

การจัดการด้านความปลอดภัยและลดทรัพยากรการใช้งานให้กับระบบ

Management Security Hardening

นาย พิรษร อัครวุฒิ

TC

โครงงานสหกิจ<mark>ศึก</mark>ษานี้เป็นส่<mark>ว</mark>นหนึ่งของการศึกษาตา</mark>มหลักสูตร ้ปริญญาวิทย<mark>าศาส</mark>ตรบัณฑิ<mark>ต</mark> สาขาวิ<mark>ชาเท</mark>คโนโล<mark>ยีสา</mark>รสนเทศ คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยี ไทย-ญี่ปุ่น W.A. 2001 INSTITUTE OF

การจัดการด้านความปลอดภัยและลดทรัพยากรการใช้งานให้กับระบบ Management Security Hardening

นาย พิรษร อัครวุฒิ

โครงงานสหกิจศึกษานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

วิทยาศาสตรบัณฑิต สาขาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีไทย - ญี่ปุ่น ปีการศึกษา 2561

คณะกรรมการสอบ

.....ประธานกรรมการสอบ

(อาจารย์ อดิศักดิ์ เสือสมิง)

...... กรรม<mark>การส</mark>อบ

(ผู้ช่วยศาส<mark>ตรา</mark>จารย์ ดร.ป<mark>ระ</mark>จักษ์ เ<mark>ฉิดโฉม</mark>)

......อาจาร<mark>ย์ที่ป</mark>รึกษา

(ผู้ช่วยศาส<mark>ตรา</mark>จารย์ คร.นรังสรรค์ วิไล<mark>สกุ</mark>ลยง)

.....ประธานสหกิจศึกษาสาขาวิชา

(อาจารย์ สลิลา ชีวกิดาการ)

ลิขสิทธิ์ของสถาบันเทคโนโลยีไทย – ญี่ปุ่น

ชื่อโครงงานการจัดการด้านความปลอดภัยและลดทรัพยากรการใช้งานให้กับระบบผู้เขียนนายพิรษร อัครวุฒิคณะวิชาเทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศอาจารย์ที่ปรึกษาดร.นรังสรรค์ วิไลสกุลยงพนักงานที่ปรึกษานายภูดิศ ดุพัสกูลชื่อบริษัทบริษัท เอ-โฮสต์ จำกัดประเภทธุรกิจ/สินค้าให้บริการทางด้าน Hosting Service และ IBM & Oracle Product

บทสรุป 8

ในการสหกิจศึกษาได้รับมอบหมายในตำแหน่ง System Engineer ช่วยในการทำ OS Security Hardening บนระบบปฏิบัติการ Linux และ Windows Server โดยพบว่าสามารถพัฒนาได้ทั้งความปลอดภัย และประสิทธิภาพการทำงานของระบบ

จากประสบการณ์ที่ได้จากการไปสหกิจศึกษา ทำให้ได้เรียนรู้เรื่องระบบความปลอดภัยทั้งในด้านของ การเข้าถึงและการใช้งาน การที่ได้ทำ Hardening ทำให้เกิดความเข้าใจในวิธีการที่จะเพิ่มประสิทธิภาพใน ส่วนต่างๆ ของความปลอดภัยของระบบและสามารถใช้กำสั่งต่างๆ ในระบบปฏิบัติการ Linux ได้ อีกทั้งการ ทำงานร่วมกับผู้อื่นทำให้เกิดความคุ้นชินกับการทำงานในเวลาที่จำกัด การรับผิดชอบต่อหน้าที่การทำงาน และสามารถบริหารจัดการเวลาในการทำงานได้ โดยทั้งหมดนี้จะเป็นสิ่งสำคัญต่อชีวิตการทำงานในอนากต

ก

รูปถ่ายผลงานสหกิจศึกษาที่ได้ดำเนินการ

root@education: <u>File Edit View Terminal Tabs H</u>elp # # inittab This file describes how the INIT process should set up # the system in a certain run-level # # Author: Miquel van Smoorenburg, <miquels@drinkel.nl.mugnet.org> # Modified for RHS Linux by Marc Ewing and Donnie Barnes # # Default runlevel. The runlevels used by RHS are: # 0 - halt (Do NOT set initdefault to this) 1 - Single user mode # 2 - Multiuser, without NFS (The same as 3, if you do not have networking) # # 3 - Full multiuser mode 4 - unused 5 - X11 # 6 - reboot (Do NOT set initdefault to this) # # id:3:initdefault: # System initialization. si::sysinit:/etc/rc.d/rc.sysinit l0:0:wait:/etc/rc.d/rc 0 -- INSERT --หน้า Setting ของ Linux เพื่อปิด GUI Enterprise Linux Enterprise Linux Server release 5.5 (Carthage) Kernel 2.6.18-194.el5 on an i686 education login: _

หน้า Command Line ของ Linux no GUI

Project's name	Management Security Hardening	
Writer	Mr. Pirasorn Augkaravut	
Faculty	Faculty of Information of Technology, Information of	
	Technology Program	
Faculty Advisor	Dr.Narungsun Wilaisakoolyoung	
Job Supervisor	Mr. Pudis Dupasakul	
Company's name	A-Host Company Limited	
Business Type / Product	Hosting Service and IBM & Oracle Product	

Summary

I was assigned as a System Engineer during the cooperative education, working on OS Hardening in Linux operating system and Window Server I've found that able to improve both Security and Performance of the system.

From this cooperation experience, I've learn about the security of system's access and usability. In case of doing Hardening, I've understood how to improve the performance of parts of system's security and also able to use commands in Linux operating system. And by working in team makes me more familiar to finish work on time, be responsible to duties, and able to manage time to work which are important in my real worklife.

ନ

กิตติกรรมประกาศ

ในการเข้าไปสหกิจศึกษาที่บริษัท เอ - โฮสต์จำกัดนั้น ได้รับความกรุณาและการดูแลจากพี่ๆ ได้ เรียนรู้การทำงานจริงภายในบริษัท ได้รับความมรู้ต่างๆมากมายและได้รับการดูแลใกล้ชิดทั้งการให้ คำปรึกษาและช่วยแก้ไขปัญหาต่างๆที่เกิดขึ้น ทำให้การปฏิบัติงานครั้งนี้สำเร็จลุล่วงไปได้ด้วยดี ขอขอบคุณ คุณภูดิศ ดุพัสกูล คุณเนตรปวีร์ ศิริวิชญ์วัฒนา คุณชัยยุทธ ศุภกิจรุ่งเจริญ และ ขอบคุณพี่ๆทีม SMS ที่สละเวลามากอยช่วยเหลือแก้ปัญหาและเป็นที่ปรึกษาเรื่องต่างๆในช่วงสหกิจศึกษา และพี่ๆในบริษัททุกท่านที่ได้ให้ความช่วยเหลือทุกครั้งที่เกิดข้อสงสัยต่างๆ รวมถึงการแนะนำเทคนิกในการ ทำงานต่างๆ ซึ่งสามารถใช้ทำงานได้จริง ขอขอบพระคุณทุกท่านไว้ ณ โอกาสนี้ด้วย

(0

นายพิรษร อักรวุฒิ ผู้จัดทำ

สารบัญ

บทสรุปก
กิตติกรรมประกาศง
สารบัญ จ
สารบัญรูปฏ
บทที่ 1
1.1 ชื่อและสถานที่ตั้งของสถานประกอบการ1
1.2 ลักษณะธุรกิจของสถานประกอบการหรือการให้บริการขององค์กร
1.2.1 Hosting & Outsource Service
1.2.2 Oracle Core Technology Products and Advanced Services
1.3 รูปแบบการจัดองค์กรและการบริหารองค์กร
1.4 ตำแหน่งและหน้าที่งานที่นักศึกษาได้รับมอบหมาย
1.5 พนักงานที่ปรึกษาและตำแหน่งของพนักงานที่ปรึกษา
1.6 ระยะเวลาที่ปฏิบัติงาน
1.7 วัตถุประสงค์ของการปฏิบัติงานและโครงงานที่ได้รับมอบหมาย
1.8 ผลที่คาดว่าจะ ได้รับจากการปฏ <mark>ิบัติง</mark> านและ โคร <mark>งงานที่ได้</mark> รับม <mark>อ</mark> บหมา <mark>ย</mark>
บทที่2
2.1 ระบบปฏิบัติการ Linux
2.1.1 ข้อคีของ Linux
2.1.1.1 ใช้งานได้ไม่เสียค่าใช้จ่าย10
2.1.1.2 ความปลอดภัยในการทำงาน10
VSTITUTE OF

2.1.1.3 เสถียรภาพในการทำงาน10
2.1.1.4 สนับสนุนฮาร์คแวร์ทั้งเก่าและใหม่10
2.1.2 โครงสร้างของ Linux11
2.1.2.1 ฮาร์ดแวร์ (Hardware)11
2.1.2.2 ยูนิกซ์ เคอร์เนล (Kernel)11
2.1.2.3 เชลล์ (Shell)11
2.2 VMware Workstation
2.3 Windows Server
2.3.1 Windows Server 2008 R2
2.3.2 Windows Server 2012 R2
2.3.3 Windows Server 2016
2.3.3.1 Nano Server ฟีเจอร์ใหม่14
2.3.3.2 สร้างมาเพื่อ Cloud Technology โดยเฉพาะ16
2.3.3.3 Hyper-V รองรับกับ Linux ชื่อดังเกือบทั้งหมด17
2.3.3.4 ปลอดภัยขึ้นด้วย Security ใหม่ ใน Windows Server 2016
2.3.3.5 จัดการ Server ได้ลึกและละเอียดขึ้นด้วย PowerShell 5.0
2.3.3.6 ReFS เสถียรและสมบูรณ์แบบ ใน Windows Server 2016
2.3.3.7 Nested Virtualization
2.3.3.8 Software-defined stora <mark>ge จั</mark> คการพื้นที่เก <mark>็บข้อมูลได้ง่ายขึ้น</mark> 21
2.3.3.9 รองรับ Containers แน <mark>วคิด</mark> Virtual Server ที่กำลังเ <mark>ป็นที่</mark> นิยม
2.4 Oracle Database 11g
2.5 ระบบป้องกันเครือค่ายคอมพิวเตอร์24
2.5.1 security life cycle

ฉ

2.5.2 การแยก list ของ hardening แบ่งเป็น 3 กลุ่มคือ	
2.5.3 กุณสมบัติของคนที่ทำ Hardening	
2.5.4 การทำ hardening บน Windows	
2.5.5 ขั้นตอนของ Hardening	25
2.5.6 การกำหนดขอบเขตและรูปแบบการ Harden	
2.5.7 Application หมายถึงการป้องกันใน 2 ระดับคือ	
2.5.8 File System	
2.5.9 Operating System	
2.5.10 Network	
2.5.11 Physical	
2.5.12 เครื่องมือ/เครื่องทุ่นแรง	
Windows คือ MBSA	
บทที่ 3	
บทที่ 3 3.1 แผนงานปฏิบัติงาน	
บทที่ 3 3.1 แผนงานปฏิบัติงาน 3.2 รายละเอียดโครงงาน	
บทที่ 3 3.1 แผนงานปฏิบัติงาน 3.2 รายละเอียด โครงงาน 3.2.1 Hardening	
บทที่ 3 3.1 แผนงานปฏิบัติงาน 3.2 รายละเอียดโครงงาน 3.2.1 Hardening 3.2.2 งานอื่นๆ	
บทที่ 3	

	3.3.1.2.5 สิ่งที่ Firewall ไม่สามารถป้องกันได้	31
3.3.2	2 NTP configuration	32
3.3.3	ง ทคสอบการตั้งค่าทั่วไปของ Hardening	33
3.3.4	เทคสอบ Hardening ที่ตั้งค่าไว้	
บทที่	i 4	34
4.1 ข้	ขั้นตอนและผลการคำเนินงาน	34
4	4.1.1 ศึกษาและทำความเข้าใจเกี่ยวHardening	34
4	1.1.1.1 ติดตั้ง Windows Server	35
4	1.1.1.2 Hardening Windows Server 2016	47
	4.1.1.2.1 Window update	47
	4.1.1.2.2 User Configuration	49
	4.1.1.2.3 Further Hardening	52
	4.1.1.2.4 Network Configuration	54
T	4.1.1.2.5 Features and Roles Configuration	57
	4.1.1.2.6 NTP Server Configuration	62
	4.1.1.2.6.1 NTP Client Configuration	63
	4.1.1.2.7 Firewall Configuration	66
	4.1.1.2.8 Remote Access Configuration	72
	4.1.1.2.9 Service Configuration	74
	4.1.1.2.10 Log & Monitoring	
	4.1.2 การติดตั้ง Linux	79
	4.1.2.1 การทำ Linux Hardening	94
	4.1.2.1.2 Yum update	94

4.1.2.1.3 World-writable Files
4.1.2.1.4 Window X disable
4.1.2.1.5 Turn off IPv6
4.1.2.1.6 Selinux
4.1.2.1.7 Quotas
4.1.2.1.8 Password Remember
4.1.2.1.9 Password auth
4.1.2.1.10 Password aging110
4.1.2.1.12 No owner file
4.1.2.1.13 Disable root login
4.1.2.1.14 User UID not set to 0
4.1.2.1.15 Secure OpenSSH Server
4.1.2.1.15.1 Configure Idle Timeout Interval
4.1.2.1.15.2 Disable Empty Password119
4.1.2.1.15.3 Limit Users'SSH Access
4.1.2.1.16 Audit
4.1.2.1.17 Encryption
4.1.2.1.18 Disable USB/firewire/thunderbolt devices
4.1.2.1.19 Secure Apache
4.1.2.1.20 Stop FTP126
4.1.2.1.21 Stop unused services
4.1.2.1.22 Physical Security
4.1.2.1.22.1 แนวทางการป้องกันความปลอคภัยทางกายภาพของระบบ128

4.2 ผลการวิเคราะห์ข้อมูล			
4.3 วิจารณ์ข้อมูล โดยเปรียบเทียบผลที่ได้รับก	าับวัตถุประสงค์กา	รจัดทำโครงการ .	131
บทที่ 5			132
5.1 สรุปผลการคำเนินงาน			
5.2 แนวทางการแก้ไขปัญหา			
5.3 ข้อเสนอแนะจากการคำเนินงาน			
เอกสารอ้างอิง			
ภาคผนวก	ula		135
ประวัติผู้จัดทำโครงงาน			

S

6

สารบัญรูป

รูป		หน้า
ภาพที่ 1.1 ที่ตั้งของบริษัท A-HOST		1
ภาพที่ 1.2 รางวัลที่ A-HOST ได้รับ.		
ภาพที่ 1.3 คณะผู้บริหาร A-Host Co	mpany Limited	6
ภาพที่ 2.1 สัญลักษณ์ของ Linux		9
ภาพที่ 2.2 โครงสร้างของ Linux		
ภาพที่ 2.3 สัญลักษณ์ของ VMware ไ	Workstation	12
ภาพที่ 2.4 สัญลักษณ์ของ Windows	Server	
ภาพที่ 2.5 Nano Server		
ภาพที่ 2.6 ความสามารถของ Nano	Server	
ภาพที่ 2.7 Layers of Security		
ภาพที่ 2.8 โลโก้ Microsoft Azure		
ภาพที่ 2.9 Hyper-V Function		
ภาพที่ 2.10 ระบบ Security ใหม่		
ภาพที่ 2.11 PowerShell 5.0		
ภาพที่ 2.12 ระบบ ReFS		
ภาพที่ 2.13 ระบบ NestedVM		
ภาพที่ 2.14 ระบบ Software <mark>-d</mark> efined	storage	
ภาพที่ 2.15 รับระบบ Containers		
ภาพที่ 2.16 Oracle Database11g		
ภาพที่ 3.2 คำเนินการเพิ่มความปล <mark>อ</mark>	<mark>คภัย</mark> ให้เครื่องข <mark>อ</mark> งเรา	
ภาพที่ 3.3 คำเนินการเพิ่มความปล <mark>อ</mark>	<mark>ดภัยให้เครื่องขอ</mark> งเรา	
ภาพที่ 3.4 หน้าที่ของ Firewall		
ภาพที่ 3.5 การทำงานของ NTP		
ภาพที่4.1 การสร้าง Virtual Machine	e(1)	

ภาพทั4.2 การสร้าง Virtual Machine(2)
ภาพที่4.3 การตั้งค่า Virtual Machine(3)
ภาพที่4.4 การเลือกลง Windows Server
ภาพที่4.5 การตั้งค่า Virtual Machine(4)
ภาพที่4.6 การระบุที่อยู่ของไฟล์ Virtual Machine
ภาพที่4.7 การตั้งค่า Virtual Machine(5)
ภาพที่4.8 การตั้งค่า Windows Server(6)
ภาพที่4.9 การ ให้ Memory กับ VM
ภาพที่4.10 การตั้งค่า Network
ภาพที่4.11 การตั้งค่า I/O40
ภาพที่4.12 การตั้งค่า Disk type40
ภาพที่4.13 การสร้าง VM
ภาพที่4.14 การตั้งค่าพื้นที่ให้Windows Server41
ภาพที่4.15 การตั้งชื่อให้กับ VM42
ภาพที่4.16 ตรวจเช็คการตั้งค่า42
ภาพที่4.17 การติดตั้ง Windows Server
ภาพที่4.18 การติดตั้ง Windows Server43
ภาพที่4.19 การใส่ Key Windows Server44
ภาพที่4.20 การตั้งค่า Windows Server
ภาพที่4.21 การยอมรับ license ของ Windows Server45
ภาพที่4.22 การตั้งค่า Windo <mark>ws Server</mark>
ภาพที่4.23 การแบ่ง Disk Windows Server
ภาพที่4.24 Install Windows Server
ภาพที่4.25 หน้าตาของ Windows S <mark>erve</mark> r47
ภาพที่4.26 window update(1)47
ภาพที่4.27 window update(2)48
ภาพที่4.28 window update(3)48
ภาพที่4.29 user configuration

STITUTE O

ภาพที่4.30	Control panel
ภาพที่4.31	หน้า Control panel ของ user accounts
ภาพที่4.32	User Accounts Setting
ภาพที่4.33	เลือก User51
ภาพที่4.34	หน้า Manage account
ภาพที่4.35	เข้า Control panel
ภาพที่4.36	User Accounts(1)
ภาพที่4.37	User Accounts(2)
ภาพที่4.38	Account control setting
ภาพที่4.39	Set ค่า User Account Control Setting
ภาพที่4.40	คลิกเปิด Network and Sharing Center
ภาพที่4.41	หน้า Network and Sharing Center
ภาพที่4.42	Network Connection
ภาพที่4.43	IP setting(1)
ภาพที่4.44	IP setting(2)
ภาพที่4.45	IP setting(3)
ภาพที่4.46	Add roles and features(1)
ภาพที่4.47	Add roles and features(2)
ภาพที่4.48	Add roles and features(3)
ภาพที่4.49	Add roles and features(4)
ภาพที่4.50	Add roles and features(5)
ภาพที่4.51	Add roles and features(6)
ภาพที่4.52	Add roles and features(7)
ภาพที่4.53	Add roles and features(8)
ภาพที่4.54	Add roles and features(9)
ภาพที่4.55	NTP Setting(1)
ภาพที่4.56	NTP Setting(2)
ภาพที่4.57	เข้า Run

STITUTE O

ภาพที่4.58 เลือก Config
ภาพที่4.59 Client NTP Config(1)
ภาพที่4.60 Client NTP Config(2)
ภาพที่4.61 Client NTP Config(3)
ภาพที่4.62 Client NTP Config(4)
ภาพที่4.63 Client NTP Config(5)
ภาพที่4.64 Fire wall Setting
ภาพที่4.65 หน้า Control panel67
ภาพที่4.66 Fire wall Setting(1)
ภาพที่4.67 Fire wall Setting(2)
ภาพที่4.68 Fire wall Setting(3)
ภาพที่4.69 Fire wall Setting(4)
ภาพที่4.70 Fire wall Setting(5)
ภาพที่4.71 Fire wall Setting(6)70
ภาพที่4.72 Fire wall Setting(7)70
ภาพที่4.73 Fire wall Setting(8)71
ภาพที่4.74 Inbound name setting71
ภาพที่4.75 Rule ที่สร้าง72
ภาพที่4.76 Remote access configuration(1)
ภาพที่4.77 Remote access configuration(2)
ภาพที่4.78 Remote access configuration(3)
ภาพที่4.79 Service74
ภาพที่4.80 Computer managemen <mark>t74</mark>
ภาพที่4.81 Service ทั้งหมดที่มีในเ <mark>ครื่อ</mark> ง
ภาพที่4.82 Disable Service
ภาพที่4.83 Windows Server Monitor(1)76
ภาพที่4.84 Windows Server Monitor(2)76
ภาพที่4.85 Windows Server Monitor(3)77

STITUTE OV

ฑ

ภาพที่4.86 Windows Server Log(1)		
ภาพที่4.87 Windows Server Log(2)	ภาพที่4.86 Windows Server Log(1)	77
กาพที่4.88 Windows Server Log(3) 7 กาพที่4.89 การสร้าง Virtual Machine(1) 7 กาพที่4.90 การสร้าง Virtual Machine(2) 7 ภาพที่4.91 การตั้งค่า Virtual Machine(2) 7 ภาพที่4.92 เลือกลง Linux 8 ภาพที่4.93 การระบุที่อยู่ของไฟล์ Virtual Machine 8 ภาพที่4.93 การระบุที่อยู่ของไฟล์ Virtual Machine 8 ภาพที่4.95 การทั้งค่า Linux 8 ภาพที่4.95 การทั้งค่า Network 8 ภาพที่4.96 การตั้งค่า Network 8 ภาพที่4.97 การตั้งค่า Disk type 8 ภาพที่4.90 การตั้งค่า Disk type 8 ภาพที่4.90 การตั้งค่า Disk type 8 ภาพที่4.101 การตั้งค่า Disk type 8 ภาพที่4.102 ครวดเช็คการตั้งค่า 8 ภาพที่4.101 การตั้งค่า VM 8 ภาพที่4.102 ครวดเช็คการตั้งค่า 8 ภาพที่4.101 การตั้งค่า YM 8 ภาพที่4.102 ตรวดเช็คการตั้งค่า 8 ภาพที่4.103 เลือกการตั้งค่า 8 ภาพที่4.104 หน	ภาพที่4.87 Windows Server Log(2)	
ภาพที่4.89 การสร้าง Virtual Machine(1) 7 ภาพที่4.91 การสร้าง Virtual Machine(2) 7 ภาพที่4.91 การตั้งกำ Virtual Machine. 8 ภาพที่4.92 เถือกลง Linux. 8 ภาพที่4.93 การระบุที่อยู่ของไฟล์ Virtual Machine. 8 ภาพที่4.93 การระบุที่อยู่ของไฟล์ Virtual Machine. 8 ภาพที่4.93 การระบุที่อยู่ของไฟล์ Virtual Machine. 8 ภาพที่4.95 การให้ Memory กับ VM. 8 ภาพที่4.97 การตั้งกำ Network 8 ภาพที่4.97 การตั้งกำ Disk type. 8 ภาพที่4.97 การตั้งกำ Disk type. 8 ภาพที่4.97 การตั้งกำ Disk type. 8 ภาพที่4.98 การตั้งกำ Mix type. 8 ภาพที่4.99 การสร้าง VM. 8 ภาพที่4.100 การตั้งกำ Disk type. 8 ภาพที่4.101 การตั้งกำ VM. 8 ภาพที่4.102 ตรวงเช็กการตั้งกำ 8 ภาพที่4.103 เลือกกาษา 8 ภาพที่4.104 หน้าการตั้งกำ 8 ภาพที่4.105 ตั้งกำ Cat. 8 ภาพที่4.106 หน	ภาพที่4.88 Windows Server Log(3)	
ภาพที่4.90 การสร้าง Virtual Machine(2) 7 ภาพที่4.91 การตั้งก่า Virtual Machine. 8 ภาพที่4.92 เถือกลง Linux. 8 ภาพที่4.93 การระบุที่อยู่ของไฟล์ Virtual Machine. 8 ภาพที่4.93 การระบุที่อยู่ของไฟล์ Virtual Machine. 8 ภาพที่4.94 การตั้งก่า Linux. 8 ภาพที่4.95 การให้ Memory กับ VM. 8 ภาพที่4.96 การตั้งก่า Network. 8 ภาพที่4.97 การตั้งก่า Network. 8 ภาพที่4.96 การตั้งก่า VO. 8 ภาพที่4.97 การตั้งก่า VO. 8 ภาพที่4.99 การสร้าง VM. 8 ภาพที่4.99 การสร้าง VM. 8 ภาพที่4.101 การตั้งก่า Mumon 8 ภาพที่4.102 ตรวจเข็ตการตั้งก่า 8 ภาพที่4.101 การตั้งก่า บา 8 ภาพที่4.102 ตรวจเข็ตการตั้งก่า 8 ภาพที่4.103 เลือกภาษา 8 ภาพที่4.104 หน้าการดั้งก่าวๆ 8 ภาพที่4.105 ห้งก่าวา 8 ภาพที่4.106 เข้าไปที่ Software Selection 8	ภาพที่4.89 การสร้าง Virtual Machine(1)	
ภาพที่4.91 การตั้งก่า Virtual Machine	ภาพที่4.90 การสร้าง Virtual Machine(2)	79
ภาพที่4.92 เสือกลง Linux	ภาพที่4.91 การตั้งค่า Virtual Machine	
ภาพที่4.93 การระบุที่อยู่ของไฟล์ Virtual Machine	ภาพที่4.92 เลือกลง Linux	
ภาพที่4.94 การตั้งค่า Linux	ภาพที่4.93 การระบุที่อยู่ของไฟล์ Virtual Machine	
ภาพที่4.95 การทั้งค่า Network 8 ภาพที่4.96 การทั้งค่า Network 8 ภาพที่4.97 การทั้งค่า Disk type 8 ภาพที่4.98 การทั้งค่า Disk type 8 ภาพที่4.99 การสั่งค่า Disk type 8 ภาพที่4.90 การสั่งค่า Disk type 8 ภาพที่4.100 การตั้งค่าที่นี่ที่ให้ Linux 8 ภาพที่4.101 การตั้งค่าที่นี่ที่ให้ Linux 8 ภาพที่4.102 ตรวจเช็คการตั้งค่า 8 ภาพที่4.103 เลือกภาษา 8 ภาพที่4.104 หน้าการตั้งค่าต่างๆ 8 ภาพที่4.105 ตั้งค่าเวลา 8 ภาพที่4.106 เข้าไปที่ Software Selection 8 ภาพที่4.107 เลือก Environment ที่ส้องการ 8 ภาพที่4.108 เข้าไปที่ Installation Destination 8 ภาพที่4.109 ตั้งค่า Disk ให้กับ Os Linux 8 ภาพที่4.110 ตั้งค่า Network 9 ภาพที่4.111 ตั้งค่า Network 9 ภาพที่4.112 เข้าไปที่ KDUMP 90	ภาพที่4.94 การตั้งค่า Linux	
ภาพที่4.96 การตั้งค่า Network 8 ภาพที่4.97 การตั้งค่า Dosk type 8 ภาพที่4.98 การสร้าง VM 8 ภาพที่4.99 การสร้าง VM 8 ภาพที่4.100 การตั้งค่าพื้นที่ให้ Linux 8 ภาพที่4.101 การตั้งจ่อให้กับ VM 8 ภาพที่4.101 การตั้งจ่อให้กับ VM 8 ภาพที่4.102 ตรวจเช็กการตั้งค่า 8 ภาพที่4.103 เลือกภาษา 8 ภาพที่4.104 หน้าการตั้งค่าต่างๆ 8 ภาพที่4.105 ตั้งค่าเวลา 8 ภาพที่4.106 เข้าไปที่ Software Selection 8 ภาพที่4.106 เข้าไปที่ Software Selection 8 ภาพที่4.107 เลือก Environment ที่ด้องการ 8 ภาพที่4.108 เข้าไปที่ Installation Destination 8 ภาพที่4.109 ตั้งค่า Disk ให้กับ Os Linux 8 ภาพที่4.110 เข้าไปที่ Network & Host name 8 ภาพที่4.111 ตั้งค่า Network 9 ภาพที่4.111 ห้งก่า Network 9 ภาพที่4.111 ห้งก่า Network 9	ภาพที่4.95 การให้ Memory กับ VM	
ภาพที่4.97 การตั้งก่า I/O	ภาพที่4.96 การตั้งค่า Network	
ภาพที่4.98 การตั้งค่า Disk type	ภาพที่4.97 การตั้งก่า I/O	
ภาพที่4.99 การสร้าง VM	ภาพที่4.98 การตั้งก่า Disk type	
ภาพที่4.100 การดั้งก่าพื้นที่ให้ Linux	ภาพที่4.99 การสร้าง VM	
ภาพที่4.101 การตั้งชื่อให้กับ VM	ภาพที่4.100 การตั้งก่าพื้นที่ให้ Linux	
ภาพที่4.102 ตรวจเช็คการตั้งค่า	ภาพที่4.101 การตั้งชื่อให้กับ VM	
ภาพที่4.103 เถือกภาษา	ภาพที่4.102 ตรวจเช็คการตั้งค่า	
ภาพที่4.104 หน้าการตั้งค่าต่างๆ	ภาพที่4.103 เลือกภาษา	
ภาพที่4.105 ตั้งค่าเวลา	ภาพที่4.104 หน้าการตั้งค่าต่างๆ	
ภาพที่4.106 เข้าไปที่ Software Selection	ภาพที่4.105 ตั้งค่าเวลา	
ภาพที่4.107 เลือก Environment ที่ต้องการ	ภาพที่4.106 เข้าไปที่ Softw <mark>are Selection</mark>	
ภาพที่4.108 เข้าไปที่ Installation Destination	ภาพที่4.107 เลือก Environment ที่ <mark>ต้องก</mark> าร	
ภาพที่4.109 ตั้งก่า Disk ให้กับ Os Linux	ภาพที่4.108 เข้าไปที่ Installation <mark>Desti</mark> nation	
ภาพที่4.110 เข้าไปที่ Network & Host name	ภาพที่4.109 ตั้งค่า Disk ให้กับ Os <mark>Linu</mark> x	
ภาพที่4.111 ตั้งค่า Network	ภาพที่4.110 เข้าไปที่ Network & <mark>Host n</mark> ame	
ภาพที่4.112 เข้าไปที่ KDUMP90	ภาพที่4.111 ตั้งค่า Network	
	ภาพที่4.112 เข้าไปที่ KDUMP	
ภาพที่4.113 ตั้งค่า KDUMP9	ภาพที่4.113 ตั้งค่า KDUMP	

STITUTE O

ภาพที่4.114	เลือก Begin Installation
ภาพที่4.115	เข้าไปที่ Root password
ภาพที่4.116	ตั้งค่า Root password
ภาพที่4.117	ทำการ Reboot
ภาพที่4.118	หน้า Login
ภาพที่4.119	หน้า CentOS 794
ภาพที่4.120	Yum update(1)
ภาพที่4.121	Yum update(2)
ภาพที่4.122	World-writable Files
ภาพที่4.123	ตรวจเช็คไฟล์
ภาพที่4.124	การปิค GUI (1)96
ภาพที่4.125	การปิด GUI (2)97
ภาพที่4.126	การปิค GUI (3)97
ภาพที่4.127	การปิค GUI (4)
ภาพที่4.128	การปิด GUI (5)
ภาพที่4.129	การปิด IPv6 ใน Linux
ภาพที่4.130	การเปิด Security-Enhanced Linux(1)
ภาพที่4.131	การเปิด Security-Enhanced Linux(2)
ภาพที่4.132	การเปิด Security-Enhanced Linux(3)100
ภาพที่4.133	การเปิด Security-Enhanced Linux(4)101
ภาพที่4.134	การเปิด Security-Enhanced Linux(5)
ภาพที่4.135	การกำหนดพื้นที่ Dis <mark>k ให้</mark> User(1)
ภาพที่4.136	การกำหนดพื้นที่ Dis <mark>k ให้</mark> User(2)
ภาพที่4.137	การกำหนดพื้นที่ Disk ให้ User(3)
ภาพที่4.138	การกำหนดพื้นที่ Dis <mark>k ให้</mark> User(4)
ภาพที่4.139	การกำหนดพื้นที่ Disk ให้ User(5)
ภาพที่4.140	การกำหนดพื้นที่ Disk ให้ User(6)103
ภาพที่4.141	การกำหนดพื้นที่ Disk ให้ User(7)104

