การจัดการด้านความปลอดภัยและลดทรัพยากรการใช้งานให้กับระบบ

Management Security Hardening

นาย พิรษร อัครวุฒิ

โครงงานสหกิจศึกษานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

ปริญญาวิทยาศาสตรบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยี ไทย-ญี่ปุ่น

พ.ศ. 2561

การจัดการด้านความปลอดภัยและลดทรัพยากรการใช้งานให้กับระบบ

Management Security Hardening

นาย พิรษร อัครวุฒิ

โครงงานสหกิจศึกษานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรบัณฑิต สาขาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีไทย - ญี่ปุ่น
ปีการศึกษา 2561

คณะกรรมการสอบ

..... ประธานกรรมการสอบ
(อาจารย์ อดิศักดิ์ เสือสมิง)
..... กรรมการสอบ
(ผู้ช่วยศาสตราจารย์ ดร.ประจักษ์ เฉิดโฉม)
..... อาจารย์ที่ปรึกษา
(ผู้ช่วยศาสตราจารย์ ดร.นรังสรรค์ วิไลสกุลยง**)**
..... ประธานสหกิจศึกษาสาขาวิชา
(อาจารย์ สลิลา ชีวกิดาการ)

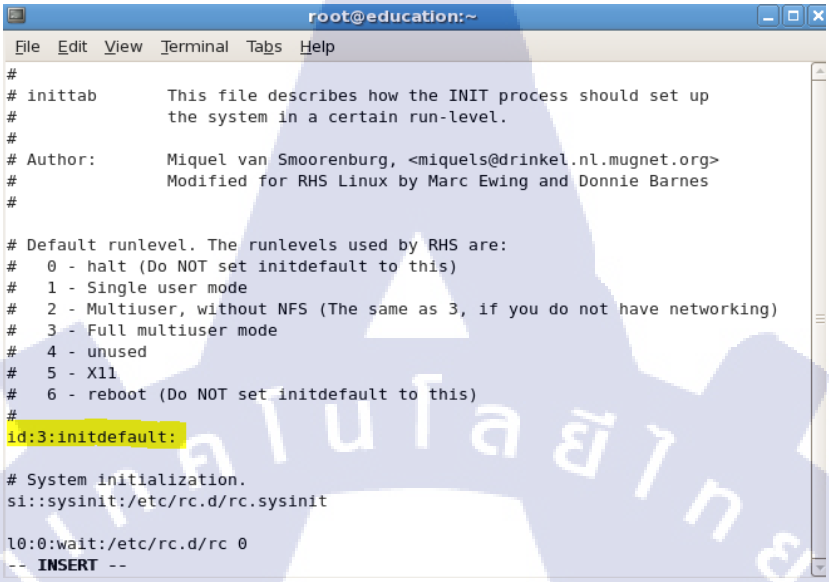
ชื่อโครงงาน	การจัดการด้านความปลอดภัยและลดทรัพยากรการใช้งานให้กับระบบ
ผู้เขียน	นายพิรษร อัครวุฒิ
คณะวิชา	เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ
อาจารย์ที่ปรึกษา	ดร.นรังสรรค์ วิไลสกุลยง
พนักงานที่ปรึกษา	นายภูดิศ ดุพัสกูล
ชื่อบริษัท	บริษัท เอ-โฮสต์ จำกัด
ประเภทธุรกิจ/สินค้า	ให้บริการทางด้าน Hosting Service และ IBM & Oracle Product

บทสรุป

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

จากประสบการณ์ที่ได้จากการไปสหกิจศึกษา ทำให้ได้เรียนรู้เรื่องระบบความปลอดภัยทั้งในด้านของการเข้าถึงและการใช้งาน การที่ได้ทำ Hardening ทำให้เกิดความเข้าใจในวิธีการที่จะเพิ่มประสิทธิภาพในส่วนต่างๆ ของความปลอดภัยของระบบและสามารถใช้คำสั่งต่างๆ ในระบบปฏิบัติการ Linux ได้ อีกทั้งการทำงานร่วมกับผู้อื่นทำให้เกิดความคุ้นชินกับการทำงานในเวลาที่จำกัด การรับผิดชอบต่อหน้าที่การทำงานและสามารถบริหารจัดการเวลาในการทำงานได้ โดยทั้งหมดนี้จะเป็นสิ่งสำคัญต่อชีวิตการทำงานในอนาคต

รูปถ่ายผลงานสหกิจศึกษาที่ได้ดำเนินการ



หน้า Setting ของ Linux เพื่อปิด GUI

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.

กิตติกรรมประกาศ

ในการเข้าไปสหกิจศึกษาที่บริษัท เอ - โฮสต์จำกัดนั้น ได้รับความกรุณาและการดูแลจากพี่ๆ ได้เรียนรู้การทำงานจริงภายในบริษัท ได้รับความมรู้ต่างๆมากมายและได้รับการดูแลใกล้ชิดทั้งการให้คำปรึกษาและช่วยแก้ไขปัญหาต่างๆที่เกิดขึ้น ทำให้การปฏิบัติงานครั้งนี้สำเร็จลุล่วงไปได้ด้วยดี

ขอขอบคุณ คุณภูดิศ ดุพัสกูล คุณเนตรปวีร์ ศิริวิชญ์วัฒนา คุณชัยยุทธ ศุภกิจรุ่งเจริญ และขอบคุณพี่ๆทีม SMS ที่สละเวลามาคอยช่วยเหลือแก้ปัญหาและเป็นที่ปรึกษาเรื่องต่างๆในช่วงสหกิจศึกษาและพี่ๆในบริษัททุกท่านที่ได้ให้ความช่วยเหลือทุกครั้งที่เกิดข้อสงสัยต่างๆ รวมถึงการแนะนำเทคนิคในการทำงานต่างๆ ซึ่งสามารถใช้ทำงานได้จริง ขอขอบพระคุณทุกท่านไว้ ณ โอกาสนี้ด้วย

นายพิรษร อัครวุฒิ

ผู้จัดทำ

สารบัญ

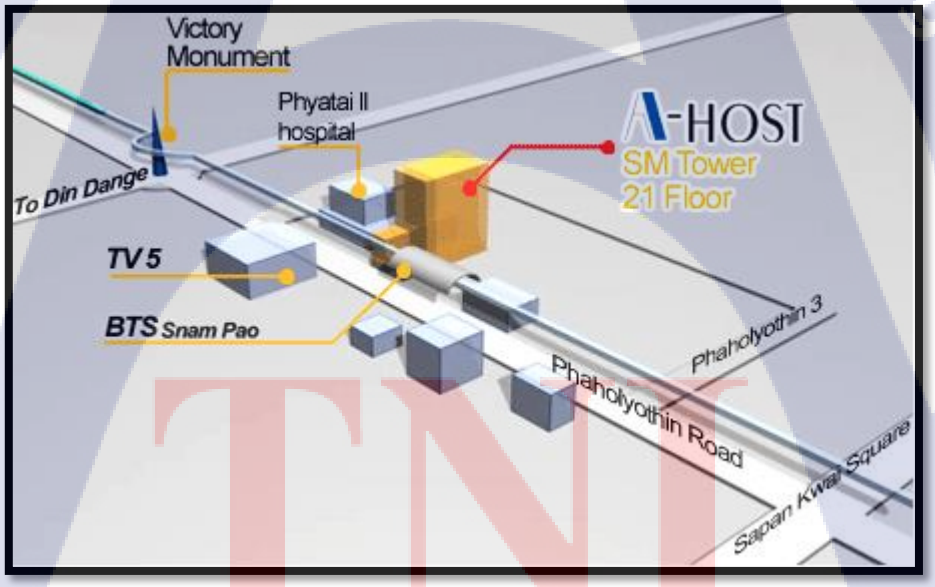
สารบัญรูป

รูป **หน้า**

บทที่ 1
บทนำ

1.1 ชื่อและสถานที่ตั้งของสถานประกอบการ

ชื่อสถานประกอบการ	:	บริษัท เอ-โฮสต์ 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 ในฐานะหนึ่งบริษัทในเครือของบริษัทซิสเต็มส์คอร์ปอเรชั่น (มหาชน) จำกัดและเป็นผู้เชี่ยวชาญด้านการบริการจัดวางระบบสารสนเทศ (Information Technology : IT) และบริการเสริมต่างๆสำหรับลูกค้าตั้งแต่ธุรกิจขนาดย่อมไปจนถึงขนาดกลางธุรกิจหลักของบริษัทเอ-โฮสต์คือการให้บริการโฮสติ้ง (Hosting) ซึ่งเป็นการเปิดเครื่องคอมพิวเตอร์แม่ข่ายในการให้เช่าพื้นที่เพื่อวางระบบและบริการระบบสารสนเทศด้วยผลิตภัณฑ์ของออราเคิล (Oracle) เป็นซอฟต์แวร์สำหรับการวางแผนบริหารทรัพยากรของระดับแนวหน้าของโลก

เอ-โฮสต์ถือกำเนิดขึ้นจากกลุ่มผู้เชี่ยวชาญด้านสารสนเทศท่ามกลางภาวะเศรษฐกิจตกต่ำทั่วภูมิภาคเอเชีย แต่เอ-โฮสต์ก็สามารถเติบโตอย่างรวดเร็วและมั่นคงตั้งแต่แรกก่อตั้งด้วยจุดแข็งในฐานะผู้บุกเบิกธุรกิจโฮสติงเซอร์วิสพร้อมทั้งนำธุรกิจแนวใหม่อย่างการให้บริการระบบโปรแกรมประยุกต์หรือ ASP (Application Services Provider) เข้ามาให้บริการเป็นรายแรกในเมืองไทยอีกทั้งยังถือเป็นผู้ให้บริการรายแรกนอกประเทศสหรัฐอเมริกาด้วย

ในฐานะผู้นำในอุตสาหกรรมนี้เป็นเวลามากกว่า 10 ปีเอ-โฮสต์ได้เสริมสร้างความแข็งแกร่งทางธุรกิจด้วยบริการที่มีความโดดเด่นและรวบรวมเอาทรัพยากรบุคคลซึ่งได้สั่งสมประสบการณ์และความชำนาญไว้อย่างพร้อมเพรียงส่งผลให้ศูนย์ข้อมูลของเอ-โฮสต์ในปัจจุบันมีความสมบูรณ์ด้วยกลุ่มเซิร์ฟเวอร์ (Server) ที่เชื่อมต่อกันในลักษณะการจัดกลุ่ม (Clustering) ซึ่งเปี่ยมสมรรถนะสามารถให้บริการแก่ผู้ใช้จำนวนมากได้ในเวลาเดียวกัน

นอกจากนี้เอ-โฮสต์ยังติดตั้งระบบรักษาความปลอดภัยระบบสำรองข้อมูลและระบบบริหารจัดการรวมถึงอุปกรณ์ต่างๆอย่างครบครันเพื่อให้เอ-โฮสต์สามารถตอบสนองต่อระดับความต้องการในระดับสูงสุดที่ลูกค้าคาดหวังได้ตลอดจนเป็นการสร้างความมั่นใจให้แก่ลูกค้าที่ใช้บริการโฮสติงและแอพพลิเคชันต่างๆของเอ-โฮสต์ว่าจะได้รับทั้งประสิทธิภาพและความปลอดภัยอย่างครบครันธุรกิจการให้บริการระบบโปรแกรมประยุกต์ในรูปแบบ ASP เอ-โฮสต์ไม่เพียงแต่ให้บริการด้านโปรแกรมประยุกต์ด้านการดำเนินธุรกิจทางอิเล็กทรอนิกส์ระดับโลกของออราเคิลพร้อมโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศเท่านั้นแต่ยังมีบริการที่ครอบคลุมตั้งแต่การให้คำปรึกษาการสนับสนุนและการให้บริการทั่วไปอย่างพรั่งพร้อมครบครัน

นอกจากธุรกิจโฮสติ้งและธุรกิจการให้บริการโปรแกรมประยุกต์ในรูปแบบ ASP ซึ่งถือเป็นธุรกิจหลักเอ-โฮสต์ยังเดินหน้าธุรกิจอย่างต่อเนื่องโดยการขยายหน่วยงานใหม่เพิ่มขึ้นนั่นก็คือ Core Technology

Division หน่วยงานเทคโนโลยีหลักที่ให้คำตอบเบ็ดเสร็จแก่ลูกค้าด้วยระบบฐานข้อมูลและเครื่องมือต่างๆ ของออราเคิลซึ่งช่วยเพิ่มความสามารถของลูกค้าในการออกแบบพัฒนาปรับเปลี่ยนระบบแอพพลิเคชันให้เหมาะสมกับธุรกิจนั้นๆภายใต้คำปรึกษาแนะนำและการวางระบบของเอ-โฮสต์ลูกค้าสามารถบริหารระบบฐานข้อมูลของตนเองและดูแลระบบดังกล่าวได้อย่างมีประสิทธิภาพ

ตลอดระยะเวลามากกว่า10ปีในการดำเนินธุรกิจของเอ-โฮสต์ไม่เพียงแต่ในฐานะผู้บุกเบิกธุรกิจโฮสติงและธุรกิจการให้บริการโปรแกรมประยุกต์ในรูปแบบ ASP เท่านั้นแต่เอ-โฮสต์ยังได้ทำการติดตั้งระบบสารสนเทศรวมทั้งผลิตภัณฑ์ของออราเคิลให้กับลูกค้าจนประสบความสำเร็จเป็นจำนวนมากซึ่งหลายรายเป็นหนึ่งในร้อยบริษัทชั้นนำของประเทศไทยแต่สิ่งที่สำคัญกว่านั้นก็คือการที่เอ-โฮสต์ได้สานสัมพันธ์กับลูกค้าและพันธมิตรทางธุรกิจอย่างแนบแน่นจนกลายเป็นหุ้นส่วนทางกลยุทธ์และได้รับตั้งแต่งให้เป็น OCAP (Oracle Certified Advantage Partner) รายแรกในประเทศไทย

รูปที่ 1.2 รางวัลที่บริษัท A-HOST ได้รับ

ปัจจุบันเอ-โฮสต์มีประเภทของสินค้าและการบริการซึ่งสามารถแบ่งออกเป็น 3 กลุ่มใหญ่ได้แก่

1.2.1 Hosting & Outsource Service

เอ-โฮสต์ได้ปรับปรุงและขยายการบริการ Hosting และการให้บริการภายนอก (Outsource) จนสามารถครอบคลุมความต้องการของลูกค้าได้อย่างหลากหลายโดยยึดหลักในการในการให้บริการที่เรียกว่า “Peace of Mind for the customer” ซึ่งหมายถึงการที่จะทำงานให้กับลูกค้าแบบครบวงจรเพื่อที่ลูกค้าจะได้สามารถใช้งานระบบสารสนเทศได้อย่างมีประสิทธิภาพได้อย่างสบายใจไร้ความกังวลต่อความเสี่ยงต่างๆไม่ว่าจะเป็นเรื่องของปัญหาทางเทคนิคการจัดทำระบบและข้อมูลสำรองการปรับแต่งระบบให้ได้ประสิทธิภาพสูงสุด (Performance Tuning) และที่สำคัญที่สุดคือการที่เข้ามารับภาระในด้านการบริหารจัดการบุคลากรทางด้านสารสนเทศทั้งหมดแทนลูกค้า

การใช้บริการ Hosting และ Outsource จะทำให้ลูกค้าสามารถทุ่มเทกำลังสมองเวลาและทรัพยากรขององค์กรให้กับธุรกิจที่เป็นแกนหลัก (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 สามารถครอบคลุมได้ทั้งระบบที่ใช้เทคโนโลยีของออราเคิลและระบบที่ใช้เทคโนโลยีอื่นๆ

1.2.2 Oracle Core Technology Products and Advanced Services

เอ-โฮสต์เป็นผู้นำในการดำเนินธุรกิจในฐานะผู้แทนจำหน่ายเพิ่มมูลค่าให้กับออราเคิลโดยไม่เพียงแต่ทำหน้าที่ในการจัดจำหน่ายสินค้าในกลุ่มแกนหลักของเทคโนโลยี (Core Technology) ของออราเคิลทุกประเภทแต่ยังมีทีมผู้เชี่ยวชาญที่จะให้การสนับสนุนและบริการเสริมอย่างครบวงจรแก่บริษัทคู่ค้าและลูกค้าไม่ว่าจะเป็นการร่วมจัดกิจกรรมทางการตลาดการฝึกอบรมการติดตั้งระบบและการให้คำปรึกษาเพื่อ

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

ผลสำเร็จในการดำเนินธุรกิจประเภทนี้ทั้งในด้านการตลาดและบริการทำให้เอ-โฮสต์ได้รับรางวัล ASEAN Partner of the Year ในปี 2005

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

ความต้องการสูงสุดประการหนึ่งของผู้บริหารในการนำเอาระบบสารสนเทศมาใช้ในองค์กรไม่ว่าจะเป็นภาคราชการหรือเอกชนคือการทำให้ผู้บริหารสามารถได้ข้อมูลที่แสดงให้เห็นถึงสถานะในการดำเนินธุรกิจได้อย่างแม่นยำรวดเร็วและการนำเอาข้อมูลมาวิเคราะห์และวางแผนทั้งในระดับปฏิบัติการและในระดับกลยุทธ์เพื่อให้ธุรกิจสามารถได้เปรียบในการแข่งขันปรับตัวตามเศรษฐกิจได้ในทุกสถานการณ์ Oracle Enterprise Performance Management (EPM) และ Hyperion Business Intelligence จัดเป็นซอฟต์แวร์ชั้นแนวหน้าของโลกที่สามารถสนองตอบต่อความต้องการในลักษณะดังกล่าวได้เป็นอย่างดี

เอ-โฮสต์มีทีมงานที่ปรึกษาที่มีประสบการณ์ทั้งทางด้านธุรกิจและทางด้านเทคนิครวมถึงความเข้าใจในระบบ ERP ของออราเคิลอย่างลึกซึ้งจึงทำให้สามารถให้บริการที่ปรึกษาเพื่อออกแบบติดตั้งเชื่อมโยงและปรับใช้ระบบให้กับลูกค้าจนเกิดประสิทธิภาพสูงสุดอีกทั้งยังมีความยืดหยุ่นและให้การตอบสนองที่เร็วกว่าเมื่อเทียบกับการว่าจ้างที่ปรึกษาจากต่างประเทศ

