuntu-14-04-server-</u> install ion-guide-and-lamp-setup/ [2017, June 26]

> กุกโนโลยั7 กุง

TC

STITUTE OF

ประวัติผู้จัดทำโครงงาน

ชื่อ – สกุล

นายศุภณัฐ ไวยานิกรณ์

28 กันยายน 2538

วัน เดือน ปีเกิด

ประวัติการศึกษา ระดับประถมศึกษา

ระดับมัธยมศึกษา

ระดับอุดมศึกษา

ทุนการศึกษา

ประวัติการฝึกอบรม

ผลงานที่ได้รับการตีพิมพ์

ประถมศึกษาตอนปลาย พ.ศ. 2551 โรงเรียนอนุบาลราชบุรี (ปวช.) ประกาศนียบัตรวิชาชีพ พ.ศ. 2557 วิทยาลัยอาชีวศึกษาครุณาราชบุรี คณะเทคโนโลยีสารสนเทศ สาขาเทคโนโลยีสารสนเทศ พ.ศ. 2561 สถาบันเทคโนโลยีไทย - ญี่ปุ่น

- ไม่มี -

- 1) MiSS Conference 1
- 2) Hackaron 2017
- 3) MiSS Conference 3
- 4) SysAdmin 2017
- 5) OWASP Conference 2017 ຄ^{ື້} 2 ແລະ 3
- 6) DriodCON Bangkok 2017

Supanut V.,Patsawee T.,Kotchaporn S.,การพัฒนาโมบายแอฟลิเคชัน ตรวจจับควันและผู้สูบบุหรึ่แบบอัตโนมัติบนระบบปฏิบัติการ แอนครอย ,TNI Academic Conference 2017, No. 209, (2017). (Accepted).

76