WSTITUTE OF

ภาพที่4.142 การกำหนดพื้นที่ Disk ให้ User(8)	
ภาพที่4.143 การตั้งค่า Password Remember(1)	
ภาพที่4.144 การตั้งค่า Password Remember(2)	
ภาพที่4.145 การตั้งค่า Password Remember(3)	
ภาพที่4.146 การตั้งค่า Password Remember(4)	
ภาพที่4.147 การตั้งค่า Password Remember(5)	
ภาพที่4.148 การตั้งค่า Password auth(1)	
ภาพที่4.149 การตั้งก่า Password auth(2)	
ภาพที่4.150 การตั้งค่า Password auth(3)	
ภาพที่4.151 เพิ่มเติมเงื่อนไข	
ภาพที่4.152 คำสั่งเช็คค่า	
ภาพที่4.153 เช็คค่าที่ตั้งไว้	
ภาพที่4.154 ลองตั้ง Password	
ภาพที่4.155 เช็คค่า	110
ภาพที่4.156 ตั้งค่า Password aging(1)	
ภาพที่4.158 เช็คค่า Password(1)	
ภาพที่4.159 ลบ Password	
ภาพที่4.160 เช็คค่า Password(2)	112
ภาพที่4.161 เช็คสิทธิของไฟล์(1)	
ภาพที่4.162 ตั้งค่าสิทธิ	113
ภาพที่4.163 เช็คสิทธิของไฟล์(2)	
ภาพที่4.164 เข้าไปแก้ไขไฟ <mark>ล์</mark>	
ภาพที่4.165 ไม่มีสิทธิเข้าถึง	
ภาพที่4.166 กำหนดสิทธิ	
ภาพที่4.167 เข้าไปเช็คสิทธิการเข <mark>้าถึง</mark>	
ภาพที่4.168 ข้อความที่ตอนแรกไม่เห็น	
ภาพที่4.169 Disable Root login(1)	
ภาพที่4.170 Disable Root login(2)	



ภาพที่4.171	Disable Root login(3)	116
ภาพที่4.173	3 เช็ก UID(1)	117
ภาพที่4.174	เ ลองเปลี่ยน UID	117
ภาพที่4.175	ร เช็ค UID(2)	117
ภาพที่4.176	ร แก้ไขไฟล์	118
ภาพที่4.177	ซึ่งค่า ClientAlive(1)	118
ภาพที่4.178	< ตั้งค่า ClientAlive(2)	118
ภาพที่4.179	ตั้งค่า Empty password	
ภาพที่4.180) ตั้งค่าการใช้ Protocol(1)	119
ภาพที่4.181	ตั้งค่าการใช้ Protocol(2)	
ภาพที่4.182	2 Audit Setting(1)	
ภาพที่4.183	3 Audit Setting(2)	
ภาพที่4.184	Audit Setting(3)	
ภาพที่4.185	5 Audit Setting(4)	
ภาพที่4.186	5 Audit Setting(5)	
ภาพที่4.187	V Audit Setting(6)	
ภาพที่4.188	gyum install	122
ภาพที่4.189) สร้างไฟล์	122
ภาพที่4.190) เช็คไฟล์	
ภาพที่4.191	เช็ควิธีการ Decrypt	123
ภาพที่4.192	2 เช็กไฟล์	123
ภาพที่4.193	s ดูข้อความในไฟถ์	123
ภาพที่4.194	เรียกดูข้อความ	123
ภาพที่4.195	ร ทำการถบไฟถ์	
ภาพที่4.196	5 เรียกดูไฟล์ที่ทำการ E <mark>ncry</mark> pt ไว้	124
ภาพที่4.197	ทำการ Decrypt ไฟล์	
ภาพที่4.198	3 zip ไฟล์	124
ภาพที่4.199	ดูไฟล์	124

STITUTE O

ภาพที่4.200 ทำการ Decrypt ไฟล์			
ภาพที่4.201 ทำการ blacklist			
ภาพที่4.202 เข้า path conf			
ภาพที่4.203 แก้ไขไฟล์			
ภาพที่4.204 เพิ่มคำสั่ง			
ภาพที่4.205 Restart Service			
ภาพที่4.206 Check Status			
ภาพที่4.207 Stop service			
ภาพที่4.208 ดู Service ต่างๆ			
ภาพที่4.209 เช็ก httpd service	<u>u i g</u>	<u>. E</u>	
ภาพที่4.210 Stop httpd service			
ภาพที่4.211 เช็ก Service			

ຄ

S

C

บทที่ 1 บทนำ

1.1 ชื่อและสถานที่ตั้งของสถานประกอบการ

ชื่อสถานประกอบการ	:	บริษัท เอ-โฮสต์์ จำกัด (A-HOST Company Limited)
ที่ตั้งของสถานประกอบการ	:	979/53-55 ชั้น 21 ตึก SM Tower ถนนพหลโยธิน
		แขวงสามเสนใน เขตพญาไท กรุงเทพฯ 10400
โทรศัพท์		(66) 2298-0625-32
โทรสาร	:	(66) 2298-0053
E-mail	:	Marketing@a-host.co.th
Website	:	www.a-host.co.th



ภาพที่ 1.1 ที่ตั้งของบริษัท A-HOST

1.2 ลักษณะธุรกิจของสถานประกอบการหรือการให้บริการขององค์กร

บริษัทเอ-โฮสต์จำกัดได้ก่อตั้งขึ้นเมื่อปีพ.ศ.2542 ในฐานะหนึ่งบริษัทในเครือของบริษัทซิสเต็มส์คอร์ ปอเรชั่น (มหาชน) จำกัดและเป็นผู้เชี่ยวชาญด้านการบริการจัดวางระบบสารสนเทศ (Information Technology : IT) และบริการเสริมต่างๆสำหรับลูกค้าตั้งแต่ธุรกิจขนาดย่อมไปจนถึงขนาดกลางธุรกิจหลัก ของบริษัทเอ-โฮสต์คือการให้บริการโฮสติ้ง (Hosting) ซึ่งเป็นการเปิดเครื่องคอมพิวเตอร์แม่ข่ายในการให้เช่า พื้นที่เพื่อวางระบบและบริการระบบสารสนเทศด้วยผลิตภัณฑ์ของออราเคิล (Oracle) เป็นซอฟต์แวร์ สำหรับการวางแผนบริหารทรัพยากรของระดับแนวหน้าของโลก

เอ-โฮสต์ถือกำเนิดขึ้นจากกลุ่มผู้เชี่ยวชาญด้านสารสนเทศท่ามกลางภาวะเศรษฐกิจตกต่ำทั่วภูมิภาคเอเชีย แต่เอ-โฮสต์ก็สามารถเติบโตอย่างรวดเร็วและมั่นคงตั้งแต่แรกก่อตั้งด้วยจุดแข็งในฐานะผู้บุกเบิกธุรกิจโฮสติง เซอร์วิสพร้อมทั้งนำธุรกิจแนวใหม่อย่างการให้บริการระบบโปรแกรมประยุกต์หรือ ASP (Application Services Provider) เข้ามาให้บริการเป็นรายแรกในเมืองไทยอีกทั้งยังถือเป็นผู้ให้บริการรายแรกนอกประเทศ สหรัฐอเมริกาด้วย

ในฐานะผู้นำในอุตสาหกรรมนี้เป็นเวลามากกว่า 10 ปีเอ-โฮสต์ได้เสริมสร้างความแข็งแกร่งทางธุรกิจ ด้วยบริการที่มีความโดดเด่นและรวบรวมเอาทรัพยากรบุคกลซึ่งได้สั่งสมประสบการณ์และความชำนาญไว้ อย่างพร้อมเพรียงส่งผลให้ศูนย์ข้อมูลของเอ-โฮสต์ในปัจจุบันมีความสมบูรณ์ด้วยกลุ่มเซิร์ฟเวอร์ (Server) ที่เชื่อมต่อกันในลักษณะการจัดกลุ่ม (Clustering) ซึ่งเปี่ยมสมรรถนะสามารถให้บริการแก่ผู้ใช้จำนวนมาก ได้ในเวลาเดียวกัน

นอกจากนี้เอ-โฮสต์ยังติดตั้งระบบรักษาความปลอดภัยระบบสำรองข้อมูลและระบบบริหารจัดการ รวมถึงอุปกรณ์ต่างๆอย่างครบครันเพื่อให้เอ-โฮสต์สามารถตอบสนองต่อระดับความต้องการในระดับสูงสุด ที่ลูกค้าคาดหวังได้ตลอดจนเป็นการสร้างความมั่นใจให้แก่ลูกค้าที่ใช้บริการโฮสติงและแอพพลิเคชันต่างๆ ของเอ-โฮสต์ว่าจะได้รับทั้งประสิทธิภาพและความปลอดภัยอย่างครบครันธุรกิจการให้บริการระบบ โปรแกรมประยุกต์ในรูปแบบ ASP เอ-โฮสต์ไม่เพียงแต่ให้บริการค้านโปรแกรมประยุกต์ค้านการดำเนิน ธุรกิจทางอิเล็กทรอนิกส์ระดับโลกของออราเกิลพร้อมโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศเท่านั้น แต่ยังมีบริการที่ครอบคลุมตั้งแต่การให้กำปรึกษาการสนับสนุนและการให้บริการทั่วไปอย่างพรั่งพร้อมครบ ครัน

นอกจากธุรกิจโฮสติ้งและธุรกิจการให้บริการโปรแกรมประยุกต์ในรูปแบบ ASP ซึ่งถือเป็นธุรกิจหลัก เอ-โฮสต์ยังเดินหน้าธุรกิจอย่างต่อเนื่องโดยการขยายหน่วยงานใหม่เพิ่มขึ้นนั่นก็คือ Core Technology Division หน่วยงานเทคโนโลยีหลักที่ให้คำตอบเบ็คเสร็จแก่ลูกค้าด้วยระบบฐานข้อมูลและเครื่องมือต่างๆ ของออราเคิลซึ่งช่วยเพิ่มความสามารถของลูกค้าในการออกแบบพัฒนาปรับเปลี่ยนระบบแอพพลิเคชันให้ เหมาะสมกับธุรกิจนั้นๆภายใต้คำปรึกษาแนะนำและการวางระบบของเอ-โฮสต์ลูกค้าสามารถบริหารระบบ ฐานข้อมูลของตนเองและดูแลระบบคังกล่าวได้อย่างมีประสิทธิภาพ

ตลอดระยะเวลามากกว่า10ปีในการดำเนินธุรกิจของเอ-โฮสต์ไม่เพียงแต่ในฐานะผู้บุกเบิกธุรกิจโฮสติง และธุรกิจการให้บริการโปรแกรมประยุกต์ในรูปแบบ ASP เท่านั้นแต่เอ-โฮสต์ยังได้ทำการติดตั้งระบบ สารสนเทศรวมทั้งผลิตภัณฑ์ของออราเคิลให้กับลูกค้าจนประสบความสำเร็จเป็นจำนวนมากซึ่งหลายรายเป็น หนึ่งในร้อยบริษัทชั้นนำของประเทศไทยแต่สิ่งที่สำคัญกว่านั้นก็คือการที่เอ-โฮสต์ได้สานสัมพันธ์กับลูกค้า และพันธมิตรทางธุรกิจอย่างแนบแน่นจนกลายเป็นหุ้นส่วนทางกลยุทธ์และได้รับตั้งแต่งให้เป็น OCAP (Oracle Certified Advantage Partner) รายแรกในประเทศไทย



ร**ูปที่ 1.2** รางวัล<mark>ท</mark>ี่บริษัท A-HOS</mark>T ได้รับ

้ ปัจจุบันเอ-โฮสต์มีประเภทของสินค้าและการบริการซึ่งสามารถแบ่งออกเป็น 3 กลุ่มใหญ่ได้แก่

3

1.2.1 Hosting & Outsource Service

เอ-โฮสต์ได้ปรับปรุงและขยายการบริการ Hosting และการให้บริการภายนอก (Outsource) จน สามารถครอบคลุมความต้องการของลูกค้าได้อย่างหลากหลายโดยยึดหลักในการในการให้บริการที่เรียกว่า "Peace of Mind for the customer" ซึ่งหมายถึงการที่จะทำงานให้กับลูกค้าแบบครบวงจรเพื่อที่ลูกค้าจะได้ สามารถใช้งานระบบสารสนเทศได้อย่างมีประสิทธิภาพได้อย่างสบายใจไร้ความกังวลต่อความเสี่ยงต่างๆ ไม่ ว่าจะเป็นเรื่องของปัญหาทางเทคนิคการจัดทำระบบและข้อมูลสำรองการปรับแต่งระบบให้ได้ประสิทธิภาพ สูงสุด (Performance Tuning) และที่สำคัญที่สุดคือการที่เข้ามารับภาระในด้านการบริหารจัดการบุคลากร ทางด้านสารสนเทศทั้งหมดแทนลูกค้า

การใช้บริการ Hosting และ Outsource จะทำให้ลูกค้าสามารถทุ่มเทกำลังสมองเวลาและทรัพยากร ขององค์กรให้กับธุรกิจที่เป็นแกนหลัก (Core Business) ซึ่งเป็นสิ่งที่ลูกค้าถนัดกว่าโดยทั่วไปแล้วบริการ Hosting และOutsource จะประกอบด้วยส่วนประกอบและบริการย่อยๆดังต่อไปนี้

- 1. High Availability and High Performance IT Infrastructure
- 2. Dedicated or Co-Location Service
- 3. Disaster Site
- 4. Oracle E-Business Application (ERP, CRM, SCM)
- 5. ERP Implementation Service
- 6. System and Database Administration
- 7. Help Desk

8. On-Request Service i.e. On-Site Support, Software Customization ทั้งนี้การบริการ Hosting และ Outsource สามารถครอบคลุมได้ทั้งระบบที่ใช้เทคโนโลยีของออรา เคิลและระบบที่ใช้เทคโนโล<mark>ยีอื่</mark>นๆ

1.2.2 Oracle Core Technology Products and Advanced Services

เอ-โฮสต์เป็นผู้นำในการ<mark>คำเนินธุรกิจใน</mark>ฐานะผู้แทนจำหน่ายเพิ่มมูลค่าให้กับออราเคิลโดยไม่ เพียงแต่ทำหน้าที่ในการจัดจำหน่ายสินค้าในกลุ่มแกนหลักของเทคโนโลยี (Core Technology) ของออราเคิล ทุกประเภทแต่ยังมีทีมผู้เชี่ยวชาญที่จะให้การสนับสนุนและบริการเสริมอย่างครบวงจรแก่บริษัทคู่ค้าและ ลูกค้าไม่ว่าจะเป็นการร่วมจัดกิจกรรมทางการตลาดการฝึกอบรมการติดตั้งระบบและการให้คำปรึกษาเพื่อ แก้ไขปัญหาต่างๆสินค้าและบริการที่อยู่ในกลุ่ม Oracle Core Technology Products and Advanced Services ได้แก่

- 1. Oracle Database and database options
- 2. Oracle Business Intelligence Suite
- 3. Business Partner Development
- 4. System Installation, Integration and Optimization
- 5. Oracle Fusion Middleware (รวมถึง BEA)
- 6. สินค้าอื่นๆทุกประเภทของออราเคิล
- 7. Marketing and Lead Generation Activities
- 8. SOA-Based Development and Implementation

ผลสำเร็จในการคำเนินธุรกิจประเภทนี้ทั้งในด้านการตลาดและบริการทำให้เอ-โฮสต์ได้รับรางวัล ASEAN Partner of the Year ในปี 2005

1.2.3 Oracle Enterprise Performance Management (EPM) 1182 Hyperion Business Intelligence Products and Services

ความต้องการสูงสุดประการหนึ่งของผู้บริหารในการนำเอาระบบสารสนเทศมาใช้ในองค์กรไม่ว่าจะ เป็นภาคราชการหรือเอกชนคือการทำให้ผู้บริหารสามารถได้ข้อมูลที่แสดงให้เห็นถึงสถานะในการคำเนิน ธุรกิจได้อย่างแม่นยำรวดเร็วและการนำเอาข้อมูลมาวิเคราะห์และวางแผนทั้งในระดับปฏิบัติการและใน ระดับกลยุทธ์เพื่อให้ธุรกิจสามารถได้เปรียบในการแข่งขันปรับตัวตามเศรษฐกิจได้ในทุกสถานการณ์ Oracle Enterprise Performance Management (EPM) และ Hyperion Business Intelligence จัดเป็นซอฟต์แวร์ชั้น แนวหน้าของโลกที่สามารถสนองตอบต่อกวามต้องการในลักษณะดังกล่าวได้เป็นอย่างดี

เอ-โฮสต์มีทีมงานที่ปรึกษาที่มี<mark>ประ</mark>สบการณ์ทั้งทางด้านธุรกิจและทางด้านเทคนิครวมถึงความเข้าใจใน ระบบ ERP ของออราเคิลอย่างลึกซึ้งจึงทำให้สามารถให้บริการที่ปรึกษาเพื่อออกแบบติดตั้งเชื่อมโยงและ ปรับใช้ระบบให้กับลูกค้าจนเกิดประสิทธิภาพสูงสุดอีกทั้งยังมีความยืดหยุ่นและให้การตอบสนองที่เร็วกว่า เมื่อเทียบกับการว่าจ้างที่ปรึกษาจากต่างประเทศ

1.3 รูปแบบการจัดองค์กรและการบริหารองค์กร



คุณอนันต์ ลี้ตระกูล ประธานกรรมการ



คุณบุญประสิทธิ์ ตั้งเวัยสุข กรรมการพู้จัดการ



คุณเลิศ รักษ์ศิริวณิช กรรมการพู้จัสการ ABCs Company Limited





คุณประสงค์ เอื้อสุริยมันท์ พู้อำนวยการฟ้าย Hosting and Outsourcing Services



คุณทนกวรรณ หะลีท์รัตนวัฒนา พู้อำนวยการฟ่ายการตลาด



คุณวิชัย วงศ์จริยกุล พู้อำนวยการพ่ายให้ค่าปรึกษา

ภาพที่ 1.3 คณะผู้บริหาร A-HOST Company Limited

1.4 ตำแหน่งและหน้าที่งานที่นักศึกษาได้รับมอบหมาย

ตำแหน่ง : System Engineer หน่วยงาน : SMS STITUTE OF

T

6

1.5 พนักงานที่ปรึกษาและตำแหน่งของพนักงานที่ปรึกษา

นาย ภูดิศ คุพัสกูล

ตำแหน่ง : System Engineer

KPI Description	Expected Results
1. ศึกษา Security Hardening และมีหัวข้อต่อไปนี้เป็น	- สามารถ present feature ใด้และมีเอกสาร ppt ประกอบการนำสนอโดยมี
ส่วนหนึ่งด้วย	เอกสาร 2 ชุคสำหรับนำเสนอสอง session คังนี้
- แต่ละ option เหมาะกับการนำมาใช้งานอย่างไร	- Technical session
- ข้อจำกัดอะไรบ้าง	- Sale session โดยใน session นี้จะต้องมี sale เข้าร่วมฟังด้วยอย่างน้อย 1 คน
- มิใน os อะไรบ้าง	- เอกสารได้รับการ review และ approve จาก mentor
2 Install OS Linux and Configuration	นี้การ พร้อม การ และต้องบำสมอต่อ เมละซึ่งเ
Install Oracle Database	
- Database ตัวอื่นๆ	technical เต
- Configure hardening	- มเขาถามาว่า conngure เป็น step by step แถะมาปามาพบาราชบถาหาบ
	แต่ถะ step
	- lotid is loss approve v iff mentor
3. Install OS Windows and Configuration	- มี Demo system ฟร์อม Test Case และต่องน้ำเสนอตอ mentor และทีม
- Install Oracle Database	technical ได้
- Database ตัวอนๆ	- มีเอกสาเพเรตัวอย่างขั้นตอนการทำงาน และ concept การทำงาน
- Configure hardening	พร้อมแผนภาพการทำงานของระบบ
	- เอกสารได้รับการ review และ approve จาก mentor
4. Install OS AIX and Configuration	- ม <mark>ี Demo system พ</mark> ร้อม T <mark>est Ca</mark> se และต้องนำเสนอต่อ mentor และทีม
- Install Oracle Database	technical ได้
- Database ตัวอื่นๆ	- ม <mark>ีเ</mark> อกสารกา <mark>ร con</mark> figure เ <mark>ป็น s</mark> tep by step และมีรูปภาพประกอบสำหรับ
- Configure hardening	-แต่ละ step
	- เอกสารได้รับการ review และ approve จาก mentor
5. จัดทำ Individual Work List	- นำเสนอ IWL เป็นประจำทุกเดือน
NST	ITUTE OF

1.6 ระยะเวลาที่ปฏิบัติงาน

ระยะเวลาปฏิบัติงานสหกิจศึกษาเป็นเวลา 4 เดือน

- เริ่มต้นปฏิบัติงานสหกิจศึกษา วันที่ 4 มิถุนายน 2561
- สิ้นสุดงานสหกิงศึกษา วันที่ 4 กันยายน 2561

1.7 วัตถุประสงค์ของการปฏิบัติงานและโครงงานที่ได้รับมอบหมาย

- 1. เพื่อศึกษาการและหาประสบการณ์การทำงานจริงภายในองค์กร
- 2. เพื่อนำความรู้ที่ได้ไปใช้ในการพัฒนาโครงงานและการทำงานในอนาคต

1.8 ผลที่คาดว่าจะได้รับจากการปฏิบัติงานและโครงงานที่ได้รับมอบหมาย

1. ได้ประสบการณ์ในการทำงานจริง

10

2. ได้นำความรู้มาประยุกต์ใช้ในการทำงาน

บทที่2 ทฤษฎีและเทคโนโลยีที่ใช้ในการปฏิบัติงาน

2.1 ระบบปฏิบัติการ Linux



ภาพที่ 2.1 สัญลักษณ์ของ Linux

Linux ก็คือระบบปฏิบัติการหนึ่งที่ใช้ในการเชื่อมต่อกับฮาร์ดแวร์ หรืออาจจะรู้จัก ในภาษาอังกฤษ กือ Operating System เช่นเดียวกับ Windows, Dos หรือ Unix ซึ่งลีนุกซ์ถูก สร้างขึ้นโดย Linus Tovalds นักศึกษาภากวิชาวิทยาการคอมพิวเตอร์ มหาวิทยาลัย Helsinki โดยทา เป็นโปรเจคตอนที่เขากำลังศึกษาอยู่ที่ นั้น ในปี ค.ศ. 1989 ซึ่งเขาได้ต่อยอดมาจาก ระบบปฏิบัติการ Unix Linus Tovalds ได้สร้าง Linux ขึ้นมา และ ได้เชิญชวนผู้ร่วมพัฒนา คนอื่นๆ ทางอินเทอร์เน็ต ซึ่งต่อมากลายเป็นทีมผู้พัฒนาที่ทำงานและติดต่อกัน ทาง อินเทอร์เน็ต ซึ่งทุกคนต่างกันพัฒนาโดยไม่มีค่าแรงหรือผลตอบแทนประการใด พวกเขา พัฒนา Linux ขึ้นมาด้วยใจรักในสิ่งที่พวกเขากำลังทำโดยส่วนมากแล้วผู้คนจะใช้ OS Linux ไปใช้ทำเซิฟเวอร์เพราะกิน แรงเครื่องน้อย และเครื่องจะเสถียรกว่าการใช้ OS ทั่วไป และที่สำคัญก็คือ Linux เป็น Software แบบ Open Source ที่คุณสามารถ ปรับแต่งได้ตาม ต้องการ ด้วยเหตุนี้เองจึงทำให้ Linux ได้มีผู้ที่นำไปพัฒนาจน กลายเป็นระบบที่หลากหลายและในเวลา ต่อมา จึงมี OS เกิดขึ้นมากมาย ที่แตกแขนงมาจาก Linux อาทิเช่น Ubuntu, Debian, Redhat และอื่นอีกมากมายอย่างนับไม่ถ้านิ่งนิ่งใน เกาเป็น Linux Distribution

2.1.1 ข้อดีของ Linux

2.1.1.1 ใช้งานได้ไม่เสียค่าใช้จ่าย

ระบบปฏิบัติการอย่าง Linux เป็น Open Source อยู่ภายใต้ลิขสิทธิ์ที่เรียกกันว่า General License (GPL) ซึ่งหมายความว่า สามารถโหลดมาใช้ได้กันอย่างฟรีๆ และ ดัดแปลงแก้ไขได้ตามความ ต้องการ

2.1.1.2 ความปลอดภัยในการทำงาน

Virus ทั้งประเภท Adware, Malware, Trojan ล้วนโจมตีแต่ระบบปฏิบัติการที่ใช้ กันทั่วไปใน โลกนี้ นั่นก็คือ Windows อีกทั้งโดยปกติการรันโปรแกรมใน Linux และ Unix ทั้งหลายจะต้องใช้สิทธิ root หรือความเป็นเจ้าของเครื่องเท่านั้น ซึ่งจะใช้สิทธิ root ได้ก็ ต่อเมื่อใส่ Password ทุกครั้งเท่านั้น ดังนั้นหาก โปรแกรมหรือระบบใด ๆ ที่ต้องการติดตั้ง ลงในเครื่องจะต้องผ่าน root ทุกครั้ง

2.1.1.3 เสถียรภาพในการทำงาน

ลีนุกซ์มีเสถียรภาพในการทำงานสูง ปัญหาระบบลุ่มในระหว่างทำงานจะไม่ค่อยมี ให้พบ โดย ความสามารถพิเศษของลีนุกซ์อยู่ที่การตรวจสอบความสัมพันธ์ของโปรแกรม ในการทำงาน เช่น ถ้าติดตั้ง โปรแกรม 1 ลีนุกซ์จะทำการตรวจสอบว่าโปรแกรม 1 มีการ เรียกใช้งานโปรแกรมอื่นทำงานด้วยหรือไม่ นอกจากนี้ถ้าทำการติดตั้งหรือลบโปรแกรม ออกจากระบบ โดยไม่จำเป็นต้องบู๊ตเครื่องใหม่ สามารถทำงาน ต่อไปได้ทันที

2.1.1.4 สนับสนุนฮาร์ดแวร์ทั้งเก่าและใหม่

เทคโนโลยีของอุปกรณ์ฮาร์ดแวร์มีการเปลี่ยนแปลงไปอย่างรวดเร็ว ระบบปฏิบัติการโดยส่วน ใหญ่มักจะออกมาเพื่อรองรับประสิทธิภาพการทำงานของ ฮาร์ดแวร์ที่พัฒนาขึ้น จนทำให้บางครั้งต้องการ อัพเกรดเครื่องตาม แต่สำหรับลีนุกซ์จะ ยังคงสนับสนุนฮาร์ดแวร์เก่าให้สามารถใช้งานได้ โดยจะเพิ่มส่วน ของการสนับสนุน ฮาร์ดแวร์ตัวใหม่ลงไปเท่านั้นทำให้ไม่จำเป็นต้องเปลี่ยนฮาร์ดแวร์ซึ่งช่วยประหยัด ค่าใช้จ่ายลงไปได้มาก

STITUTE O

2.1.2 โครงสร้างของ Linux



11

ภาพที่ 2.2 โครงสร้างของ Linux

ระบบปฏิบัติการ Linux สามารถแบ่งโครงสร้างหลัก ๆ ได้ 4 ระดับ แต่ละระดับก็จะทำหน้าที่ต่างกัน 2.1.2.1 ฮาร์ดแวร์ (Hardware)

หมายถึงอุปกรณ์หรือทุกชิ้นส่วนของคอมพิวเตอร์ ที่สามารถจับต้องได้ เช่น จอภาพ คียบ์ อร์ค เม้าส์ ดิกส์ไดรซ์ ซีดีรอม เป็นต้น

2.1.2.2 ยูนิกซ์ เคอร์เนล (Kernel)

เกอร์เนล จะทาหน้าที่ควบคุมการทางานทั้งหมดของระบบ ได้แก่ การจัดสรร ทรัพยากร การจัดการข้อมูลบริการหน่วยความจา ซึ่งเกอร์เนลนี้จะขึ้นกับฮาร์ดแวร์ เช่น ถ้ามี การเปลี่ยนแปลง ฮาร์ดแวร์ เกอร์เนลนี้ก็จะถูกเปลี่ยนไปด้วย เป็นต้น

2.1.2.3 เชลล์่ (Shell)

ตัวกลางระหว่างผู้ใช้กับตัวเค<mark>อ</mark>ร์เนล ทาหน้าที่รับคาสั่งจากผู้ใช้ แล้วนาไปแปลเป็น ภาษาที่ เครื่องคอมพิวเตอร์เขา∴ี่ใจ เรียกอีกอย่างหนึ่งได้ว่า command interpreter แต่ถ้ามีการ นา เชลล์หลาย ๆ ตัวมา เขียนรวมกัน (คล้าย ๆ กับ batch fil<mark>e ใน</mark>ระบบปฏิบ<mark>ต</mark>ิ๊การ DOS) จะ เรียกว่<mark>า เชล</mark>ล์สคริปต์

2.2 VMware Workstation

ภาพที่ 2.3 สัญลักษณ์ของ VMware Workstation

mware

โปรแกรม VMware เป็นโปรแกรมที่ถูกกิดก้นขึ้นมาเพื่อสร้างกอมพิวเตอร์เสมือน (Virtual Machine) ขึ้นบนระบบปฏิบัติการเดิมที่มีอยู่ ตัวอย่างเช่น เกรื่องกอมพิวเตอร์ที่ลง ระบบปฏิบัติการ Windows XP อยู่เดิม แล้วทำการลงระบบปฏิบัติการ Windows NT ผ่าน โปรแกรม VMware อีกทีหนึ่ง ซึ่งเมื่อลงแล้ว ทั้งสองระบบสามารถทำงานพร้อมกันได้โดย แขกจากกันก่อนข้างเด็ดขาด (เสมือนเป็นคนละเครื่อง) โดย กอมพิวเตอร์เสมือนที่สร้าง ขึ้นมานั้น จะมีสภาพแวดล้อมเหมือนกับกอมพิวเตอร์จริงๆ เกรื่องหนึ่ง ซึ่งจะ ประกอบด้วย พื้นที่ดิสก์ที่ใช้ร่วมกับพื้นที่ดิสก์ของเครื่องนั้นๆ การ์ดแสดงผล การ์ดเน็ตเวิร์ก พื้นที่ หน่วยความจำซึ่งจะแบ่งการทำงานมาจากหน่วยความจำของเครื่องนั้นๆ เช่นกัน สำหรับข้อจำกัดของการ ทำงานบน VMware ก็คือ VMware จะสร้าง สภาพแวดล้อมของฮาร์ดแวร์ท่างๆ ซึ่งเป็นของตัวโปรแกรม VMware เอง ดังนั้นการใช้ ฮาร์ดแวร์ของคอมพิวเตอร์หลักและกอมพิวเตอร์เสมือนจะไม่เหมือนกัน จึงไม่ สำหรับการใช้ไปรแกรมนี้จะแบ่งหน่วยความจำของเครื่องหลักไปใช้ด้วยหาก หน่วยความจำเของเครื่องมี ขนาดไม่มากเพียงพอ ก็อาจทำให้เครื่องทำงานช้าลงมาก ดังนั้น หากมีหน่วยความจำเยอะ การทำงานของ โปรแกรมนี้ก็จะดีขึ้น