1.3 รูปแบบการจัดองค์กรและการบริหารองค์กร

ภาพที่ 1.3 คณะผู้บริหาร A-HOST Company Limited

1.4 ตำแหน่งและหน้าที่งานที่นักศึกษาได้รับมอบหมาย

ตำแหน่ง : System Engineer

หน่วยงาน : SMS

1.5 พนักงานที่ปรึกษาและตำแหน่งของพนักงานที่ปรึกษา

นาย ภูดิศ ดุพัสกูล

ตำแหน่ง : System Engineer

KPI Description	Expected Results
1. ศึกษา Security Hardening และมีหัวข้อต่อไปนี้เป็นส่วนหนึ่งด้วย - แต่ละ option เหมาะกับการนำมาใช้งานอย่างไร - ข้อจำกัดอะไรบ้าง - มีใน OS อะไรบ้าง	- สามารถ present feature ได้และมีเอกสาร ppt ประกอบการนำสนอโดยมีเอกสาร 2 ชุดสำหรับนำเสนอสอง session ดังนี้ - Technical session - Sale session โดยใน session นี้จะต้องมี sale เข้าร่วมฟังด้วยอย่างน้อย 1 คน - เอกสารได้รับการ review และ approve จาก mentor
2. Install OS Linux and Configuration - Install Oracle Database - Database ตัวอื่นๆ - Configure hardening	- มี Demo system พร้อม Test Case และต้องนำเสนอต่อ mentor และทีม technical ได้ - มีเอกสารการ configure เป็น step by step และมีรูปภาพประกอบสำหรับแต่ละ step - เอกสารได้รับการ review และ approve จาก mentor
3. Install OS Windows and Configuration - Install Oracle Database - Database ตัวอื่นๆ - Configure hardening	- มี Demo system พร้อม Test Case และต้องนำเสนอต่อ mentor และทีม technical ได้ - มีเอกสาIWLsตัวอย่างขั้นตอนการทำงาน และ concept การทำงานพร้อมแผนภาพการทำงานของระบบ - เอกสารได้รับการ review และ approve จาก mentor
4. Install OS AIX and Configuration - Install Oracle Database - Database ตัวอื่นๆ - Configure hardening	- มี Demo system พร้อม Test Case และต้องนำเสนอต่อ mentor และทีม technical ได้ - มีเอกสารการ configure เป็น step by step และมีรูปภาพประกอบสำหรับแต่ละ step - เอกสารได้รับการ review และ approve จาก mentor
5. จัดทำ Individual Work List	- นำเสนอ IWL เป็นประจำทุกเดือน

1.6 ระยะเวลาที่ปฏิบัติงาน

ระยะเวลาปฏิบัติงานสหกิจศึกษาเป็นเวลา 4 เดือน

- เริ่มต้นปฏิบัติงานสหกิจศึกษา วันที่ 4 มิถุนายน 2561
- สิ้นสุดงานสหกิจศึกษา วันที่ 4 กันยายน 2561

1.7 วัตถุประสงค์ของการปฏิบัติงานและโครงงานที่ได้รับมอบหมาย

1. เพื่อศึกษาการและหาประสบการณ์การทำงานจริงภายในองค์กร
2. เพื่อนำความรู้ที่ได้ไปใช้ในการพัฒนาโครงงานและการทำงานในอนาคต

1.8 ผลที่คาดว่าจะได้รับจากการปฏิบัติงานและโครงงานที่ได้รับมอบหมาย

1. ได้ประสบการณ์ในการทำงานจริง
2. ได้นำความรู้มาประยุกต์ใช้ในการทำงาน

บทที่2
ทฤษฎีและเทคโนโลยีที่ใช้ในการปฏิบัติงาน

2.1 ระบบปฏิบัติการ Linux

ภาพที่ 2.1 สัญลักษณ์ของ Linux

Linux ก็คือระบบปฏิบัติการหนึ่งที่ใช้ในการเชื่อมต่อกับฮาร์ดแวร์ หรืออาจจะรู้จัก ในภาษาอังกฤษ คือ Operating System เช่นเดียวกับ Windows, Dos หรือ Unix ซึ่งลีนุกซ์ถูก สร้างขึ้นโดย Linus Tovalds นักศึกษาภาควิชาวิทยาการคอมพิวเตอร์ มหาวิทยาลัย Helsinki โดยทา เป็นโปรเจคตอนที่เขากำลังศึกษาอยู่ที่นั้น ในปี ค.ศ. 1989 ซึ่งเขาได้ต่อยอดมาจาก ระบบปฏิบัติการ Unix Linus Tovalds ได้สร้าง Linux ขึ้นมา และได้เชิญชวนผู้ร่วมพัฒนา คนอื่นๆ ทางอินเทอร์เน็ต ซึ่งต่อมากลายเป็นทีมผู้พัฒนาที่ทำงานและติดต่อกันทาง อินเทอร์เน็ต ซึ่งทุกคนต่างกันพัฒนาโดยไม่มีค่าแรงหรือผลตอบแทนประการใด พวกเขา พัฒนา Linux ขึ้นมาด้วยใจรักในสิ่งที่พวกเขากำลังทำโดยส่วนมากแล้วผู้คนจะใช้ OS Linux ไปใช้ทำเซิฟเวอร์เพราะกินแรงเครื่องน้อย และเครื่องจะเสถียรกว่าการใช้ OS ทั่วไป และที่สำคัญก็คือ Linux เป็น Software แบบ Open Source ที่คุณสามารถ ปรับแต่งได้ตาม ต้องการ ด้วยเหตุนี้เองจึงทำให้ Linux ได้มีผู้ที่นำไปพัฒนาจนกลายเป็นระบบที่หลากหลายและในเวลา ต่อมา จึงมี OS เกิดขึ้นมากมาย ที่แตกแขนงมาจาก Linux อาทิเช่น Ubuntu, Debian, Redhat และอื่นอีกมากมายอย่างนับไม่ถ้วน จนกลายเป็น Linux Distribution

2.1.1 ข้อดีของ Linux

2.1.1.1 ใช้งานได้ไม่เสียค่าใช้จ่าย

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

2.1.1.2 ความปลอดภัยในการทำงาน

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

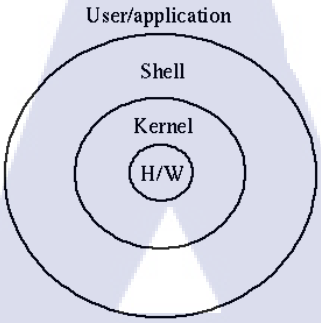
2.1.1.3 เสถียรภาพในการทำงาน

ลีนุกซ์มีเสถียรภาพในการทำงานสูง ปัญหาระบบล่มในระหว่างทำงานจะไม่ค่อยมี ให้พบ โดยความสามารถพิเศษของลีนุกซ์อยู่ที่การตรวจสอบความสัมพันธ์ของโปรแกรม ในการทำงาน เช่น ถ้าติดตั้งโปรแกรม 1 ลีนุกซ์จะทำการตรวจสอบว่าโปรแกรม 1 มีการ เรียกใช้งานโปรแกรมอื่นทำงานด้วยหรือไม่ นอกจากนี้ถ้าทำการติดตั้งหรือลบโปรแกรม ออกจากระบบ โดยไม่จำเป็นต้องบู๊ตเครื่องใหม่ สามารถทำงานต่อไปได้ทันที

2.1.1.4 สนับสนุนฮาร์ดแวร์ทั้งเก่าและใหม่

เทคโนโลยีของอุปกรณ์ฮาร์ดแวร์มีการเปลี่ยนแปลงไปอย่างรวดเร็ว ระบบปฏิบัติการโดยส่วนใหญ่มักจะออกมาเพื่อรองรับประสิทธิภาพการทำงานของ ฮาร์ดแวร์ที่พัฒนาขึ้น จนทำให้บางครั้งต้องการอัพเกรดเครื่องตาม แต่สำหรับลีนุกซ์จะ ยังคงสนับสนุนฮาร์ดแวร์เก่าให้สามารถใช้งานได้ โดยจะเพิ่มส่วนของการสนับสนุน ฮาร์ดแวร์ตัวใหม่ลงไปเท่านั้นทำให้ไม่จำเป็นต้องเปลี่ยนฮาร์ดแวร์ซึ่งช่วยประหยัดค่าใช้จ่ายลงไปได้มาก

2.1.2 โครงสร้างของ Linux



ภาพที่ 2.2โครงสร้างของ Linux

ระบบปฏิบัติการ Linux สามารถแบ่งโครงสร้างหลัก ๆ ได้ 4 ระดับ แต่ละระดับก็จะทำหน้าที่ต่างกัน

2.1.2.1 ฮาร์ดแวร์ (Hardware)

หมายถึงอุปกรณ์หรือทุกชิ้นส่วนของคอมพิวเตอร์ ที่สามารถจับต้องได้ เช่น จอภาพ คียบ์อร์ด เม้าส์ ดิกส์ไดรซ์ ซีดีรอม เป็นต้น

2.1.2.2 ยูนิกซ์ เคอร์เนล (Kernel)

เคอร์เนล จะท าหน้าที่ควบคุมการท างานทั้งหมดของระบบ ได้แก่ การจัดสรร ทรัพยากร การจัดการข้อมูลบริการหน่วยความจ า ซึ่งเคอร์เนลนี้จะขึ้นกับฮาร์ดแวร์ เช่น ถ้ามี การเปลี่ยนแปลงฮาร์ดแวร์ เคอร์เนลนี้ก็จะถูกเปลี่ยนไปด้วย เป็นต้น

2.1.2.3 เชลล์ (Shell)

ตัวกลางระหว่างผู้ใช้กับตัวเคอร์เนล ท าหน้าที่รับค าสั่งจากผู้ใช้ แล้วน าไปแปลเป็น ภาษาที่เครื่องคอมพิวเตอร์เขา้ใจ เรียกอีกอย่างหนึ่งได้ว่า command interpreter แต่ถ้ามีการ น า เชลล์หลาย ๆ ตัวมาเขียนรวมกัน (คล้าย ๆ กับ batch file ในระบบปฏิบตัิการ DOS) จะ เรียกว่า เชลล์สคริปต์

2.2 VMware Workstation

ภาพที่ 2.3 สัญลักษณ์ของ VMware Workstation

โปรแกรม VMware เป็นโปรแกรมที่ถูกคิดค้นขึ้นมาเพื่อสร้างคอมพิวเตอร์เสมือน (Virtual Machine) ขึ้นบนระบบปฏิบัติการเดิมที่มีอยู่ ตัวอย่างเช่น เครื่องคอมพิวเตอร์ที่ลง ระบบปฏิบัติการ Windows XP อยู่เดิม แล้วทำการลงระบบปฏิบัติการ Windows NT ผ่าน โปรแกรม VMware อีกทีหนึ่ง ซึ่งเมื่อลงแล้ว ทั้งสองระบบสามารถทำงานพร้อมกันได้โดย แยกจากกันค่อนข้างเด็ดขาด (เสมือนเป็นคนละเครื่อง) โดยคอมพิวเตอร์เสมือนที่สร้าง ขึ้นมานั้น จะมีสภาพแวดล้อมเหมือนกับคอมพิวเตอร์จริงๆ เครื่องหนึ่ง ซึ่งจะประกอบด้วย พื้นที่ดิสก์ที่ใช้ร่วมกับพื้นที่ดิสก์ของเครื่องนั้นๆ การ์ดแสดงผล การ์ดเน็ตเวิร์ก พื้นที่หน่วยความจำซึ่งจะแบ่งการทำงานมาจากหน่วยความจำของเครื่องนั้นๆ เช่นกัน สำหรับข้อจำกัดของการทำงานบน VMware ก็คือ VMware จะสร้าง สภาพแวดล้อมของฮาร์ดแวร์ต่างๆ ซึ่งเป็นของตัวโปรแกรม VMware เอง ดังนั้นการใช้ ฮาร์ดแวร์ของคอมพิวเตอร์หลักและคอมพิวเตอร์เสมือนจะไม่เหมือนกัน จึงไม่สามารถที่จะ ติดตั้งไดรเวอร์ของฮาร์ดแวร์จริงๆ ให้กับคอมพิวเตอร์เสมือนที่ลงผ่านโปรแกรม VMware ได้ สำหรับการใช้โปรแกรมนี้จะแบ่งหน่วยความจำของเครื่องหลักไปใช้ด้วยหาก หน่วยความจำของเครื่องมีขนาดไม่มากเพียงพอ ก็อาจทำให้เครื่องทำงานช้าลงมาก ดังนั้น หากมีหน่วยความจำเยอะ การทำงานของโปรแกรมนี้ก็จะดีขึ้น

2.3 Windows Server

ภาพที่ 2.4 สัญลักษณ์ของ Windows Server

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

2.3.1 Windows Server 2008 R2

Windows Server 2008 R2 เป็น server OS สามารถให้บริการไดห้ลายประเภทใน เวลาเดียวกัน โดย ที่ส าคัญ windows server 2008 R2 สามารถควบคุมผู้ใชไ้ดค้รอบคลุมทุก กรณีไม่ว่าจะย้ายไปท างานที่เครื่องใดก็ตาม ก็คือ สามารถควบคุมเครื่องในเครือข่ายได้โดย ไม่ต้องไปจัดการที่เครื่องลูกข่ายเลย ก าหนดสิทธิ์การเข้าถึงอุปกรณ์ของเครื่องลูกข่ายได้ ไม่ ว่าจะเป็นการเขา้ถึงไดร์วก าหนดการใชแ้ฟลชไดร์วได้การคอนโทรลต่างๆ ก าหนดเวลาใน การเข้าถึงเครือข่าย (LAN) หรือ อินเทอร์เน็ตได้

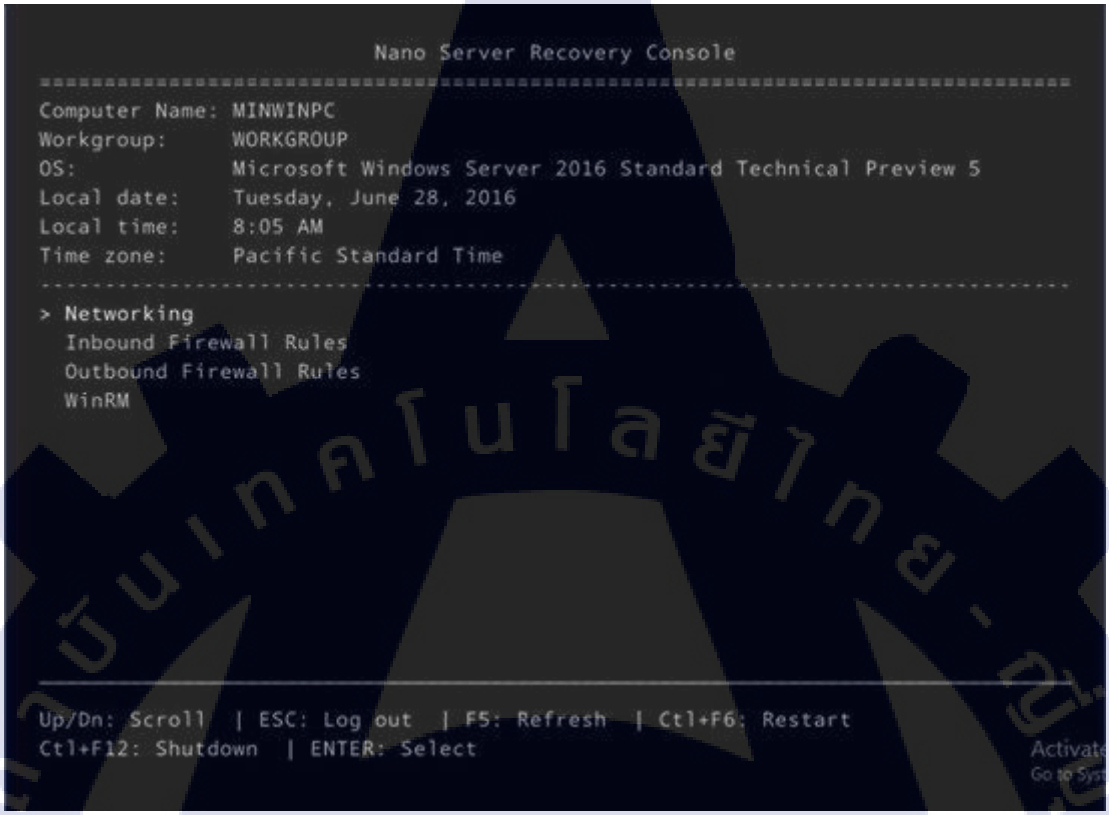
2.3.2 Windows Server 2012 R2

Windows Server 2012 R2 คือระบบปฏิบัติการคอมพิวเตอร์ที่ใช้รันงานทางฝั่งเซิฟ เวอร์ (Server) เพื่อให้บริการแก่เครื่องลูกข่าย (Client) เป็นผลิตภณัฑ์หรือซอฟตแ์วร์ของ ไมโครซอฟต์ บริษัทยักษ์ใหญ่ที่มีชื่อเสียงดา้นการพฒันาซอฟตแ์วร์ ความสามารถของตวั ระบบนั้นได้แก่ Hyper-V หรือก็คือระบบเสมือน สามารถจ าลองเครื่องคอมพิวเตอร์ได้ หลายเครื่องโดยไม่เสียค่าใช้จ่ายในการติดตั้ง Windows Server ในระบบเสมือน

2.3.3 Windows Server 2016

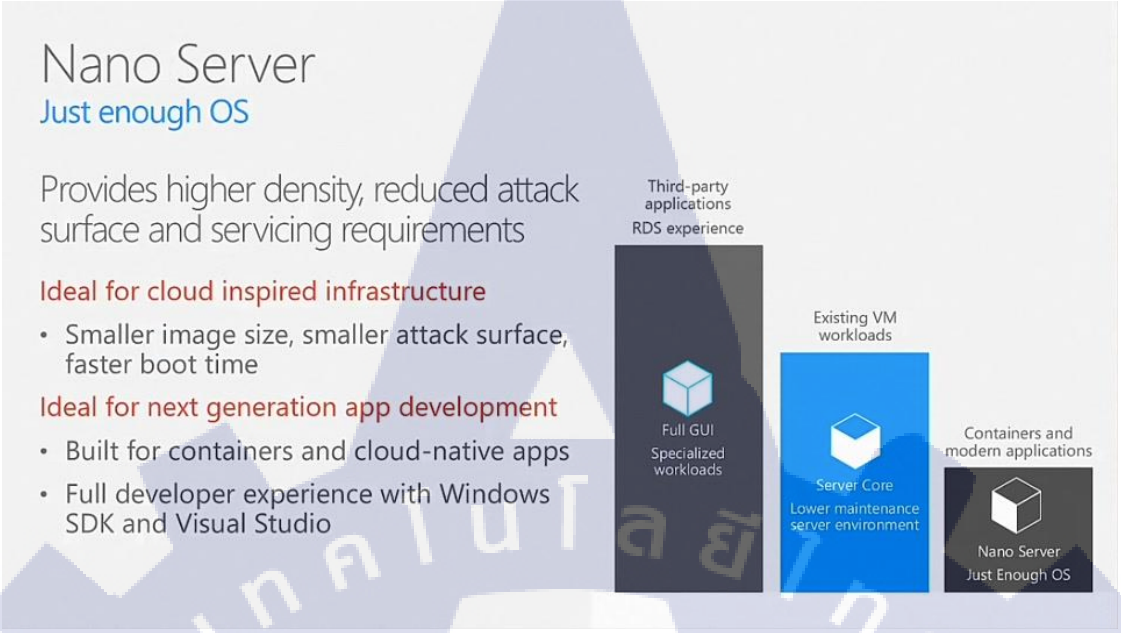
Windows Server 2016 เป็นระบบปฏิบัติการสำหรับเครื่อง Server รุ่นใหม่ล่าสุดที่จะมาทดแทน Windows Server 2012 R2 ที่เปิดตัวไปเมื่อปี 2556 โดยในคราวนี้ Windows Server 2016 ได้มีการปรับปรุงเปลี่ยนแปลงฟีเจอร์ภายในมากมาย เพื่อให้รองรับกับการใช้ Server ในหลากหลายรูปแบบในปัจจุบัน และได้มาการเพิ่มมาหลักๆ 9 ข้อคือ

2.3.3.1 Nano Server ฟีเจอร์ใหม่



ภาพที่ 2.5 Nano Server

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

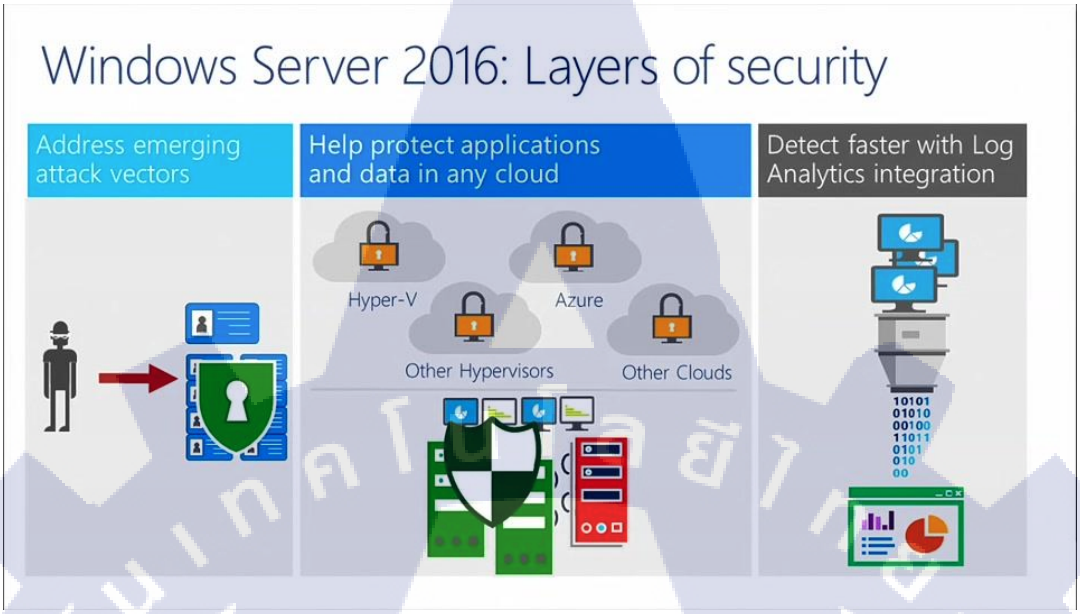


ภาพที่ 2.6 ความสามารถของ Nano Server

สำหรับ **Nano Server** วิธีการติดตั้งจะไม่เหมือนกับ **Windows Server** ปกติ คือไม่ต้องมีกระบวนการ Install หรือการกำหนดไดร์ฟสำหรับ Boot แต่จะใช้วิธีติดตั้งแบบ Image File แบบเดียวกับการติดตั้ง OS ในระบบ Cloud โดยขั้นแรกของการติดตั้งจะต้องทำการเลือกส่วนประกอบต่าง ๆ ที่จะใช้ใน **Nano Server** แล้วสร้างเป็นไฟล์ Image ขึ้นมาก่อน (ทั้งหมดนี้ทำผ่าน Command line โดยใช้ tools ในแผ่นติดตั้ง **Windows Server 2016**) แล้วจึงค่อยนำไฟล์ Image ไปติดตั้งลงบนเครื่อง Server หรือใน Virtual Server ใน Cloud

Nano Server เป็น OS ที่ไม่มี UI คือไม่สามารถควบคุมและสั่งงานตัว **Nano Server** ที่หน้าเครื่องได้ ที่หน้าเครื่องทำได้เฉพาะการตั้งค่า 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

2.3.3.2 สร้างมาเพื่อ Cloud Technology โดยเฉพาะ



ภาพที่ 2.7 Layers of Security

Windows Server 2016 ถูกพัฒนามาเพื่อรองรับสถาปัตยกรรมแบบ Cloud โดยเฉพาะ จึงมีฟีเจอร์เด็ดๆ ที่ออกมารองรับกับ Cloud Technology หลายฟีเจอร์ อาทิ

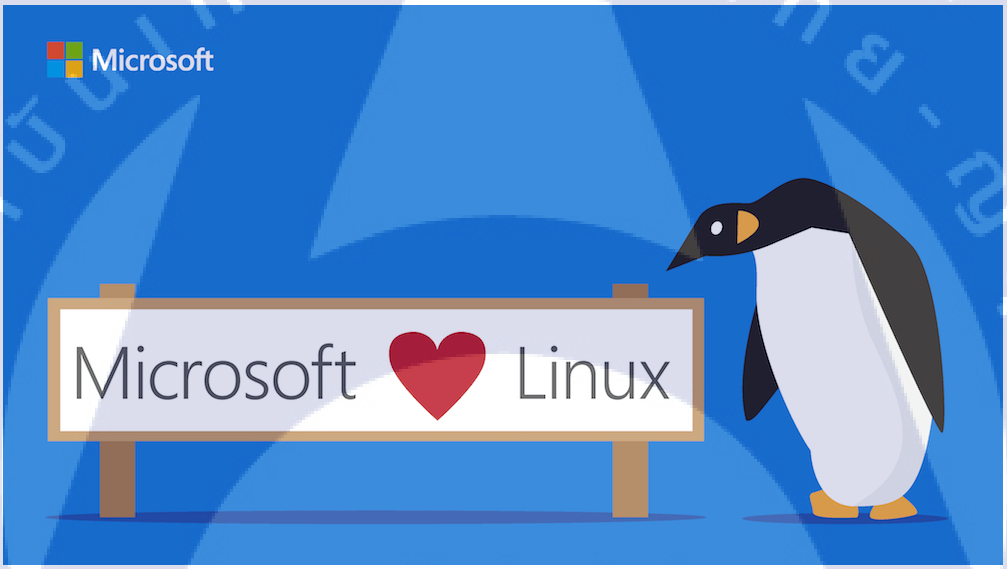
- **Hyper-V** รุ่นใหม่ ที่ถูกปรับปรุงให้ดีขึ้น และรองรับการทำงานแบบ Container
- **Nano Server** ที่สามารถนำไปสร้างเป็น Server เล็กๆบน Cloud เพื่อใช้งานได้อย่างคุ้มค่าทรัพยากร
- **Shielded Virtual Machine** ยกเครื่องระบบความปลอดภัยใหม่ สำหรับ Hyper-V ช่วยให้มั่นใจได้มากขึ้นว่าจะไม่มีช่วงโหว่ที่ร้ายแรงจากตัวของระบบ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

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

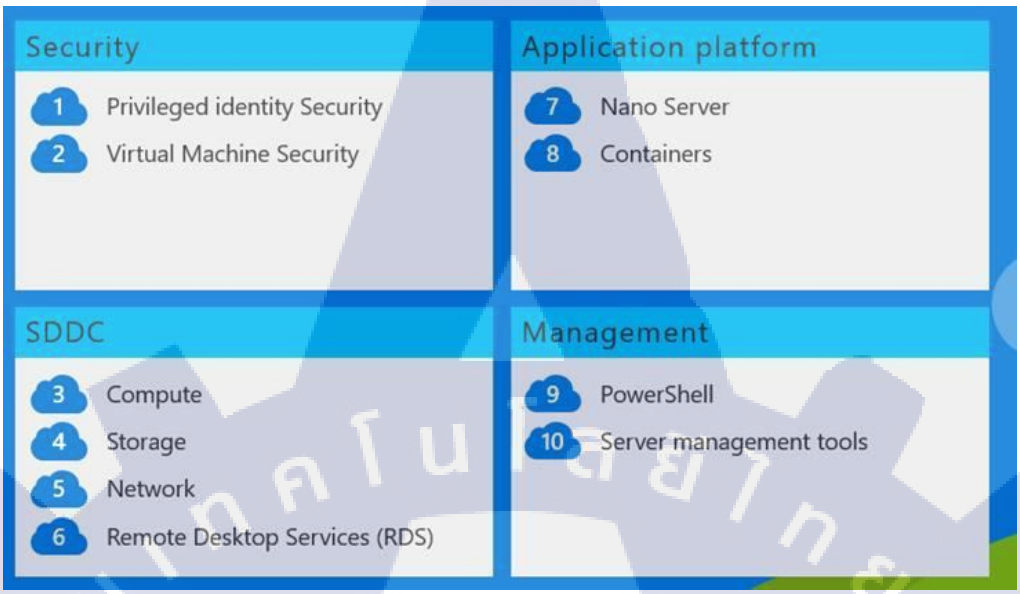
2.3.3.3 Hyper-V รองรับกับ Linux ชื่อดังเกือบทั้งหมด



ภาพที่ 2.9 Hyper-V Function

ด้วยความเป็น Cloud Ready ของ **Windows Server 2016** ทำให้ต้องเปิดเพื่อรองรับการทำงานร่วมกับระบบปฏิบัติการอื่น 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



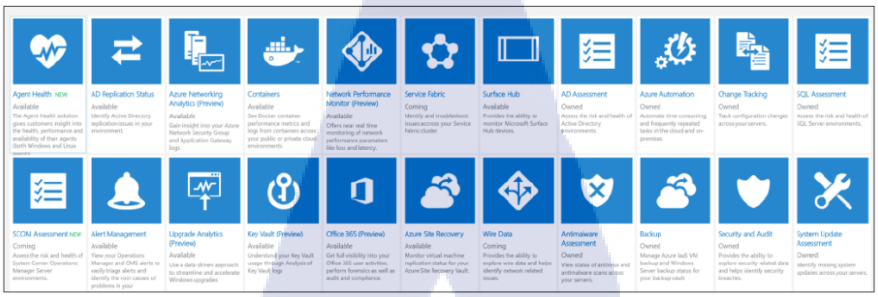
ภาพที่ 2.10 ระบบ Security ใหม่

ใน **Windows Server 2016** มีการปรับปรุงระบบ Security ใหม่ในหลายส่วน อาทิ

- **Shielded VMs** - ระบบที่ช่วยรักษาความปลอดภัยให้กับ Virtual Machines ต่างๆ ในเครื่อง ป้องกันไม่ได้เกิดการละเมิดความปลอดภัยระกว่าง VM ด้วยกันเอง หรือแม้แต่จาก VM เข้ามายังเครื่องแม่
- **"Headless" Windows Defender** - โปรแกรม **Windows Defender** ที่ใช้จัดการกับไวรัสต่างๆ ในเวอร์ชันที่แถมมากับ **Windows Server 2016** ได้มีการเพิ่มความสามารถในการจัดการกับมัลแวร์รวมทั้งมาในรูปแบบ Headless คือทำงานในลักษณะเป็น Command Service ที่ไม่มี GUI ช่วยให้กินทรัพยากรน้อยลง และตรวจพบปัญหาต่างๆ ได้เร็วขึ้น
- **Linux Secure Boot** - เดิมใน Windows Server จะไม่สามารถ Secure Boot กับ Linux บน VM ที่สร้างขึ้นใน Windows Server ได้ แต่ด้วยระบบ Security ใหม่ใน **Windows Server 2016** ได้มีการปรับปรุงจนทำให้สามารถ Secure Boot ใน VM ได้กับ Linux ทุกตัว ช่วยยกระดับความปลอดภัยให้กับ VM มากขึ้น

และนอกเหนือจากที่กล่าวมานี้ยังมีระบบ Security อื่นๆ อีกมากที่ถูกเพิ่มมาใน **Windows Server 2016** อีกมาก ที่จะช่วยให้มั่นใจได้ว่าจะไม่พบปัญหาน่าปวดหัวเรื่อง Security เหมือนกับ Windows Server เวอร์ชันที่ผ่านๆ มา อย่างแน่นอน

2.3.3.5 จัดการ Server ได้ลึกและละเอียดขึ้นด้วย PowerShell 5.0



ภาพที่ 2.11 PowerShell 5.0

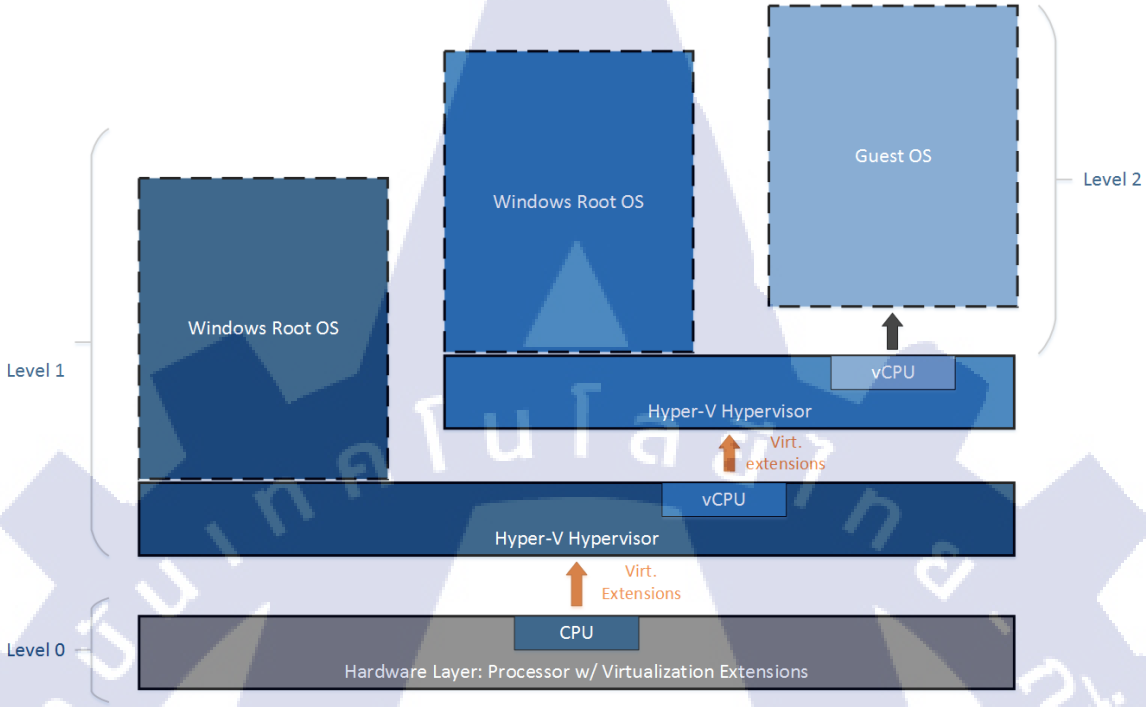
Windows Server 2016 มาพร้อมด้วย PowerShell 5.0 ที่จะช่วยให้สามารถเข้าควบคุมและจัดการแทบทุกอย่างใน Server ได้ทั้งหมดผ่าน Command line นอกไปจากนั้น หากต้องการควบคุมและจัดการในแบบที่ซับซ้อนมากขึ้น หรือลงรายละเอียดมากขึ้น ก็สามารถพัฒนาสคริปขึ้นมาใช้งานเองได้ผ่าน Windows Management Framework 5.0 ใน **Windows Server 2016** ตัว PowerShell ยังสามารถสั่งงานไปยังเครื่อง Virtual Server ในระบบโดยสั่งงานบนเครื่อง Host ได้เลยผ่าน option “-VMName” ไม่ต้องไปนำคำสั่ง 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 ตัวใหม่ที่ไมโครซอฟต์พยายามผลักดันเพื่อใช้แทน NTFS เดิม แต่ด้วยความไม่เสถียรภาพของระบบไฟล์ นับตั้งแต่เริ่มเปิดให้ใช้ใน **Windows Server 2012** ทำให้ระบบไฟล์นี้ยังไม่ได้รับความนิยม ทั้งๆที่เป็นระบบไฟล์ที่ถูกออกแบบมาเป็นอย่างดี และมีประสิทธิภาพสูงกว่าระบบไฟล์แบบ NTFS แต่ใน**Windows Server 2016** ระบบ **ReFS** ได้ถูกพัฒนาขึ้นมาอย่างสมบูรณ์และพร้อมใช้งานอย่างที่สุด มีความประสิทธิภาพและเสถียรภาพสูง สามารถใช้งานแทน NTFS ได้อย่างสมบูรณ์และไม่ก่อให้เกิดปัญหาอีกด้วย