STITUTE OV

2.3 Windows Server



ภาพที่ 2.4 สัญลักษณ์ของ Windows Server

Window Server คือ Hosting ที่ใช้ระบบปฏิบัติการ Windows 2000 Server เป็น Hosting รองรับ ภาษา html, shtml, java, cgi, perl, php, asp, aspx

2.3.1 Windows Server 2008 R2

Windows Server 2008 R2 เป็น server OS สามารถให้บริการไคห้ลายประเภทใน เวลาเคียวกัน โดย ที่ส าคัญ windows server 2008 R2 สามารถควบคุมผู้ใชไ่้คค้รอบคลุมทุก กรณีไม่ว่าจะย้ายไปท างาน ที่เครื่องใคก็ตาม ก็คือ สามารถควบคุมเครื่องในเครือข่ายได้โดย ไม่ต้องไปจัดการที่เครื่องถูกข่ายเลย ก าหนดสิทธิ์การเข้าถึงอุปกรณ์ของเครื่องถูกข่ายได้ ไม่ ว่าจะเป็นการเขา:ั้ถึงไดร์วก าหนดการใชแ่้ฟลช ไดร์วได้การคอนโทรลต่างๆ ก าหนดเวลาใน การเข้าถึงเครือข่าย (LAN) หรือ อินเทอร์เน็ตได้

2.3.2 Windows Server 2012 R2

Windows Server 2012 R2 คือระบบปฏิบติ๊การคอมพิวเตอร์ที่ใช้รันงานทางฝั่งเซิฟ เวอร์ (Server) เพื่อให้บริการแก่เครื่องลูกข่าย (Client) เป็นผลิตภณัฑ์หรือซอฟตแ่๋วร์ของ ไมโครซอฟต์ บริษัท ยักษ์ใหญ่ที่มีชื่อเสียงคา ั้นการพฒันาซอฟตแ่๋วร์ ความสามารถของตวั ระบบนั้นได้แก่ Hyper-V หรือก็คือ ระบบเสมือน สามารถจ าลองเครื่องคอมพิวเตอร์ได้ หลายเครื่องโดยไม่เสียค่าใช้ง่ายในการติดตั้ง Windows Server ในระบบเสมือน

2.3.3 Windows Server 2016

Windows Server 2016 เป็นระบบปฏิบัติการสำหรับเครื่อง Server รุ่นใหม่ล่าสุดที่จะมาทดแทน Windows Server 2012 R2 ที่เปิดตัวไปเมื่อปี 2556 โดยในคราวนี้ Windows Server 2016 ได้มีการปรับปรุง เปลี่ยนแปลงฟีเจอร์ภายในมากมาย เพื่อให้รองรับกับการใช้ Server ในหลากหลายรูปแบบในปัจจุบัน และได้มาการเพิ่มมาหลักๆ 9 ข้อคือ

2.3.3.1 Nano Server ฟีเจอร์ใหม่

10



14

ภาพที่ 2.5 Nano Server

มากราวนี้ใน Windows Server 2016 ไมโกรซอต์เลยพัฒนาฟีเจอร์ใหม่ล่าสุดออกมา คือ Nano Server ซึ่งก็คือ Windows Server ขนาดเล็กกว่าเดิม มีขนาดหลังจากติดตั้งเสร็จแล้ว เหลือเพียง 500MB กว่าๆ แต่ก็มีความสามารถด้าน Server ก่อนข้างจะครบกรัน และสามารถติดตั้งโปรแกรม หรือ Services ต่าง ๆ เพิ่มได้ เรียกได้ว่า Nano Server ดูจะเป็นคู่แข่งที่สมน้ำสมเนื้อกับ OS Server ตระกูล Unix/Linux มากขึ้น หรือบางทีอาจจะล้ำหน้าด้านนวัตกรรมไปนิดๆเสียด้วยซ้ำ

Nano Server Just enough OS

Provides higher density, reduced attack surface and servicing requirements

Ideal for cloud inspired infrastructure

• Smaller image size, smaller attack surface, faster boot time

Ideal for next generation app development

- Built for containers and cloud-native apps
- Full developer experience with Windows SDK and Visual Studio



ภาพที่ 2.6 ความสามารถของ Nano Server

สำหรับ Nano Server วิธีการติดตั้งจะ ไม่เหมือนกับ Windows Server ปกติ คือไม่ต้องมี กระบวนการ Install หรือการกำหนดไดร์ฟสำหรับ Boot แต่จะใช้วิธีติดตั้งแบบ Image File แบบเดียวกับการ ติดตั้ง OS ในระบบ Cloud โดยขั้นแรกของการติดตั้งจะต้องทำการเลือกส่วนประกอบต่าง ๆ ที่จะใช้ ใน Nano Server แล้วสร้างเป็นไฟล์ Image ขึ้นมาก่อน (ทั้งหมดนี้ทำผ่าน Command line โดยใช้ tools ใน แผ่นติดตั้ง Windows Server 2016) แล้วจึงก่อยนำไฟล์ Image ไปติดตั้งลงบนเครื่อง Server หรือใน Virtual Server ใน Cloud

Nano Server เป็น OS ที่ไม่มี UI คือไม่สามารถควบคุมและสั่งงานตัว Nano Server ที่หน้าเครื่องได้ ที่หน้าเครื่องทำได้เฉพาะการตั้งก่า Network เพื่อให้ตัว Nano Server ต่อออก Network ได้เท่านั้น(Nano Server ไม่รองรับการต่อ Network ผ่าน Proxy) การจะควบคุมสั่งการ Nano Server ทำได้โดยการใช้ Command line โดยผ่าน Windows Remote Management (WinRM) เท่านั้น

15
2.3.3.2 สร้างมาเพื่อ Cloud Technology โดยเฉพาะ



ภาพที่ 2.7 Layers of Security

Windows Server 2016 ถูกพัฒนามาเพื่อรองรับสถาปัตยกรรมแบบ Cloud โดยเฉพาะ จึงมีฟีเจอร์ เด็ดๆ ที่ออกมารองรับกับ Cloud Technology หลายฟีเจอร์ อาทิ

- Hyper-V รุ่นใหม่ ที่ถูกปรับปรุงให้ดีขึ้น และรองรับการทำงานแบบ Container
 - Nano Server ที่สามารถนำไปสร้างเป็น Server เล็กๆบน Cloud เพื่อใช้งานได้อย่างกุ้มค่าทรัพยากร
 - Shielded Virtual Machine ยกเครื่องระบบความปลอดภัยใหม่ สำหรับ Hyper-V ช่วยให้มั่นใจ ได้มากขึ้นว่าจะไม่มีช่วงโหว่ที่ร้ายแรงจากตัวของระบบ Virtual Machine เอง
 - ผสานระบบ Active Directory กับระบบ Cloud ไปด้วยกัน ทำให้คุณสามารถเชื่อม Server หรือ Service ที่อยู่ใน Cloud เข้ามาอยู่ในกลุ่ม Active Directory เดียวกัน เหมือนอยู่ใน LAN วงเดียวกัน

STITUTE O

Microsoft Azure

ภาพที่ 2.8 โลโก้ Microsoft Azure

นอกจากนี้แล้ว Windows Server 2016 ยังถูกออกแบบมาให้เข้ากันได้ดีกับ platform Microsoft Azure ช่วยให้สามารถย้ายระบบ Server เดิม ๆ เข้าสู่ Cloud ของ Azure ได้อย่าง

2.3.3.3 Hyper-V รองรับกับ Linux ชื่อดังเกือบทั้งหมด



ภาพท<mark>ี่</mark> 2.9 <mark>Hyper-V</mark> Funct<mark>io</mark>n

ด้วยความเป็น Cloud Ready ของ Windows Server 2016 ทำให้ต้องเปิดเพื่อรองรับการทำงาน ร่วมกับระบบปฏิบัติการอื่น โดยเฉพาะ Linux Server ซึ่งมีจำนวนผู้ใช้งานอยู่ในปัจจุบันเป็นจำนวนมาก ใน Hyper-V ของ Windows Server 2016 รองรับการทำงานร่วมกับ Linux ชื่อดังเหล่านี้ได้อย่างเต็ม 100% และสามารถเชื่อมต่อระบบ Linux Server เพื่อเข้าใช้งานร่วมกับกลุ่ม Server ที่ใช้ผลิตภัณฑ์ Microsoft Windows Server ได้อย่างไม่มีปัญหา เช่น Red Hat Linux, SUSE, OpenSUSE, CentOS, Ubuntu, Debian, Oracle Linux 2.3.3.4 ปลอดภัยขึ้นด้วย Security ใหม่ ใน Windows Server 2016

Security	Application platform
 Privileged identity Security Virtual Machine Security 	Nano ServerContainers
SDDC	Management
 3 Compute 4 Storage 5 Network 6 Remote Desktop Services (RDS) 	9 PowerShell10 Server management tools

ภาพที่ 2.10 ระบบ Security ใหม่

ใน Windows Server 2016 มีการปรับปรุงระบบ Security ใหม่ในหลายส่วน อาทิ

- Shielded VMs ระบบที่ช่วยรักษาความปลอดภัยให้กับ Virtual Machines ต่างๆ ในเครื่อง ป้องกัน ไม่ได้เกิดการละเมิดความปลอดภัยระกว่าง VM ด้วยกันเอง หรือแม้แต่จาก VM เข้ามายังเครื่องแม่
- "Headless" Windows Defender โปรแกรม Windows Defender ที่ใช้จัดการกับไวรัสต่างๆ ใน เวอร์ชันที่แถมมากับ Windows Server 2016 ได้มีการเพิ่มความสามารถในการจัดการกับมัลแวร์ รวมทั้งมาในรูปแบบ Headless คือทำงานในลักษณะเป็น Command Service ที่ไม่มี GUI ช่วยให้กิน ทรัพยากรน้อยลง และตรวจพบปัญหาต่างๆ ได้เร็วขึ้น
- Linux Secure Boot เดิมใน Windows Server จะ ไม่สามารถ Secure Boot กับ Linux บน VM ที่ สร้างขึ้นใน Windows Server ได้ แต่ด้วยระบบ Security ใหม่ใน Windows Server 2016 ได้มีการ ปรับปรุงจนทำให้สามารถ Secure Boot ใน VM ได้กับ Linux ทุกตัว ช่วยยกระดับความปลอดภัย ให้กับ VM มากขึ้น

และนอกเหนือจากที่กล่าวมานี้ยังมีระบบ Security อื่นๆ อีกมากที่ถูกเพิ่มมาใน Windows Server 2016 อีก มาก ที่จะช่วยให้มั่นใจได้ว่าจะไม่พบปัญหาน่าปวดหัวเรื่อง Security เหมือนกับ Windows Server เวอร์ชันที่ ผ่านๆ มา อย่างแน่นอน

NSTITUTE OF

2.3.3.5 จัดการ Server ได้ลึกและละเอียดขึ้นด้วย PowerShell 5.0

•	₽			٠	☆		絙	j.Cjr		۶
Agent Health NEW Available The Agent Realth solution gives customers might into the health, performance and analability of their agents (both Windows and Linux	AD Replication Status Available Unrifly Active Directory replicationissues in your environment.	Azure Networking Analytics (Preview) Available Gain insight into your Azare Network Security Goup and Application Cateway logs	Containers Available See Ducker container performance metrics and logi from containers across your public or private cloud your public or private cloud	Network Performance Nonitor (Preview) Analiable Offers near real Sine monitoring of network performance parameters like loss and latency.	Service Fabric Corning Interesty and troubleshoot Issues accross year Service Fabric cluster	Surface Hub Available Provides the ability to montor Microsoft Surface Hub devices.	AD Assessment Owned Assess the risk and health of Active Directory provonments.	Asure Automation Osmed Automate time consuming and frequently repeated tasks in the doubland en- premises.	Change Tracking Owned Track configuration changes acrossyour servers.	SQL Assessment Dwmed Assess the tak and health-of SQL Server environments.
這	١	₩	Ŷ	ŋ	2	<	*	ð	۷	×
SCOM Assessment New Coming Assess the risk and health of System Conter Operations Manager Server anvironments.	Alert Management Available View your Operations Manager and OMS alerts to early things alerts and thereify the root causes of problems in your	Upgrade Analytics (Preview) Available Use a data-stheen approach to streamline and accelerate Windows upgrades.	Key Vault (Preview) Available Understand your Key Vault usage through Analysis of Key Vault logs	Office 365 (Preview) Anailable Get full visibility into your Office 365 user activities, perform forensics as well as audit and compliance.	Azure Site Recovery Available Monitor vistual machine replication status for your Azure Site Recovery likult	Wire Data Coming Provides the ability to explore whe data and helps identify network related tasas.	Antimalware Assessment Owned View status of antinesis and antimalware scare across your servers.	Backup Owned Manage Azure IaaS VM backup and Windows Server backup status for your backup vault	Security and Audit Owned Povides the ability to explore security valated data and helps identify security towactes.	System Update Assessment Owned stentify maxing system updates accessiour servers.

ภาพที่ 2.11 PowerShell 5.0

Windows Server 2016 มาพร้อมด้วย PowerShell 5.0 ที่จะช่วยให้สามารถเข้าควบคุมและจัดการ แทบทุกอย่างใน Server ได้ทั้งหมดผ่าน Command line นอกไปจากนั้น หากต้องการควบคุมและจัดการใน แบบที่ซับซ้อนมากขึ้น หรือลงรายละเอียดมากขึ้น ก็สามารถพัฒนาสคริปขึ้นมาใช้งานเองได้ผ่าน Windows Management Framework 5.0 ใน Windows Server 2016 ตัว PowerShell ยังสามารถสั่งงานไปยังเครื่อง Virtual Server ในระบบโดยสั่งงานบนเครื่อง Host ได้เลยผ่าน option "-VMName" ไม่ต้องไปนำกำสั่ง Run ในเครื่อง Virtual Server อีกต่อไป

2.3.3.6 ReFS เสถียรและสมบูรณ์แบบ ใน Windows Server 2016



ภาพที่ 2.12 ระบบ ReFS

Resilient File System (ReFS) ระบบ File System ตัวใหม่ที่ไมโกรซอฟต์พยายามผลักดันเพื่อใช้ แทน NTFS เดิม แต่ด้วยความไม่เสถียรภาพของระบบไฟล์ นับตั้งแต่เริ่มเปิดให้ใช้ใน Windows Server 2012 ทำให้ระบบไฟล์นี้ยังไม่ได้รับความนิยม ทั้งๆที่เป็นระบบไฟล์ที่ถูกออกแบบมาเป็นอย่างดี และมี ประสิทธิภาพสูงกว่าระบบไฟล์แบบ NTFS แต่ในWindows Server 2016 ระบบ ReFS ได้ถูกพัฒนาขึ้นมา อย่างสมบูรณ์และพร้อมใช้งานอย่างที่สุด มีความประสิทธิภาพและเสถียรภาพสูง สามารถใช้งานแทน NTFS ได้อย่างสมบูรณ์และไม่ก่อให้เกิดปัญหาอีกด้วย

2.3.3.7 Nested Virtualization

Level 1

Level 0

Windows Root OS



Hyper-V Hypervisor

CPU

Virt. Extensions

or w/ Virtualization Extensions

Windows Root OS

20

Level 2

1

vCPU

Hyper-V Hypervisor

Virt. extension vCPU

ฟีเจอร์ Nested Virtualization ที่ช่วยให้คุณสามารถสร้าง Virtual Server ซ้อนในเครื่องที่เป็น Virtual Server เป็นหนึ่งในฟีเจอร์ยอดฮิตที่เคยถูกตัดออกจาก Hyper-V และ ได้ถูกนำกลับมาใหม่อีก ครั้ง Windows Server 2016 ทำให้คุณสามารถบริหารจัดการเครื่อง Virtual Server ได้อย่างไม่มีขีดจำกัดอีก ต่อไป



2.3.3.8 Software-defined storage จัดการพื้นที่เก็บข้อมูลได้ง่ายขึ้น

ภาพที่ 2.14 ระบบ Software-defined storage

10

การจัดการพื้นที่เก็บข้อมูล หรือ storage ในสมัยก่อนของ Windows Server จะทำได้ก่อนข้างยาก เพราะระบบจัดการจะยึดตาม Hardware ที่ใช้เก็บข้อมูลเป็นหลัก แต่ด้วยระบบจัดการพื้นที่เก็บข้อมูลแบบ ใหม่ของ Windows Server 2016 ที่มองพื้นที่เก็บข้อมูลเป็นแบบ Software ทำให้สามารถปรับเปลี่ยนและ บริหารจัดการได้ง่ายขึ้น โดยไม่สร้างความเสียหายให้กับข้อมูลที่ถูกจัดเก็บไว้อยู่แล้ว เช่น กุณสามารถจะสร้าง high availability storage ได้ง่ายขึ้นโดยไม่ต้องเสียเงินซื้อ Hardware storageราคา แพง, หรือสามารถสร้าง Storage Replica ในระดับ volume level และแถมด้วย Storage QoS ที่ช่วยบริหาร จัดการคิวการเข้าถึงพื้นที่เก็บข้อมูล ช่วยให้ Virtual Server เข้าถึงพื้นที่เก็บข้อมูลอย่างมีเสลียรภาพและ ประสิทธิภาพเท่าเทียมกันในทุก Virtual Server <complex-block><complex-block><complex-block><complex-block><complex-block><complex-block><complex-block><complex-block>

2.3.3.9 รองรับ Containers แนวคิด Virtual Server ที่กำลังเป็นที่นิยม

ภาพที่ 2.15 รับระบบ Containers

(0)

Containers คือการกำหนดสภาพแวดล้อมให้เหมาะสำหรับซอฟต์แวร์นั้น ๆ เพื่อให้เกิด ความปลอดภัยของตัวซอฟต์แวร์ และป้องกันเรื่องรบกวนกันระหว่างซอฟต์แวร์ต่าง ๆ แนวกิดนี้ กำลังได้รับความนิยมอย่างสูงในปัจจุบันอันเนื่องมาจากการพัฒนาของ Cloud Technology เพราะ แนวกิดของ Containers ทำให้เราสามารถบริหารจัดการระบบซอฟต์แวร์ได้ง่ายขึ้น คล่องตัวขึ้น Windows Server 2016 ถูกออกแบบมาให้รองรับกับ Cloud Technology โดยเฉพาะ จึงถูกกำหนดมา ให้รองรับการทำงานแบบ Containers ด้วย โดยใน Windows Server 2016 มีการ รองรับ Containers ถึง 2 แบบคือ

- Windows Server Container เป็นการสร้าง Containers บนตัว Windows Server โดยตรง จะเป็นการจัดการสภาพแวดล้อมของแต่ละซอฟต์แวร์ให้ต่างกันไป แต่ยัง ใช้ทรัพยากรด้านฮาร์ดแวร์ร่วมกัน
- Hyper-V Container เป็นการสร้าง Containers แบบที่เรียกว่า super isolated คือ แยกทั้งสภาพแวคล้อมของแต่ละซอฟต์แวร์ และแยกทรัพยากรที่แต่ละซอฟต์แวร์ จะใช้งานได้ ออกกันอย่างชัดเจน

2.4 Oracle Database 11g



ภาพที่ 2.16 Oracle Database11g

Database Management System เริ่มมีใช้ใน ทศวรรษ 1960 ซึ่งยังเป็นฐานข้อมูลที่มีโครงสร้างแบบ ลำดับชั้น (hierarchies) และ แบบ network อยู่ ซึ่งยากลำบากในการเขียน Application จนกระทั่ง Dr.Ted Codd ซึ่ง ทำงานอยู่ที่ บริษัท IBM ในขณะนั้น มีความคิดในการ จัด organize data ใหม่ ซึ่ง Dr.Codd เรียกมันว่า Relational Model Relational Model นี้ ใช้ ตาราง 2 มิติ ประกอบด้วย แถว (row) และ คอลัมน์ (column) โดย ข้อมูลในตาราง สามารถ เชื่อมความสัมพันธ์ (relationship) ระหว่างตารางกันได้ แต่ช่วงนั้น relational model ของ Codd ก็ยัง ไม่มีการเอาไปทำ ในเชิงพาณิชย์ และ บริษัท IBM เองก็ไม่มีแผนเอา ไอเดีย ของ Dr. Codd ไปใช้งาน

Oracle Database 11 Oracle Database เป็นฐานข้อมูลที่ออกแบบเป็นพิเศษสำหรับกริดคอมพิวติ้ง (Grid Computing) และด้วยรีลีสล่าสุด Oracle Database 11g ออราเกิลช่วยเพิ่มความสะดวกในการบริหารจัดการ ข้อมูลภายในองก์กร ทั้งยังช่วยให้ลูกค้าเข้าใจ เกี่ยวกับธุรกิจได้มากขึ้นและสร้างสรรก์นวัตกรรมได้รวดเร็ว ขึ้น โดย Oracle Database 11g มีคุณสมบัติที่เหนือกว่าทั้งในแง่ของประสิทธิภาพ ความยืดหยุ่นในการปรับ ขนาด ความพร้อมใช้งาน ความปลอดภัย และความสะดวกในการจัดการ บน ระบบกริดราคาประหยัดซึ่ง ประกอบด้วยสตอเรจและเซิร์ฟเวอร์มาตรฐานอุตสาหกรรม Oracle Database 11g สามารถติดตั้งได้อย่างมี ประสิทธิภาพบนทุกระบบ ตั้งแต่เบลดเซิร์ฟเวอร์ขนาดเล็ก ไปจนถึงเซิร์ฟเวอร์ SMP ที่มีขนาดใหญ่ที่สุด รวมถึงกลัสเตอร์ทุกขนาด โดยประกอบด้วยความสามารถด้านการจัดการแบบอัตโนมัติเพื่อการจำเนินการที่ ทั้งหมด ตั้งแต่ข้อมูลธุรกิจแบบเก่า ไปจนถึงข้อมูล XML และข้อมูลเชิงพื้นที่ 3 มิติ จึงนับเป็นทางเลือกที่ เหมาะสมที่สุดสำหรับการประมวลผลทรานแซคชั่น ระบบคลังข้อมูล และการจัดการคอนเทนต์ 2.5 ระบบป้องกันเครือค่ายคอมพิวเตอร์

Hardening Os (Operating System) เป็นกระบวนการของการกำหนดค่า (Parameter) บน ระบบปฏิบัติการเพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต ป้องกันผู้บุกรุก แฮกเกอร์ และช่องโหว่ด้านความ ปลอดภัยอื่น ๆ OS Hardening ทำให้ระบบคอมพิวเตอร์เชื่อถือได้มากขึ้น มีความปลอดภัย และช่วยเพิ่ม ประสิทธิภาพการทำงานเนื่องจากใช้หลักการ "ลดสิ่งที่ไม่ได้ใช้ออกไปจากระบบ" ดังนั้น วัตถุประสงค์หลัก ของการ Hardening กือการ ลดความเสี่ยงที่จะเกิดด้านความปลอดภัยให้ได้มากที่สุดซึ่งผมขอย้ำอีกครั้งกับ ผู้อ่านว่าการทำ Hardening นั้นเป็นการเพิ่มความปลอดภัยให้ระบบปฏิบัติการที่เราใช้อยู่โดยมีค้นทุน ค่าใช้ง่ายต่ำมาก ไม่ต้องซื้อ Hardware / Software ราคาแพงเราก็สามารถเพิ่มความปลอดภัยให้กับ คอมพิวเตอร์ของเราได้เป็นอย่างดี เพียงแค่เราใส่ใจที่จะนำเอา Security Best Practice ของระบบปฏิบัติการที่ เราใช้อยู่นำมาลงมือทำ (ซึ่งโดยส่วนใหญ่มักจะมีแจกจ่ายฟรีให้ผู้ใช้งานโดยบรรคาผู้ผลิตอยู่แล้ว) หากจะ มองในมุมมองขององค์กรด้วยแล้ว กระบวนการทำ Hardening เป็นหนึ่งในส่วนสำคัญในการสร้างมาตรฐาน ของการบริหารจัดการระบบรักษาความปลอดภัยข้อมูลอย่างเป็นระบบและมีประสิทธิภาพ

2.5.1 security life cycle

ที่ต้องทำเพราะมีการเปลี่ยนแปลงบ่อยและต้องกลับมา recheck เพื่อไม่ให้มีอะไรเปลี่ยน แปลงจากที่ควรจะเป็น โดย security life cycle จะมีอยู่ด้วยกัน 10 ข้อคือ

1. Risk & Vulnerability Management (ประเมินความเสี่ยง)

2. วางแผนกำหนดว่าจะ hardening อะไรบ้างเพื่ออะไรและต้องระวังให้ดี เพราะบาง key อาจจะทำให้ระบบ เสียทั้งระบบ

- 3. เตรียมแผนรองรับหาก fa<mark>il</mark>s
- 4. ทำ full backup
- 5. ขอ mail aproove จากผู้บริหาร
- มีเอกสารรองรับในขั้นตอนการทำงาน
- 7. ทคสอบระบบหลังทำงานเสร็จ

8. security health check (ตรวจสอบทุกเดือนเพื่อที่จะยืนยันว่า key ที่ harden ไปจะอยู่ปกติ)

9. re hardening หรือ hardening ซ้ำอีกรอบ สำหรับค่าที่เปลี่ยนแปลง 10. วางแผนการสำหรับปีหน้าเพื่อศึกษาช่องโหว่ใหม่ๆที่เกิดขึ้น

2.5.2 การแยก list ของ hardening แบ่งเป็น 3 กลุ่มคือ

1. กลุ่มที่ไม่มี ผลกระทบ(impact) กับระบบที่มีอยู่(สามารถทำทีเดียวพร้อมกันได้)
 2. กลุ่มที่มี ผลกระทบ(impact) ปานกลางกับระบบที่มีอยู่ (ค่อยๆ ทำแล้วค่อยๆ test ไปด้วย)
 3. กลุ่มที่มี impact มากกับระบบที่มีอยู่ (full backup ,ทำ 1 ครั้ง test 1 ครั้ง ,เตรียมแผน rollback)

2.5.3 คุณสมบัติของคนที่ทำ Hardening

คือ ต้องเป็นผู้มีความอดทน เพราะงานนี้เป็นงานที่อยู่เบื้องหลังมากๆ ผู้ใช้ระบบรู้ว่าระบบ ที่ Harden แล้วแข็งแรง แต่มันไม่มี function อะไรใหม่ๆ และอาจโดนตำหนิหากทำระบบของเขาใช้งานช้า หรือแย่กว่านั้นอาจไม่ได้เลย ต้องรักการเรียนรู้และมีเหตุผลเพราะควร Harden แบบพอดี ถ้าทำมากเกินไป อนากต update program ไม่ได้จะยุ่ง และสุดท้ายตรงคือต้องสมาธและมีสติอันนี้สำคัญตอนแก้ไขอะไรใน ระบบต้องรู้ตัวว่าทำอะไร เพราะทำแบบเบลอจะทำให้งานเสียได้ เราลองมาเปิดมุมมองใหม่กับงาน Security hardening ว่าเขาทำอะไรกัน

2.5.4 การทำ hardening บน Windows

การทำ Security hardening บน Windows หรืออาจเรียกว่า Security lockdown คือ กระบวนการเสริมความแข็งแรงด้านความปลอดภัยให้กับ Windows ด้วยขั้นตอนผสมผสานมากมาย เมื่อ เครื่องแข็งแรง ปลอดภัย ผู้ใช้งานก็มั่นใจ แต่มักมีความเข้าใจผิดๆ เช่น การทำ Harden ทำให้เสียเวลา

2.5.5 ขั้นตอนของ Hardening

- ศึกษาการทำงานของ Application บน Server และทุคสอบใช้งาน Basic function
- จัดทำ Hardware และ Software inventory เพื่อใช้สำหรับการดูแลว่าเรามีอะไรอยู่บ้าง และส่วนใด ต้องการดูแลเรื่องความปลอดภัย
- ถ้า Application นั้นซื้อมาหรือไม่ได้พัฒนาเอง ต้องศึกษา Security Guide จากผู้พัฒนาก่อน เพื่อ ป้องกันการแก้ไขระบบโดยไม่ได้รับอนุญาต หรือมีปัญหาเรื่องการ Support
- กำหนดขอบเขตการ Harden ให้เหมาะสมหรือตรงกับหน้าที่หรือ Application บน Server

- หาเกรื่องมือทุนแรงช่วยประเมินความปลอดภัยเช่น Microsoft MBSA, Best Pracrtise Analyzer เป็น ต้น
- หา Hotfix/Patch certification list สำหรับ Application ถ้าหาได้
- ศึกษาวิธีการ Harden จากแหล่งต่างๆ
- มีการ Backup / Recovery
- ถงมือ Harden และหมั่นทดสอบการใช้เบื้องต้นเป็นระยะๆ
- ส่งมอบระบบคืนให้ผู้ทุดสอบระบบงาน
- มีการ Review security อย่างน้อยปีละ 1 ครั้ง

2.5.6 การกำหนดขอบเขตและรูปแบบการ Harden

จากภาพด้านบน แสดงให้เห็นว่าการ Harden ให้มอง Server แบ่งออกเป็นหมวดหมู่ เพื่อให้ ความสะดวกเราก็จะเจาะไปทีละเรื่องอย่างเป็นขั้นเป็นตอน คำอธิบายของแต่ละกล่องมีดังนี้

2.5.7 Application หมายถึงการป้องกันใน 2 ระดับคือ

- ระดับของตัว Application ให้ดูเรื่องการสร้างกำหนดสิทธิการใช้งานต่างๆ, การลบข้อมูลทดสอบ, การเขียน Code ที่ไม่มีจุดอ่อนด้าน Security
- ระดับของ Platform ที่ใช้ Run ตัว Application เช่น ถ้าเป็น Web .Net เป็น Microsoft IIS หรือ J2EE ก็เป็น TomCat พวกนี้ต้องไปศึกษา Security Guide ได้

2.5.8 File System

ไปดูเรื่องการกำหนดสิทธิ Folder ต่างๆ ให้สิทธิเฉพาะคนที่มีหน้าที่เข้าไปเห็นข้อมูล หรือ Application คนอื่นห้ามเข้า ใน Folder ที่เก็บ Application นั้น มีความสำคัญมาก หากผู้ไม่ประสงค์ดีนำ โปรแกรมที่ไม่ได้รับอนุญาตไปลง <mark>อาจ</mark>ทำให้เกิดคว<mark>า</mark>มเสีย<mark>หายร้ายแ</mark>รงได้

ITUTE OF

2.5.9 Operating System

ศึกษาจากคู่มือ Security ของ OS ว่าต้องทำอย่างไร เช่น

- User Account/Group,
- การปิด Service, Uninstall program ที่ไม่ใช้,

- การดู Port ด้วย netstat ว่าเกรื่องเปิด service อะไรบน TCP/UDP protocol
- ถ้าเป็น Windows เราจะ ใช้ Group Policy ช่วยกี่ได้ เพื่อช่วยให้ดูแถง่ายขึ้นด้วย
- ติดตั้ง Anti-Virus และอย่าลืมดูว่ามัน Update signature ได้
- ติดตั้ง Windows Update Agent แต่ Server อาจกำหนดไม่ใช้มัน update เองได้เดี๋ยวทำเครื่องพัง แต่ ใช้ประโยชน์ให้มัน warning เวลามี hotfix ออกใหม่ได้