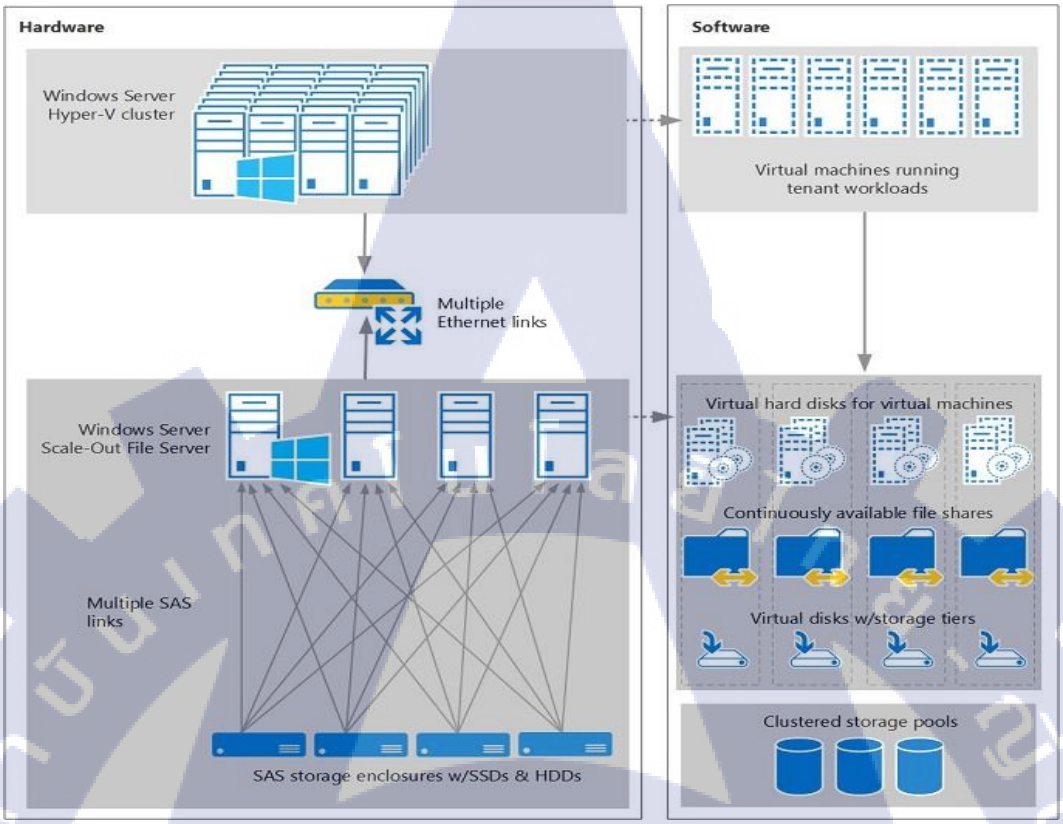
2.3.3.7 Nested Virtualization



ภาพที่ 2.13 ระบบ Nested VM

ฟีเจอร์ **Nested Virtualization** ที่ช่วยให้คุณสามารถสร้าง Virtual Server ซ้อนในเครื่องที่เป็น Virtual Server เป็นหนึ่งในฟีเจอร์ยอดฮิตที่เคยถูกตัดออกจาก Hyper-V และได้ถูกนำกลับมาใหม่อีกครั้ง **Windows Server 2016** ทำให้คุณสามารถบริหารจัดการเครื่อง Virtual Server ได้อย่างไม่มีขีดจำกัดอีกต่อไป

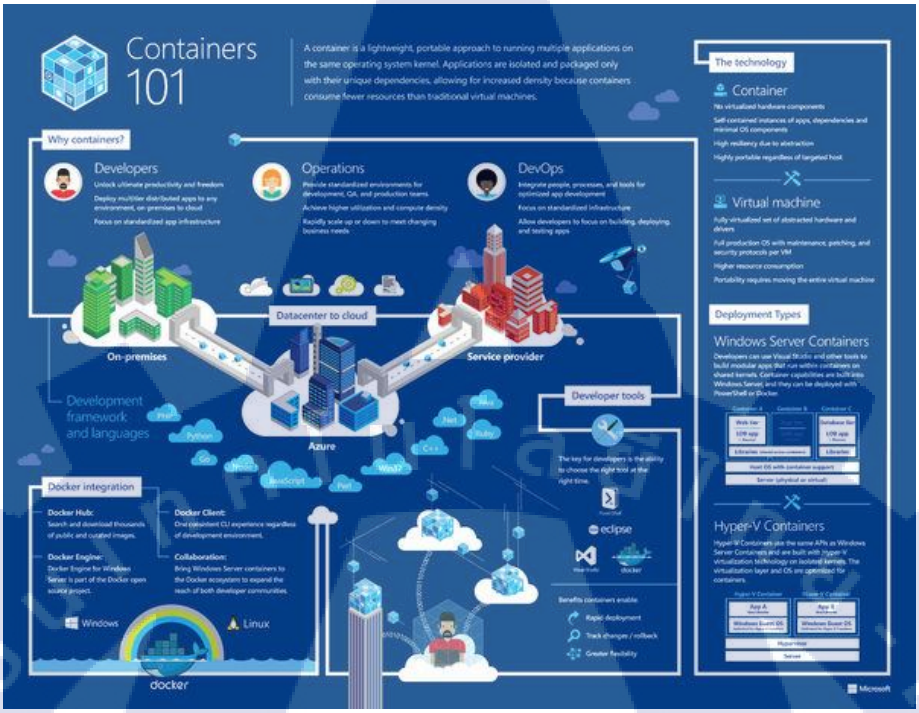
2.3.3.8 Software-defined storage จัดการพื้นที่เก็บข้อมูลได้ง่ายขึ้น



ภาพที่ 2.14 ระบบ Software-defined storage

การจัดการพื้นที่เก็บข้อมูล หรือ storage ในสมัยก่อนของ Windows Server จะทำได้ค่อนข้างยาก เพราะระบบจัดการจะยึดตาม Hardware ที่ใช้เก็บข้อมูลเป็นหลัก แต่ด้วยระบบจัดการพื้นที่เก็บข้อมูลแบบใหม่ของ **Windows Server 2016** ที่มองพื้นที่เก็บข้อมูลเป็นแบบ Software ทำให้สามารถปรับเปลี่ยนและบริหารจัดการได้ง่ายขึ้น โดยไม่สร้างความเสียหายให้กับข้อมูลที่ถูกจัดเก็บไว้อยู่แล้ว เช่น คุณสามารถจะสร้าง **high availability storage** ได้ง่ายขึ้นโดยไม่ต้องเสียเงินซื้อ Hardware storageราคาแพง, หรือสามารถสร้าง **Storage Replica** ในระดับ volume level และแถมด้วย Storage QoS ที่ช่วยบริหารจัดการคิวการเข้าถึงพื้นที่เก็บข้อมูล ช่วยให้ Virtual Server เข้าถึงพื้นที่เก็บข้อมูลอย่างมีเสถียรภาพและประสิทธิภาพเท่าเทียมกันในทุก Virtual Server

2.3.3.9 รองรับ Containers แนวคิด Virtual Server ที่กำลังเป็นที่นิยม



ภาพที่ 2.15 รับระบบ Containers

Containers คือการกำหนดสภาพแวดล้อมให้เหมาะสำหรับซอฟต์แวร์นั้น ๆ เพื่อให้เกิดความปลอดภัยของตัวซอฟต์แวร์ และป้องกันเรื่องรบกวนกันระหว่างซอฟต์แวร์ต่าง ๆ แนวคิดนี้กำลังได้รับความนิยมอย่างสูงในปัจจุบันอันเนื่องมาจากการพัฒนาของ Cloud Technology เพราะแนวคิดของ Containers ทำให้เราสามารถบริหารจัดการระบบซอฟต์แวร์ได้ง่ายขึ้น คล่องตัวขึ้น Windows Server 2016 ถูกออกแบบมาให้รองรับกับ Cloud Technology โดยเฉพาะ จึงถูกกำหนดมาให้รองรับการทำงานแบบ Containers ด้วย โดยใน Windows Server 2016 มีการรองรับ Containers ถึง 2 แบบคือ

- **Windows Server Container** - เป็นการสร้าง Containers บนตัว Windows Server โดยตรง จะเป็นการจัดการสภาพแวดล้อมของแต่ละซอฟต์แวร์ให้ต่างกันไป แต่ยังใช้ทรัพยากรด้านฮาร์ดแวร์ร่วมกัน
- **Hyper-V Container** - เป็นการสร้าง Containers แบบที่เรียกว่า super isolated คือ แยกทั้งสภาพแวดล้อมของแต่ละซอฟต์แวร์ และแยกทรัพยากรที่แต่ละซอฟต์แวร์จะใช้งานได้ 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 ซึ่งทำงานอยู่ที่ 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 ออราเคิลช่วยเพิ่มความสะดวกในการบริหารจัดการข้อมูลภายในองค์กร ทั้งยังช่วยให้ลูกค้าเข้าใจ เกี่ยวกับธุรกิจได้มากขึ้นและสร้างสรรค์นวัตกรรมได้รวดเร็วขึ้น โดย Oracle Database 11g มีคุณสมบัติที่เหนือกว่าทั้งในแง่ของประสิทธิภาพ ความยืดหยุ่นในการปรับขนาด ความพร้อมใช้งาน ความปลอดภัย และความสะดวกในการจัดการ บนระบบกริดราคาประหยัดซึ่งประกอบด้วยสตอเรจและเซิร์ฟเวอร์มาตรฐานอุตสาหกรรม Oracle Database 11g สามารถติดตั้งได้อย่างมีประสิทธิภาพบนทุกระบบ ตั้งแต่เบลดเซิร์ฟเวอร์ขนาดเล็ก ไปจนถึงเซิร์ฟเวอร์ SMP ที่มีขนาดใหญ่ที่สุด รวมถึงคลัสเตอร์ทุกขนาด โดยประกอบด้วยความสามารถด้านการจัดการแบบอัตโนมัติเพื่อการดำเนินการที่สะดวกง่ายดายและประหยัดค่าใช้จ่าย Oracle Database 11g มีความสามารถที่โดดเด่นในการจัดการข้อมูล

ทั้งหมด ตั้งแต่ข้อมูลธุรกิจแบบเก่า ไปจนถึงข้อมูล XML และข้อมูลเชิงพื้นที่ 3 มิติ จึงนับเป็นทางเลือกที่เหมาะสมที่สุดสำหรับการประมวลผลทรานแซคชั่น ระบบคลังข้อมูล และการจัดการคอนเทนต์

2.5 ระบบป้องกันเครือค่ายคอมพิวเตอร์

Hardening Os (Operating System) เป็นกระบวนการของการกำหนดค่า (Parameter) บนระบบปฏิบัติการเพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต ป้องกันผู้บุกรุก แฮกเกอร์ และช่องโหว่ด้านความปลอดภัยอื่น ๆ OS Hardening ทำให้ระบบคอมพิวเตอร์เชื่อถือได้มากขึ้น มีความปลอดภัย และช่วยเพิ่มประสิทธิภาพการทำงานเนื่องจากใช้หลักการ "ลดสิ่งที่ไม่ได้ใช้ออกไปจากระบบ" ดังนั้น วัตถุประสงค์หลักของการ Hardening คือการ ลดความเสี่ยงที่จะเกิดด้านความปลอดภัยให้ได้มากที่สุดซึ่งผมขอย้ำอีกครั้งกับผู้อ่านว่าการทำ Hardening นั้นเป็นการเพิ่มความปลอดภัยให้ระบบปฏิบัติการที่เราใช้อยู่โดยมีต้นทุนค่าใช้จ่ายต่ำมาก ไม่ต้องซื้อ Hardware / Software ราคาแพงเราก็สามารถเพิ่มความปลอดภัยให้กับคอมพิวเตอร์ของเราได้เป็นอย่างดี เพียงแค่เราใส่ใจที่จะนำเอา Security Best Practice ของระบบปฏิบัติการที่เราใช้อยู่นำมาลงมือทำ (ซึ่งโดยส่วนใหญ่มักจะมีแจกจ่ายฟรีให้ผู้ใช้งานโดยบรรดาผู้ผลิตอยู่แล้ว) หากจะมองในมุมมองขององค์กรด้วยแล้ว กระบวนการทำ Hardening เป็นหนึ่งในส่วนสำคัญในการสร้างมาตรฐานของการบริหารจัดการระบบรักษาความปลอดภัยข้อมูลอย่างเป็นระบบและมีประสิทธิภาพ

2.5.1 security life cycle

ที่ต้องทำเพราะมีการเปลี่ยนแปลงบ่อยและต้องกลับมา recheck เพื่อไม่ให้มีอะไรเปลี่ยนแปลงจากที่ควรจะเป็นโดย security life cycle จะมีอยู่ด้วยกัน 10 ข้อคือ

1. Risk & Vulnerability Management (ประเมินความเสี่ยง)
2. วางแผนกำหนดว่าจะ hardening อะไรบ้างเพื่ออะไรและต้องระวังให้ดี เพราะบาง key อาจจะทำให้ระบบเสียทั้งระบบ
3. เตรียมแผนรองรับหาก fails
4. ทำ full backup
5. ขอ mail aproove จากผู้บริหาร
6. มีเอกสารรองรับในขั้นตอนการทำงาน
7. ทดสอบระบบหลังทำงานเสร็จ
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 ผู้ใช้ระบบรู้ว่าระบบที่ Harden แล้วแข็งแรง แต่มันไม่มี function อะไรใหม่ๆ และอาจโดนตำหนิหากทำระบบของเขาใช้งานช้าหรือแย่กว่านั้นอาจไม่ได้เลย ต้องรักการเรียนรู้และมีเหตุผลเพราะควร Harden แบบพอดี ถ้าทำมากเกินไปอนาคต update program ไม่ได้จะยุ่ง และสุดท้ายตรงคือต้องสมาธและมีสติอันนี้สำคัญตอนแก้ไขอะไรในระบบต้องรู้ตัวว่าทำอะไร เพราะทำแบบเบลอจะทำให้งานเสียได้ เราลองมาเปิดมุมมองใหม่กับงาน Security hardening ว่าเขาทำอะไรกัน

2.5.4 การทำ hardening บน Windows

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

2.5.5 ขั้นตอนของ Hardening

- ศึกษาการทำงานของ Application บน Server และทดสอบใช้งาน Basic function
- จัดทำ Hardware และ Software inventory เพื่อใช้สำหรับการดูแลว่าเรามีอะไรอยู่บ้าง และส่วนใดต้องการดูแลเรื่องความปลอดภัย
- ถ้า Application นั้นซื้อมาหรือไม่ได้พัฒนาเอง ต้องศึกษา Security Guide จากผู้พัฒนาก่อน เพื่อป้องกันการแก้ไขระบบโดยไม่ได้รับอนุญาต หรือมีปัญหาเรื่องการ Support
- กำหนดขอบเขตการ Harden ให้เหมาะสมหรือตรงกับหน้าที่หรือ Application บน Server

- หาเครื่องมือทุนแรงช่วยประเมินความปลอดภัยเช่น Microsoft MBSA, Best Pracrtise Analyzer เป็นต้น
- หา Hotfix/Patch certification list สำหรับ Application ถ้าหาได้
- ศึกษาวิธีการ Harden จากแหล่งต่างๆ
- มีการ Backup / Recovery
- ลงมือ Harden และหมั่นทดสอบการใช้เบื้องต้นเป็นระยะๆ
- ส่งมอบระบบคืนให้ผู้ทดสอบระบบงาน
- มีการ Review security อย่างน้อยปีละ 1 ครั้ง

2.5.6 การกำหนดขอบเขตและรูปแบบการ Harden

จากภาพด้านบน แสดงให้เห็นว่าการ Harden ให้มอง Server แบ่งออกเป็นหมวดหมู่ เพื่อให้ความสะดวกเราก็จะเจาะไปทีละเรื่องอย่างเป็นขั้นเป็นตอน 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 ให้สิทธิเฉพาะคนที่มีหน้าที่เข้าไปเห็นข้อมูลหรือ Application คนอื่นห้ามเข้า ใน Folder ที่เก็บ Application นั้น มีความสำคัญมาก หากผู้ไม่ประสงค์ดีนำโปรแกรมที่ไม่ได้รับอนุญาตไปลง อาจทำให้เกิดความเสียหายร้ายแรงได้

2.5.9 Operating System

ศึกษาจากคู่มือ Security ของ OS ว่าต้องทำอย่างไร เช่น

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

- การดู Port ด้วย netstat ว่าเครื่องเปิด service อะไรบน TCP/UDP protocol
- ถ้าเป็น Windows เราจะใช้ Group Policy ช่วยก็ได้ เพื่อช่วยให้ดูแลง่ายขึ้นด้วย
- ติดตั้ง Anti-Virus และอย่าลืมดูว่ามัน Update signature ได้
- ติดตั้ง Windows Update Agent แต่ Server อาจกำหนดไม่ใช้มัน update เองได้เดี๋ยวทำเครื่องพัง แต่ใช้ประโยชน์ให้มัน warning เวลามี hotfix ออกใหม่ได้

2.5.10 Network

บางครั้งเครื่องเราอาจป้องกันด้วย Software แล้วอาจไม่เพียงพอก็ใช้ Firwall หรืออุปกรณ์ Network security มาช่วยอีกแรง

2.5.11 Physical

เครื่อง Server ควรควบคุมให้ผู้มีหน้าที่เข้าไปยุ่งกับมันได้เท่านั้น นอกจากนี้ก็ควรดูว่าที่ตั้ง server นั้น เรียบร้อยไหม เช่น ไม่มีน้ำจากแอร์หรือดับเพลิงหยดลงเครื่อง, พวกสายไฟหรือสายต่างๆ ติดตั้งเรียบร้อยดี เป็นต้น

2.5.12 เครื่องมือ/เครื่องทุ่นแรง

เราควรให้เวลาในการศึกษาข้อมูลของ Software/Hardware ที่ Inventory ที่เราเตรียมไว้ Software บางตัวก็มีผู้พัฒนา Tool สำหรับทำ Security scan มันช่วยให้ประหยัดเวลาและเป็นมาตราดีกว่าเสียเวลามานั่งทำ ซึ่งเราก็ควรรู้อยู่แล้วว่าต้องตรวจตราในหัวไหนด้วย ไม่ใช่ปล่อยเครื่องทำอย่างเดียว เพราะมันทำพังก็ไม่รู้ว่าเป็นเรื่องอะไร ตัวอย่างของเครื่องมือสำหรับ Windows คือ MBSA

บทที่ 3
แผนงานการปฏิบัติงานและขั้นตอนการดำเนินงาน

3.1 แผนงานปฏิบัติงาน

หัวข้องาน	เดือนที่ 1				เดือนที่ 2				เดือนที่ 3				เดือนที่ 4			
ศึกษา VMware & OS (Windows server)(Linux)																
ศึกษา Concept Hardening																
Install VMware																
ศึกษา Feature ที่ใช้ในการทำ Hardening																
ทำ Demo เกี่ยวกับ Feature ที่ใช้																
ทำ Hardening ใน - Windows server 2016 - Linux																
ทำการ Test																
ทำรูปเล่มรายงาน																
สรุปผลงาน																
เรียบเรียงจัดทำรูปเล่มรายงาน																

ตาราง 3.1 แผนปฏิบัติงานสหกิจศึกษา

3.2 รายละเอียดโครงงาน

3.2.1 Hardening

การปฏิบัติงานสหกิจศึกษา ข้าพเจ้าได้อยู่ส่วนงานของ System Engineer ของ แผนก SMS จึงมีแผนปฏิบัติงานออกแบบในการเพิ่มความปลอดภัยให้กับ OS และ Server ให้มากขึ้นทำให้ระบบมีความปลอยภัยและมีความน่าเชื่อถือมากยิ่งขึ้น

ภาพที่ 3.2 ดำเนินการเพิ่มความปลอดภัยให้เครื่องของเรา

3.2.2 งานอื่นๆ

3.2.2.1 ทำการศึกษาและทดลองติดตั้ง Linux

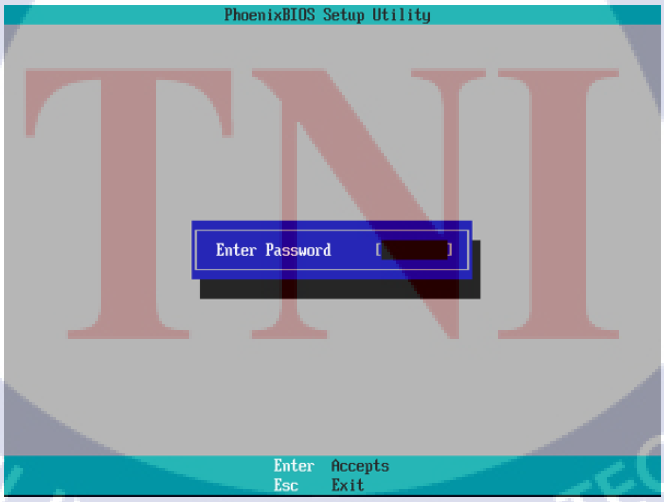
3.2.2.2 ทำการศึกษาและทดลองติดตั้ง Windows Server

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

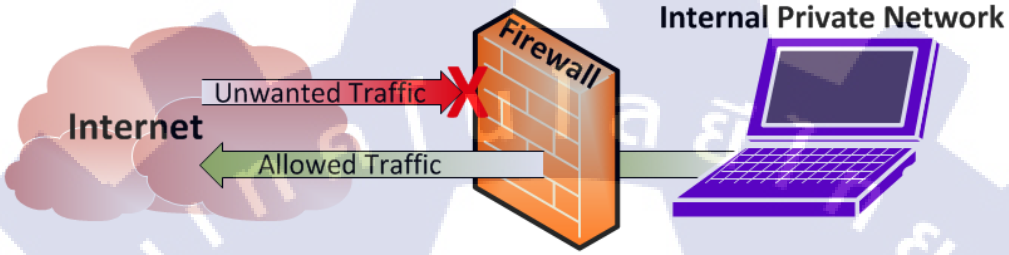
3.3 ขั้นตอนการดำเนิน



ภาพที่ 3.3 ดำเนินการเพิ่มความปลอดภัยให้เครื่องของเรา

3.3.1 ศึกษาข้อมูลที่จำเป็นก่อนการทำการ Hardening

อย่างละเอียด ในด้านความ ต้องการของระบบของ OS ต่างๆ การสร้าง VM เพื่อสร้าง Test System รวมไป ถึงศึกษาซอฟท์แวร์ที่เกี่ยวข้องในด้านวิธีการใช้งานและการติดตั้ง เช่น การติดตั้ง AIX , Linux และการติดตั้ง Windows Server อย่างละเอียดว่าในแต่ละ ระบบนั้นต้องทำอะไรบ้าง 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 โดยที่เครื่องมือที่ว่านี้อาจจะเป็น 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

ไฟร์วอลล์เป็นเครื่องมือที่ทำงานในเชิงการป้องกัน โดย packet ที่จะสามารถผ่านเข้า-ออกได้นั้น จะต้องเป็น packet ที่มันเห็นว่าปลอดภัย หาก packet ใดที่มันเห็นว่าไม่ปลอดภัย มันก็จะไม่อนุญาตให้ผ่าน โดยการตัดสินว่า packet ปลอดภัยหรือไม่นั้นขึ้นอยู่กับกฎพื้นฐานที่ Administrator ได้กำหนดไว้

3.3.1.2.2 Access Control

ไฟร์วอลล์จะควบคุมการ Access ของ Host ต่างๆ ให้เป็นไปตามกฎพื้นฐานที่ Administrator ได้กำหนดไว้

3.3.1.2.3 Rule Base

ไฟร์วอลล์จะทำการควบคุมการ Access โดยอาศัยการเปรียบเทียบคุณสมบัติของ Packet ที่จะผ่านเข้า-ออก กับกฎพื้นฐานที่ Administrator ได้กำหนดไว้ หากพบว่าไม่มีกฎห้ามไว้ก็จะอนุญาตให้ผ่านไปได้ แต่ถ้ามีกฎข้อใดข้อหนึ่งห้ามมันก็จะไม่ยอมให้ผ่าน

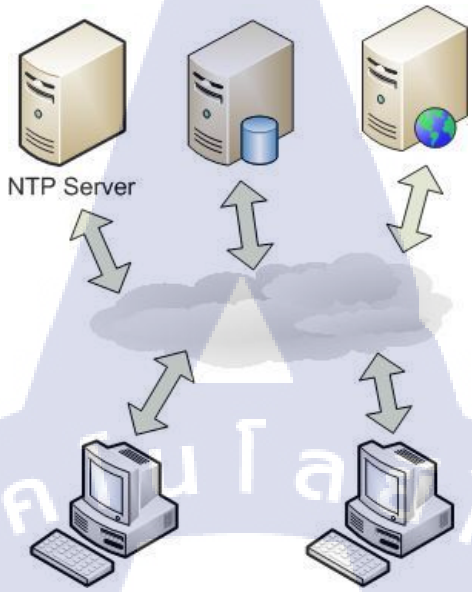
3.3.1.2.4 สิ่งที่ Firewall สามารถป้องกันได้

1. Network Scanning – ด้วยคุณสมบัติที่ Firewall สามารถควบคุมการเข้า-ออก ของ packet ได้ มันจึงสามารถจำกัดปลายทางของ 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 เช่นการทำให้เน็ตเวิร์กท่วมไปด้วยข้อมูล (Network Flooding) ทำการส่ง packet จำนวนมากไปยัง Host เพื่อขอใช้บริการ (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. การดักอ่านข้อมูลโดย Sniffer
7. Spammed Mail
8. Administration Mistake

3.3.2 NTP configuration



ภาพที่ 3.5 การทำงานของ NTP

Network Time Protocol หรือ NTP คือ networking protocol ที่ใช่สำหรับ sync time ของ server ทุกเครื่องใน network ให้ตรงกัน ผ่าน packet-switch ซึ่ง ntp เป็น protocol ที่เก่าแก่มากและมีมาตั้งแต่ 1985 และใช้คงใช้งานจนถึงปัจจุบัน เริ่มต้นคิดค้นโดย David L. Mills ที่ University of Delaware สาเหตุที่ต้องมี NTP นั้นก็เพราะ นาฬิกา หรือ clock ของ server, computer ใน network ไม่ได้เที่ยงตรงเท่ากันหมด บางครั้งการคลาดเคลื่อนกันเพียงหลักวินาทีอาจจะทำให้ application ที่ใช้งานสื่อสารกันผิดพลาดได้ และยิ่งในระบบ server ขนาดใหญ่ที่มีการ run ต่อเนื่องกันเป็นเวลานานหลายปี ย่อมมีความคลาดเคลื่อนไปบ้างอยู่แล้ว เพราะฉะนั้น NTP จึงเข้ามาช่วยในการทำ synchronize computer ในระบบ network เราให้แม่นยำในระดับ 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)

3.3.3 ทดสอบการตั้งค่าทั่วไปของ Hardening

ได้แก่ การตั้งค่ารหัสตั้งแต่ BIOS และ ตั้งค่าการปิด port ที่ไม่จำเป็นต่างๆในเครื่องและทำการเซ็คFirewall เพื่อ Block สิ่งต่างๆที่เข้ามาทาง Internet และ ยังทำการ

3.3.4 ทดสอบ Hardening ที่ตั้งค่าไว้

เช่น ลองล็อกอินเข้าเครื่องที่มีการทำ Hardening เอาไว้ว่า ที่ตั้งค่าเอาไว้แสดงผลยังไง และตรวจสอบดูว่ายังมีช่องโหว่ตรงไหนที่ยังสามารถปิดได้

บทที่ 4
ผลการดำเนินงาน การวิเคราะห์และสรุปผลต่างๆ

4.1 ขั้นตอนและผลการดำเนินงาน

ในช่วงระยะเวลาสองเดือนแรกของการปฏิบัติงานสหกิจศึกษาจะเป็นช่วงของ การศึกษาข้อมูลที่จำเป็นในการลง OS ต่างๆและ Basic command ของ Linux อย่างละเอียดซึ่งเป็นในส่วนของการติดตั้ง OS ที่นำมาใช้งานจะทำการติดตั้งภายใน VM เพื่อนำไปทำ Hardening รวมไปถึงศึกษาการติดตั้งซอฟต์แวร์ เช่น Linux และ Windows Server โดยในช่วงเดือนที่สามเป็นต้นไปได้เริ่มศึกษาการทำ Hardening เพื่อเพิ่มความปลอดภัยให้แก่เครื่องของเราลงใน 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 คือการลดความเสี่ยงที่จะเกิดให้ได้มากที่สุดเพื่อเพิ่มความมั่นใจในระบบปฏิบัติการและป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตอีกทั้งยัง ป้องกันผู้บุกรุก แฮกเกอร์ และช่องโหว่ด้านความปลอดภัยอื่น ๆ

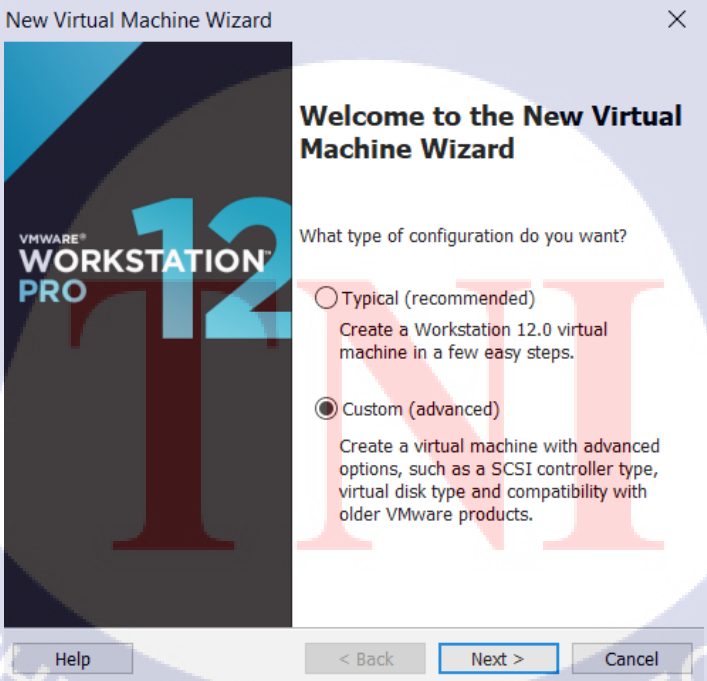
OS Hardening ทำให้ระบบคอมพิวเตอร์เชื่อถือได้มากขึ้น มีความปลอดภัย และช่วยเพิ่มประสิทธิภาพการทำงานเนื่องจาก "ลดสิ่งที่ไม่ได้ใช้ออกไปจากระบบ" การทำ Hardening นั้นเมีต้นทุนและค่าใช้จ่ายที่ต่ำมาก เพราะไม่ต้องซื้อ Hardware หรือ Software ราคาแพงเราก็สามารถเพิ่มความปลอดภัยให้กับคอมพิวเตอร์ของเราได้เพียงแค่เรานำเอา Security Best Practice ของระบบปฏิบัติการที่เราใช้อยู่นำมาลงมืออีกทั้งมองในมุมมองขององค์กรด้วยแล้ว กระบวนการทำ Hardening เป็นหนึ่งในส่วนสำคัญในการสร้างมาตรฐานของการบริหารจัดการระบบรักษาความปลอดภัยข้อมูลอย่างเป็นระบบและมีประสิทธิภาพ

4.1.1.1 ติดตั้ง Windows Server

- ทำการสร้าง Virtual Machine ด้วยการกดปุ่ม Create a New Virtual Machine

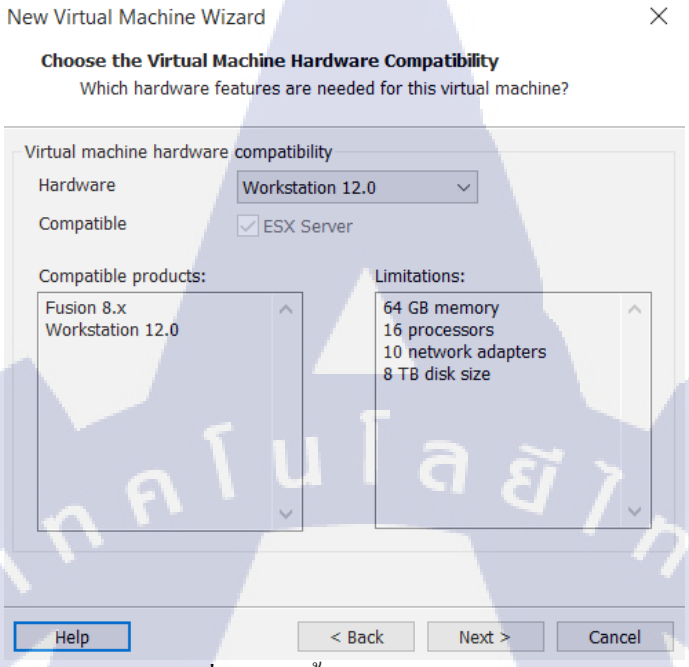
ภาพที่4.1 การสร้าง Virtual Machine(1)

- เลือกแบบ Custom เพื่อทำการตั้งค่าต่างๆ



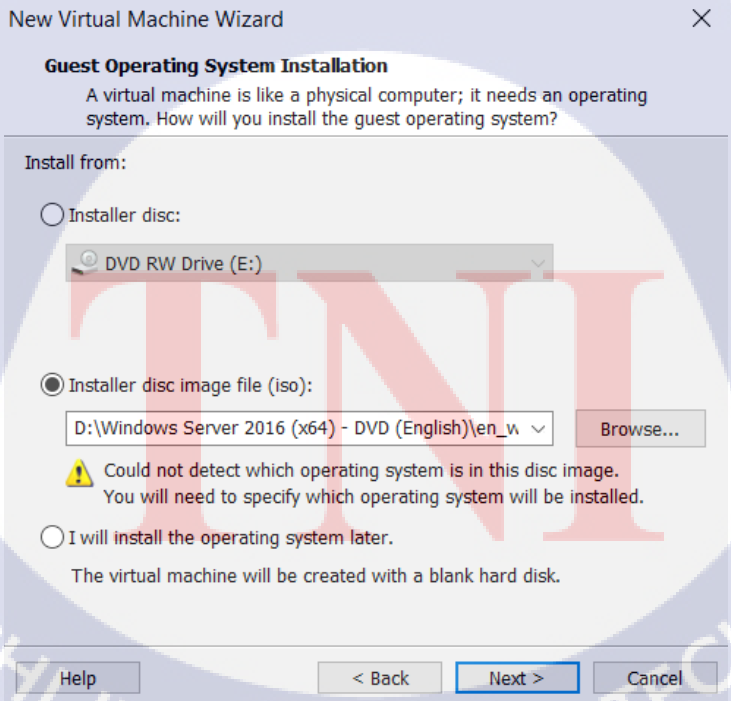
ภาพที่4.2 การสร้าง Virtual Machine(2)

- ให้เลือก Hardware เป็น Version ที่ตรงกับเราในที่นี้เลือกเป็น 12.0



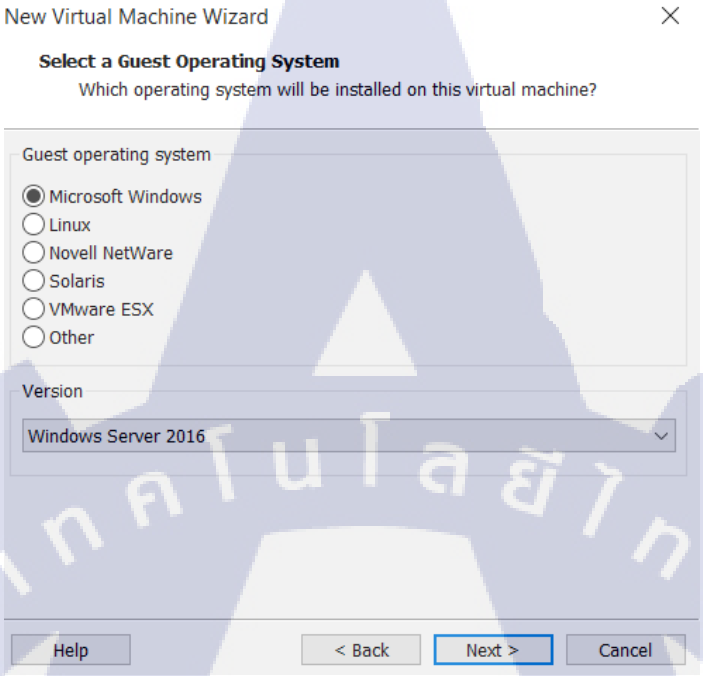
ภาพที่4.3 การตั้งค่า Virtual Machine(3)