27

2.5.10 Network

บางครั้งเครื่องเราอาจป้องกันด้วย Software แล้วอาจไม่เพียงพอก็ใช้ Firwall หรืออุปกรณ์ Network security มาช่วยอีกแรง

2.5.11 Physical

เกรื่อง Server ควรควบคุมให้ผู้มีหน้าที่เข้าไปยุ่งกับมันได้เท่านั้น นอกจากนี้ก็ควรดูว่าที่ตั้ง server นั้น เรียบร้อยไหม เช่น ไม่มีน้ำจากแอร์หรือดับเพลิงหยดลงเครื่อง, พวกสายไฟหรือสายต่างๆ ติดตั้ง เรียบร้อยดี เป็นต้น

2.5.12 เครื่องมือ/เครื่องทุ่นแรง

เรากวรให้เวลาในการศึกษาข้อมูลของ Software/Hardware ที่ Inventory ที่เราเตรียมไว้ Software บางตัวก็มีผู้พัฒนา Tool สำหรับทำ Security scan มันช่วยให้ประหยัดเวลาและเป็นมาตราดีกว่า เสียเวลามานั่งทำ ซึ่งเราก็ควรรู้อยู่แล้วว่าต้องตรวจตราในหัวไหนด้วย ไม่ใช่ปล่อยเครื่องทำอย่างเดียว เพราะ มันทำพังก็ไม่รู้ว่าเป็นเรื่องอะไร ตัวอย่างของเครื่องมือสำหรับ Windows คือ MBSA

บทที่ 3 แผนงานการปฏิบัติงานและขั้นตอนการดำเนินงาน

3.1 แผนงานปฏิบัติงาน

หัวข้องาน		เดือ	นที่ 1	1	เดือ	นที่ :	2		เดือ	นที่ :	3		เดือ	นที่ 4	ŀ
ศึกษา VMware & OS (Windows server)(Linux)															
ศึกษา Concept Hardening															
Install VMware	a			7											
ศึกษา Feature ที่ใช้ในการทำ Hardening						5				1					
ทำ Demo เกี่ยวกับ Feature ที่ใช้						-	¢	>							
ทำ Hardening ใน - Windows server 2016									1	ŝ	~	· ·			
ทำการ Test											.C	1		1	
ทำรูปเล่มรายงาน												C			
สรุปผลงาน															
เรียบเรียงจัดทำรูปเล่มรายงาน													0		

<mark>ตาราง 3.1</mark> แผนปฏิบัติงานสหกิจศึกษา

3.2 รายละเอียดโครงงาน

3.2.1 Hardening

การปฏิบัติงานสหกิจศึกษา ข้าพเจ้าได้อยู่ส่วนงานของ System Engineer ของ แผนก SMS จึงมี แผนปฏิบัติงานออกแบบในการเพิ่มความปลอดภัยให้กับ OS และ Server ให้มากขึ้นทำให้ระบบมีความป ลอยภัยและมีความน่าเชื่อถือมากยิ่งขึ้น



ภาพที่ 3.2 คำเนินการเพิ่มความปลอคภัยให้เครื่องของเรา

3.2.2 งานอื่นๆ

3.2.2.1 ทำการศึกษาและทคลองติดตั้ง Linux

3.2.2.2 ทำการศึกษาและทุคลองติดตั้ง Windows Server

3.2.2.3 การจัดทำเอกสาร Report Health Check ให้ลูกค้า

3.2.2.4 ทำการ Hardening ใน OS ต่างๆที่ได้ทำการติดตั้งมา

3.2.2.5 รับหน้าที่เป็น TA ไปเป็นผู้ช่วยสอนให้กับนักศึกษาที่เข้ามาเตรียมสหกิจบริษัท a-host

3.3 ขั้นตอนการดำเนิน



Enter Accepts Esc Exit ภาพที่ 3.3 ดำเนินการเพิ่มความปลอดภัยให้เครื่องของเรา

3.3.1 ศึกษาข้อมูลที่จำป็นก่อนการทำการ Hardening

อย่างละเอียด ในด้านความ ต้องการของระบบของ OS ต่าง ๆ การสร้าง VM เพื่อสร้าง Test System รวมไป ถึงศึกษาซอฟท์แวร์ที่เกี่ยวข้องในด้านวิธีการใช้งานและการติดตั้ง เช่น การ ติดตั้ง AIX, Linux และการติดตั้ง Windows Server อย่างละเอียดว่าในแต่ละ ระบบนั้นต้องทำ อะไรบ้าง เช่น ใน Window Serverการทำ Hardening firewall และ การทำ NTP Configuration นั้นต้องรู้ก่อนว่า firewall คืออะไรทำอะไรได้



ภาพที่ 3.4 หน้าที่ของ Firewall

3.3.1.1 firewall คือ เครื่องมือที่ใช้ในการป้องกันเน็ตเวิร์กจากการสื่อสารทั่วไปที่ไม่ได้รับอนุญาต โดยที่ เครื่องมือที่ว่านี้อาจจะเป็น Hardware หรือ Software หรือทั้งสองรวมกันขึ้นอยู่กับวิธีการหรือ Firewall Architecture ที่ใช้ไฟร์วอลล์ (Firewall) เป็นเครื่องมือที่ทำหน้าที่รักษาความปลอดภัยในเชิงการป้องกัน (Protect) ซึ่งจะทำหน้าที่ควบคุมการเข้าถึงเน็ตเวิร์ก (Access Control) โดยอาศัยกฎพื้นฐานที่เรียกว่า Rule Base

3.3.1.2 คุณสมบัติของ Firewall

คุณสมบัติทั่วไปของ Firewall นั้นจะมีอยู่ 3 อย่างด้วยกันคือ

3.3.1.2.1 Protect

ไฟร์วอลล์เป็นเครื่องมือที่ทำงานใ<mark>นเชิง</mark>การป้องกัน โดย packet ที่จะสามารถผ่านเข้า-ออกได้นั้น จะต้อง เป็น packet ที่มันเห็นว่าปลอดภัย หาก packet ใดที่มันเห็นว่าไม่ปลอดภัย มันก็จะไม่อนุญาตให้ผ่าน โดย การตัดสินว่า packet ปลอดภัยหรื<mark>อไม่น</mark>ั้นขึ้นอยูกับกฏพื้นฐานที่ Administrator ได้กำหนดไว้

3.3.1.2.2 Access Control

้ไฟร์วอลล์จะควบคุมการ Access ของ Host ต่างๆ ให้เป็นไปตามกฏพื้นฐานที่ Administrator ได้กำหนดไว้

3.3.1.2.3 Rule Base

ไฟร์วอลล์จะทำการควบคุมการ Access โดยอาศัยการเปรียบเทียบคุณสมบัติของ Packet ที่จะผ่านเข้า-ออก กับกฏพื้นฐานที่ Administrator ได้กำหนดไว้ หากพบว่าไม่มีกฏห้ามไว้ก็จะอนุญาตให้ผ่านไปได้ แต่ ถ้ามีกฏข้อใดข้อหนึ่งห้ามมันก็จะไม่ยอมให้ผ่าน

3.3.1.2.4 สิ่งที่ Firewall สามารถป้องกันได้

 Network Scanning – ด้วยคุณสมบัติที่ Firewall สามารถควบคุมการเข้า-ออก ของ packet ได้ มันจึง สามารถจำกัดปลายทางของ packet ที่ผ่านเข้ามาเฉพาะ Host ที่ได้รับอนุญาตให้ติดต่อได้เท่านั้น

- 2. Host Scanning Firewall จะทำการตรวจจับการ scan เพื่อหาว่ามีการรัน Service อะไรบ้างบน host
- 3. Inbound Access ควบคุมการเข้ามาของ packet เฉพาะที่ได้รับอนุญาตตาม Rule Base
- 4. Outbound Access ควบคุมการออกไปของ packet เฉพาะที่ได้รับอนุญาตตาม Rule Base
- 5. การลักลอบส่งข้อมูล

6. Network Denial of Service – ป้องกันการก่อกวนเพื่อไม่ให้ Host สามารถให้บริการได้ เช่นการทำ ให้เน็ตเวิร์กท่วมไปด้วยข้อมูล (Network Flooding) ทำการส่ง packet จำนวนมากไปยัง Host เพื่อขอ ใช้บริการ (SYN Flooding)

7. Trojan Horse, Backdoor, Back Orifice

3.3.1.2.5 สิ่งที่ Firewall ไม่สามารถป้องกันได้

- 1. Hacker
- 2. Allowed Services
- 3. Application Vulnerability
- 4. OS Vulnerability
- 5. Virus
- 6. การดักอ่านข้อมูลโด<mark>ย</mark> Snif<mark>fer</mark>
- 7. Spammed Mail
- 8. Administration Mistake

3.3.2 NTP configuration

ภาพที่ 3.5 การทำงานของ NTP

NTP Server

Network Time Protocol หรือ NTP คือ networking protocol ที่ใช่สำหรับ sync time ของ server ทุก เครื่องใน network ให้ตรงกัน ผ่าน packet-switch ซึ่ง ntp เป็น protocol ที่เก่าแก่มากและมีมาตั้งแต่ 1985 และใช้คงใช้งานจนถึงบัจจุบัน เริ่มต้นคิดค้นโดย David L. Mills ที่ University of Delaware สาเหตุที่ต้องมี NTP นั้นก็เพราะ นาพิกา หรือ clock ของ server, computer ใน network ไม่ได้เที่ยงตรงเท่ากันหมด บางครั้งการคลาดเคลือนกันเพียงหลักวินาทีอาจจะทำให้ application ที่ใช้งานสื่อสารกันผิดพลาดได้ และ ยิ่งในระบบ server ขนาดใหญ่ที่มีการ run ต่อเนื่องกันเป็นเวลานานหลายปี ย่อมมีความคลาดเคลือนไป บ้างอยู่แล้ว เพราะฉะนั้น NTP จึงเข้ามาช่วยในการทำ synchronize computer ในระบบ network เราให้ แม่นยำในระดับ millisecond ความคลาดเคลื่อนที่อาจจะเกินขึ้นใน network latency มีเพียงแค่ 10 ms. สำหรับบน Internet และจะเหลือเพียง 1 ms. ภายใน local network Protocol ที่ใช้จะอยู่ในรูป client-server หรือ peer-to-peer โดยจพทำการรับส่งข้อมูล timestamps ผ่านทาง UDP (port 123)

STITUTE OV

3.3.3 ทดสอบการตั้งค่าทั่วไปของ Hardening

ได้แก่ การตั้งค่ารหัสตั้งแต่ BIOS และ ตั้งก่าการปิด port ที่ไม่จำเป็นต่างๆในเครื่องและทำการ เซ็กFirewall เพื่อ Block สิ่งต่างๆที่เข้ามาทาง Internet และ ยังทำการ

3.3.4 ทดสอบ Hardening ที่ตั้งค่าไว้

IC

เช่น ลองล็อกอินเข้าเครื่องที่มีการทำ Hardening เอาไว้ว่า ที่ตั้งค่าเอาไว้แสดงผลยังไง และตรวจสอบดูว่ายังมีช่องโหว่ตรงไหนที่ยังสามารถปิดได้

> ุกคโนโลฮั7 ง

บทที่ 4 ผลการดำเนินงาน การวิเคราะห์และสรุปผลต่างๆ

4.1 ขั้นตอนและผลการดำเนินงาน

ในช่วงระยะเวลาสองเดือนแรกของการปฏิบัติงานสหกิจศึกษาจะเป็นช่วงของ การศึกษาข้อมูลที่จำเป็น ในการลง OS ต่างๆและ Basic command ของ Linux อย่างละเอียดซึ่งเป็นในส่วนของการติดตั้ง OS ที่ นำมาใช้งานจะทำการติดตั้งภายใน VM เพื่อนำไปทำ Hardening รวมไปถึงศึกษาการติดตั้งซอฟต์แวร์ เช่น Linux และ Windows Server โดยในช่วงเดือนที่สามเป็นต้นไปได้เริ่มศึกษาการทำ Hardening เพื่อเพิ่มตวาม ปลอดภัยให้แก่เครื่องของเราลงใน OS Linux และ Windows Server เป็นหลัก

> โดยหลักแล้ว จะแบ่งการทำงานหลักๆ ออกเป็น 3 ขั้นตอนคือ 4.1.1 ทำการสร้าง Environment ที่เหมาะสม 4.1.2 ทำการ Hardening บน Windows server 2016

4.1.3 ทำการ Hardening บน Linux CentOS 7 และ RedHat

4.1.1 ศึกษาและทำความเข้าใจเกี่ยวHardening

วัตถุประสงค์หลักของการ Hardening คือการลดความเสี่ยงที่จะเกิดให้ได้มากที่สุดเพื่อเพิ่มความมั่นใจ ในระบบปฏิบัติการและป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตอีกทั้งยัง ป้องกันผู้บุกรุก แฮกเกอร์ และช่องโหว่ ด้านกวามปลอดภัยอื่น ๆ

OS Hardening ทำให้ระบบคอมพิวเตอร์เชื่อถือได้มากขึ้น มีความปลอดภัย และช่วยเพิ่มประสิทธิภาพ การทำงานเนื่องจาก "ลดสิ่งที่ไม่ได้ใช้ออกไปจากระบบ" การทำ Hardening นั้นเมีต้นทุนและค่าใช้จ่ายที่ต่ำ มาก เพราะไม่ต้องซื้อ Hardware หรือ Software ราคาแพงเราก็สามารถเพิ่มความปลอดภัยให้กับคอมพิวเตอร์ ของเราได้เพียงแค่เรานำเอา Security Best Practice ของระบบปฏิบัติการที่เราใช้อยู่นำมาลงมืออีกทั้งมองใน มุมมองขององค์กรด้วยแล้ว กระบวนการทำ Hardening เป็นหนึ่งในส่วนสำคัญในการสร้างมาตรฐานของ การบริหารจัดการระบบรักษาความปลอดภัยข้อมูลอย่างเป็นระบบและมีประสิทธิภาพ

4.1.1.1 ติดตั้ง Windows Server

10

- ทำการสร้าง Virtual Machine ด้วยการกดปุ่ม Create a New Virtual Machine



- ให้เลือก Hardware เป็น Version ที่ตรงกับเราในที่นี้เลือกเป็น 12.0
- New Virtual Machine Wizard × Choose the Virtual Machine Hardware Compatibility Which hardware features are needed for this virtual machine? Virtual machine hardware compatibility Hardware Workstation 12.0 \sim Compatible ESX Server Compatible products: Limitations: Fusion 8.x 64 GB memory Workstation 12.0 16 processors 10 network adapters 8 TB disk size Help < Back Next > Cancel ภาพที่4.3 การตั้งค่า Virtual Machine(3) เลือกแผ่นหรือไฟล์ที่เราทำการเก็บ Windows Server ไว้ New Virtual Machine Wizard \times **Guest Operating System Installation** A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system? Install from: O Installer disc: DVD RW Drive (E:) Installer disc image file (iso): D:\Windows Server 2016 (x64) - DVD (English)\en_w \sim Browse... Could not detect which operating system is in this disc image. You will need to specify which operating system will be installed. I will install the operating system later. The virtual machine will be created with a blank hard disk. Cancel < Back Next > Help ภาพที่4.4 การเลือกลง Windows Server

- เลือก Windows Server แล้วเลือก Version ที่จะลงในที่นี้เลือก Window Server 2016

	New Virtual Machine Wizard
	Select a Guest Operating System
	Which operating system will be installed on this virtual machine?
	- Guest operating system
	Microsoft Windows Linux
	Novell NetWare
	VMware ESX
	Other
	Version
	Windows Server 2016
	Help < Back Next > Cancel
	ภาพที่4.5 การตั้งค่า Virtual Machine(4)
	ตั้งชื่อและระบที่อยู่ให้กับ VM ที่เรากำลังจะสร้าง
	New Virtual Machine Wizard ×
	Name the Virtual Machine
	What name would you like to use for this virtual machine?
	Virtual machine name:
	Windows Server 2016 TEST
	Location:
	D:\Documents\Virtual Machines\Windows Server 2016 TEST Browse
	The default location can be changed at Edit > Preferences.
1/2	
	< Back Next > Cancel
	ภาพที่4.6 การระบุที่อยู่ของไฟล์ Virtual Machine
	VSTITI ITE OF

- เลือก BIOS แล้วกด Next

New Virtual Machine Wizard

Firmware Type

Firmware type BIOS EFI

What kind of boot device should this virtual machine have?

 < Back</th>
 Next >
 Cancel

 ภาพที่4.7 การตั้งค่า Virtual Machine(5)

เถือกจำนวน Core ให้กับ VM

T

Processors	
number of processors:	2 ~
Number of cores per processor:	1 ~
Fotal processor cores:	2
Help	< Back Next > Cancel
d	2

- เลือกจำนวน Ram ให้กับ VM

New Virtual Machine Wizard

Memory for the Virtual Machine

How much memory would you like to use for this virtual machine?



ภาพที่4.9 การให้ Memory กับ VM

เถือก Network แบบ NAT

New Virtual Machine Wizard

Network Type

What type of network do you want to add?

Network connection

- Ouse bridged networking
 - Give the guest operating system direct access to an external Ethernet network. The guest must have its own IP address on the external network.
- Use network address translation (NAT) Give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address.
- O Use host-only networking Connect the guest operating system to a private virtual network on the host computer.
- O Do not use a network connection

Help

Cancel

ภาพที่4.10 การตั้งค่า Network

< Back

 \times

- เถือกI/O Controller แบบ SAS

New Virtual Machine Wizard

Select I/O Controller Types

Which SCSI controller type would you like to use?

I/O controller types SCSI Controller:

Help

10

BusLogic (Not available for 64-bit guests)

OLSI Logic (Not supported by Windows Server 2016)

LSI Logic SAS (Recommended)

(ula aj

< Back Next >

ภาพที่4.11 การตั้งค่า I/O

เลือกการทำงาน Disk แบบ SCSI

New Virtual Machine Wizard Select a Disk Type What kind of disk do you want to create? Virtual disk type DE SCSI (Recommended) SATA Help < Back Next > Cancel ภาพที่4.12 การตั้งค่า Disk type

Х

Cancel

- เลือก Create a new virtual disk เพื่อสร้าง

New Virtual Machine Wizard

Select a Disk

Which disk do you want to use?

Disk Create a new virtual disk A virtual disk is composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts. Use an existing virtual disk Choose this option to reuse a previously configured disk. Use a physical disk (for advanced users) Choose this option to give the virtual machine direct access to a local hard disk.

Help < Back Next > Cancel

ภาพที่4.13 การสร้าง VM

เลือกพื้นที่ให้กับ VM เป็นแบบ Split disk

New Virtual Machine Wizard

Specify Disk Capacity

How large do you want this disk to be?

Maximum disk size (GB):

Recommended size for Windows Server 2016: 60 GB

100.0 🔔

Allocate all disk space now.

Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.

○ Store virtual disk as a single file

Split virtual disk into multiple files

Help

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

< Back

ภาพที่4.14 การตั้งค่าพื้นที่ให้Windows Server

Next >

Cancel

 \times

×

ตั้งชื่อ Disk

New Virtual Machine Wizard

Specify Disk File

Where would you like to store the disk file?

Disk File

Help

One disk file will be created for each 2 GB of virtual disk capacity. File names for each file beyond the first will be automatically generated using the file name provided here as a basis.

Windows Server 2016 TEST.vmdk

ภาพที่4.15 การตั้งชื่อให้กับ VM

< Back Next >

ตรวจเช็คดูว่าเป็นไปตามที่เราตั้งค่าไว้ไหม

New Virtual Machine Wizard

Ready to Create Virtual Machine

Click Finish to create the virtual machine. Then you can install Windows Server 2016.

The virtual machine will be created with the following settings:

Name:		Windows Server 2016 TEST
Location:		D:\Documents\Virtual Machines\Windows Server 2016
Version:		Workstation 12.0
Operating Sy	stem:	Windows Server 2016
Hard Disk:		100 GB, Split
Memory:		2048 MB
Network Ada	pter:	NAT
Other Device	s:	2 CPU cores, C <mark>D</mark> /DVD, USB Controller, Printer <mark>, Soun</mark> d C

Customize Hardware...

Cancel

Finish

ภาพที่4.16 ตรวจเช็คการตั้งค่า

< Back

 \times

Browse...

Cancel

- เลือกภาษา

🖆 Windows Setup		
	vvindows Server 2016	
Langua <u>ge</u> to i	nstall: English (United States)	
Time and currency fo	ormat: English (United States)	·
<u>K</u> eyboard or input m	ethod: US	
	นเล่มง	
Enter your lang	juage and other preferences and click "Next" to	continue.
S 2016 Microsoft Corporation. All right	ts reserved.	Next
	าพที่4 17 อารติดตั้ง Windows Se	NTION .
ð	TWM4.17 THEFT WINDOWS SE	
- กด Install now		
🏜 Windows Setup		
	windows Server 2016	
	<u>I</u> nstall now	
		Q
Popair your computer		
© 2016 Microsoft Corporation All rig	hts reserved.	A.
	y 9	
J J	าาพที4.18 การติดตั้ง Windows Se	erver
"VSTr		

- ใส่ Key ของ Windows Server 2016 หรือ จะกด I don't have a product key เพื่อข้าม

							<
\bigcirc	🔏 Windows Setup						
	Activate Window	ws					
	If this is the first time you need to enter a v email you received at Windows came in.	you're installing W valid Windows prod fter buying a digital	indows on this PC (d uct key. Your produc copy of Windows o	or you're installin ct key should be r on a label insic	ng a different editi in the confirmation de the box that	on), on	
	The product key look	ks like this: XXXXX-X	xxxx-xxxxx-xxxx	x-xxxxx			
	If you're reinstalling automatically activat	Windows, select I do ted later.	on't have a product l	key. Your copy o	of Windows will be		
	ักโ		તે દ				
					ં છે		4
	rivacy statement		I don't	have a product	kev	Next	
- T							
7		ภาพที่4.19	การใส่ Key W	Vindows Se	erver	S	
เลือก) Windows Serv	ภาพที่4,19 'er 2016(Desk	การใส่ Key W top Experience	Vindows Se ce)	erver	2.	-
ເລືອກ) Windows Serv	ภาพที่4.19 /er 2016(Desk	การใส่ Key W top Experienc	Vindows Se	erver	ی۔ ۲.	
เลือก	Windows Serv	ภาพที่4,19 /er 2016(Desk) system you want t	การใส่ Key W ctop Experienc	Vindows Se	erver	×	
ເລືອ r	Windows Serv Windows Setup Select the operating Operating system	ภาพที่4.19 ⁷ er 2016(Desk	การใส่ Key W ctop Experienc	Vindows Se ce) Architecture	Date modified	× • •	
เลือก ©	Windows Serv Windows Setup Select the operating Operating system Windows Server 2016	ภาพที่4.19 /er 2016(Desk) system you want t i Standard	การใส่ Key W ctop Experienc to install	Vindows Se ce) Architecture x64	Date modified 11/21/2016	×	
ເລືອກ	O Windows Serv Windows Setup Select the operating Vindows Server 2016 Windows Server 2016 Windows Server 2016	ภาพที่4.19 rer 2016(Desk) system you want t i Standard Standard (Desktop i Datacenter	การใส่ Key W ctop Experienc to install	Vindows Se ce) Architecture x64 x64 x64	Date modified 11/21/2016 11/21/2016 11/22/2016	× • •	
រតឺ១ក 🃀	Windows Serv Windows Setup Select the operating Operating system Windows Server 2016 Windows Server 2016 Windows Server 2016	ภาพที่4,19 rer 2016(Desk) system you want f i Standard Standard (Desktop i Datacenter Datacenter	การใส่ Key W ctop Experienc to install Experience)	Vindows Se ce) Architecture x64 x64 x64	Date modified 11/21/2016 11/21/2016 11/21/2016 11/21/2016		
เลือก ©	O Windows Serv Windows Setup Select the operating Operating system Windows Server 2016 Windows Server 2016 Windows Server 2016	ภาพที่4.19 rer 2016(Desk system you want t Standard Standard Datacenter Datacenter Datacenter	การใส่ Key W ctop Experienc to install Experience)	Vindows Se ce) Architecture x64 x64 x64	Date modified 11/21/2016 11/21/2016 11/21/2016 11/21/2016	2. 	
រតឺ១ក 🃀	O Windows Serv Windows Setup Select the operating Vindows Server 2016 Windows Server 2016 Windows Server 2016	ภาพที่4,19 rer 2016(Desk) system you want t) Standard Standard (Desktop B Datacenter) Datacenter) Datacenter (Desktop	การใส่ Key W ctop Experienc to install Experience)	Vindows Se ce) Architecture x64 x64 x64 x64	Date modified 11/21/2016 11/21/2016 11/21/2016 11/21/2016	×	
เลือก ©	O Windows Serve Windows Setup Select the operating Operating system Windows Server 2016 Windows Server 2016 Windows Server 2016 Windows Server 2016 Windows Server 2016	ภาพที่4,19 rer 2016(Desk ; system you want f ; Standard ; Standard ; Datacenter ; Datacenter ; Datacenter (Desktop	การใส่ Key W ctop Experienc to install Experience)	Vindows Se ce) Architecture x64 x64 x64	Date modified 11/21/2016 11/21/2016 11/21/2016 11/21/2016		
เลือก	O Windows Serve Windows Setup Select the operating Operating system Windows Server 2016 Windows Server 2016 Windows Server 2016 Windows Server 2016 Windows Server 2016 Description: This option is useful w application that canno supported. For more d	ภาพที่4,19 rer 2016(Desk) system you want t) Standard) Standard) Datacenter)	การใส่ Key W ctop Experienc to install Experience) b Experience) dfor example, to pr Core installation All Server Installation Op	Vindows Se ce) Architecture x64 x64 x64 x64 x64 ovide backward a server roles and f	Date modified 11/21/2016 11/21/2016 11/21/2016 11/21/2016 11/21/2016		
เลือก ©	O Windows Serve Windows Setup Select the operating Operating system Windows Server 2016 Windows Server 2016 Windows Server 2016 Windows Server 2016 Description: This option is useful w application that canno supported. For more d	ภาพที่4,19 ver 2016(Desk system you want f standard Standard (Desktop f Datacenter Datacenter Datacenter (Desktop Datacenter Datacenter (Desktop Datacenter Datacenter (Desktop	การใส่ Key W ctop Experience to install Experience) b Experience) d—for example, to pr Core installation. All Server Installation Op	Vindows Se ce) Architecture x64 x64 x64 x64 x64	Date modified 11/21/2016 11/21/2016 11/21/2016 11/21/2016		
เลือก ©	O Windows Serv Windows Setup Select the operating Operating system Windows Server 2016 Windows Server 2016 Windows Server 2016 Windows Server 2016 Description: This option is useful w application that canno supported. For more d	ภาพที่4.19 ver 2016(Desk system you want t Standard Standard (Desktop B Datacenter Data	การใส่ Key W ctop Experience to install experience) d—for example, to pr Gore installation. All Server Installation Op	Vindows Se ce) Architecture x64 x64 x64 x64 x64	Date modified 11/21/2016 11/21/2016 11/21/2016 11/21/2016		
เลือก	O Windows Serv Windows Setup Select the operating Operating system Windows Server 2016 Windows Server 2016 Windows Server 2016 Windows Server 2016	ภาพที่4,19 /er 2016(Desk) system you want f i Standard Standard (Desktop i Datacenter i Datacenter i Datacenter (Desktop i Datacenter (Desktop i Datacenter (Desktop i Datacenter (Desktop	การใส่ Key W ctop Experience to install Experience) b Experience)	Vindows Se ce) Architecture x64 x64 x64 x64 ovide backward of server roles and f	Date modified 11/21/2016 11/21/2016 11/21/2016 11/21/2016		
เลือก ©	O Windows Serve Windows Setup Select the operating Operating system Windows Server 2016 Windows Server 2016	ภาพที่4,19 ver 2016(Desk ; system you want t ; Standard ; Standard (Desktop f ; Datacenter ; Datacenter ; Datacenter (Desktop ; Datacenter ; Datacenter (Desktop ; Datacenter (Desktop ; Datacenter (Desktop	การใส่ Key W ctop Experience to install Experience) a Experience) dfor example, to pr Core installation All Server Installation Op	Vindows Se ce) Architecture x64 x64 x64 x64	Date modified 11/21/2016 11/21/2016 11/21/2016 11/21/2016		

TC

ภาพที่4.20 การตั้งค่า Windows Server

- No accept license



Applicable notices and license terms

IMPORTANT NOTICE (followed by LICENSE TERMS)

Diagnostic and Usage Information. Microsoft automatically collects this information over the internet, and uses it to help improve your installation, upgrade, and user experience, and the quality and security of Microsoft products and services. Consistent with these purposes, the information may be associated with your organization. Windows Server 2016 has four (4) information collection settings (Security, Basic, Enhanced, and Full), and uses the "**Enhanced**" setting by default. This level includes information technologies; (ii) understand device quality, and application usage and compatibility; and (iii) identify quality issues in the use and performance of the operating system and applications.

☑ I accept the license terms

ภาพที่4.21 การยอมรับ license ของ Windows Server

เถือก Custom

🕒 💰 Windows Setup

Which type of installation do you want?

Upgrade: Install Windows and keep files, settings, and applications The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.

Custom: Install Windows only (advanced)

The files, settings, and applications aren't moved to Windows with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.

Help me decide

ภาพที่4.22 การตั้งค่า Windows Server

<u>×</u>

Next

กด	Next

🔏 Windows Setup Where do you w	ant to install Window	vs?		
Name		Total size	Free space Type	
Drive 0 Unall	ocated Space	100.0 GB	100.0 GB	
<u>R</u> efresh Load driver	Delete		* New	

ภาพที่4.23 การแบ่ง Disk Windows Server

รอการติดตั้ง

TC

🔏 Windows Setup

Installing Windows

Status

Copying Windows files Getting files ready for installation (1%) Installing features Installing updates Finishing up

ภาพที่4.24 Install Windows Server

- ถงเสร็จจะได้หน้าจอ window เป็นอันเสร็จ



ภาพที่4.25 หน้าตาของ Windows Server

4.1.1.2 Hardening Windows Server 2016



(0

- เข้าไปที่ Setting



ภาพที่4.26 window update(1)



4.1.1.2.2 User Configuration

- เข้าไปที่ Control Panel



ภาพที่4.29 user configuration

เข้าไปที่ User Accounts

10



- เลือกไปที่ User Accounts

Personalization Clock, Language, and Region Ease of Access

ภาพที่4.31 หน้า Control panel ของ user accounts

_คโนโลยั7ก



- 🗆 ×

Q

- เลือก User ที่ต้องการเข้าไปจัดการ



ภาพที่4.33 เลือก User

- สามารถเปลี่ยนชื่อ,เปลี่ยนรหัส,เปลี่ยนสิทธิและลบได้


4.1.1.2.3 Further Hardening

(

เข้าไปที่ Control Panel



ภาพที่4.36 User Accounts(1)

- เลือก Manage another account

🚨 User Accounts _ $\leftarrow \rightarrow \checkmark \uparrow$ 82 > Control Panel > User Accounts > ✓ じ Search Control Panel User Accounts Chang User Accounts Creder passwords for people who share this Control Panel Home System and Security Network and Internet Hardware Manage computer. Credentials Programs User Accounts Appearance and Personalization Clock, Language, and Region Ease of Access ุกุ โ น โ ล ฮี ไ ก จ

ภาพที่4.37 User Accounts(2)

เลือก Change User Account Control settings

(.