- เลือกแผ่นหรือไฟล์ที่เราทำการเก็บ Windows Server ไว้



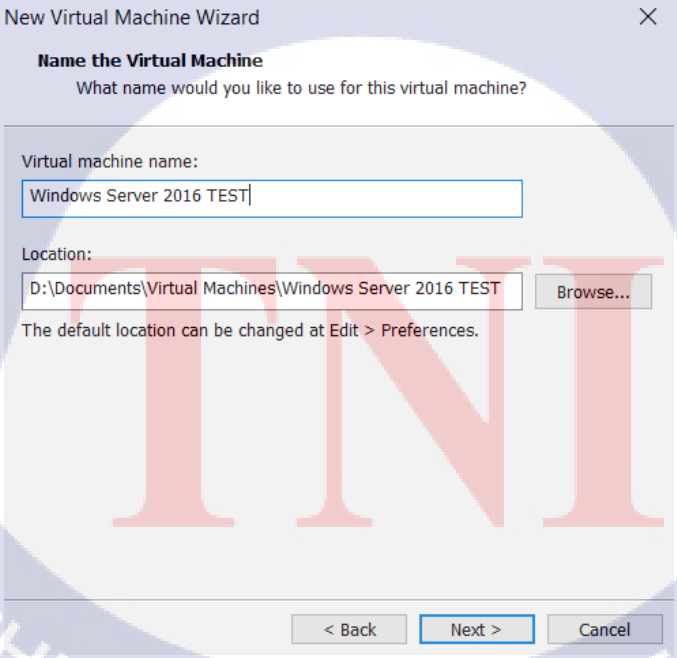
ภาพที่4.4 การเลือกลง Windows Server

- เลือก Windows Server แล้วเลือก Version ที่จะลงในที่นี้เลือก Window Server 2016



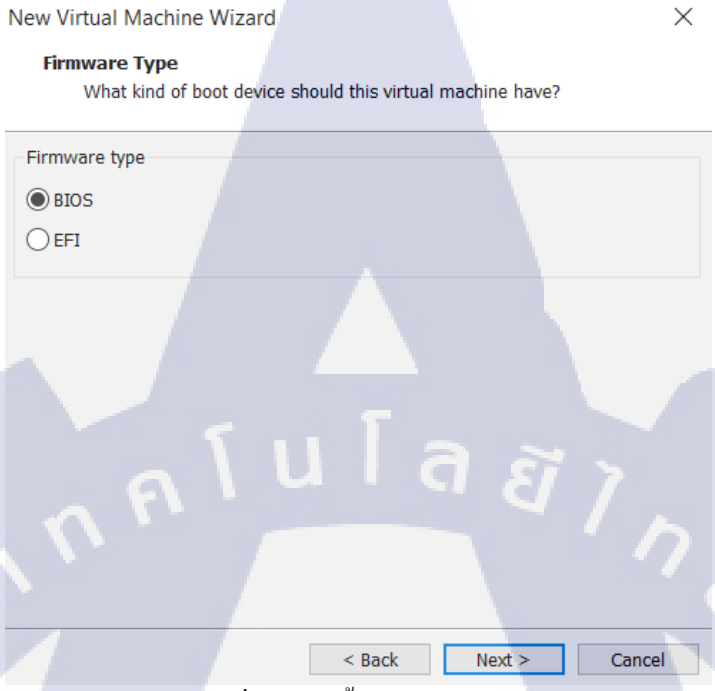
ภาพที่4.5 การตั้งค่า Virtual Machine(4)

- ตั้งชื่อและระบุที่อยู่ให้กับ VM ที่เรากำลังจะสร้าง



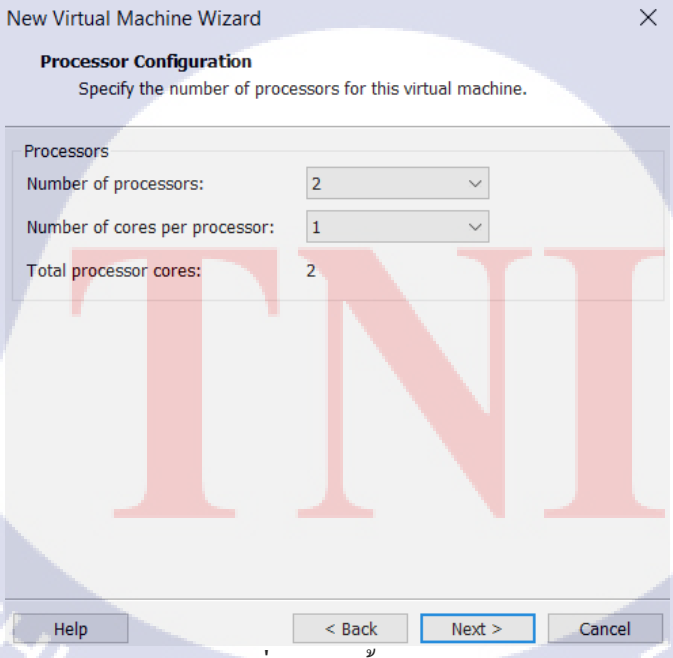
ภาพที่4.6 การระบุที่อยู่ของไฟล์ Virtual Machine

- เลือก BIOS แล้วกด Next



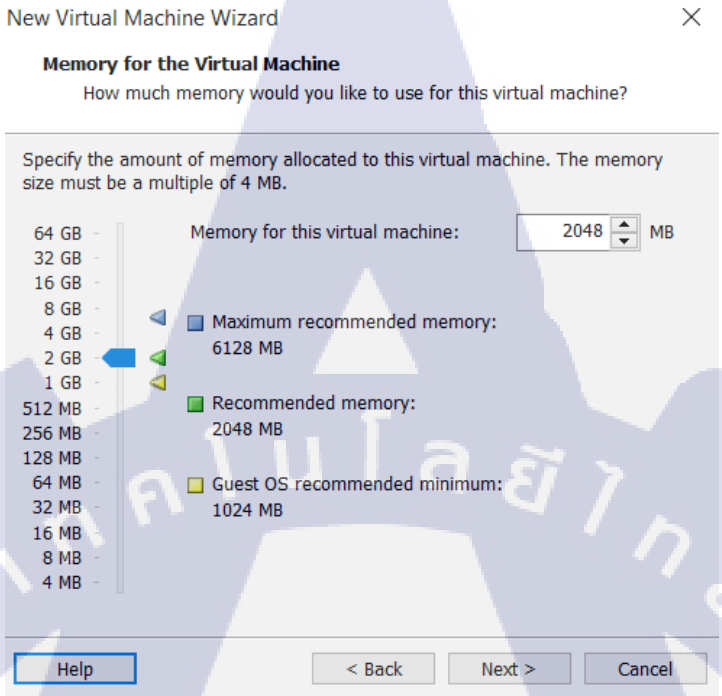
ภาพที่4.7 การตั้งค่า Virtual Machine(5)

- เลือกจำนวน Core ให้กับ VM



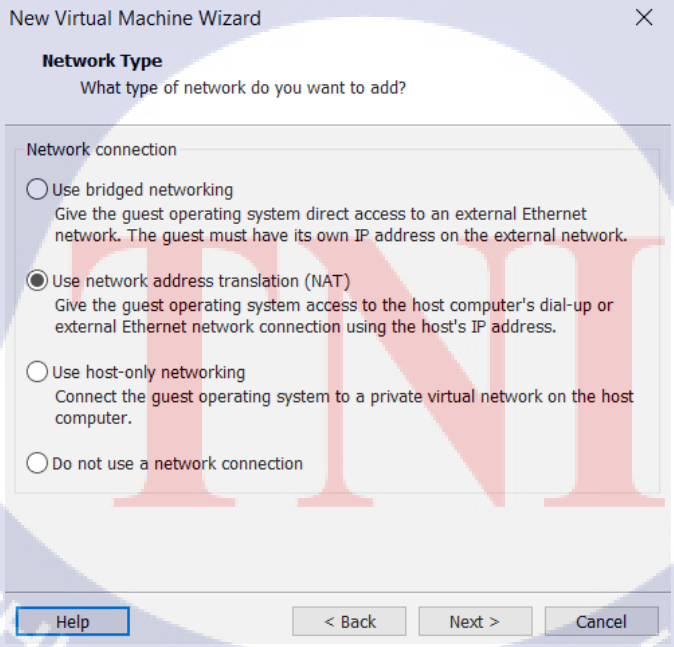
ภาพที่4.8 การตั้งค่า Windows Server(6)

- เลือกจำนวน Ram ให้กับ VM



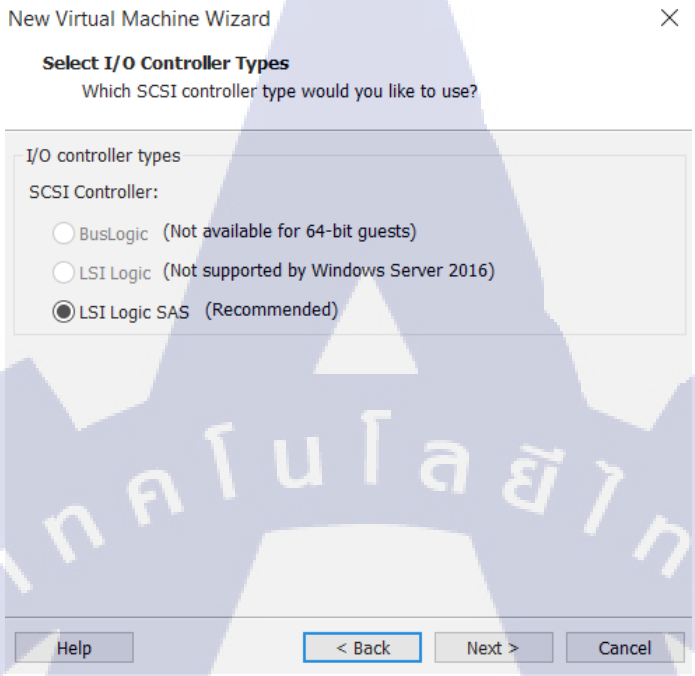
ภาพที่4.9 การให้ Memory กับ VM

- เลือก Network แบบ NAT



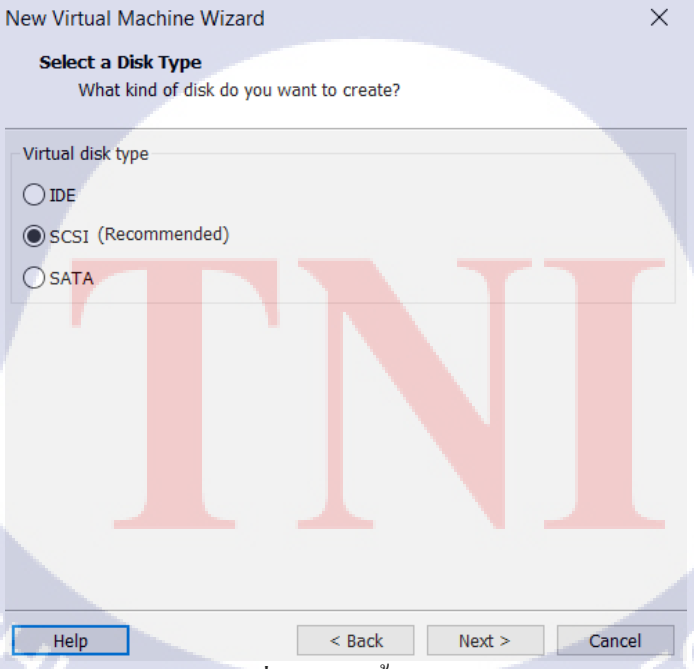
ภาพที่4.10 การตั้งค่า Network

- เลือกI/O Controller แบบ SAS



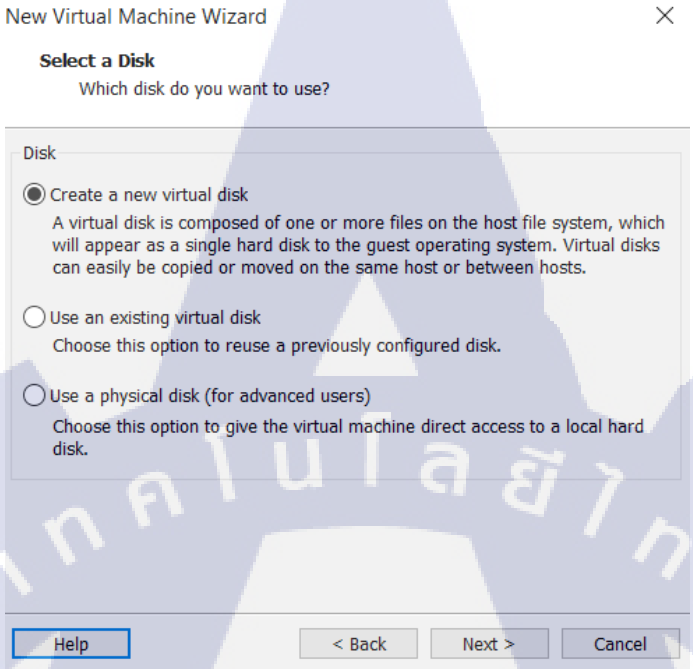
ภาพที่4.11 การตั้งค่า I/O

- เลือกการทำงาน Disk แบบ SCSI



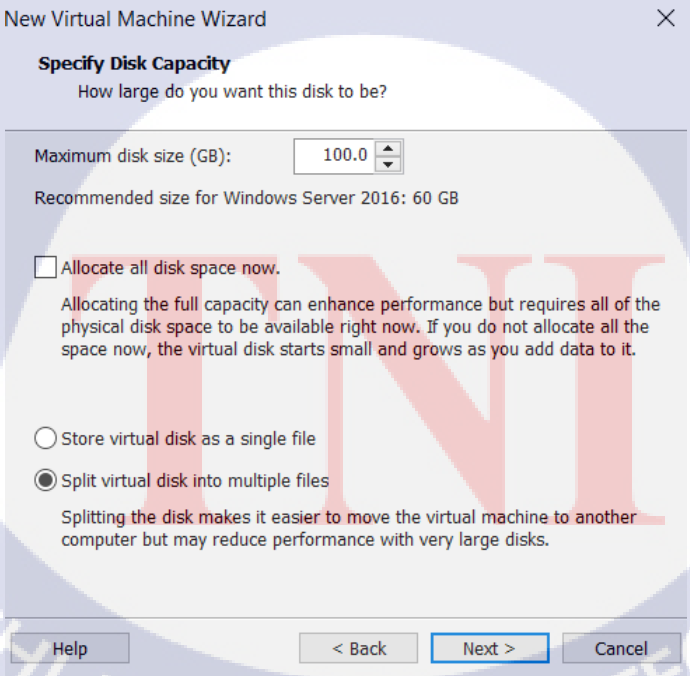
ภาพที่4.12 การตั้งค่า Disk type

- เลือก Create a new virtual disk เพื่อสร้าง



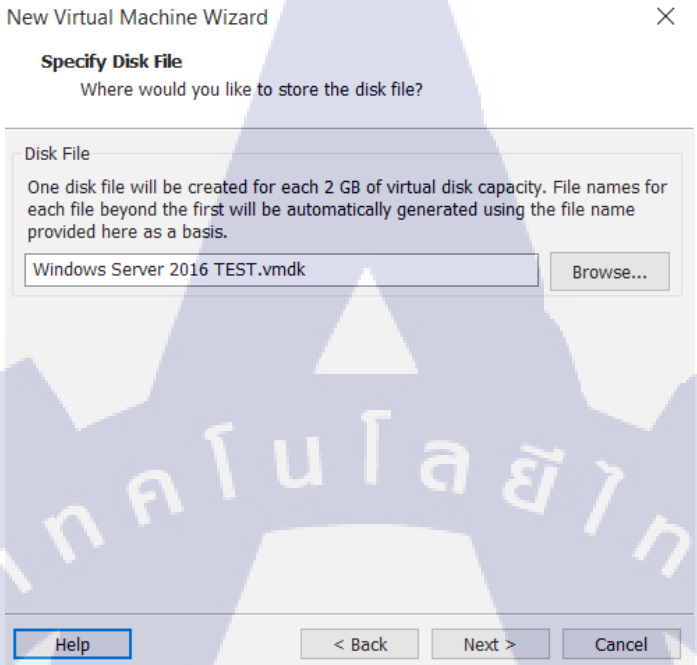
ภาพที่4.13 การสร้าง VM

- เลือกพื้นที่ให้กับ VM เป็นแบบ Split disk



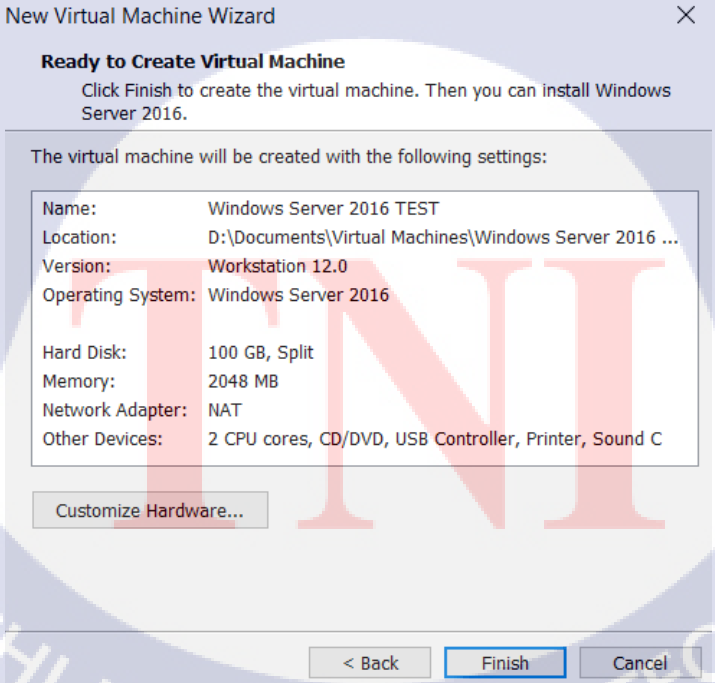
ภาพที่4.14 การตั้งค่าพื้นที่ให้Windows Server

- ตั้งชื่อ Disk



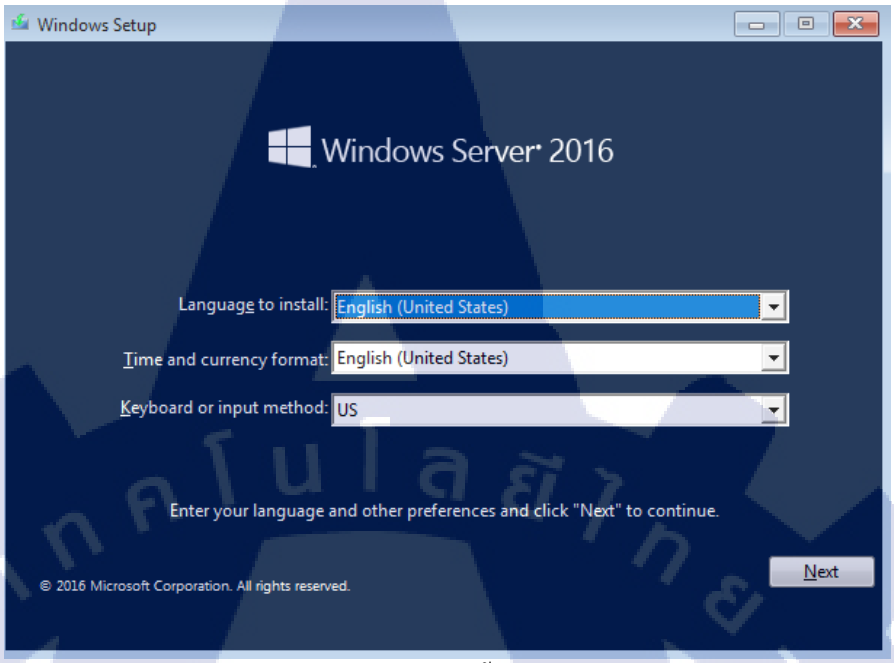
ภาพที่4.15 การตั้งชื่อให้กับ VM

- ตรวจเช็คดูว่าเป็นไปตามที่เราตั้งค่าไว้ไหม



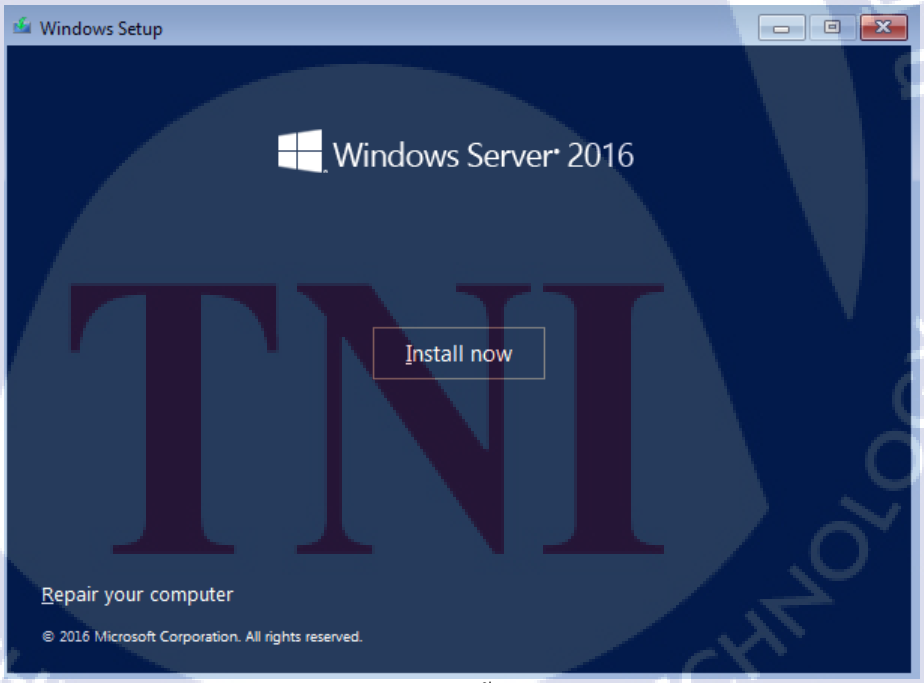
ภาพที่4.16 ตรวจเช็คการตั้งค่า

- เลือกภาษา



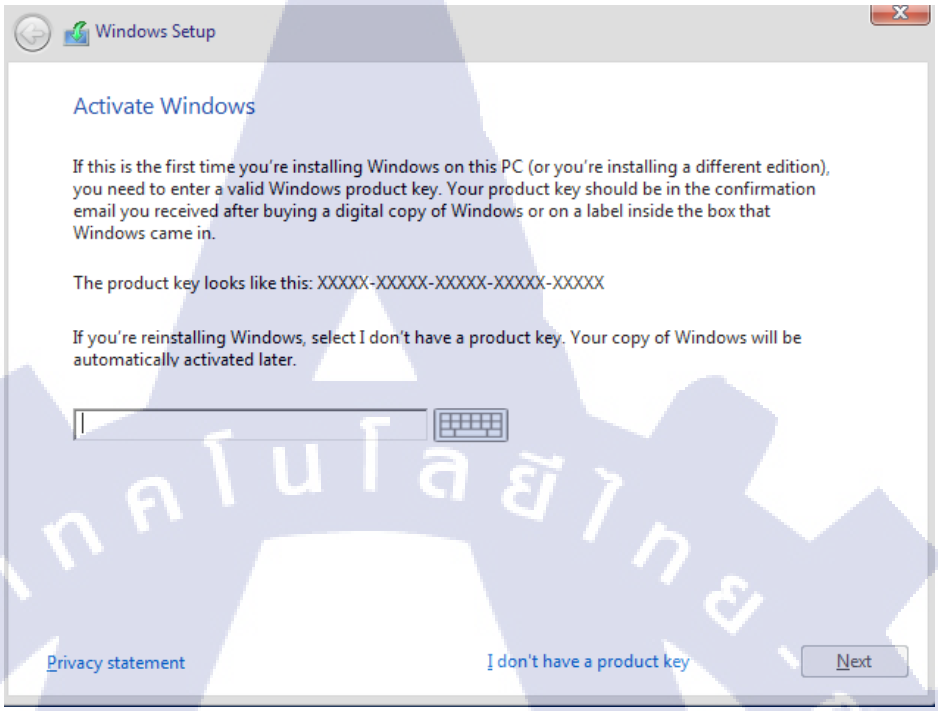
ภาพที่4.17 การติดตั้ง Windows Server

- กด Install now



ภาพที่4.18 การติดตั้ง Windows Server

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

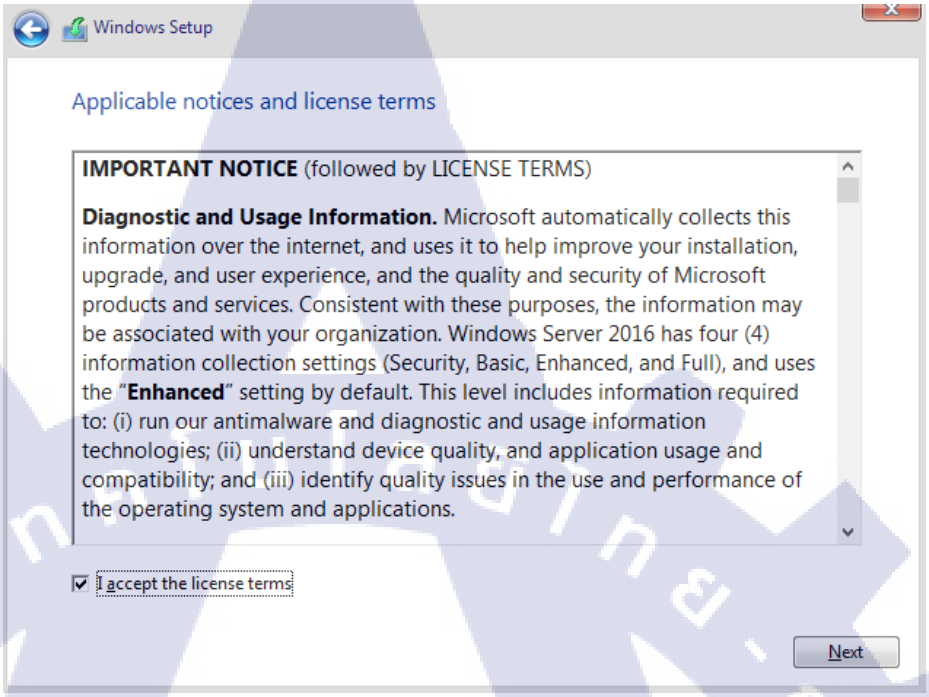


ภาพที่4.19 การใส่ Key Windows Server

- เลือก Windows Server 2016(Desktop Experience)

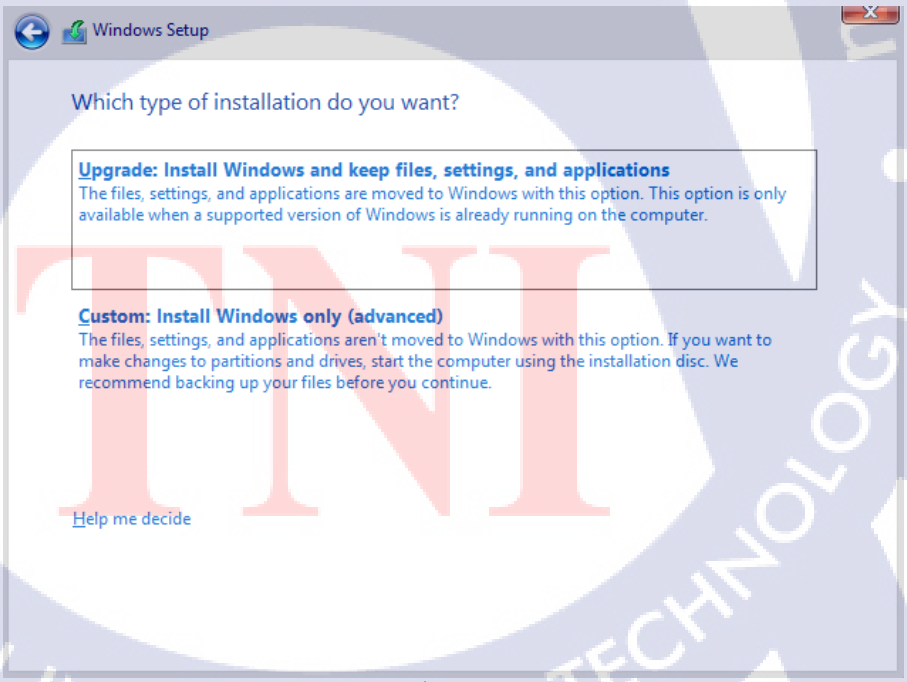
ภาพที่4.20 การตั้งค่า Windows Server

- กด accept license



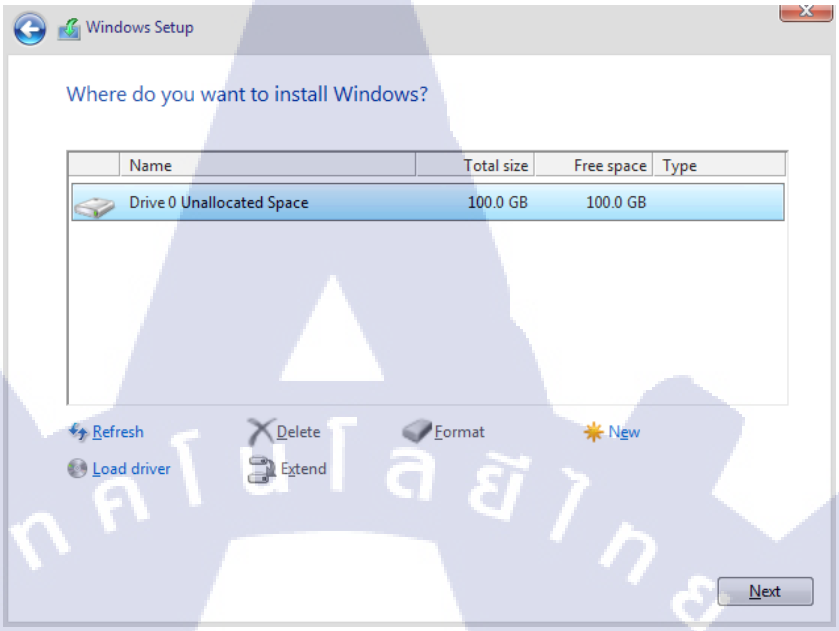
ภาพที่4.21 การยอมรับ license ของ Windows Server

- เลือก Custom



ภาพที่4.22 การตั้งค่า Windows Server

- กด Next

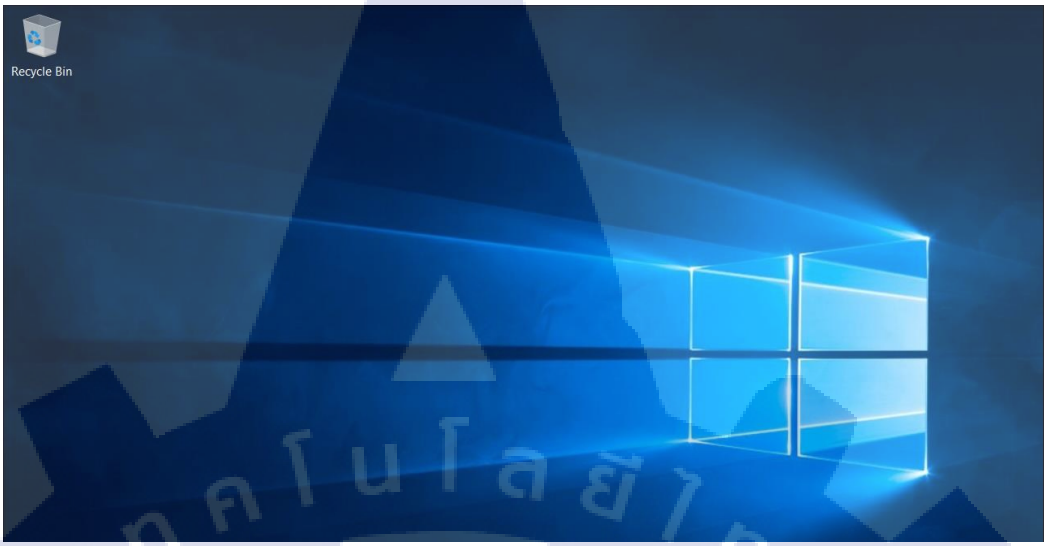


ภาพที่4.23 การแบ่ง Disk Windows Server

- รอการติดตั้ง

ภาพที่4.24 Install Windows Server

- ลงเสร็จจะได้หน้าจอ window เป็นอันเสร็จ

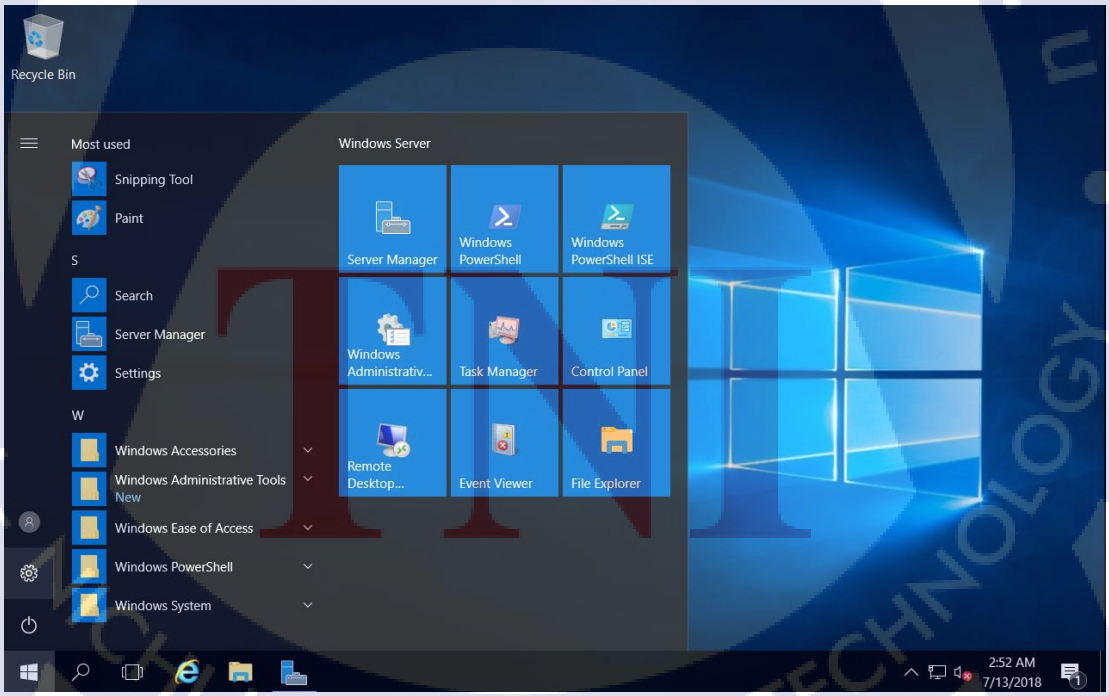


ภาพที่4.25 หน้าตาของ Windows Server

4.1.1.2 Hardening Windows Server 2016

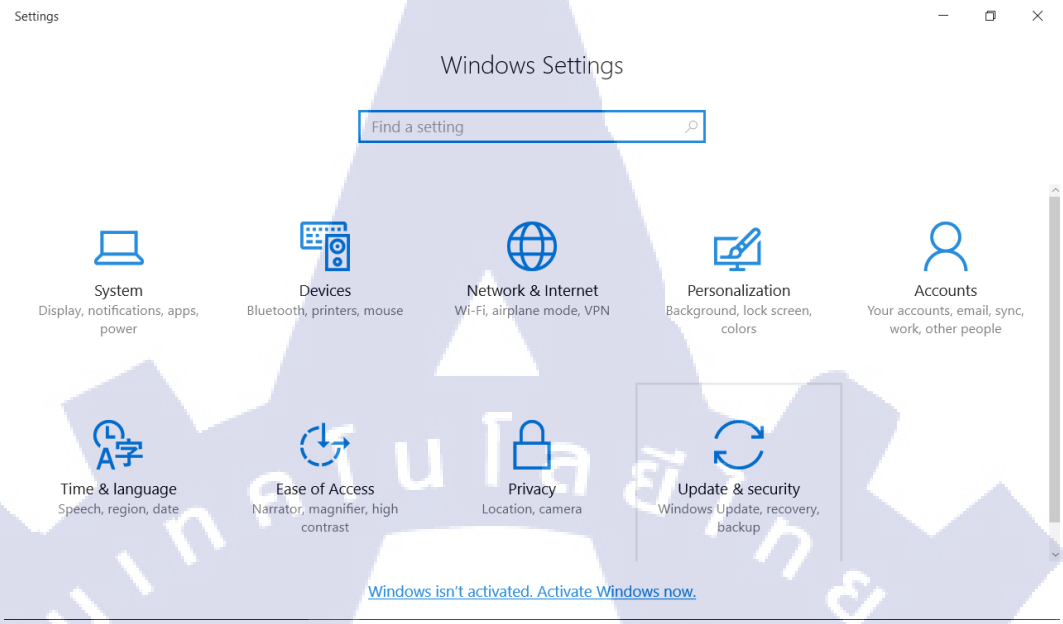
4.1.1.2.1 Window update

- เข้าไปที่ Setting



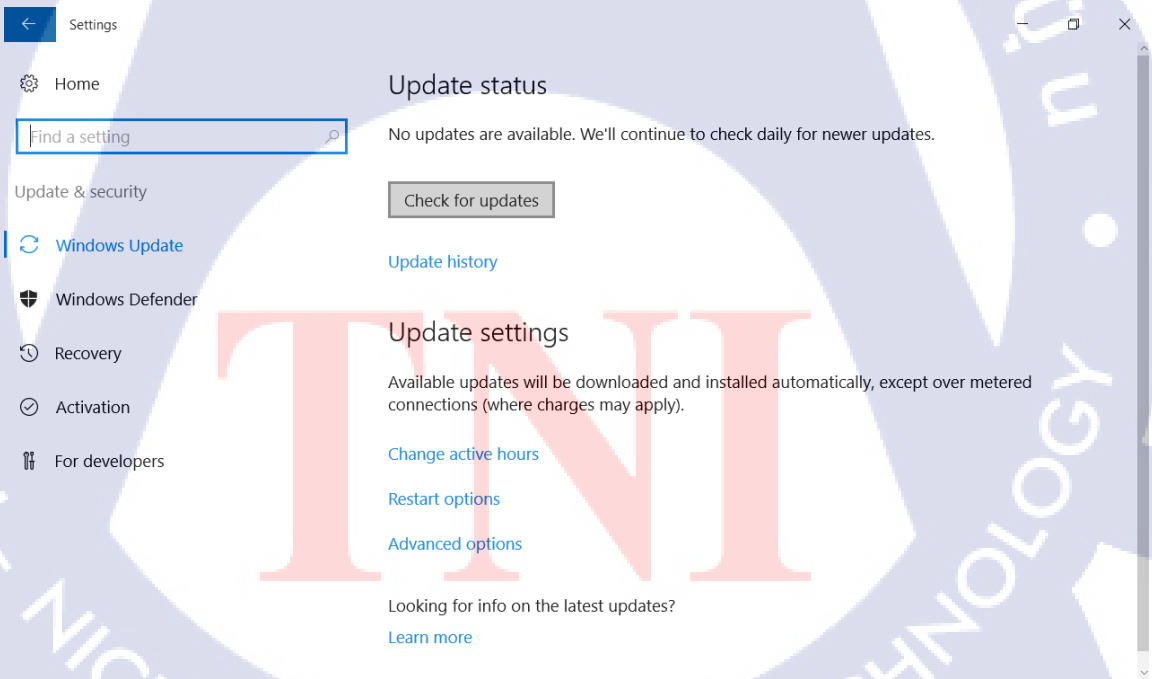
ภาพที่4.26 window update(1)