ภาพที่4.38 Account control setting

 \times

م

เลื่อนขึ้นไปให้เป็น Always notify

)	User Acco	unt Contro	I Settings
-			-

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer. Tell me more about User Account Control settings

Always notify	
	Always notify me when:
	 Apps try to install software or make changes to my computer
	I make changes to Windows settings
	 Recommended if you routinely install new software and visit unfamiliar websites.
Never notify	ulaaj
	©OK Cancel

ภาพที่4.39 Set ค่า User Account Control Setting

4.1.1.2.4 Network Configuration

e

Image: A start start

10

- คลิกซ้ายที่ Network logo แล้ว เลือก Open Network and Sharing Center

Troubleshoot problems Open Network and Sharing Center

ภาพที่4.40 คลิกเปิด Network and Sharing Center

- เข้าไปที่ Change adapter settings

Network and Sharing Center	×
\leftarrow \rightarrow \checkmark \Uparrow Metwork and Internet	> Network and Sharing Center V 🕑 Search Control Panel P
Control Panel Home	your basic network information and set up connections
View you Change adapter settings	ur active networks
Change advanced sharing Network Settings	work Access type: Internet ate network Connections:
Change y	your networking settings
	Set up a new connection or network Set up a broadband, dial-up, or VPN connection; or set up a router or access point. Troubleshoot problems Diagnose and repair network problems, or get troubleshooting information.
See also	
Internet Options	C'A
Windows Firewall	
ภาพที่4.41	หน้า Network and Sharing Center

-เลือก Properties

🛬 Network Connections						-	o x	
🔶 🚽 🗸 🛧 💆 « Net	work and Internet >	Network Conn	nections >	~ Ŭ	Search Netwo	rk Connect	tions 🔎	
Organize Disable this	s network device	Diagnose this	connection	Rename this connection	»			
Ethernet0								
Intel(R) 8257	Disable Status Diagnose							
	Bridge Connections Create Shortcut Delete Rename Properties							5

1 item 1 item selected

ภาพที่4.42 Network Connection

F



- ทำการตั้ง IP Address ที่เราต้องการเพื่อกำหนดช่องทางและดูแลการเชื่อมต่อ

Internet Protocol Version 4 (TCP/IPv4) Properties $\qquad \qquad \qquad$	
General	
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings. Obtain an IP address automatically Ouse the following IP address:	
IP address: 192 . 168 . 239 . 131	
Subnet mask: 255 . 255 . 255 . 0	
Default gateway: 192 . 168 . 239 . 2	
Obtain DNS server address automatically	
Preferred DNS server:	
Alternate DNS server:	
Validate settings upon exit Advanced	
OK Cancel	
ภาพที่4.45 IP setting(3)	

4.1.1.2.5 Features and Roles Configuration

TC

- เถือก Add roles and Features

📠 Server Manager			- 0 ×	
Server M	lanager • Dashboard	🕶 🗭 🚩 Manage Tr	ools View Help	
Dashboard Local Server	WELCOME TO SERVER MANAGER			
■ All Servers ■ File and Storage Services ▷	1 Configure this loc	al server		
	2 Add roles and real 3 Add other servers WHAT'S NEW	to manage		
	4 Create a server gr 5 Connect this serve	pup er to cloud services	Hide	
	ROLES AND SERVER GROUPS Poles 1. J. Sense groups 1. J. Senser total 1			
	File and Storage 1 Services 1	rver 1	x	
	รับอาร์ ภาพที่4.46 Add roles and	features(1)		

กด Next _

Da

(1



ภาพที4.47 Add roles and features(2)

เถือก Role-based or feature-based installation



- เลือก Server จาก Server Pool

Server Manager		- 0 ×
Add Roles and Features W	tard	− □ × ols View Help
Select destinati	on server	DESTINATION SERVER A
Dashbo		
All Serve Installation Type	Select a server or a virtual naro disk on which to install roles and leatures. Select a server from the server pool	
File and Server Selection	Select a virtual hard disk	
Server Roles	Server Pool	
Confirmation	Filter:	
Results	Name IP Address Operating System	
	WIN-H7GGI7RUJG0 192.168.239.128 Microsoft Windows Server 201	16 Standard
		Hide
	1 Computer(a) found	
	This page shows servers that are running Windows Server 2012 or a newer relea	ase of Windows Server,
	and that have been added by using the Add servers command in Server Manage newly-added servers from which data collection is still incomplete are not show	ger. Offline servers and vn.
	< Previous Next >	Install Cancel
	22W 14 40 Add rates and feature	mag(4)
	JIIWI4.49 Add foles and leatur	res(4)
- ทำการเลือ	ก Roles ที่ต้องการ	
Add Roles and Features W	Izard	
C 1 1	1	DESTINATION SERVER
Select server re	DIes	WIN-H7GGI7RUJG0
Defere Very Deele	Select one or more roles to install on the selected server	r
Before You Begin	Palas	Description
Server Selection		Active Directory Domain Services
Server Roles	 Active Directory Certificate Services Active Directory Domain Services (Installed) 	(AD DS) stores information about
Features	Active Directory Federation Services	objects on the network and makes this information available to users
	Active Directory Rights Management Services	and network administrators. AD DS
	Device Health Attestation DHCP Server	network users access to permitted
	DNS Server	resources anywhere on the network
	 Fax Server File and Storage Services (1 of 12 installed) 	through a single logon process.
	Host Guardian Service	
	MultiPoint Services	
	Network Policy and Access Services Print and Document Services	
	Remote Access	
	Remote Desktop Services	
	Web Server (IIS)	
	Windows Deployment Services	
	< Previous	Next > Install Cancel
	ภาพที่4.50 Add roles and featur	res(5)

- ให้กด Add Features



ในกรณีที่ Add เพิ่มเข้ามาจะมีการอธิบายให้กด Next

_

📥 Add Roles and Features Wizard DESTINATION SERVER Active Directory Domain Services VIN-H7GGI7RUIGO Dashb Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource Local Se Before You Begin All Serv Installation Type sharing and collaboration between users. File and Server Selection Things to note: Server Roles • To help ensure that users can still log on to the network in the case of a server outage, install a Features minimum of two domain controllers for a domain. AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine. Confirmation Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps. Learn more about Azure Active Directory Hide Configure Office 365 with Azure Active Directory Connect Cancel < Previous Next > Install Events Event ภาพที4.53 Add roles and features(8) กด Install 📥 Add Roles and Features Wizard × Help DESTINATION SERVER WIN-H7GGI7RUJG0 Confirm installation selections Da Local Se To install the following roles, role services, or features on selected server, click Install. Before You Begin All Serve Installation Type Restart the destination server automatically if required File and Server Selection Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear Server Roles their check boxes. Features Active Directory Domain Services AD DS Group Policy Management Confirmation Remote Server Administration Tools Role Administration Tools AD DS and AD LDS Tools Active Directory module for Windows PowerShell AD DS Tools Hide Active Directory Administrative Center AD DS Snap-Ins and Command-Line Tools Export configuration settings Specify an alternate source path Install Cancel < Previous Next > Events Events ภาพที4.54 Add roles and features(9)

4.1.1.2.6 NTP Server Configuration

- NTP(Network Time Protocol)ใช้สำหรับ sync time ของ server ทุกเครื่องใน network ให้

ตรงกัน ผ่าน packet-switch

l	🔀 Administrator: Windows PowerShell	- 🗆 ×	
F	PS C:\Users\Administrator> w32tm /config /ma	anualpeerlist:pool.ntp.org /sync	^
1	fromflags:MANUAL		
ŀ	The command completed successfully.		
F	PS C:\Users\Administrator> Start-Service w32	2time	
F	PS C:\Users\Administrator> w32tm /resync		
5	Sending resync command to local computer		
$\left \right $	The command completed successfully.		

ภาพที4.55 NTP Setting(1)

สาเหตุที่ต้องมี NTP นั้นก็เพราะ นาฬิกา หรือ clock ของ server, computer ใน network ไม่ได้ตรง เท่ากันหมด ถ้าเกิดการกลาดเคลือนกันเพียงหลักวินาทีก็อาจจะทำให้ application ที่ใช้งานสื่อสาร กันผิดพลาดได้ และยิ่งในระบบ server ขนาดใหญ่ที่มีการ run ต่อเนื่องกันเป็นเวลานานหลายปี ย่อม มีความคลาดเกลือนไปบ้างอยู่แล้ว เพราะฉะนั้น NTP จึงเข้ามาช่วยในการทำ synchronize computer ในระบบ network เราให้แม่นยำในระดับ millisecond

```
PS C:\Users\Administrator> w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 3 (secondary reference - syncd by (S)NTP)
Precision: -6 (15.625ms per tick)
Root Delay: 0.2554483s
Root Dispersion: 7.7980608s
ReferenceId: 0x34A37644 (source IP: 52.163.118.68)
Last Successful Sync Time: 7/5/2018 9:24:36 PM
Source: time.windows.com,0x8
Poll Interval: 6 (64s)
```

```
PS C:\Users\Administrator> 🗕
```

ภาพท<mark>ี่4</mark>.56 NTP Setting(2)

4.1.1.2.6.1 NTP Client Configuration



STITUTE OF



เข้าไปที่ Administrative Templates แล้วเลือก System

_

เลือก Windows Time Service แล้วเลือก Time Providers



- เข้าไปที่ Enable Windows NTP Client แล้วเลือกเป็น Enable

Enable Windows	NTP Client	X
🔄 Enable Windows	NTP Client	Previous Setting Next Setting
O Not Configured	Comment:	^
Enabled		
O Disabled	Supported on:	At least Windows Server 2003 operating systems or Windows XP Professional
Options:		Help:
1	í u	This policy setting specifies whether the Windows NTP Client is enabled. Enabling the Windows NTP Client allows your computer to synchronize its computer clock with other NTP servers. You might want to disable this service if you decide to use a third-party time provider. If you enable this policy setting, you can set the local computer clock to synchronize time with NTP servers. If you disable or do not configure this policy setting, the local computer clock does not
		OK Cancel Apply

ภาพที่4.61 Client NTP Config(3)

เข้าไปที่ Configure Windows NTP Client เลือก Enable แล้ว Setting ค่าเป็น

10

Type=NTP,CrossSite=2,ResolvePeermin=15,max=7,SpecialPollInterval=3600

Configure Windows NTP Client		— 🗆 X
Configure Windows NTP Client		Previous Setting Next Setting
O Not Configured Comment:		^
Enabled		
O Disabled Supported on:	At lea Wind	ast Windows Server 2003 operating systems or ows XP Professional
Options:		Help:
NtpServer	^	This policy setting specifies a set of parameters for
time.windows.com,0x9		controlling the windows wire cheft.
Type NT5DS V		If you enable this policy setting, you can specify the following parameters for the Windows NTP
CrossSiteS <mark>yncFlags</mark> 2		Client.
ResolvePe <mark>erBacko</mark> ffMinutes		If you disable or do not configure this policy
15		setting, the WIndows NTP Client uses the defaults
ResolvePeerBackoffMaxTimes		of each of the following parameters.
7		NtpServer
SpecialPollInterval 3600		The Domain Name System (DNS) name or IP
Eventl eaElags		form of ""dnsName,flags"" where ""flags"" is a
	Ť	

OK Cancel Apply

ภาพที่4.62 Client NTP Config(4)

- เข้าไปที่ Server manager เลือก Tool แล้วไปที่ Service เลือก Windows Time ให้ Stop แล้ว Start ใหม่อีกที

Services (Local)					
Windows Time	Name	Description	Windows Time Properties (Local Compute	r)	×
	Windows Event Collec	This service	General Log On Recovery Dependencies	3	
Stop the service	🆏 Windows Event Log	This service			
Restart the service	🔍 Windows Firewall	Windows Fi	Service name: W32Time		
	Windows Font Cache	Optimizes p	Display name: Windows Time		
Description:	🌼 Windows Image Acqu	Provides im	Maintains date and time	synchronization on all clients	
Maintains date and time	🔍 Windows Insider Servi	wisvc	and servers in the netwo	ork. If this service is stopped,	
synchronization on all clients	🍓 Windows Installer	Adds, modi			
and servers in the network. If this service is stopped, date	🔍 Windows License Man	Provides inf	Path to executable:		
and time synchronization will	🌼 Windows Manageme	Provides a c	C:\Windows\system32\svchost.exe -k Local	Service	
be unavailable. If this service	🍓 Windows Mobile Hots	Provides th	Startup type: Automatic	~	
is disabled, any services that	🗟 Windows Modules Ins	Enables inst			
explicitly depend on it will	🔍 Windows Push Notific	This service			
fail to start.	🖏 Windows Push Notific	This service	Service status: Bunning		
	🧠 Windows Remote Ma	Windows R	Service status. Truining		
	Windows Search	Provides co	Start Stop	Pause Resume	
	🤐 Windows Time	Maintains d	You can specify the start parameters that an	nly when you start the service from	
	🔍 Windows Update	Enables the	here.	biy when you start the Service norm	
	🖏 WinHTTP Web Proxy	WinHTTP i	Charterstein		
	🍓 Wired AutoConfig	The Wired	Start parameters:	S	
	WMI Performance Ad	Provides pe			
	🖏 Workstation	Creates and	OK	Consel Araba	
	🖏 Xbox Live Auth Mana	Provides au	OK	Cancer Apply	
	🖏 Xbox Live Game Save	This service	Manual (Trig Local Syst		

ภาพที่4.63 Client NTP Config(5)

4.1.1.2.7 Firewall Configuration

TC

- เข้าไปที่ Control Panel



ภาพที่4.64 Fire wall Setting

- เข้าไปที่ System and Security



ภาพที่4.65 หน้า Control panel

เถือก Windows Firewall

System and Security



ภาพที่4.66 Fire wall Setting(1) ASTITUTE OF

เลือก Advanced settings

Windows Firewall

→ 🗸 ↑ 💣 > Control Panel > System and Security > Windows Firewall \leftarrow

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Allow an app or feature through Windows Firewall 🗣 Change notification settings 👎 Turn Windows Firewall on or

Control Panel Home

off

- Restore defaults
- Advanced settings Troubleshoot my network



✓ ひ Search Control Panel

See also Security and Maintenance

Network and Sharing Center

ภาพที่4.67 Fire wall Setting(2)

เลือก Inbound

Pindows Firewall with A	dvanced Security		
File Action View Help			
💠 🌩 🛛 🚾 🕞 📓 🖬			
PWindows Firewall with A	Inbound Rules		
🗱 Inbound Rules	Name	Group	Pro
Contraction Constitution	Active Directory Domain Control	Active Directory Dom	All
Monitoring	Active Directory Domain Control	Active Directory Dom	All
/ ag monitoring	Active Directory Domain Control	Active Directory Dom	All
	Active Directory Domain Control	Active Directory Dom	All
	Active Directory Domain Control	Active Directory Dom	All
	Active Directory Domain Control	Active Directory Dom	All
	Active Directory Domain Control	Active Directory Dom	All

AllJoyn Router (TCP-In)

AllJoyn Router (UDP-In)

Cast to David

Actions Profile Enabled Ai / Inbound Rules Yes A 🗱 New Rule... y Domain Control... Active Directory Dom... All Yes AI Filter by Profile y Domain Control... Active Directory Dom... All Yes AI 7 Filter by State v Domain Control... Active Directory Dom... All Yes AI y Domain Control... Active Directory Dom... All Yes AI Filter by Group y Domain Control... Active Directory Dom... All Yes A View Yes A Refresh Active Directory Domain Control... Active Directory Dom... All Yes AI Active Directory Domain Control... Active Directory Dom... All Yes AI 🔒 Export List... Active Directory Domain Control... Active Directory Dom... All Yes AI ? Help Active Directory Domain Control... Active Directory Dom... All Yes AI Active Directory Domain Control... Active Directory Dom... All Yes AI Active Directory Domain Control... Active Directory Dom... All Yes AI Active Directory Web Services (T... Active Directory Web ... All AI Yes Domai... Yes AI Domai... Yes AI

A

AI

AI

A

A

No

No

No

Yes

Yes

Yes

ภาพที่4.68 Fire wall Setting(3)

Cast to Dovice function

AllJoyn Router

AllJoyn Router

BranchCache Content Retrieval (... BranchCache - Conten... All

BranchCache Hosted Cache Serv... BranchCache - Hosted... All

BranchCache Peer Discovery (WS... BranchCache - Peer Di... All

Ocast to Device functionality (qW... Cast to Device functio... Private...

Cast to Device functionality (qW... Cast to Device functio... Private...

Cast to Device SSDP Discovery (... Cast to Device functio... Public

na conjor (

×

م

- เถือก New Rule

Windows Firewall with A	dvanced Security					- 🗆 X
File Action View Help						
🔶 🄿 🙍 📰 🕞 🔒 🗾						
PWindows Firewall with A	Inbound Rules					Actions
🗱 Inbound Rules	Name	Group	Profile	Enabled	Α ^	Inbound Rules
Outbound Rules	Active Directory Domain Control	Active Directory Dom	All	Yes	Α	New Rule
Monitoring	Active Directory Domain Control	Active Directory Dom	All	Yes	Α	
/ Se Wontoning	Active Directory Domain Control	Active Directory Dom	All	Yes	Α	✓ Filter by Profile
	Active Directory Domain Control	Active Directory Dom	All	Yes	Α	▼ Filter by State
	Active Directory Domain Control	Active Directory Dom	All	Yes	Α	Filter by Group
	Active Directory Domain Control	Active Directory Dom	All	Yes	Α	View
	Active Directory Domain Control	Active Directory Dom	All	Yes	A	
	Active Directory Domain Control	Active Directory Dom	All	Yes	A	C Refresh
	Active Directory Domain Control	Active Directory Dom	All	Yes	A	🗟 Export List
	Active Directory Domain Control	Active Directory Dom	All	Yes	A	Help
	Active Directory Domain Control	Active Directory Dom	All	Yes	A	
	Active Directory Domain Control	Active Directory Dom	All	Yes	A	
	Active Directory Domain Control	Active Directory Dom	All	Yes	A	
	Active Directory Web Services (T	Active Directory Web	All	Yes	A	
	AllJoyn Router (TCP-In)	AllJoyn Router	Domai	Yes	A	
	AllJoyn Router (UDP-In)	AllJoyn Router	Domai	Yes	A	
	BranchCache Content Retrieval (BranchCache - Conten	All	No	A	
	BranchCache Hosted Cache Serv	BranchCache - Hosted	All	No	Α	
	BranchCache Peer Discovery (WS	BranchCache - Peer Di	All	No	Α	
	Cast to Device functionality (qW	Cast to Device functio	Private	Yes	A	
	Cast to Device functionality (qW	Cast to Device functio	Private	Yes	A	
	Cast to Device SSDP Discovery (Cast to Device functio	Public	Yes	A v	
	The Cast to Daviso streaming conjor (Cast to Dovice functio	hobbe	Voc	^	

ภาพที่4.69 Fire wall Setting(4)



- ตั้งค่าให้ Inbound รับ Port ที่ตั้งค่าไว้เท่านั้น



เลือกให้ Rule ของเราแสดงมีผลที่ไหนบ้าง



- จะเห็น Rule ที่สร้างโผล่ขึ้นมา

File Action View Help Windows Firewall with A Windows Firewall with A Mame Group Profile Finabled A Connection Security A Control Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Dom All Yes A Active Directory Dom All Yes A Ac	Pindows Firewall with A	dvanced Security						- 🗆	\times
Inbound Rules Inbound Rules Active Directory Domain Control Active Directory Dom All Yes	File Action View Help								
Windows Firewall with A Inbound Rules Actions Connection Security R Name Group Profile Enabled A Soutbound Rules Soutbound Rules All Yes A Connection Security R Soutbound Rules All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes Yes Active Directory Domain Control Active Directory Dom All Yes Yes Active Directory Domain Control Active Directory Dom All Yes Yes Active Directory Domain Control Active Directory Dom All Yes Yes Active Directory Domain Control Active Directory Dom All Yes Yes Active Directory Domain Control Active Directory Dom All Yes Yes Active Directory Domain Control Active Directory Dom All Yes Yes Active Directory Domain Control Active Directory Dom All Yes Yes	🔶 🏟 🙍 📰 🗟 🚺								
Inbound Rules Name Group Profile Enabled A Souncound Rules Soll TCP Port All Yes A Sometoin Security R Soll TCP Port All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes <	PWindows Firewall with A	Inbound Rules					Acti	ons	
SQL TCP Port All Yes A © Connection Security R © Active Directory Domain Control Active Directory Dom All Yes A © Active Directory Domain Control Active Directory Domain Control Active Directory Dom All Yes A © Active Directory Domain Control Active Directory Dom All Yes A © Active Directory Domain Control Active Directory Dom All Yes A © Active Directory Domain Control Active Directory Dom All Yes A © Active Directory Domain Control Active Directory Dom All Yes A © Active Directory Domain Control Active Directory Dom All Yes A © Active Directory Domain Control Active Directory Dom All Yes A © Active Directory Domain Control Active Directory Dom All Yes A © Active Directory Domain Control Active Directory Dom All Yes A © Active Directory Domain Control Active Directory Dom All Yes A © Active Directory Doma	🖾 Inbound Rules	Name	Group	Profile	Enabled	A ^	Inbo	ound Rules	
 Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom Al	Outbound Rules	SQL TCP Port			Yes	Α	2-2	Now Pulo	
 Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Domain Control Active Directory Dom	Monitoring	Active Directory Domain Control	Active Directory Dom	All	Yes	Α	-	New Kule	
 Active Directory Domain Control Active Directory Dom All Yes A Yes Yes<td>> Ha wonitoring</td><td>Active Directory Domain Control</td><td>Active Directory Dom</td><td>All</td><td>Yes</td><td>Α</td><td> ▼</td><td>Filter by Profile</td><td>•</td>	> Ha wonitoring	Active Directory Domain Control	Active Directory Dom	All	Yes	Α	▼	Filter by Profile	•
● Active Directory Domain Control Active Directory Dom All Yes A ● Active Directory Domain Control Active Directory Domain Control Active Directory Dom All Yes A ● Active Directory Domain Control Active Directory Dom All Yes A ● Active Directory Domain Control Active Directory Dom All Yes A ● Active Directory Domain Control Active Directory Dom All Yes A ● Active Directory Domain Control Active Directory Dom All Yes A ● Active Directory Domain Control Active Directory Dom All Yes A ● Active Directory Domain Control Active Directory Dom All Yes A ● Active Directory Domain Control Active Directory Dom All Yes A ● Active Directory Domain Control Active Directory Dom All Yes A ● Active Directory Domain Control Active Directory Dom All Yes A ● Active Directory Domain Control Active Directory Dom All Yes A <td< td=""><td></td><td>Active Directory Domain Control</td><td>Active Directory Dom</td><td>All</td><td>Yes</td><td>Α</td><td>7</td><td>Filter by State</td><td>•</td></td<>		Active Directory Domain Control	Active Directory Dom	All	Yes	Α	7	Filter by State	•
Active Directory Domain Control Active Directory Dom All Yes All Yes Allyon Router Ontrol Active Directory Dom All Yes All Yes A Disable Rule Active Directory Domain Control Active Directory Dom All Yes All Yes A Disable Rule Allyon Rou		Active Directory Domain Control	Active Directory Dom	All	Yes	Α	7	Filter by Group	•
Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A A		Active Directory Domain Control	Active Directory Dom	All	Yes	Α		View	
Active Directory Domain Control Active Directory Dom All Yes All Yes All Yes All Yes All Yes All Yes All Yes All Yes All Yes All Yes All Yes All Yes All Yes All Yes All Yes All Yes All Yes All Yes All Yes		Active Directory Domain Control	Active Directory Dom	All	Yes	Α		view	,
 Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Domain Control Active Directory Dom All Yes Active Directory Web Services (T Active Directory Dom All Yes Alloyn Router (UDP-In) Alloyn Router Domai Yes Copy Alloyn Router (UDP-In) Alloyn Router Domai Yes Copy Properties BranchCache Content Retrieval (BranchCache - Conten All No Help Help 		Active Directory Domain Control	Active Directory Dom	All	Yes	Α	Q	Refresh	
Ø Active Directory Domain Control Active Directory Dom All Yes A Ø Active Directory Domain Control Active Directory Dom All Yes A Ø Active Directory Domain Control Active Directory Dom All Yes A Ø Active Directory Domain Control Active Directory Dom All Yes A Ø Active Directory Domain Control Active Directory Dom All Yes A Ø Active Directory Domain Control Active Directory Dom All Yes A Ø Active Directory Domain Control Active Directory Dom All Yes A Ø Active Directory Web Services (T Active Directory Web All Yes A Ø Active Directory UP-In) AllUoyn Router Domai Yes A Cut Ø AllJoyn Router (UDP-In) AllUoyn Router Domai Yes A Delete BranchCache Content Retrieval (BranchCache - Serv BranchCache - Hosted All No A Properties BranchCache Peer Discovery (WS BranchCache - Peer Di All No <		Active Directory Domain Control	Active Directory Dom	All	Yes	Α		Export List	
Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Web Services (T Active Directory Web All Yes A Active Directory Web Services (T Active Directory Web All Yes A Active Directory Web Services (T Active Directory Web All Yes A AllJoyn Router (TCP-In) AllJoyn Router Domai Yes A AllJoyn Router (UDP-In) AllJoyn Router Domai Yes A BranchCache Content Retrieval (BranchCache - Conten All No A BranchCache Peer Discovery (WS BranchCache - Peer Di All No A		Active Directory Domain Control	Active Directory Dom	All	Yes	Α	?	Help	
Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Web Services (T Active Directory Web All Yes A Active Directory Web Services (T Active Directory Web All Yes A All Yes A All Yes A All Yes A All Yes A All Yes A All Yes A All Yes A All Yes A All Yes A All Yes A All Yes A A		Active Directory Domain Control	Active Directory Dom	All	Yes	А	-		_
Active Directory Domain Control Active Directory Dom All Yes A Active Directory Domain Control Active Directory Dom All Yes A Active Directory Web Services (T Active Directory Web All Yes A All Yes All Yes All Yes All Yes All Yes All Yes A A		Active Directory Domain Control	Active Directory Dom	All	Yes	Α	SQL	. TCP Port	•
Ø Active Directory Domain Control Active Directory Dom All Yes A All Yes A X Cut Ø Active Directory Web Services (T Active Directory Web All Yes All Yes <		Active Directory Domain Control	Active Directory Dom	All	Yes	Α	۲	Disable Rule	
Image: Active Directory Web Services (T Active Directory Web All Yes All Yes A Image: Active Directory Web Services (T Active Directory Web All Services (T Active Directory Web Yes A Image: Content of the services (T Active Directory Web Yes Image: AllJoyn Router (UDP-In) AllJoyn Router Domai Yes A Image: Content of the services (T Active Directory Web All Services (T Active Directory Meb All No A Image: Content of the services (T Active Directory Meb All No A Image: Properties (T Active Directory Meb All No A Image: Properties (T Active Directory Active Directory Meb All No A Image: Properties (T Active Directory Active Directory Meb All No Image: Properties (T Active Directory Active Directory Active Directory Active Directory Meb All No A Image: Properties (T Active Directory Directory Active Directory Directory Active Directory Active Directory Active Directory Directory Active Directory		Active Directory Domain Control	Active Directory Dom	All	Yes	Α	X	Cut	
Image: AllJoyn Router (TCP-In) AllJoyn Router Domai Yes A Image: Copy Image: AllJoyn Router (UDP-In) AllJoyn Router Domai Yes A Image: Copy Image: BranchCache Content Retrieval (BranchCache - Conten All No A Image: Properties Image: BranchCache Hosted Cache Serv BranchCache - Hosted All No A Image: Help Image: BranchCache Peer Discovery (WS BranchCache - Peer Di All No A Image: Help		Active Directory Web Services (T	Active Directory Web	All	Yes	Α		c	
Image: AllJoyn Router (UDP-In) AllJoyn Router Domai Yes A Image: AllJoyn Router BranchCache Content Retrieval (BranchCache - Conten All No A Image: AllJoyn Router BranchCache Content Retrieval (BranchCache - Hosted All No A Image: AllJoyn Router BranchCache Hosted Cache Serv BranchCache - Hosted All No A Image: Help		AllJoyn Router (TCP-In)	AllJoyn Router	Domai	Yes	Α	42	Сору	
BranchCache Content Retrieval (BranchCache - Conten All No A Properties BranchCache Hosted Cache Serv BranchCache - Hosted All No A Help BranchCache Peer Discovery (WS BranchCache - Peer Di All No A Help		AllJoyn Router (UDP-In)	AllJoyn Router	Domai	Yes	Α	×	Delete	
BranchCache Hosted Cache Serv BranchCache - Hosted All No A BranchCache Peer Discovery (WS BranchCache - Peer Di All No A		BranchCache Content Retrieval (BranchCache - Conten	All	No	Α		Properties	
BranchCache Peer Discovery (WS BranchCache - Peer Di All No A		BranchCache Hosted Cache Serv	BranchCache - Hosted	All	No	Α	2	Holp	
		BranchCache Peer Discovery (WS	BranchCache - Peer Di	All	No	Α		нер	
Cast to Device functionality (qW Cast to Device functio Private Yes A		Cast to Device functionality (qW	Cast to Device functio	Private	Yes	Α			
Cast to Device functionality (qW Cast to Device function Private Yes A		Cast to Device functionality (qW	Cast to Device functio	Private	Yes	A			
Cart to Davido SSDD Directivant (Cart to Davido function Dublic Var A	<	Cast to Davisa SSDB Discovary (Cast to Davisa functio	Dublic	Vor	> ×			

ภาพที่4.75 Rule ที่สร้าง

4.1.1.2.8 Remote Access Configuration

T



ภาพที่4.76 Remote access configuration(1)

- เถือก Remote settings

10

🧏 System			- 🗆 X
← → ✓ ↑ 😒 > Control Pan	el > System and Security > Sys	stem v Ö Se	arch Control Panel
Control Panel Home	View basic information	about your computer	0
🗣 Device Manager	Windows edition		
🗣 <u>Remote settings</u>	Windows Server 2016 Star	odard	
Advanced system settings	© 2016 Microsoft Corpora reserved.	ation. All rights	lows Server 2016
	System Processor:	Intel(R) Core(TM) i5-8250U CPU @ 1.6	0GHz 1.80 GHz (2 processors)
	Installed memory (RAM):	2.00 GB	
	System type:	64-bit Operating System, x64-based p	rocessor
	Pen and Touch:	No Pen or Touch Input is available for	this Display
	Computer name, domain, and	workgroup settings	
	Computer name:	WIN-H7GGI7RUJG0	Change settings
	Full computer name:	WIN-H7GGI7RUJG0	
	Computer description:		
	Workgroup:	WORKGROUP	
	Windows activation		
	Windows is not activated.	Read the Microsoft Software License Te	erms
See also Security and Maintenance	Product ID: 00377-60000-	00000-AA175	Activate Windows

ภาพที่4.77 Remote access configuration(2)

- เข้าไปที่ Remote แล้วเลือก Don't allow remote connection to this computer

	System Properties	×
	Computer Name Hardware Advanced Remote	
	Remote Assistance	
	Allow Remote Assistance connections to this computer	
	Advanced	
	Remote Desktop	
	Choose an option, and then specify who can connect.	
	Don't allow remote connections to this computer	
	Allow remote connections to this computer	
	Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)	
1/2	Help me choose Select Users	
	UN Cancel App	y
	ภาพท4.78 Remote access configuration(3)	

4.1.1.2.9 Service Configuration

- เถือก Computer Management



ภาพที่4.79 Service



เข้าไปที่หมวด Standard ค้านถ่าง

(*

😼 Computer Management							- 0	×
File Action View Help								
🗢 🄿 🖄 📰 🖻 🔒								
🎥 Computer Management (Local	Name	Description	Status	Startup Type	Log On As	^	Actions	
V 🎁 System Tools	ActiveX Installer (AxInstSV)	Provides Us		Manual	Local Syste		Services	
Firent Viewer	AllJoyn Router Service	Routes AllJo		Manual (Trig	Local Service		More Actions	•
Shared Folders	App Readiness	Gets apps re		Manual	Local Syste			
> 🚂 Local Users and Groups	Application Identity	Determines		Manual (Trig	Local Service			
> N Performance	Application Information	Facilitates t	Running	Manual (Trig	Local Syste			
🗄 Device Manager	Application Layer Gateway	Provides su		Manual	Local Service			
✓ Storage	Application Management	Processes in		Manual	Local Syste			
> 뉈 Windows Server Backup	AppX Deployment Service (Provides inf		Manual	Local Syste			
📅 Disk Management	Auto Time Zone Updater	Automatica		Disabled	Local Service			
 Bervices and Applications 	Background Intelligent Tran	Transfers fil		Manual	Local Syste			
> 🔂 Routing and Remote Ac	Background Tasks Infrastru	Windows in	Running	Automatic	Local Syste			
Services	Sase Filtering Engine	The Base Fil	Running	Automatic	Local Service			
🗃 WMI Control	Reluetooth Support Service	The Bluetoo		Manual (Trig	Local Service			
	CDPUserSvc_5edf6	<failed r<="" td="" to=""><td>Running</td><td>Automatic</td><td>Local Syste</td><td></td><td></td><td></td></failed>	Running	Automatic	Local Syste			
	Certificate Propagation	Copies user	Running	Manual	Local Syste			
	Client License Service (ClipS	Provides inf		Manual (Trig	Local Syste			
	CNG Key Isolation	The CNG ke	Running	Manual (Trig	Local Syste			
	COM+ Event System	Supports Sy	Running	Automatic	Local Service			
	COM+ System Application	Manages th		Manual	Local Syste			
	Computer Browser	Maintains a		Disabled	Local Syste			
	Connected Devices Platfor	This service	Running	Automatic (D	Local Service			
	Connected User Experience	The Connec	Running	Automatic	Local Syste			
	Contact Data_5edf6	Indexes con		Manual	Local Syste			
	CoreMessaging	Manages co	Running	Automatic	Local Service			
	🧠 Credential Manager	Provides se	Running	Manual	Local Syste			
	Cryptographic Services	Provides thr	Running	Automatic	Network S			
	Q Data Sharing Service	Provides da	-	Manual (Trig	Local Syste			
	Q DataCollectionPublishingSe	The DCP (D		Manual (Trig	Local Syste			
	OCOM Server Process Laun	The DCOM	Running	Automatic	Local Syste	~		
< >>	Extended Standard							

ภาพที่4.81 Service ทั้งหมดที่มีในเครื่อง

- ปิด Service ที่ไม่ใช้อย่าง Map Broker เรายังไม่มีความจำเป็นต้องไปใช้ก็ปิดทิ้งได้เลย



4.1.1.2.10 Log & Monitoring

_

10

เข้าไปค้นหา Windows Administrative Tools



ภาพที่4.83 Windows Server Monitor(1)

- เข้าไปเลือก	Performance Monitor			
🔁 🔽 🖶 = File Home Share	Shortcut Tools Administrative Tools			×
← → × ↑ 🗟 « Sy	stem and Security > Administrative Tools >	~ č) Search Admin	istrative Tools 🔎
	Name	Date modified	Type	Size
🖈 Quick access	Computer Management	7/16/2016 6:18 AM	Shortcut	2 //B
📙 Desktop 🛛 🖈	Defragment and Ontimize Drives	7/16/2016 6:18 AM	Shortcut	2 KD
💺 Downloads 🛷		7/16/2016 6:19 AM	Shortcut	2 KB
Documents	Fvent Viewer	7/16/2016 6:18 AM	Shortcut	2 KB
Pictures 🖈	Group Policy Management	7/16/2016 6:19 AM	Shortcut	2 KB
System32	scSI Initiator	7/16/2016 6:18 AM	Shortcut	2 KB
	Local Security Policy	7/16/2016 6:19 AM	Shortcut	2 KB
🧢 This PC	P Microsoft Azure Services	7/16/2016 6:19 AM	Shortcut	2 KB
💜 Network	DDBC Data Sources (32-bit)	7/16/2016 6:18 AM	Shortcut	2 KB
	DDBC Data Sources (64-bit)	7/16/2016 6:18 AM	Shortcut	2 KB
	Performance Monitor	7/16/2016 6:18 AM	Shortcut	2 KB
	🔚 Print Management	7/16/2016 6:19 AM	Shortcut	2 KB
	Resource Monitor	7/16/2016 6:18 AM	Shortcut	2 KB
	Server Manager	7/16/2016 6:19 AM	Shortcut	2 KB
	😥 Services	7/16/2016 6:18 AM	Shortcut	2 KB
	🔝 System Configuration	7/16/2016 6:18 AM	Shortcut	2 KB
	System Information	7/16/2016 6:19 AM	Shortcut	2 KB
	🕀 Task Scheduler	7/16/2016 6:18 AM	Shortcut	2 KB
	🗊 Windows Firewall with Advanced Security	7/16/2016 6:18 AM	Shortcut	2 KB
	Mindows Memory Diagnostic	7/16/2016 6:19 AM	Shortcut AC	tivate ₩iĸdow
	Windows Server Backup	7/16/2016 6:20 AM	Shortcut Go	to Settings ² t ^{KB} activa
29 items 1 item selected	1.07 KB			

ภาพที่4.84 Windows Server Monitor(2)

F

76

เข้ามาดูว่าตอนนี้เครื่องทำงานหนักเท่าไหร่ _



ภาพที่4.85 Windows Server Monitor(3)

เข้าไปที่ Event Viewer

10

8⊖ 🖸 🔳 =	Shortcut Tools Administrative Tools		-		×
File Home Share	View Manage				~ 🕐
← → × ↑ 🖶 > Cor	ntrol Panel > System and Security > Administrati	ve Tools 🗸 🧹	Search Administr	ative Tools	ρ
	Name	Date modified	Turpe	Sizo	^
📌 Quick access	Active Directory Domains and Trusts	7/16/2016 6:20 AM	Chorteut	312C	
📙 Desktop 🛛 🖈	Active Directory Module for Windows Po	7/16/2016 6:10 AM	Shortcut	2 KB	
🐌 Downloads 🖈	Active Directory Noutre for Windows Fo	7/16/2016 6:19 AM	Shortcut	2 KB	
Documents	Active Directory Users and Computers	7/16/2016 6:20 AM	Shortcut	2 KB	
Fictures	ADSI Edit	7/16/2016 6:19 AM	Shortcut	2 KB	
System32	Component Services	7/16/2016 6:18 AM	Shortcut	2 KB	
	Computer Management	7/1 <mark>6/2</mark> 016 6:18 AM	Shortcut	2 KB	
S This PC	Defragment and Optimize Drives	7/1 <mark>6/2</mark> 016 6:18 AM	Shortcut	2 KB	
Intwork 🎯	矝 Disk Cleanup	7/1 <mark>6/2</mark> 016 6:19 AM	Shortcut	2 KB	
	Event Viewer	7/16/2016 6:18 AM	Shortcut	2 KB	
	Group Policy Management	7/16/2016 6:19 AM	Shortcut	2 KB	
	scSI Initiator	7/16/2016 6:18 AM	Shortcut	2 KB	
	Local Security Policy	7/16/2016 6:19 AM	Shortcut	2 KB	
	Microsoft Azure Services	7/16/2016 6:19 AM	Shortcut	2 KB	
	ODBC Data Sources (32-bit)	7/16/2016 6:18 AM	Shortcut	2 KB	
	ODBC Data Sources (64-bit)	7/16/2016 6:18 AM	Shortcut	2 KB	
	Performance Monitor	7/16/2016 6:18 AM	Shortcut	2 KB	
	Recourse Manitor	7/16/2016 6:19 AM	Shortcut	2 KB	
	Server Manager	7/16/2016 6:19 AM	Shortcut A set	A NO	0.44
	Services	7/16/2016 6:18 AM	Shortcut ACUN	Cotting 2 KB	IOW.
20 items 1 item selected	1 14 KB	,	40 10	Settings to a	

ภาพที่4.86 Windows Server Log(1)

เถือก Windows Logs

_

Event Viewer		- 🗆 ×
File Action View Help		
le ⇒ 📰 👔 🖬		
le Event Viewer (Local)	Event Viewer (Local)	Actions
> 📮 Custom Views > 🛋 Windows Logs	Overview and Summary Last refreshed: 7/19/	Event Viewer (Local)
> 🖹 Applications and Servie	Overview	open Saved Log
Subscriptions	^	Y Create Custom View
	To view events that have occurred on your computer, select the appropriate source, log or	Import Custom View
	custom view node in the console tree. The	Connect to Another Co
	Summary of Administrative Events	View 🕨
		Refresh
	Event Type Event I Source Log Last I	👔 Help 🕨 🕨
-	⊞ Critical ·	
	Recently Viewed Nodes	
	News Desirie Medicid	
	Windows Logs App N/A 7/18/2018 9:29:42 7/13	
	<pre>viildows.cogs(hpp:::: 10/A 1/10/2010.0.20.42 1/15 </pre>	
(Λ)	· · · · · · · · · · · · · · · · · · ·	
	Log Summary	
	Log Name Size (Cu Modified E C	C/
	Active Directory we 66 KB/1 7/17/2016 6.34.11 E	
< >		

ภาพที่4.87 Windows Server Log(2)

เข้าไปที่ Application จะเห็นว่ามี log การใช้งานว่าทำอะไรไปบ้าง

	er (Local) Ap	plication Nu	imber of events: 37	2			Act	tions
 ✓ Windows Mappli ✓ Securi ✓ Setup ✓ Syster ✓ Forwa ✓ Applicati ✓ Subscription 	I logs ation ty n rded Events ions and Servi Events c	vel Da Error 7/ Error 7/ Error 7/ Informati 7/ Informati 7/ Informati 7/ General Details Unable to reac first four bytes second four by the IOSB.Inform	te and Time 19/2018 1:14:31 19/2018 1:07:55 19/2018 1:07:55 18/2018 11:14:12 18/2018 11:14:12 et 19/2018 11:14:12 et 19/2018 11:14:12 et 19/2018 11:14:12 et 19/2018 11:14:12 19/2019 01:14:14:14:14:14:14:14:14:14:14:14:14:14	Source PerfN PerfN Perflib Secur Secur ormance ata sectic SB.Status	Event 2006 2006 1008 903 16384 data from on contain and the n	Task ^ None None None None None None None None		plication Open Saved Log Open Saved Log Create Custom View Import Custom View Filter Current Log Properties Find Save All Events As Attach a Task To this View Parfach
		Log Name: Source: Event ID: Level: User: OpCode: More Informati	Application PerfNet 2006 Error N/A Info on: <u>Event Log On</u>	line.	Logged: Task Cate Keyword: Compute	7/1 gory: No s: Cla tr: Wil		Help Help

4.1.2 การติดตั้ง Linux

- ทำการสร้าง Virtual Machine ด้วยการกดปุ่ม Create a New Virtual Machine



- ให้เลือก Hardware เป็น Version ที่ตรงกับเราในที่นี้เลือกเป็น 12.0

New Virtual Machine Wizard

Choose the Virtual Machine Hardware Compatibility Which hardware features are needed for this virtual machine?

Virtual machine hardware compatibility Hardware Workstation 12.0 Compatible ESX Server Compatible products: Limitations: Fusion 8.x 64 GB memory Workstation 12.0 16 processors 10 network adapters 8 TB disk size Help < Back Next > Cancel ภาพที่4.91 การตั้งค่า Virtual Machine ทำการเลือกแผ่นหรือไฟล์ที่เราเก็บ OS ที่จะลงไว้ New Virtual Machine Wizard X **Guest Operating System Installation** A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system? Install from: O Installer disc: DVD RW Drive (E:)

Installer disc image file (iso):

D:\CentOS 7.3 x64\CentOS-7-x86_64-DVD-1611.iso

CentOS 64-bit detected.

Help

O I will install the operating system later.

The virtual machine will be created with a blank hard disk.

< Back

ภาพที่4.92 เลือกลง Linux

Next >

Browse...

Cancel

 \times

- ตั้งชื่อให้กับ VM ที่เราสร้าง

New Virtual Machine Wizard

Name the Virtual Machine

What name would you like to use for this virtual machine?

Virtual machine name:	
CentOS 64-bit TEST	
Location:	
D:\Documents\Virtual Machines\CentOS 64-bit TEST	Browse
The default location can be changed at Edit > Preferences	

Sack Next > Cancel ภาพที่4.93 การระบุที่อยู่ของไฟล์ Virtual Machine

เลือก Cores ที่จะให้นำไปงาน

(

New Virtual Machine Wizard

Processor Configuration

Specify the number of processors for this virtual machine.

2

1

 \sim

 \sim

Processors Number of processors:

Number of cores per processor:

Total processor cores:

Help

< Back Next > Cancel

ภาพที่4.94 การตั้งค่า Linux

 \times

- เลือกจำนวน Ram ให้กับ VM

New Virtual Machine Wizard

Memory for the Virtual Machine

How much memory would you like to use for this virtual machine?



ภาพที่4.95 การให้ Memory กับ VM

เถือก Network แบบ NAT

New Virtual Machine Wizard

Network Type

What type of network do you want to add?

Network connection

Help

- Ouse bridged networking
 - Give the guest operating system direct access to an external Ethernet network. The guest must have its own IP address on the external network.
- Use network address translation (NAT) Give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address.
- Use host-only networking Connect the guest operating system to a private virtual network on the host computer.

O Do not use a network connection

< Back

ภาพที่4.96 การตั้งค่า Network

Next > Cancel

 \times

X

- เถือก LSI Logic

New Virtual Machine Wizard

Select I/O Controller Types

Which SCSI controller type would you like to use?

I/O controller types SCSI Controller:

BusLogic (Not available for 64-bit guests)

LSI Logic (Recommended)

◯ LSI Logic SAS

ุกุ โ น โ ล *ฮี ไ ก*ะ

Help	< Ba	ck Next >	Cancel

ภาพที่4.97 การตั้งค่า I/O

เลือก SCSI

10

New Virtual Machine Wizard

Select a Disk Type

What kind of disk do you want to create?

Virtual disk type

SATA

Help

SCSI (Recommended)

< Back Next >

Cancel

ภาพที่4.98 การตั้งค่า Disk type

 \times

New Virtual Machine Wizard

Select a Disk

Disk

Which disk do you want to use?

Create a new virtual disk

A virtual disk is composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts.

- OUse an existing virtual disk
 - Choose this option to reuse a previously configured disk.
- Use a physical disk (for advanced users) Choose this option to give the virtual machine direct access to a local hard
 - disk.

Help	< Back	Next >	Cancel

ภาพที่4.99 การสร้าง VM

เลือกพื้นที่ให้กับ VM เป็นแบบ Split disk

New Virtual Machine Wizard

Specify Disk Capacity

How large do you want this disk to be?

Maximum disk size (GB): 100.0

Recommended size for Windows Server 2016: 60 GB

Allocate all disk space now.

Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.

○ Store virtual disk as a single file

Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Help

< Back Next >

Cancel

ภาพที่4.100 การตั้งค่าพื้นที่ให้ Linux

 \times

×

ตั้งชื่อ Disk

New Virtual Machine Wizard

Specify Disk File

Where would you like to store the disk file?

Disk File

Help

One disk file will be created for each 2 GB of virtual disk capacity. File names for each file beyond the first will be automatically generated using the file name provided here as a basis.

CentOS 64-bit TEST.vmdk

ภาพที่4.101 การตั้งชื่อให้กับ VM

< Back

Next >

เช็คดูว่าตรงกับที่เราตั้งค่าไว้ใหมแล้วไปกดเปิด VM

New Virtual Machine Wizard

Ready to Create Virtual Machine

Click Finish to create the virtual machine and start installing CentOS 64-bit.

The virtual machine will be created with the following settings:

	Name:			CentOS 64-bit TEST							
	Location:			D:\Documents\Virtual Machines\CentOS 64-bit TEST							
	Version:			Workstation 12.0							
	Opera	ating S	ystem:	CentOS	64-ł	bit					
	Hard	Disk:		100 GB,	Spli	t					
	Memo	ory:		2048 M	3						
	Netwo	ork Ada	apter:	NAT							
	Other	Device	es:	2 CPU o	ores	, CD/DVD,	USB Co	ontroller,	Printer,	Sound C	2
ļ											
	Cus	tomize	Hardwa	are							

Power on this virtual machine after creation

Finish Cancel

ภาพที่4.102 ตรวจเช็คการตั้งค่า

< Back

 \times

Browse...

Cancel

- เลือกภาษาที่ต้องการ



- เลือก Time zone ที่เราอยู่

(1


- เลือก Server with GUI แล้วเลือก Add-On ตามที่ต้องการ

SOFTWARE SELECTION CENTOS LINUX 7 INSTALLATION Help! 🖽 us Add-Ons for Selected Environment Base Environment Minimal Install Backup Server Basic functionality Software to centralize your infrastructure's backups. Compute Node DNS Name Server Installation for performing computation and This package group allows you to run a DNS name processing. server (BIND) on the system. E-mail Server Infrastructure Server Allows the system to act as a SMTP and/or IMAP e-Server for operating network infrastructure services. File and Print Server mail server. FTP Server File, print, and storage server for enterprises. Allows the system to act as an FTP server. Basic Web Server File and Storage Server Server for serving static and dynamic internet content. CIFS, SMB, NFS, iSCSI, iSER, and iSNS network storage server. Virtualization Host Hardware Monitoring Utilities Minimal virtualization host. A set of tools to monitor server hardware. Server for operating network infrastructure servic with a GUI. High Availability Infrastructure for highly available services and/or shared storage. GNOME Desktop GNOME is a highly intuitive and user friendly Identity Management Server desktop environment. Centralized management of users, servers and authentication policies. 147

ภาพที่4.107 เลือก Environment ที่ต้องการ

เลือก Installation Destination



- เลือก Disk ที่เราตั้งไว้ตั้งแต่ตอนสร้าง VM



เลือก Network & Host name



- เลือกเปิด

(.



เข้าไปปิด KDUMP

_ KDUMP CENTOS LINUX 7 INSTALLATION 🖽 us Help! Kdump is a kernel crash dumping mechanism. In the event of a system crash, kdump will capture information from your system that can be invaluable in determining the cause of the crash. Note that kdump does require reserving a portion of system memory that will be unavailable for other uses. 📄 Enable kdump Kdump Memory Reservation: Automatic 🔿 Manual Memory To Be Reserved (MB): 128 - + Total System Memory (MB): 1984 Usable System Memory (MB): 1856 ภาพที่4.113 ตั้งค่า KDUMP **N**A Begin Installation INSTALLATION SUMMARY CENTOS LINUX 7 INSTALLATION Help! 🕮 us DATE & TIME KEYBOARD CentOS Asia/Bangkok timezone English (US) LANGUAGE SUPPORT а English (United States) SOFTWARE INSTALLATION SOURCE SOFTWARE SELECTION 0 Local media Server with GUI SYSTEM INSTALLATION DESTINATION KDUMP Automatic partitioning selected Kdump is disabled **NETWORK & HOST NAME** SECURITY POLICY Wired (ens33) connected No profile selected Quit Begin Installation

ภาพที่4.114 เลือก Begin Installation

F

We won't touch your disks until you click 'Begin Installation'

- เข้าไปตั้งรหัสที่ Root password

Gent OS			CENTOS LINUX	7 INSTALLATION Help!
Centos	USER SETTINGS ROOT PASSWORD Root password is not set	2	USER CREAT	FION be created
	Creating disklabel on /dev/sda	a		
10	entOS Core SIG oduces the CentOS Linux Distribution. «i.centos.org/SpecialInterestGroup	4	12	
	A Please complete items marked with this icon ກາพที่4.115 ເ	i before continuing t ข้าไปที่ Roo	t password	

- ตั้งรหัสตามที่ต้องการ

	The root account is used for administering the system. Enter a password for the ro	ot user.	
	Root Password:		
		Weak	
	Confirm:		
			IN A
1			
	A The password you have provided is weak: The password is shorter than 8 characters. You will have confirm it.	ve to press Done twice to	
	ถาพที่4 116 ตั้งอ่า Poot pageword		
	31W14.110 WNTERCOL password		

- ติดตั้งเสร็จแล้วจะมีปุ่มขึ้นมาให้กด Reboot ด้วย



ภาพที่4.117 ทำการ Reboot

Login ด้วย Root และรหัสที่เราตั้งไว้

10

root	
Password:	T
Cancel Log in as another user	Jnlock

ภาพที่4.118 หน้า Login

- เข้าหน้า CentOS พร้อมใช้งาน

A

ภาพที่4.119 หน้า CentOS 7

4.1.2.1 การทำ Linux Hardening

(.

Applications Places

4.1.2.1.2 Yum update

ใช้คำสั่ง yum update

File Edit View Search Terminal Help
[root@localhost /]# yum update
BDB2053 Freeing read locks for locker 0x1296: 47384/140711669892928
BDB2053 Freeing read locks for locker 0x1298: 47384/140711669892928
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
* base: mirrors.bangmodhosting.com
* extras: mirrors.bangmodhosting.com
Resolving Dependencies
--> Package 389-ds-base.x86_64 0:1.3.5.10-11.el7 will be obsoleted
--> Processing Dependency: 389-ds-base >= 1.3.5.6 for package: slapi-nis-0.56.08.el7.x86_64
--> Package 389-ds-base-libs.x86_64 0:1.3.7.5-24.el7_5 will be updated
--> Package 389-ds-base-libs.x86_64 0:1.3.7.5-24.el7_5 will be ubdated
--> Package 389-ds-base-smp.x86_64 0:1.6.0-2.el7 will be updated
--> Package ModemManager.x86_64 0:1.6.10-1.el7 will be updated
--> Package ModemManager.x86_64 0:1.6.10-1.el7 will be updated
--> Package NetworkManager.x86_64 1:1.4.0-12.el7 will be obsoleted
--> Package NetworkManager.adsl.x86_64 1:1.4.0-12.el7 will be updated
--> Package NetworkManager.adsl.x86_64 1:1.4.0-1

root@localhost:/

🔒 Wed 11:57 💿 🐠 🖒

เพื่อทำให้ระบบทุกๆอย่างในเครื่องเรา update เป็นตัวล่าสุด

	root@localhost:/	_ 0 ×
File Edit View Se	earch Terminal Help	
Updating : gl	libc-2.17-222.el7.x86 64	33/2324
warning: /etc/nss	switch.conf created as /etc/nsswitch.conf.rpmnew	
Updating : li	ibstdc++-4.8.5-28.el7 5.1.x86 64	34/2324
Updating : ns	spr-4.19.0-1.el7 5.x86 64	35/2324
Updating : ns	ss-util-3.36.0-1.el7 5.x86 64	36/2324
Updating : no	curses-libs-5.9-14.20130511.el7 4.x86 64	37/2324
Updating : ba	ash-4.2.46-30.el7.x86 64	38/2324
Updating : po	cre-8.32-17.el7.x86 64	39/2324
Updating : li	ibsepol-2.5-8.1.el7.x86 64	40/2324
Updating : li	ibselinux-2.5-12.el7.x86 64	41/2324
Updating : li	ibcom_err-1.42.9-12.el7 5.x86_64	42/2324
Updating : fr	reetype-2.4.11-15.el7.x86_64	43/2324
Updating : li	ibuuid-2.23.2-52.el7.x86_64	44/2324
Updating : ch	nkconfig-1.7.4-1.el7.x86_64	45/2324
Updating : li	ibICE-1.0.9-9.el7.x86_64	46/2324
Updating : au	udit-libs-2.8.1-3.el7.x86_64	47/2324
Updating : li	ibgcrypt-1.5.3-14.el7.x86_64	48/2324
Updating : p1	11-kit-0.23.5-3.el7.x86_64	49/2324
Updating : in	nfo-5.1-5.el7.x86_64	50/2324
Updating : gr	rep-2.20-3.el7.x86_64	51/2324
Updating :li	ibtalloc-2.1.10-1.el7.x86_64	52/2324
Updating : ex	<pre>kpat-2.1.0-10.el7_3.x86_64</pre>	53/2324
_ Updating : re	eadline-6.2-10.el7.x86_64	54/2324

ภาพที่4.121 Yum update(2)

root@localhost:~

4.1.2.1.3 World-writable Files

TC

_

ใช้คำสั่ง find เพื่อเรียกดูไฟล์ทั้งหมดของ Linux Server

ł	File	Edit	View	Search	Termi	nal Help			
[roo	t@loc	alhos	t ~1#	find /	-perm	- 0=WX	-ls	

ภาพที่4.122 World-writable Files

_ 0

ใช้คำสั่งนี้เป็นระยะๆ เพื่อตรวจดูว่าช่วงที่ผ่านมามีไฟล์ที่ World-writable หรือ World-_

executable อะไรเพิ่มขึ้นมาบ้างมีไฟล์ไหนแปลกปลอมไหม root@localhost:~

File Edit View Search T	Ferminal Help		
/C/anome-help/figures/	network-cellula	r-umts-svmbo	lic.sva 🛛
34992157 0 lrwxrwxr	wx 1 root	root	78 Aug 8 15:54 /usr/share/
help/hu/anome-help/fia	ures/network-ce	llular-signa	l-none-symbolic.svg -> /usr/sha
re/help/C/anome-help/f	igures/network-	cellular-sig	nal-none-symbolic.svg
35003207 0 1 rwx rwx ri	wy 1 root	root	57 Aug 8 15:54 /usr/share/
help/hu/anome-help/fia	ures/shell-work	snaces nnd -:	> /usr/share/heln/(/gnome-heln/
figures/shell-workspace		spaces plig	y usi y shure, neep, e, ghome neep,
35003182 0 1 rwy rwy r	wy 1 root	root	76 Aug 8 15:54 /usr/share/
belp/bu/gnome_belp/fig	wros/network_wi	reless-conner	cted_symbolic_sym_s_/usr/share
/holp/(/gnome-holp/fig	uros/network-wi	roloss conno	cted-symbolic syg -> /usi/share
25002182 0 Invynym	wy 1 root	root	76 Aug = 8 15.54 /usr/sharo/
bolp/bu/gnomo bolp/fig	with a second se	rolocc operv	To Aug o 15.54 /usi/share/
/help/((gnome_help/fig	ures/network-wi	reless-encry	pted-symbolic.svg -> /usi/share
	ures/network-wi	recess-encry	Pied-Symbolic.Svg
55005164 0 LTWXTWXT	WX I TOOL	root	os Aug o 15:54 /usr/share/
netp/nu/gnome-netp/iig	ures/network-wi	retess-signa	l-excellent-symbolic.svg -> /us
r/snare/netp/t/gnome-n	etp/rigures/net	work-wireles	s-signal-excellent-symbolic.svg
32003182 0 LTWXTWXT	WX I root	root	/8 Aug 8 15:54 /usr/snare/
nelp/nu/gnome-nelp/Tig	ures/network-wi	.reless-signa	l-good-symbolic.svg -> /usr/sna
re/nelp/C/gnome-nelp/T	igures/network-	wireless-sig	nal-good-symbolic.svg
35003186 0 Lrwxrwxri	wx 1 root	root	/8 Aug 8 15:54 /usr/share/
help/hu/gnome-help/fig	ures/network-wi	.reless-signa	l-none-symbolic.svg -> /usr/sha
re/help/C/gnome-help/f	igures/network-	wireless-sig	nal-none-symbolic.svg
35003187 0 lrwxrwxr	wx 1 root	root	76 Aug 8 15:54 /usr/share/
help/hu/gnome-help/fig	ures/network-wi	.reless-signa	l-ok-symbolic.svg -> /usr/share

ภาพที่4.123 ตรวจเช็คไฟล์

4.1.2.1.4 Window X disable

T

- ใช้คำกสั่ง vi เข้าไปแก้ไขไฟล์

root@education: File Edit View Terminal Tabs Help [root@education ~]# vi /etc/inittab

ภาพที4.124 เกรร ASTITUTE OF ภาพที่4.124 การปิด GUI (1) _ 0 X

เข้าไปเปลี่ยน id:5:initdefault: ให้เป็น id:3:initdefault:

_

root@education:~	2							
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>T</u> erminal Ta <u>b</u> s <u>H</u> elp								
<pre># inittab This file describes how the INIT process should set up # the system in a certain run-level. #</pre>	b.							
<pre># Author: Miquel van Smoorenburg, <miquels@drinkel.nl.mugnet.org> # Modified for RHS Linux by Marc Ewing and Donnie Barnes #</miquels@drinkel.nl.mugnet.org></pre>								
<pre># Default runlevel. The runlevels used by RHS are: # 0 - halt (Do NOT set initdefault to this) # 1 - Single user mode</pre>								
<pre># 2 - Multiuser, without NFS (The same as 3, if you do not have networking) # 3 - Full multiuser mode # 4 - unused # 5 - X11</pre>								
<pre># 6 - reboot (Do NOT set initdefault to this) # id:5:initdefault:</pre>								
<pre># System initialization. si::sysinit:/etc/rc.d/rc.sysinit</pre>								
l0:0:wait:/etc/rc.d/rc 0 "/etc/inittab" 55L, 1735C	~							

ภาพที่4.125 การปิด GUI (2)

จากนั้นใช้กด esc แล้วกด : แล้วใช้กำสั่ง wq เพื่อบันทึกแล้วออก

root@education;~
File Edit View Terminal Tabs Help
#
inittab This file describes how the INIT process should set up
the system in a certain run-level.
#
Author: Miquet van Smoorenburg, <miquets@arinket.ht.mugnet.org></miquets@arinket.ht.mugnet.org>
#
Default runlevel. The runlevels used by RHS are:
0 - halt (Do NOT set initdefault to this)
2 - Multiuser without NES (The same as 3 if you do not have networking)
3 - Full multiuser mode
4 - unused
5 - X11
6 - reboot (Do NOT set initdefault to this)
id:3:initdefault:
System initialization.
si::sysinit:/etc/rc.d/rc.sysinit
10:0:wait:/etc/rc_d/rc_0
INSERT
ภาพท4.126 การบด GUI (3)
Western OF

ใช้คำสั่ง init 3 เพื่อเป็นการปิด GUI

 root@education:~

 File
 Edit
 View
 Terminal
 Tabs
 Help

 [root@education ~]# vi /etc/inittab

 [root@education ~]# init 3

ภาพที่4.127 การปิด GUI (4)

กุคโนโลยั7 กุ*ค*

หน้าจอ GUI จะหายไปกลายเป็นหน้า command line

TC

Enterprise Linux Enterprise Linux Server release 5.5 (Carthage) Kernel 2.6.18-194.el5 on an i686 education login: _

ภาพที่4.128 การปิด GUI (5)

_ **– ×**

4.1.2.1.5 Turn off IPv6

- ปิด ipv6 ด้วยกำสั่ง sysctl -w net.ipv6.conf.all.disable_ipv6=1 และ sysctl -w

root@localhost:/

net.ipv6.conf.default.disable_ipv6=1 ถ้าจะเปิคก็ให้เซ็คกลับมาเป็น 0

File Edit View Search Terminal Help
[root@localhost /]# sysctl -w net.ipv6.conf.all.disable_ipv6=1
net.ipv6.conf.all.disable_ipv6 = 1
[root@localhost /]# sysctl -w net.ipv6.conf.default.disable_ipv6=1
net.ipv6.conf.default.disable_ipv6 = 1
[root@localhost /]#

ภาพที่4.129 การปิด IPv6 ใน Linux

กุ ก โ น โ ล *ฮั ไ ก* ะ

4.1.2.1.6 Selinux

(0)

- ใช้กำสั่ง sestatus เพื่อเช็คว่า Selinux เปิดหรือปิดอยู่

 root@education:~

 File
 Edit
 View
 Terminal
 Tabs
 Help

 [root@education ~]#
 sestatus

 SELinux
 status:
 disabled

 [root@education ~]#

ภาพที่4.130 การเปิด Security-Enhanced Linux(1)

п х

ใช้คำสั่ง Vi เข้าไปแก้ไขไฟล์

 root@education:~

 File
 Edit
 View
 Terminal
 Tabs
 Help

 [root@education ~]#
 sestatus

 SELinux status:
 disabled

 [root@education ~]# vi /etc/selinux/config

 [root@education ~]#

ภาพที่4.131 การเปิด Security-Enhanced Linux(2)

แก้ไข SELIINUX=disable เป็น permissive

10

Foot@education;~
<u>File Edit View Terminal Tabs H</u> elp
This file controls the state of SELinux on the system. # SELINUX= can take one of these three values:
<pre># enforcing - SELinux security policy is enforced.</pre>
permissive - SELinux prints warnings instead of enforcing.
disabled - SELinux is fully disabled.
SELINUX=disabled
<pre># SELINUXTYPE= type of policy in use. Possible values are:</pre>
targeted - Only targeted network daemons are protected.
strict - Full SELinux protection.
SELINUXTYPE=targeted

กุกโนโลยั/ก

"/etc/selinux/config" 10L, 447C

ภาพที่4.132 การเปิด Security-Enhanced Linux(3)

จากนั้น save แล้วออกค้วย :wq

~ ~ ~ ~ ~

10

Image in the image is a set of s

ภาพที่4.133 การเปิด Security-Enhanced Linux(4)

lucation:~

ุ า เ โ ล *ยั ไ ก*

ใช้กำสั่ง sestatus เพื่อเช็กกราวนี้จะขึ้นเป็น enable แล้ว

nabled
selinux
ermissive
ermissive
1
argeted

ภาพที่4.134 การเปิด Security-Enhanced Linux(5)

4.1.2.1.7 Quotas

- ใช้คำสั่ง quota แล้วตามด้วย user ที่จะเช็ก ในที่นี้จะให้ user เป็น oracle

root@localhost:~ File Edit View Search Terminal Help [root@localhost ~]# quota oracle Disk quotas for user oracle (uid 1000): none [root@localhost ~]#

ภาพที่4.135 การกำหนดพื้นที่ Disk ให้ User(1)

ใช้กำสั่ง edquota เพื่อเข้าไปแก้ไข quotas disk ของ user oracle

root@localhost:~

File Edit View Search Terminal Help [root@localhost ~]# quota oracle Disk quotas for user oracle (uid 1000): none [root@localhost ~]# edquota -u oracle

คำสั่ง :wa

ภาพที่4.136 การกำหนดพื้นที่ Disk ให้ User(2)

เข้าไปเพิ่มพื้นที่ให้กับ user oracle ในช่อง soft และ hard จากนั้น save แล้วออก ด้วย

1						
	root@lo	ocalhost:"		-	• ×	
File Edit View Search Terr	ninal Help					
Disk quotas for user orac	le (uid 1000):					
Filesystem	blocks	soft	hard	inodes	soft	
hard						
/dev/mapper/r <mark>hel-home</mark>	4564	100000	200000	144	0	
Θ						

ภาพที่4.1<mark>3</mark>7 กา<mark>รกำหนด</mark>พื้นที่ Disk ให้ User(3)

×

ใช้คำสั่ง repquota -a เพื่อเช็กก่า quota ของทุก user จะเห็นว่า user oracle มีพื้นที่ใน ส่วนที่เราเพื่อ โผล่ขึ้นมาแล้ว

				100	t@localhos	st:~			-	×
File Edit	View	Search	Terminal	Help						
[root@localhost ~]# repquota -a *** Report for user quotas on device /dev/mapper/rhel-home 3lock grace time: 7days; Inode grace time: 7days										
User		used	Block soft	limits hard	grace	used	File l: soft	imits hard	grace	
root nobody oracle	Ë	0 8 4564	0 0 100000	0 0 200000		8 2 144	000000000000000000000000000000000000000	0 0 0		
testi filetest		24 24 24	0 0	0	a	S 13 13	0	0		

ภาพที่4.138 การกำหนดพื้นที่ Disk ให้ User(4)

- ทำการลอง add ค่าเข้าไปที่ root

(0)

```
[root@localhost ~]# dd if=/dev/zero of=file-50M.bin bs=1000000 count=50
50+0 records in
50+0 records out
50000000 bytes (50 MB) copied, 0.6848 s, 73.0 MB/s
```

ภาพที่4.139 การกำหนดพื้นที่ Disk ให้ User(5)

ใช้กำสั่ง 1s -1 เพื่อดูไฟล์ที่พึ่ง add เข้าไปว่ามีพื้นที่เท่าไหร่

[root@localhos	st ~]#	#ls	-l					
total 48840								
-rw 1	root	root		1843	Aug	1	23:38	anaconda-ks.cfg
drwxr-xr-x. 3	root	root		47	Aug	8	11:40	Desktop
drwxr-xr-x. 2	root	root		21	Aug	6	14:06	Documents
drwxr-xr-x. 2	root	root		6	Aug	3	14:50	Downloads
-rw-rr 1	root	root	50	000000	Aug	9	15:40	file-50M.bin
drwxr-xr-x. 2	root	root		6	Aug	7	11:08	home
-rw 1	root	root		1930	Aug	1	15:43	initial-setup-ks.cfg
drwxr-xr-x. 2	root	root		6	Aug	3	14:50	Music
drwxr-xr-x. 2	root	root		6	Aug	3	14:50	Pictures
drwxr-xr-x. 2	root	root		6	Aug	3	14:50	Public
drwxr-xr-x. 2	root	root		6	Aug	3	14:50	Templates
drwxr-xr-x. 2	root	root		6	Aug	7	11:08	test1
drwxr-xr-x. 2	root	root		6	Aug	3	14:50	Videos
		_			<u> </u>			

ภาพที่4.140 การกำหนดพื้นที่ Disk ให้ User(6)

ลองมา add ให้ user oracle บ้างโดย add ตั้งแต่ 50,60,70,80 จะเห็นได้ว่าพอ add 80 เข้า
 ไปจะมีข้อความขึ้นมาแจ้งว่าพื้นที่เต็มแล้วไม่สามารถเพิ่มได้อีก เป็นการป้องกันไม่ให้
 user สามารถ add ค่าเข้าไปเกินกว่าที่เรากำหมดได้

```
[root@localhost ~]# su - oracle
Last login: Mon Aug 6 16:03:24 ICT 2018 on pts/0
[oracle@localhost ~]$ dd if=/dev/zero of=file-50M.bin bs=1000000 count=50
50+0 records in
50+0 records out
50000000 bytes (50 MB) copied, 2.44752 s, 20.4 MB/s
[oracle@localhost ~]$ dd if=/dev/zero of=file-60M.bin bs=1000000 count=60
60+0 records in
60+0 records out
60000000 bytes (60 MB) copied, 3.12131 s, 19.2 MB/s
[oracle@localhost ~]$ dd if=/dev/zero of=file-70M.bin bs=1000000 count=70
70+0 records in
70+0 records out
70000000 bytes (70 MB) copied, 4.27759 s, 16.4 MB/s
[oracle@localhost ~]$ dd if=/dev/zero of=file-80M.bin bs=1000000 count=80
dd: error writing 'file-80M.bin': Disk quota exceeded
21+0 records in
20+0 records out
20119552 bytes (20 MB) copied, 1.22331 s, 16.4 MB/s
                       ภาพที่4.141 การกำหนดพื้นที่ Disk ให้ User(7)
```

พื้นที่ของ user oracle หลังจากทำการ add เข้าไปจนเต็ม

[orac	le@localhos:	t ~]\$ quo	ota							
Disk	quotas for	user orac	le (uid	1000):						
	Filesystem	blocks	quota	limit	grace	files	quota	limit	grace	
/dev/	/mapper/rhel	-home								
		200000*	100000	200000	6days	148	0	0		

ภาพที่4.142 การกำหนดพื้นที่ Disk ให้ User(8)

4.1.2.1.8 Password Remember

- ใช้คำสั่ง cd เข้าไปที่ /etc/pam.d

	root@localhos	t:/etc/pam.d	_ ¤ ×
File Edit View Search Te	erminal Help		
<pre>[root@localhost /]# cd [root@localhost pam.d]# atd chfn chsh config-util crond cups fingerprint-auth fingerprint-auth-ac gdm-autologin gdm-fingerprint gdm-launch-environment gdm-password gdm-pin gdm.smartcard [root@localhost pam.d]#</pre>	/etc/pam.d/ ls kcheckpass kscreensaver ksu liveinst login other passwd password-auth password-auth-ac pcsd pluto polkit-1 postgresql postlogin	postlogin-ac ppp remote runuser runuser-l samba setup smartcard-auth smartcard-auth-ac smtp smtp.postfix sshd sssd-shadowutils su	sudo sudo-i su-l system-auth system-auth-ac systemd-user vlock vmtoolsd vsftpd wbem xserver

ภาพที่4.143 การตั้งค่า Password Remember(1)

ใช้คำสั่ง vi เข้าไปแก้พไขไฟล์ system-auth

(.



ภาพที่4.144 การตั้งค่า Password Remember(2)

×

- W1 password sufficient pam_unix.so sha512 shadow nullok try_first_pass

use_authtok ให้เพิ่ม remember เข้าไป

		root@localhost:/etc/pam.d _	• ×
File Edit Vie	ew Search Term	inal Help	
#%PAM-1.0			
# This file	is auto-gener	ated.	
# User chan	ges will be de	stroyed the next time authconfig is run.	
auth	required	pam_env.so	
auth	sufficient	pam_upix_so_pullek_try_first_pass	
auth	requisite	pam_succeed if so uid >= 1000 quiet success	
auth	requised	pam_succeed_11.so did >= 1000 quiet_success	
Gaen	- oquir ou		
account	required	pam unix.so	
account	sufficient	pam_localuser.so	
account	sufficient	pam_succeed_if.so uid < 1000 quiet	
account	required	pam_permit.so	
nance un red	and atta	non numurity on the first need local warms only a	not mu
-2 authtok 1	requisite	pam_pwquatity.so try_first_pass tocat_users_only	retry
password	sufficient	pam unix so sha512 shadow nullok try first pass us	se au
thtok	Sarrietone		JC_dd
password	required	pam deny.so	
session	optional	pam_keyinit.so revoke	
session	required	pam_limits.so	
-session	optional	pam_systemd.so	
system-autr	1" Z3L, 1015C		
	d	a I	

ภาพที4.145 การตั้งค่า Password Remember(3)

ให้ remember = 2 จากนั้น save ด้วยคำสั่ง :wq

10

		root@localho	st:/etc/pam.d			×
File Edit V	iew Search Ter	minal Help				
#%PAM-1.0						
# This file	e is auto-gene	rated.				
# User char	nges will be d	estroyed the next	t time authcon	fig is run.		
auth	required	pam_env.so				- 1
auth	sufficient	pam_fprintd.so				
auth	sufficient	pam_unix.so nu	llok try_first	pass		
auth	requisite	pam_succeed_if	.so uid >= 100	9 quiet_succes	S	
auth	required	pam_deny.so				×.
	-					
account	required	pam_unix.so				
account	sufficient	pam_cucacuser.		quiet		
account	roquirod	pam_succeeu_ii	.50 010 < 1000	quier		11
account	required	pam_permitt.so				
nassword	requisite	nam nwquality (so try first n	ass local user	s only ret	rv
=3 authtok	type=	pam_pwquuttty.	so cry_risc_p	uss cocuc_user	s_oney rec	' y
password	sufficient	pam unix.so sha	a512 shadow nu	llok trv first	pass use	au
thtok remen	iber=2			······································		
password	required	pam deny.so				
	1					
session	optional	pam keyinit.so	revoke			- 1
session	required	pam limits.so				
-session	optional	pam_systemd.so				
			-			

ภาพที่4.146 การตั้งค่า Password Remember(4)

- ทีนี้ถ้า User ที่เคยตั้งรหัสไปแล้วจะไม่สามารถใช้รหัสเดิมมาตั้งได้อีก

[test@localhost ~]\$ passwd Changing password for user test. Changing password for test. (current) UNIX password: New password: BAD PASSWORD: The password is just rotated old one New password:

root@education:/

ภาพที่4.147 การตั้งค่า Password Remember(5)

4.1.2.1.9 Password auth

(

- ใช้คำสั่ง cd เข้าไปที่ /etc/pam.d

<u>File Edit View Terminal Tabs Help</u> [root@education /]# cd /etc/pam.d



ใช้คำสั่ง Vi เข้าไปแก้ไขไฟล์ system-auth

Fie Edit View Terminal Tabs Help [root@education /]# vi system-auth [root@education pam.d]# vi system-auth ภาพที่4.149 การตั้งก่า Password auth(2)

root@education:/etc/pam.d

เปลี่ยนเงื่อนไขในการตั้งรหัสผ่านในบรรทัคที่คไว้

_

TC

				ro	oot@education:/etc/pam.d _ C	JX
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>T</u> erminal	Ta <u>b</u> s	5 <u>H</u> elp	
#%PA	M-1.0					-
# Th	is fi	le is	auto-gen	erate	ed.	
# Us	er ch	anges	will be	destr	royed the next time authconfig is run.	
auth		rec	quired	pa	am_env.so	
auth		sut	fficient	pa	am_unix.so nullok try_first_pass	
auth		reo	quisite	pa	am_succeed_if.so uid >= 500 quiet	
auth		rec	quired	pa	am_deny.so	
acco	unt	rec	quired	pa	am_unix.so	
acco	unt	su	fficient	pa	am_succeed_if.so uid < 500 quiet	
acco	unt	rec	quired	pa	am_permit.so	
_					an analysis as they first seen action 2	=
pass	word	rec	quisite	pa	am_cracktip.so_try_first_pass_retry=5	
pass	word	su	fiftent	pa	am_unix.so mus snadow nuclok try_first_pass use_autr	11
Dace	word	ro	nuired	0.2	am denv. so	
pass	woru	Tet	latien	pa	am_deny.so	
Sess	ion	ont	tional	na	am kevinit so revoke	
sess	ion	rec	nuired	pa	am_helyinits.so	
sess	ion	[si	uccess=1	defau	ult=ignorel pam succeed if so service in crond quiet	E I I
use	uid					
sess	ion	red	quired	pa	am unix.so	
~						

ภาพที่4.150 การตั้งค่า Password auth(3)

แก้ไขและเพิ่มเงื่อนไขเข้าไป ทำให้การตั้งรหัสผ่านมีข้อแม้มากขึ้นละปลอคภัยยิ่งขึ้น

				ro	ot@edu	cation:,	/etc/pa	m.d				×
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	Termin	al Ta <u>b</u> s	<u>H</u> elp							
#%PA	M-1.0)										
# Th	is fi	le is	auto-g	enerate	d.							
#Us	er ch	anges	will b	e destr	oyed th	e next	time a	uthconf	ig is	run.		
auth	1	ree	quired	pa	m_env.s	0						
auth	1	su	fficien	t pa	m unix.	so null	lok try	first	pass			
auth	1	re	quisite	pa	m_succe	ed_if.s	so uid	>= 500	quiet			
auth	1	re	quired	pa	m_deny.	S 0						
acco	unt	ree	quired	pa	m_unix.	S0						
acco	unt	su	fficien	t pa	m_succe	ed_if.s	so uid	< 500 q	uiet			
acco	unt	ree	quired	pa	m_permi	t.so						
		-										_
pass	word	re	quisite	pa	m_pas <mark>s</mark> w	dqc.so	min=di	.sabled,	12,8,6	6,5 max=4	0 passphras	5
e=3	match	=4 sin	nilar=d	<mark>eny r</mark> an	dom=42	enforce	e=every	one ret	ry=3			
pass	word	su	fficien	t pa	m_unix.	so md5	shadov	nullok	try_	first_pas	s use_auth1	t
ok												1
pass	word	ree	quir <mark>ed</mark>	pa	m_den <mark>y</mark> .	S0						
sess	ion	op	tional	pa	m_keyin	it.so ı	revoke					
sess	ion	ree	quired	pa	m_lim <mark>it</mark>	5.50						
sess	ion	[s	iccess=	1 defau	lt=igno	re] par	n_succe	ed_if.s	o serv	vice in c	rond quiet	
use_	uid											
sess	ion	ree	quired	pa	m_unix.	S 0						
"sys	tem-a	uth"	20L, 91	9C								~
					-	d			1. 			
					វា	11/11/14	ען וכו	11161111				

ใช้กำสั่ง man pam_passwdqc เพื่อเข้าไปตรวจสอบว่าที่เราตั้งไว้ขึ้นไหม



ลองตั้ง password ให้ user test จะเห็นว่ารหัสที่ระบบทำการสุ่มตัวอย่างมาให้ดูนั้นยาก _ ขึ้บยาวขึ้บบีตัวอักษรพิเศษอย่ด้วยทำให้รหัสยากแก่การขาดเดาอย่างมาก

	root@education:~	
	<u>File E</u> dit <u>V</u> iew <u>T</u> erminal Ta <u>b</u> s <u>H</u> elp	
	Enter new password: Weak password: not enough different characters or classes for this length. passwd: Authentication token manipulation error [root@education ~]# passwd test Changing password for user test.	
	A valid password should be a mix of upper and lower case letters, digits, and other characters. You can use a 6 character long password with characters from at least 3 of these 4 classes, or a 5 character long password containing characters from all the classes. An upper case letter that begins the password and a digit that ends it do not count towards the number of character classes used.	
	A passphrase should be of at least 3 words, 8 to 40 characters long and contain enough different characters.	
	Alternatively, if noone else can see your terminal now, you can pick this as your password: "visit:three;accuse".	
	Enter new password:	. t
1.2.1.10	Password aging ใช้ดำสั่ง chage -1 เพื่อเชื่อว่าตั้งค่าไว้ยังไงบ้าง	
		~
		î
File Edit	View Search Terminal Help	
Last pas Password Account Minimum Maximum Number o [root@lo	<pre>sword change : Aug 10, 2018 expires : never inactive : never expires : never number of days between password change : 0 number of days between password change : 99999 f days of warning before password expires : 7 calhost /]#</pre>	,00¢
1/0	ภาพที่4.155 เช็คค่า	
	VSTITUTE OF	

(

- คำสั่ง -M รหัสหมดอายุการใช้งานในเวลาที่กำหนด

[root@localhost /]# chage -M 10 test1			
[root@localhost /]# chage -l test1			
Last password change	:	Aug 10,	2018
Password expires	:	Aug 20,	2018
Password inactive	:	never	
Account expires	:	Jan 11,	1970
Minimum number of days between password change	:	0	
Maximum number of days between password change	:	10	
Number of days of warning before password expires	:	7	
[root@localhost /]#			

ภาพที่4.156 ตั้งค่า Password aging(1)

กำสั่ง chage -w เอาไว้เตือนว่ารหัสจะหมดอายุเมื่อไหร่และให้เตือนก่อนหมดอายุกี่วัน

[root@localhost /]# chage -I 10 test1	
[root@localhost /]# chage -l test1	
Last password change	: Aug 10, 2018
Password expires	: Aug 20, 2018
Password inactive	: Aug 30, 2018
Account expires	: Jan 11, 1970
Minimum number of days between password change	: 0
Maximum number of days between password change	: 10
Number of days of warning before password expin	es : 7

ภาพที่4.157 ตั้งค่า Password aging(2)

4.1.2.1.11 No Password

- ใช้กำสั่งเพื่อเช็กดูว่ามี user คนใหนในระบบไม่มีรหัสบ้าง

root@localhost:/

File Edit V	/iew Search	Terminal Help			
[root@loca bin daemon adm lp sync shutdown halt mail operator games ftp nobody [root@loca	lhost /]# ge lhost /]#	etent shadow	grep '^[^	:]*:.\?:' c	ut -d: -f1

ภาพที4.158 เช็คค่า Password(1) STITUTE

ลองลบรหัสของ user test1 ออกดูว่าจะเป็นยังไง _

root@lo	calhost:/ –	×
File Edit View Search Terminal Help		
[root@localhost /]# passwddelete test] Removing password for user test1.		
passwd: Success [root@localhost /]#		

ภาพที่4.159 ลบ Password

ใช้คำสั่ง้พื่อหา user ที่ไม่มีรหัสอีกทีและจะพบว่ามี user test1 โผล่ขึ้นมา

root@localhost:/

File Edit View Search Terminal Help [root@localhost /]# getent shadow | grep '^[^:]*:.\?:' | cut -d: -f1 bin daemon adm lp sync shutdown halt mail operator games ftp nobody test1 [root@localhost /]#

ภาพที่4.160 เช็คค่า Password(2)

112

4.1.2.1.12 No owner file

TC

ใช้คำสั่งเช็คดูว่าไฟล์เจ้าของเป็นใครมีสิทธิอะไรในไฟล์บ้าง

ภาพที่4.161 เช็คสิทธิของไฟล์(1)

ใช้สิทธิ Root เปลี่ยนเจ้าของไฟล์ให้เป็น nobody:nobody

root@localhost:/home/filetest/desktop File Edit View Search Terminal Help [root@localhost desktop]# chown nobody:nobody public.txt

nníulagin

ภาพที่4.162 ตั้งค่าสิทธิ **STITUTE**

ใช้กำสั่งดูอีกที่จะเห็นว่าเจ้าของไฟล์และกลุ่มเปลี่ยนไปเป็น nobody แล้ว

[root@localhost desktop]# ls -l
total 0
-----. 1 nobody nobody 0 Aug 7 14:18 public.txt
[root@localhost desktop]#

ภาพที่4.163 เช็คสิทธิของไฟล์(2)

ใช้กำสั่ง vi โดยใช้ user test1 เข้าไปดูไฟล์ public.txt

[test1@localhost desktop]\$ vi public.txt

ภาพที่4.164 เข้าไปแก้ไขไฟล์

จะมีข้อความขึ้นมาข้างล่างว่าเราไม่มีสิทธิที่จะทำอะไรกะไฟล์นี้เลย

test1@localhost:/home/filetest/desktop File Edit View Search Terminal Help

"public.txt" [Permission Denied] ภาพที่4.165 ไม่มีสิทธิเข้าถึง 0,0-1

All

ใช้คำสั่ง chm<mark>od 7</mark>77 กับไฟล์ <mark>p</mark>ublic.txt

[root@localhost desktop]# chmod 777 public.txt
[root@localhost desktop]# ls -l
total 0
-rwxrwxrwx. 1 nobody nobody 0 Aug 7 14:18 public.txt
[root@localhost desktop]#

ภาพที่4.166 กำหนดสิทธิ

ลองให้ user test1 เข้าไปดูไฟล์อีกที _

> [test1@localhost desktop]\$ vi public.txt ภาพที่4.167 เข้าไปเช็คสิทธิการเข้าถึง

รอบนี้จะเห็นข้องความที่อยู่ด้านในแล้วและยังสามารถแก้ไขได้อีกด้วยโดยที่ทุกๆ user _ ก็สามารถทำได้เช่นกัน

	test1@localhost:/home/filetest/desktop	_ 🗆 ×
File Edit View Search	Terminal Help	
root access file	ulaă,	
		e 51
~ ~ ~ ~ "public.txt" 1L, 17C	อาพซึ่น 140 สังอาจารเชื่องอานารงไปนั	1,15 All
	111MN4.108 101111111110101011111111	
4.1.2.1.13 Disable root login		
- ใช้คำสั่ง vi เข้าไปแก้ไข	ไฟล์ sshd_config	
	root@localhost:/	- 🙃 ×
File Edit View Search Terminal	Help	

[root@localhost /]# vi /etc/ssh/sshd_config

10

4.1.2.1

ภาพที่4.169 Disable Root login(1)

- เข้าไปเปลี่ยน PermitRootLogin จาก yes เป็น no

root@localhost:/

File Edit View Search Terminal Help # Ciphers and keying

#RekeyLimit default none

Logging
obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INF0

Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

ภาพที่4.170 Disable Root login(2)

- ใช้คำสั่ง :wq เพื่อ save

root@localhost:/

File Edit View Search Terminal Help # Ciphers and keying #RekeyLimit default none

Logging
obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INF0

Authentication:

#LoginGraceTime 2m
#PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

ภา<mark>พที่4.171</mark> Disable Roo<mark>t logi</mark>n(3)

จากนั้น resta<mark>rt</mark>

root@localhost:~

File Edit View Search Terminal Help
[root@localhost ~]# /etc/init.d/sshd restart

ภาพที่4.172 Restart sshd

4.1.2.1.14 User UID not set to 0

- ใช้คำสั่งเพื่อเช็คว่ามี user คนใหนในระบบมี UID 0 ใหมถ้ามีจะต้องเปลี่ยนให้เป็น

UID อื่น

(

oracle@localhost:/ _ □
File Edit View Search Terminal Help
[root@localhost /]# awk -F: '/\/home/ {printf "%s:%s\n",\$1,\$3}' /etc/passwd
oracle:1000
test1:1001
test2:1002
[root@localhost /]#

n f u l a ă j n s

ภาพที่4.173 เช็ค UID(1)

- ใช้คำสั่ง usermod เพื่อเปลี่ยน UID ของ user ให้เป็น UID อื่น

[root@localhost /]# usermod -u 2000 test1

ภาพที่4.174 ลองเปลี่ยน UID

- เห็นได้ว่า UID ของ user test1 เปลี่ยนแล้ว

[root@localhost /]# awk -F: '/\home/ {printf "%s:%s\n",\$1,\$3}' /etc/passwd
oracle:1000
test1:2000
test2:1002

ภาพที่4.175 เช็ค UID(2)

4.1.2.1.15 Secure OpenSSH Server

4.1.2.1.15.1 Configure Idle Timeout Interval

เพื่อหลีกเลี่ยงการเกิดSSH Session เราจึงต้อง set timeout เพื่อไม่ให้มี SSH ที่ไม่ได้ใช้งานแล้วค้างไว้

- ใช้คำสั่ง vi เข้าไปแก้ไขไฟล์ที่ /etc/ssh/sshd_config

[root@localhost /]# vi /etc/ssh/sshd_config

ภาพที่4.176 แก้ไขไฟล์

เข้าไปแก้ #ClientAliveInterval 0 และ #ClientAliveCountMax 3

#AllowAgentForwarding yes #GateWayPorts no X11Forwarding yes #X11DisplayOffset 10 #X11UseLocalhost yes #PermitTTY yes #PrintLastLog yes #TCPKeepAlive yes #UseLogin no UsePrivilegeSeparation sandbox #PermitUserEnvironment no #Compression delayed #ClientAliveInterval 0 #ShowPatchLevel no #UseDNS yes #PidFile /var/run/sshd.pid #MaxStartups 10:30:100 #PermitTunnel no @ChrootDirectory none

Default for new installations.

ภาพที่4.177 ตั้งค่า ClientAlive(1)

แก้เป็น #ClientAliveInterval 360 และ #ClientAliveCountMax 0

#AllowAgentForwarding yes #AllowTcpForwarding yes #GatewayPorts no X1IForwarding yes #X11DisplayOffset 10 #X11UseLocalhost yes #PermitTTY yes #PrintLastLog yes #PrintLastLog yes #TCPKeepAlive yes #UseLogin no UsePrivilegeSeparation sandbox #PermitUserEnvironment no #Compression delayed #ClientAliveInterval 360 #Cli

Default for new installations.

ภาพที่4.178 ตั้งค่า ClientAlive(2)

4.1.2.1.15.2 Disable Empty Password

เข้าไปเปลี่ยน PermitEmptyPasswords จาก yes เป็น no

To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
PasswordAuthentication yes

ภาพที่4.179 ตั้งค่า Empty password

4.1.2.1.15.3 Limit Users'SSH Access

SSH ใช้ Portocal ได้ทั้ง 1 และ 2 เพื่อความปลอดภัยให้ปิด Protocal 1 เพราะว่า Protocal นั้นเก่ากว่า และปลอดภัยน้อยกว่ามากจึงจำเป็นต้องเปลี่ยนให้ใช้แค่ Protocal ที่ 2

เปลี่ยน #Protocal ให้เหลือแค่ 2

The default requires explicit activation of protocol 1
#Protocol 2, 1

ภาพที่4.180 ตั้งค่าการใช้ Protocol(1)

จากนั้นลบ # แล้วใช้กำสั่ง :wq เพื่อ save แล้วทำการ restart ด้วยกำสั่ง service sshd

restart

The default requires explicit activation of protocol 1
Protocol 2

ภาพที่4.181 ตั้งค่าการใช้ Protocol(2)

4.1.2.1.16 Audit

ใช้คำ<mark>สั่</mark>งเพื่อเ<mark>ปิดใช้</mark>งาน <mark>a</mark>uditd

[root@localhost /]# chkconfig auditd on Note: Forwarding request to 'systemctl enable auditd.service'.

<mark>ภาพที่4.182 Au</mark>dit Set<mark>ting(</mark>1)

ใช้คำสั่ง Vi เข้าไปแก้ไขไฟล์

[root@localhost /]# vi /etc/audit/auditd.conf ภาพที่4.183 Audit Setting(2) เข้ามาแก้ไข flush , max_log_file และ freq

This file controls the configuration of the audit daemon
#

```
local_events = yes
write_logs = yes
log_file = /var/log/audit/audit.log
log_group = root
log_format = RAW
flush = INCREMENTAL_ASYNC
freq = 50
max_log_file = 8
num_logs = 5
priority_boost = 4
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
verify_email = yes
```

ภาพที4.184 Audit Setting(3)

แก้ไข tcp_listen_port

```
dispatcher = /sbin/audispd
name format = NONE
##name = mydomain
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
verify_email = yes
action mail acct = root
admin space left = 50
admin space left action = SUSPEND
disk full action = SUSPEND
disk error action = SUSPEND
use libwrap = yes
##tcp listen port = 60
tcp_listen queue = 5
tcp max per addr = 1
##tcp_client_ports = 1024-65535
tcp_client_max_idle = 0
enable krb5 = no
krb5 principal = auditd
##krb5 key file = /etc/audit/audit.key
distribute network = no
```

ภาพที4.185 Audit Setting(4)

- แก้ใบ flush = INCREMENTAL_ASYNC เป็น INCREMENTAL max_log_file = 8

เป็น 6 และ freq = 50 เป็น 20

```
log file = /var/log/audit/audit.log
\log \text{group} = \text{root}
log format = RAW
flush = INCREMENTAL
freq =20
max log file = 6
num logs = 5
priority_boost = 4
disp_qos = lossy
dispatcher = /sbin/audispd
name format = NONE
##name = mydomain
max log file action = ROTATE
space left = 75
space left action = SYSLOG
verify email = yes
action mail acct = root
admin space left = 50
admin space left action = SUSPEND
disk_full_action = SUSPEND
disk_error action = SUSPEND
```

ภาพที4.186 Audit Setting(5)

แก้ไข tcp_listen_port = 60 เป็น ไม่มี

```
disp gos = lossy
dispatcher = /sbin/audispd
name format = NONE
##name = mydomain
max log file action = ROTATE
space left = 75
space left action = SYSLOG
verify email = yes
action mail acct = root
admin space left = 50
admin space left action = SUSPEND
disk full action = SUSPEND
disk_error_action = SUSPEND
use \overline{libwrap} = yes
##tcp listen port =
tcp listen queue = 5
tcp_max_per_addr = 1
##tcp_client_ports = 1024-65535
tcp client max idle = 0
enable_krb5 = no
krb5 principal = auditd
#krb5 key file = /etc/audit/audit.key
```

ภาพที4.187 Audit Setting(6)

4.1.2.1.17 Encryption

- ใช้คำสั่ง yum install gnupg เพื่อทำการลง package ที่จะนำมาใช้งาน

[root@localhost ~]# yum install gnupg		
Loaded plugins: fastestmirror, langpacks		
base	3.6 kB	00:00
extras	3.4 kB	00:00
updates	3.4 kB	00:00
updates/7/x86_64/primary_db	5.2 MB	00:12
Loading mirror speeds from cached hostfile		
* base: mirror2.totbb.net		
<pre>* extras: mirror2.totbb.net</pre>		
* updates: mirror2.totbb.net		
Resolving Dependencies		
> Running transaction check		
> Package gnupg2.x86_64 0:2.0.22-4.el7 will	be updated	
> Package gnupg2.x86_64 0:2.0.22-5.el7_5 will	ll be an update	
> Finished Dependency Resolution		

Dependencies Resolved

Package	Arch	Version	Repository	Size
Updating: gnupg2	×86_64	2.0.22-5.el7_5	updates	1.5 M

ภาพที่4.188 yum install

ใช้คำสั่ง gpg -c ~/Desktop/test.txt เพื่อทำการสร้างไฟล์ gpg ขึ้นมาจากไฟล์ test.txt

```
[root@localhost /]# gpg -c ~/Desktop/test.txt
gpg: directory `/root/.gnupg' created
gpg: new configuration file `/root/.gnupg/gpg.conf' created
gpg: WARNING: options in `/root/.gnupg/gpg.conf' are not yet active during this
run
gpg: keyping `/root/ gpupg/pubring gpg' created
```

gpg: keyring `/root/.gnupg/pubring.gpg' created

ภาพที่4.189 สร้างไฟล์

ใช้คำ<mark>สั่ง</mark> ls ที<mark>่ Des</mark>ktop เ<mark>พื่อดูไฟล์ที่เราสร้างไว้</mark>

```
[root@localhost /]# ls -l ~/Desktop
total 4
-rw-r--r--. 1 root root 0 Aug 30 10:48 test.txt
-rw-r--r--. 1 root root 47 Aug 30 10:50 test.txt.gpg
[root@localhost /]#
```

ภาพที่4.190 เช็คไฟล์

- ใช้คำสั่ง gpg –version เพื่อเช็คว่าไฟล์ที่เรา Encrypt ไปสามารถ Decrypt ได้ด้วย

Cipher ใดได้บ้าง

[root@localhost /]# gpg --version
gpg (GnuPG) 2.0.22
libgcrypt 1.5.3
Copyright (C) 2013 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licens€
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.</pre>

Home: ~/.gnupg Supported algorithms: Pubkey: RSA, ?, ?, ELG, DSA Cipher: IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH, CAMELLIA128, CAMELLIA192, CAMELLIA256 Hash: MD5, SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224 Compression: Uncompressed, ZIP, ZLIB, BZIP2

ภาพที่4.191 เช็ควิธีการ Decrypt

ใช้คำสั่ง vi เพื่อเข้าไปดูไฟล์ test.txt

[root@localhost Desktop]# vi test.txt ภาพที่4.192 เช็กไฟล์

ข้อความในไฟล์ test.txt

Hello ~

ภ<mark>า</mark>พที่4.193 <mark>ดูข้อ</mark>ความ<mark>ในไฟ</mark>ล์

ใช้คำสั่ง cat คพื่อดูข้อกวามที่อยู่ในไฟล์

-- INSERT --

[root@localhost Desktop]# cat ~/Desktop/test.txt Hello

ภาพที่4.194 เรียกดูข้อความ
- ใช้คำสั่ง rm เพื่อลบไฟล์ test.txt ออก

```
[root@localhost /]# rm ~/Desktop/test.txt
ภาพที่4.195 ทำการถบไฟล์
```

ใช้กำสั่ง cat เพื่อดูไฟล์ test.txt.gpg ที่ได้ทำการ Encrypt ไว้จะเห็นได้ว่าข้อความจะนั้น
 จะไม่แสดงออกมาให้เห็นแต่จะออกมาในรูปแบบข้อความที่ถูกเข้ารหัสเอาไว้แล้ว

ภาพที่4.196 เรียกดูไฟล์ที่ทำการ Encrypt ไว้

ใช้คำสั่งเพื่อ Decrypt ไฟล์ gpg แต่เราจำต้องรู้รหัสที่ถูกตั้งไว้ตอน Encrypt ถึงจะ

สามารถ Decrypt ไฟล์ออกมาได้

```
[root@localhost /]# gpg ~/Desktop/test.txt.gpg
gpg: CAST5 encrypted data
gpg: encrypted with 1 passphrase
gpg: WARNING: message was not integrity protected
```

ภาพที่4.197 ทำการ Decrypt ไฟล์

การ Encrrypt ไฟล์หลายไฟล์ด้วย zip

[root@localhost Desktop]# zip --password oracle newzip.zip new.txt new2.txt new3
.txt
 adding: new.txt (stored 0%)

adding: new2.txt (stored 0%) adding: new2.txt (stored 0%) adding: new3.txt (stored_0%)

ภาพที่4.198 zip ไฟล์

ใช้กำสั่ง Is เพื<mark>่อดูไ</mark>ฟล์ที่ได้ทำ<mark>ก</mark>าร z<mark>ip ไว้</mark>

```
[root@localhost Desktop]# ls -l
total 8
-rw-r--r--. 1 root root 0 Aug 30 12:03 a.out
-rw-r--r--. 1 root root 0 Aug 30 13:45 new2.txt
-rw-r--r--. 1 root root 0 Aug 30 13:45 new3.txt
-rw-r--r--. 1 root root 0 Aug 30 11:27 new.txt
-rw-r--r--. 1 root root 536 Aug 30 13:53 newzip.zip
-rw-r--r--. 1 root root 48 Aug 30 11:03 test.txt.gpg
```

ภาพที่4.199 ดูไฟล์

ใช้กำสั่ง unzip เพื่อ Decrypt โดยการใส่รหัสแตกไฟล์ที่ได้ทำการ zip เอาไว้

[root@localhost Desktop]# unzip newzip.zip Archive: newzip.zip [newzip.zip] new.txt password: replace new.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: y extracting: new1xt replace new2.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: y extracting: new2.txt replace new3.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: y extracting: new3.txt

ภาพที4.200 ทำการ Decrypt ไฟล์

4.1.2.1.18 Disable USB/firewire/thunderbolt devices

ใช้คำสั่ง echo เข้าไปในไฟล์เพื่อ blacklist fireware-core และ blacklist thunderbolt

[root@localhost ~]# echo 'install usb-storage /bin/true' >> /etc/modprobe.d/disable-usb-storage.conf [root@localhost ~]# echo "blacklist firewire-core" >> /etc/modprobe.d/firewire.conf [root@localhost ~]# echo "blacklist thunderbolt" >> /etc/modprobe.d/thunderbolt.conf

ภาพที่4.201 ทำการ blacklist

4.1.2.1.19 Secure Apache

- ใช้คำสั่ง cd เข้าไปที่ conf

[root@localhost /]# cd /etc/httpd/conf ภาพที่4.202 เข้า path conf

ใช้คำสั่ง vi เข้าไปแก้ไขไฟล์ httpd.conf

[root@localhost conf]# vi httpd.conf

ภาพที่4.203 แก้ไขไฟล์

เพิ่มคำสั่งเข้า<mark>ไปใ</mark>นไฟล์ httpd<mark>.c</mark>onf

ServerTokens Prod ServerSignature Off TraceEnable Off Options all -Indexes Header always unset X-Powered-By

ภาพที่4.204 เพิ่มคำสั่ง ANSTITUTE OF - ใช้คำสั่ง systemetl restart httpd.service เพื่อให้ค่าที่เราใส่เข้าไปทำงาน

[root@localhost conf]# systemctl restart httpd.service ภาพที่4.205 Restart Service

4.1.2.1.20 Stop FTP

- ใช้คำสั่งเช็ค status ของ vsftpd

[root@localhost Desktop]# /sbin/service vsftpd status Redirecting to /bin/systemctl status vsftpd.service • vsftpd.service - Vsftpd ftp daemon Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; disabled; vendor pres et: disabled) Active: active (running) since Thu 2018-08-30 16:08:07 ICT; 12min ago Process: 5756 ExecStart=/usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf (code=exited, status=0/SUCCESS) Main PID: 5766 (vsftpd) CGroup: /system.slice/vsftpd.service L5760 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf

Aug 30 16:08:07 localhost.localdomain systemd[1]: Starting Vsftpd ftp daemon... Aug 30 16:08:07 localhost.localdomain systemd[1]: Started Vsftpd ftp daemon. Hint: Some lines were ellipsized, use -l to show in full.

ภาพที4.206 Check Status

ใช้คำสั่ง vsftpd stop เพื่อหยุดหารทำงานของ FTP เพื่อเป็นการปิดสิ่งที่เราไม่ได้ใช้งาน

[root@localhost Desktop]# /sbin/service vsftpd stop Redirecting to /bin/systemctl stop vsftpd.service

ภาพที4.207 Stop service

4.1.2.1.21 Stop unused services

- ใช้กำสั่ง ps ax เพื่อทำการเช็ก Service ที่ทำงานอยู่บนเกรื่อง

840	1	5	0:00 /spin/anclient -a -q -st /usr/libexec/nm-ancp-nelp	31
627	?	S<	0:00 [kworker/0:2H]	
789	?	S	0:00 [kworker/u256:2]	
994	?	S	0:05 [kworker/0:1]	
000	?	S	0:00 [kworker/u256:1]	
365	?	S	0:00 [kworker/0:0]	
397	?	S<	0:00 [kworker/1:1H]	
414	?	S	0:00 [kworker/1:0]	
458	?	R	0:00 [kworker/1:1]	
565	?	S<	0:00 [kworker/1:2H]	
583	?	S	0:00 [kworker/0:2]	
594	?	S	0:00 [kworker/1:2]	
605	?	S	0:00 pickup -l -t unix -u	
650	?	Ss	0:00 /usr/sbin/httpd -DFOREGROUND	
654	?	S	0:00 /usr/libexec/nss pcache 425986 off /etc/httpd/alias	3
655	?	S	0:00 /usr/sbin/httpd -DFOREGROUND	
656	?	S	0:00 /usr/sbin/httpd -DFOREGROUND	
657	?	S	0:00 /usr/sbin/httpd -DFOREGROUND	
658	?	S	0:00 /usr/sbin/httpd -DFOREGROUND	
659	?	S	0:00 /usr/sbin/httpd -DFOREGROUND	
682	?	S<	0:00 [kworker/1:0H]	
691	?	S	0:00 sleep 60	
693	pts/0	R+	0:00 ps ax	

ภาพที่4.208 ดู Service ต่างๆ

- ใช้คำสั่ง ps ax | grep httpd เพื่อทำการดู Service ที่ทำงานอยู่และชื่อตรงกับที่เรา

กำหนดทั้งหมดออกมา

[root@localhost	Desktop]# ps	s ax grep httpd
6650 ?	Ss	0:00	/usr/sbin/httpd -DF0REGROUND
6654 ?	S	0:00	/usr/libexec/nss_pcache 425986 off /etc/httpd/alias
6655 ?	S	0:00	/usr/sbin/ httpd -DFOREGROUND
6656 ?	S	0:00	/usr/sbin/ <mark>httpd</mark> -DFOREGROUND
6657 ?	S	0:00	/usr/sbin/ <mark>httpd</mark> -DFOREGROUND
6658 ?	S	0:00	/usr/sbin/ <mark>httpd</mark> -DFOREGROUND
6659 ?	S	0:00	/usr/sbin/httpd -DFOREGROUND
6998 pts/0	R+	0:00	grepcolor=auto httpd
			ภาพที่4.209 เช็ค httpd service

ใช้คำสั่ง systemetl stop httpd เพื่อเป็นการหยุดการทำงานของ httpd

[root@localhost Desktop]# systemctl stop httpd ภาพที่4.210 Stop httpd service

ใช้กำสั่ง ps ax และ ps ax | grep httpd เพื่อทำการเช็คว่า Service httpd ที่ปิดไปยัง

ทำงานอยู่อีกไหม

16

	2840	?	S	0:00	/sbin/dhclient	-d -q	-sf
	4627	?	S<	0:00	[kworker/0:2H]		
	5789	?	S	0:00	[kworker/u256:2]	
	5994	?	S	0:05	[kworker/0:1]		
	6000	?	S	0:00	[kworker/u256:1]	
	6458	?	S	0:00	[kworker/1:1]		
	6565	?	S<	0:00	[kworker/1:2H]		
	6583	?	R	0:02	[kworker/0:2]		
	6605	?	S	0:00	pickup -l -t un	ix -u	
	6682	?	S<	0:00	[kworker/1:0H]		
	6751	?	S	0:00	[kworker/1:0]		
	6889	?	S	0:00	[kworker/1:2]		
	6991	?	S	0:00	[kworker/u256:0]	
	7006	?	S	0:00	sleep 60		
	7026	pts/0	R+	0:00	ps ax		
[root@localh <mark>ost</mark>			Deskto	p] <mark>#</mark> ps	s ax grep http	d	
	7028	pts/0	R+	0:00	grepcolor=au	to ht1	t pd
[root@localh <mark>ost</mark>		Deskto	p]#				
			ภาพที่	4.2 <mark>1</mark> 1 1	ชิ้ค Service		

4.1.2.1.22 Physical Security

(**D**-

4.1.2.1.22.1 แนวทางการป้องกันความปลอดภัยทางกายภาพของระบบ

- แบ่งแยกพื้นที่ควบคุมความปลอดภัยอย่างชัดเจน เช่น การแยกห้องที่เก็บเครื่องเซิร์ฟเวอร์และ อนุญาตให้เฉพาะผู้ดูแลระบบเท่านั้นที่เข้าถึงได้
- ใช้ระบบป้องกันและตรวจสอบการเข้าออกพื้นที่ควบคุมความปลอดภัย เช่น การใช้ key card ที่ สามารถบันทึกได้ว่าใครเข้าออกได้ หรือการใช้กล้องวิดีโอ เป็นต้น
- เก็บรักษาระบบและอุปกรณ์ต่างๆ เช่น backup tape, เซิร์ฟเวอร์ ในพื้นที่ควบคุมความปลอดภัย และอนุญาตให้เข้าถึงได้เฉพาะผู้ดูแลระบบเท่านั้น
- 4. ใช้เครื่องจ่ายกำลังไฟฟ้าสำรองหรือ UPS เพื่อให้ระบบสามารถใช้ไฟฟ้าได้อย่างต่อเนื่อง
- วางแผนสำหรับการกู้ระบบคืนเมื่อมีเหตุการณ์เลวร้ายเกิดขึ้น
- 6. ตรวจสอบข้อมูลของเจ้าหน้าที่จากภายนอกที่เข้ามาให้กำปรึกษาหรือปฏิบัติงานภายในพื้นที่ กวบคุมความปลอดภัย ถ้าหากเจ้าหน้าที่ผู้นั้นต้องการใช้สิทธิของ root ในการทำงานกับระบบ ผู้ดูแลระบบจะต้องทำการ login ให้ด้วยตนเอง หลังจากนั้นต้องกอยติดตามดูว่าผู้นั้นทำอะไร กับระบบบ้าง และเมื่อเสร็จภารกิจแล้วให้ทำการเปลี่ยนรหัสผ่านของ root ทันที

 4.1.2.1.22.2 แนวทางการป้องกันความปลอดภัยทางกายภาพภายในเครื่องคอมพิวเตอร์
 1. การล็อคเครื่องคอมพิวเตอร์ (Computer Lock) เช่น การใช้กุญแจล็อคที่ตัวเครื่อง เพื่อช่วยในการ ป้องกันเครื่องและอุปกรณ์ภายในเครื่องจากการถูกลักขโมย หรือทำการเปิดเครื่องเพื่อสร้าง ความเสียหายต่อฮาร์ดแวร์ภายในได้ และเป็นการป้องกันการรีบูตเครื่องด้วยแผ่นดิสก์หรือ ฮาร์ดแวร์อื่นๆด้วย

 การรักษาความปลอดภัยใน BIOS (BIOS Security) เนื่องจาก BIOS มีความสำคัญต่อโปรแกรม ที่ใช้บูตเข้าระบบ เช่น LILO ดังนั้นจึงควรปรับแต่งค่าใน BIOS เพื่อป้องกันผู้โจมตีทำการรีบูต เครื่อง มีวิธีการโดยสรุปดังนี้

 2.1 ปรับแต่งให้ป้อนรหัสผ่านตอนที่บูตเครื่อง ซึ่งอาจจะ ไม่สามารถป้องกันได้ 100% เนื่องจากผู้โจมตีสามารถทำการรีเซ็ตที่ BIOS ได้ แต่ก็เป็นการชะถอเวลาของผู้โจมตี
 2.2 ปรับแต่งให้เครื่องไม่สามารถใช้แผ่นดิสก์ในการบูตเครื่อง 2.3 ปรับแต่งให้ป้อนรหัสผ่านทุกครั้งก่อนที่จะทำการปรับแต่ง BIOS หมายเหตุ การตั้งรหัสผ่านตอนบูตมีข้อเสียคือ ถ้าเกิดเหตุขัดข้องบางประการ เช่น ไฟฟ้าดับเป็นเวลานาน ส่งผลให้ต้องมีการบูตใหม่ ผู้ดูแลระบบเองจะต้องอยู่ใกล้เครื่อง เพื่อที่จะป้อนรหัสผ่าน มิฉะนั้นระบบจะไม่สามารถทำงานต่อไปได้

129

- 3. การรักษาความปลอดภัยที่ Boot Loader (Boot Loader Security) โปรแกรม Boot Loader ของ Linux สามารถปรับแต่งให้ป้อนรหัสผ่านตอนบูตได้ ยกตัวอย่างเช่น LILO สามารถแก้ไฟล์ /etc/lilo.conf โดยเพิ่มส่วนของ password และ restricted ซึ่ง password นั้นเป็นการป้องกัน image (เป็นไฟล์ของ kernel ที่ใช้ในการบูต) ส่วน restricted เป็นการป้องกัน image โดยให้ป้อนรหัสผ่าน เมื่อมีการเพิ่ม ก่าพารามิเตอร์ที่ LILO prompt (เช่น single) นอกจากนี้ยังมี prompt ที่จะใช้ระบุว่าทุกครั้งที่เปิด เครื่องค้องมีการเข้าสู่ boot prompt ก่อน และ timeout นั้นใช้บอกเวลาในหน่วยวินาทีที่ใช้รอรับ อินพุตจากกีย์บอร์คว่าจะเลือกบูตไฟล์ image ใด และการปรับแต่งให้ป้อนรหัสผ่านยังคงไม่สามารถ ป้องกันการบูตจากแผ่นดิสก์ และการ mount root partition ดังนั้นควรที่จะใช้ BIOS Security ควบกู่ ไปกับ Boot Loader Security เช่น การปรับแต่งให้ไม่สามารถบูตจากแผ่นดิสก์ และให้ป้อน รหัสผ่านก่อนเข้าใช้งาน BIOS
- การถือคหน้าจอมอนิเตอร์ (Screen Lock) ในขณะที่ผู้ดูแถระบบใช้งานเครื่องค้างอยู่ และต้องหยุด การใช้งานดังกล่าวก่อนชั่วคราว แต่ยังไม่ต้องการที่จะ Logout ออกจากระบบ ก็ใช้คำสั่งในการถือค หน้าจอเพื่อป้องกันผู้อื่นที่ไม่รู้รหัสผ่านของผู้ดูแถระบบเข้ามาใช้งานเทอร์มินัลที่ทำงานค้างไว้ได้ ตัวอย่างโปรแกรมดังกล่าวเช่น xlock สำหรับ X-windows และ vlock สำหรับ Text-mode
 - 5. การตรวจสอบการเปลี่ยนแปลงของความปลอดภัยทางกายภาพ (Detecting Physical Security Compromises) วิธีที่ง่ายที่สุดในการตรวจสอบว่าเครื่องถูกผู้บุกรุกแก้ไขการทำงานใดๆ ภายใน เครื่องหรือไม่ สามารถทำได้โดยการตรวจสอบจากล็อกไฟล์ที่สร้างขึ้นจากโปรแกรม syslog daemon ที่ถูกติดตั้งใน linux ซึ่งจะทำการเก็บล็อกไฟล์ไว้ ภายในล็อกไฟล์ดังกล่าวจะเก็บข้อมูล สถานะการทำงานของเครื่องตั้งแต่เริ่มบูตเครื่อง อย่างไรก็ตาม ถ้าผู้บุกรุกทราบว่าลือกไฟล์เก็บไว้ที่ ใด ก็สามารถที่จะเข้าไปแก้ไขหรือสร้างล็อกไฟล์ได้ ดังนั้นมีอีกทางเลือกหนึ่งคือการตั้งเซิร์ฟเวอร์ที่ ใช้เก็บล็อกไฟล์ (Log Server) โดย syslog daemon สามารถปรับแต่งให้ส่งข้อมูลลีอกไฟล์ไปเก็บไว้ ยังเซิร์ฟเวอร์ที่ใช้เก็บล็อกไฟล์ได้ แต่ข้อมูลนั้นยังไม่ได้เข้ารหัส ผู้บุกรุกสามารถดูข้อมูลดังกล่าว

ขณะที่ทำการส่งได้ เพราะฉะนั้นเซิร์ฟเวอร์ที่ใช้เก็บถ็อกไฟถ์ควรตั้งอยู่ภายในองค์กร ข้อมูลของถ็อกไฟล์โดยทั่วไปที่ควรตรวจสอบ

- 5.2 ล็อกไฟล์ที่ไม่สมบูรณ์หรือที่มีข้อมูลขาดหายไป
- 5.3 ล็อกไฟล์ที่มี timestamp ผิดปกติ
- 5.4 ลีอกไฟล์ที่มี permission หรือ เจ้าของลีอกไฟล์ผิดจากที่ควรเป็น เช่นลีอกไฟล์ของ ระบบแต่เจ้าของนั้นเป็น user
- 5.5 ข้อมูลของการรีบูตเครื่องหรือรีสตาร์ท service
- 5.6 การใช้กำสั่ง su หรือการ login เข้ามาจากต้นทางที่ผิดปกติ

4.2 ผลการวิเคราะห์ข้อมูล

(

ตามที่ได้ทำการศึกษา Hardening โดยมีวัตถุประสงค์ให้ระบบมีความปลอดภัยและมี ความน่าเชื่อถือมากขึ้น ซึ่งในขณะนี้โครงการได้ดำเนินการจนแล้วเสร็จตามวัตถุประสงค์เป็นที่ เรียบร้อยแล้ว โดยสามารถวิเคราะห์ได้จากการทำงานจากผลการทดสอบซึ่งได้ผลดังนี้

4.2.1 สามารถเข้าไปแก้ไขไฟล์ใน Linux ทำให้ user ไม่สามารถตั้งรหัสซ้ำได้อีก
 4.2.2 สามารถเช็ก Log ของการใช้งานใน windows server ได้
 4.2.3 สามารถกำหนดสิทธิการเข้าถึงไฟล์ต่างๆได้
 4.2.4 สามารถ set inbound ของ firewall เพื่อกำหนด port ที่จะเข้ามาได้

สรุปได้ว่าการทำ Hardening มีประ โยชน์จริงทั้งในด้านการเพิ่มความปลอดภัยและลดการใช้ ทรัพยากรเครื่องอีกทั้งยังประห[ู]ยัดค่าใช้จ่ายได้มากเพราะการทำ Hardening ไม่จำเป็นต้องไปซื้อ software และ hardware ม<mark>าเพิ่ม</mark>ในการทำ Hardening อีกด้วย

4.3 วิจารณ์ข้อมูลโดยเปรียบเทียบผลที่ได้รับกับวัตถุประสงค์การจัดทำโครงการ

จากวัตถุประสงค์เพื่อเพิ่มความปลอดภัยและลดการใช้ทรัพยากรในเครื่องรวมถึง การลดค่าใช้ง่ายต่างๆ

จากการที่ทดสอบการทำ Hardening สามารถป้องกันช่องโหว่ต่างๆ ได้ไม่ว่าจะ เป็นการเช็คว่ามี User คนไหนมี UID 0 นอกจาก Root ไหม หรือ ปิดการใช้งาน Service ต่างๆที่ ไม่ได้มีการใช้งานหรือม่จำเป็นต่อระบบออกไปเพื่อไม่ใช่เกิดช่องโหว่และยังลดทรัพยากรการใช้ งานในเครื่องไปได้มากทำให้เครื่องมีประสิทธิภาพในการทำงานสูงขึ้น หรือ การตั้งค่าแจ้งเตือนการ หมดอายุของรหัส User เพื่อให้มาทำการเปลี่ยนใหม่เพื่อเพิ่มความปลอดภัยให้แก่ผู้ใช้งานและระบบ ของเราให้มากยิ่งขึ้นและการทำ Hardening นั้นสามารถนำมาใช้งานในองค์กรต่างๆเพื่อเพิ่มความ ปลอดภัยและความน่าเชื่อถือขององค์กรนั้นมากขึ้น

10

บทที่ 5 บทสรุปและข้อเสนอแนะ

5.1 สรุปผลการดำเนินงาน

จากการที่ได้ศึกษาและทดลองทำการ Hardening เพื่อนำไปเพิ่มความปลอดภัยให้แก่ เครื่องและ Os ของเราและลูกค้าซึ่งได้ผลลัพธ์ดังนี้

5.1.1 สามารถทำการปิด GUI ใน Linux ได้สำเร็จ

5.1.2 สามารถตั้งค่าให้ user ไม่สามารถตั้งรหัสซ้ำกับรหัสเก่าได้

5.1.3 สามารถตั้งค่า NTP ใน Window Server 2016 ใค้สำเร็จ

5.1.4 สามารถปิด Service ต่างๆที่ไม่ได้ใช้งานใน Linux และ Windows Server ได้ สำเร็จ

5.1.5 สามารถเช็คได้ว่าไม่มีผู้ใช้คนใคมีเลข UID = 0

จากผลลัพธ์ สารมารถสรุปได้ว่าการทำ Hardening สามารถตอบสนองความต้องการใน ด้านความน่าเชื่อถือ ความรวดเร็วและความปลอดภัยได้เป็นอย่างดี

5.2 แนวทางการแก้ไขปัญหา

ปัญหาที่พบในระหว่างการศึกษา Hardening ส่วนแรกจะเป็นปัญหาเรื่องการหาข้อมูลและทำความเข้าใจซึ่ง ข้อมูลเกือบทั้งหมดนั้นเป็นภาษาอังกฤษและบางเรื่องข้อมูลก่อนข้างน้อย ส่วนอีกปัญหาคือควยุ่งยากในการ ทำ ไม่ว่าจะเป็นการใช้คำสั่งต่างๆ การแก้ไขไฟล์ หากแก้ไขไม่ถูกค้องอาจจะต้องทำการลงระบบใหม่ ทั้งหมดเลยเนื่องจากไปแก้ไขไฟล์ในระบบแล้วเกิดการผิดพลาดขึ้นซึ่งแนวทางการแก้ปัญหาคือทำการ Snapshot เอาไว้ก่อนจะเข้าไปแก้ไขไฟล์ทุกครั้งเพื่อที่จะสามารถย้อนกลับมาก่อนที่จะเกิดกวามเสียหายขึ้น เนื่องจากการเข้าไปทำการแก้ไขไฟล์ในระบบ

5.3 ข้อเสนอแนะจากการดำเนินงาน

10

5.3.1 ควรมีพื้นฐานในการใช้ระบบปฏิบัติการ Linux ในการใช้คำสั่งต่างๆ
 5.3.2 ในการทำงานควรจะระมัดระวังในการเข้าไปแก้ไขไฟล์ต่างๆควรมีการ
 Snapshot ไว้เสมอก่อนจะลงมือทำ

 5.3.3 ในการทำงานต้องหาข้อมูลเพื่อเตรียมความพร้อมก่อนลงมือทำและวางแผน ในการทำงานเสมอเพราะการแก้ไขบางอย่างอาจจะส่งผลต่อการทำงานขั้นต่อๆ ไป
 5.3.4 การติดต่อประสานงานกันภายในทีม เป็นส่วนสำคัญในการทำงานจริงที่จะส่งผล กระทบที่ดีหรือไม่ดีต่องานที่ได้รับมอบหมาย ซึ่งจะต้องอาศัยความร่วมมือของทุกฝ่าย ที่จะทำให้งานสำเร็จลุล่วงไปได้ด้วยดี

5.3.5 การทำงานที่สามารถตรวจสอบได้ จะทำให้ผู้ปฏิบัติงานสามารถตรวจสอบข้อมูล หรือข้อผิดพลาดที่ได้เกิดขึ้นได้อย่างง่ายดาย และสามารถเข้าไปแก้ไขปัญหาได้ตรงจุด มากที่สุด

5.3.6 ในการทำงานจริง มีความจำเป็นอย่างยิ่งที่จะต้องศึกษาหาความรู้เพิ่มเติมอยู่ ตลอดเวลา ซึ่งความรู้บางอย่างไม่สามารถเรียนรู้ได้จากในห้องเรียน

5.3.7 ความอดทนถือเป็นส่วนสำคัญอีกอย่าง ที่ทำให้การทำงานเป็นไปได้ด้วยดีและ ประสบผลสำเร็จ ซึ่งจะต้องขึ้นอยู่กับรูปแบบของงาน, ระยะเวลาของงานและ ผู้ร่วมงานด้วย

5.3.8 ความรับผิดชอบในหน้าที่ ถือเป็นสิ่งที่ดีอย่างมากที่ได้รับจากการทำงานจริงซึ่ง สามารถนำมาใช้ในการพัฒนาตนเองได้อย่างดีเยี่ยม ทำให้มีความรับผิดชอบมากขึ้น และสามาร<mark>ถตัดสินใจไ</mark>ด้เอง

เอกสารอ้างอิง

[1.] How to Manage User Password Expiration and Aging in Linux Available:https://www.tecmint.com/manage-user-password-expiration-and-aging-in-linux/

[2.] 7 Tools to Encrypt/Decrypt and Password Protect Files in Linux Available:<u>https://www.tecmint.com/linux-password-protect-files-with-encryption/</u>

[3.] 10 Steps to Secure Open SSH

Available:https://blog.devolutions.net/2017/4/10-steps-to-secure-open-ssh

[4.] คอนฟิกลีนุกซ์ Disk Quota Available:<u>https://spalinux.com/2009/03/configure_linux_disk_quota_part_2</u>

[5.] How to prevent users from reusing old passwords in Linux Available:<u>https://www.internetblog.org.uk/post/886/how-to-prevent-users-from-reusing-old-passwords-in-linux/</u>

[6.] 40 Linux Server Hardening Security Tips [2017 edition] Available:https://www.cyberciti.biz/tips/linux-security.html

STITUTE O

รายโลสัว ภาคผนวก

(รายงานประจำสัปดาห์)

VSTITUTE O

Ş

ประวัติผู้จัดทำโครงงาน

ชื่อ – นามสกุล นายพิรษร อัครวุฒิ

วัน เดือน ปีเกิด

9 มกราคม 2540

โรงเรียนสี่พี่น้อง

ประวัติการศึกษา ระดับประถมศึกษา

ระดับมัธยมศึกษา

นโลยั) โรงเรียนเซนต์ดอมินิก

ระดับอุดมศึกษา

คณะเทคโนโลยีสารสนเทศ สาขาเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีไทย-ญี่ปุ่น

ทุนการศึกษา

Training Pre-Cooperative Education โครงการสหกิจฯ บริษัท เอ-โฮสต์ จำกัด ประวัติการฝึกอบรม ผลงานที่ได้รับการตีพิมพ์ - ไม่มี -