- เลือก Update & Security



ภาพที่4.27 window update(2)

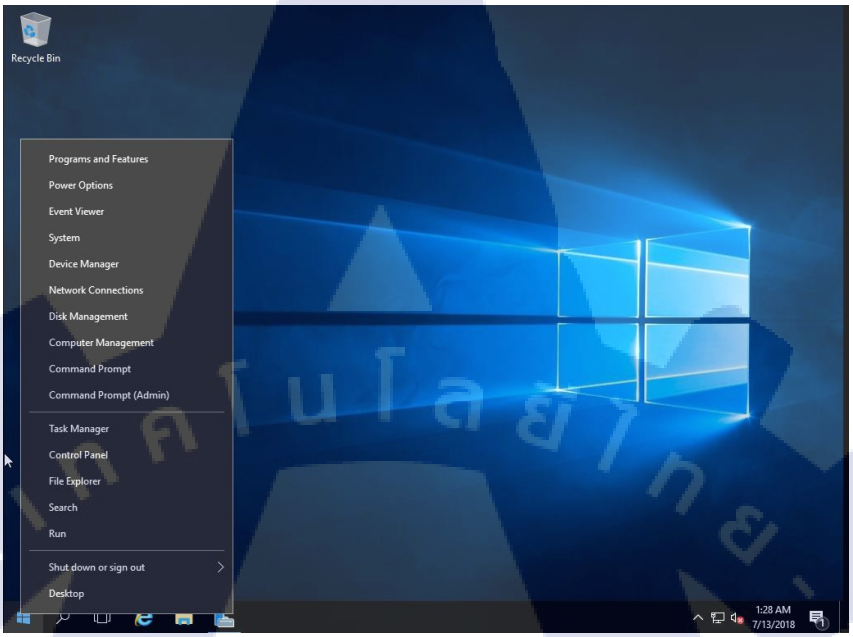
- กด Check for updates



ภาพที่4.28 window update(3)

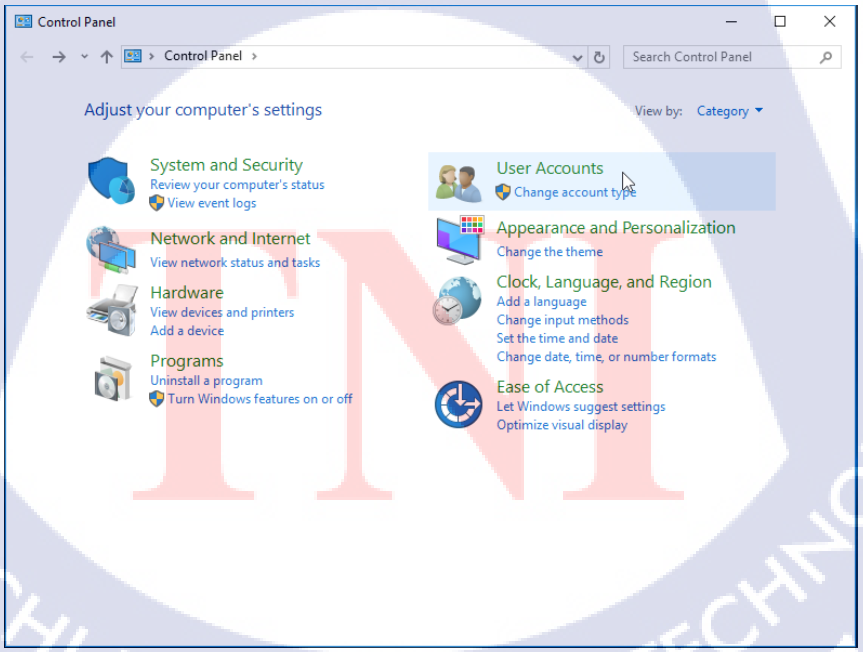
4.1.1.2.2 User Configuration

- เข้าไปที่ Control Panel



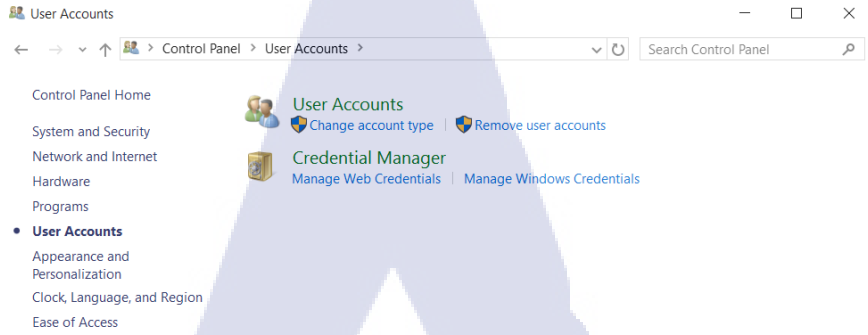
ภาพที่4.29 user configuration

- เข้าไปที่ User Accounts



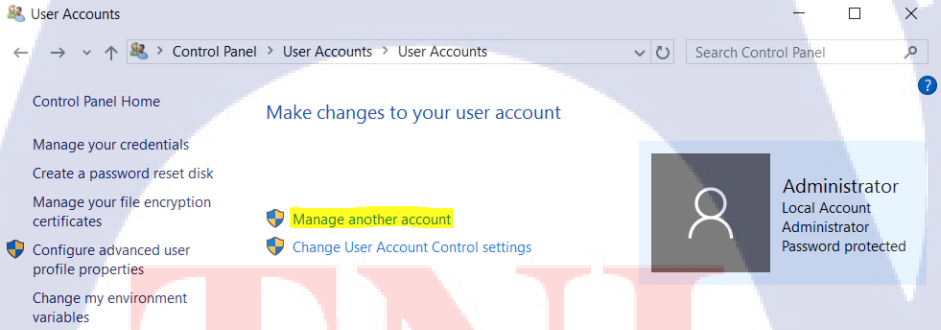
ภาพที่4.30 Control panel

- เลือกไปที่ User Accounts



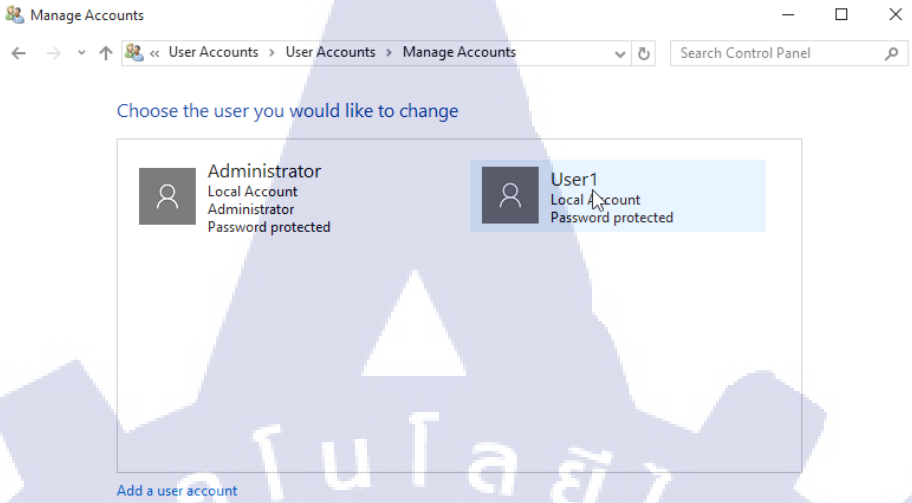
ภาพที่4.31 หน้า Control panel ของ user accounts

- เลือก Manage another account



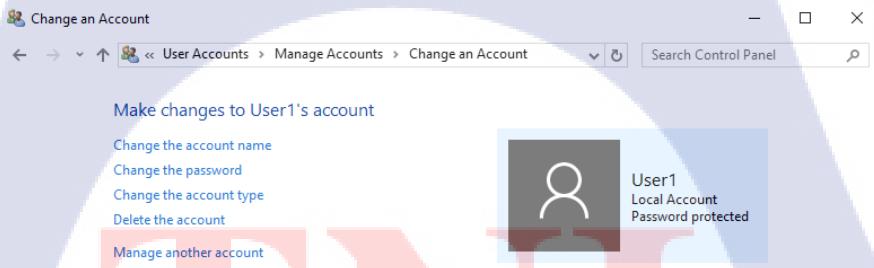
ภาพที่4.32 User Accounts Setting

- เลือก User ที่ต้องการเข้าไปจัดการ



ภาพที่4.33 เลือก User

- สามารถเปลี่ยนชื่อ,เปลี่ยนรหัส,เปลี่ยนสิทธิและลบได้



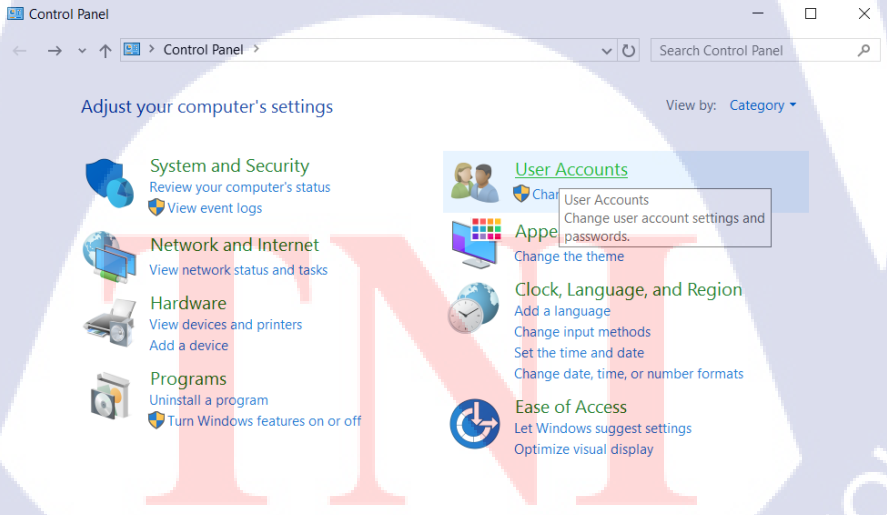
ภาพที่4.34 หน้า Manage account

4.1.1.2.3 Further Hardening

- เข้าไปที่ Control Panel

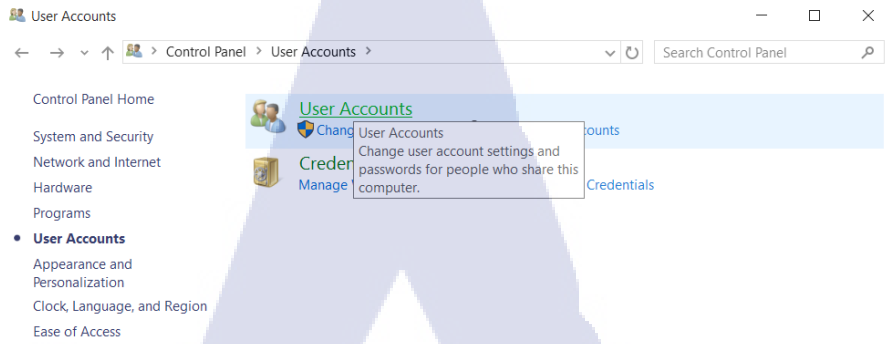
ภาพที่4.35 เข้า Control panel

- เข้าไปที่ User Accounts



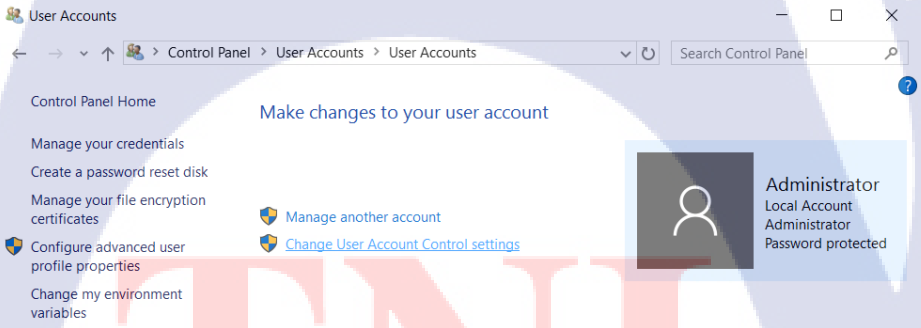
ภาพที่4.36 User Accounts(1)

- เลือก Manage another account



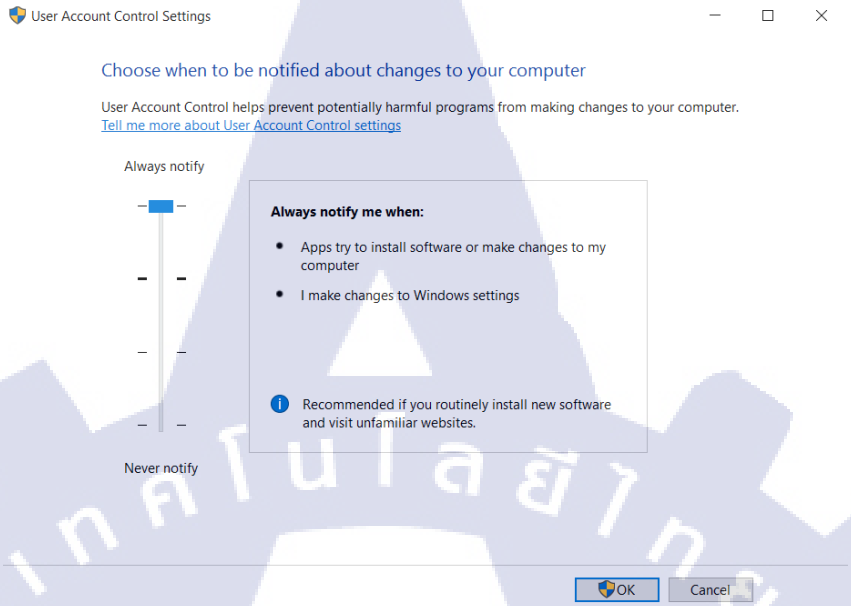
ภาพที่4.37 User Accounts(2)

- เลือก Change User Account Control settings



ภาพที่4.38 Account control setting

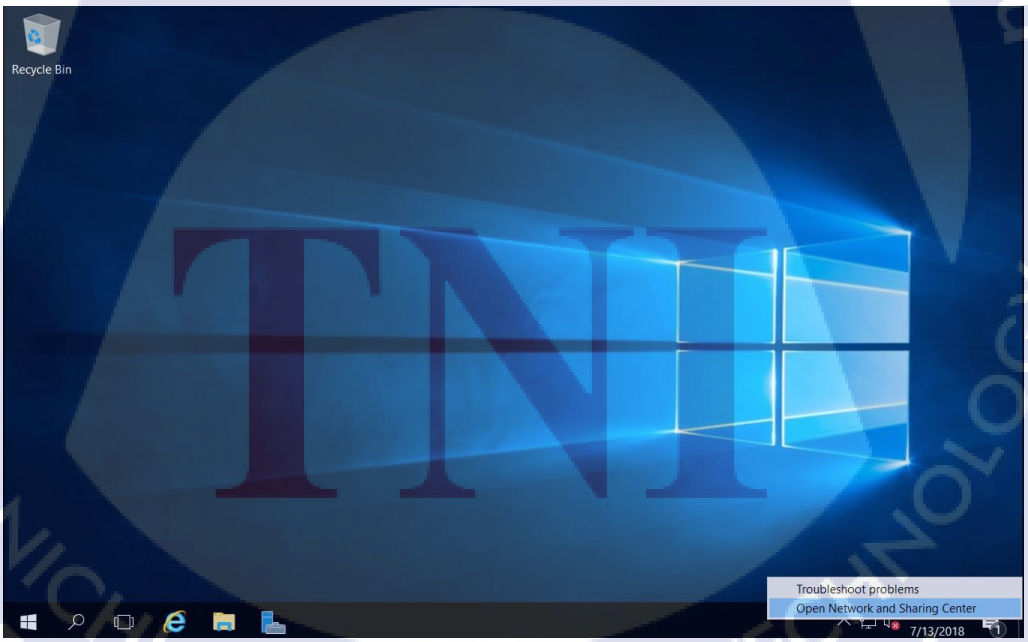
- เลื่อนขึ้นไปให้เป็น Always notify



ภาพที่4.39 Set ค่า User Account Control Setting

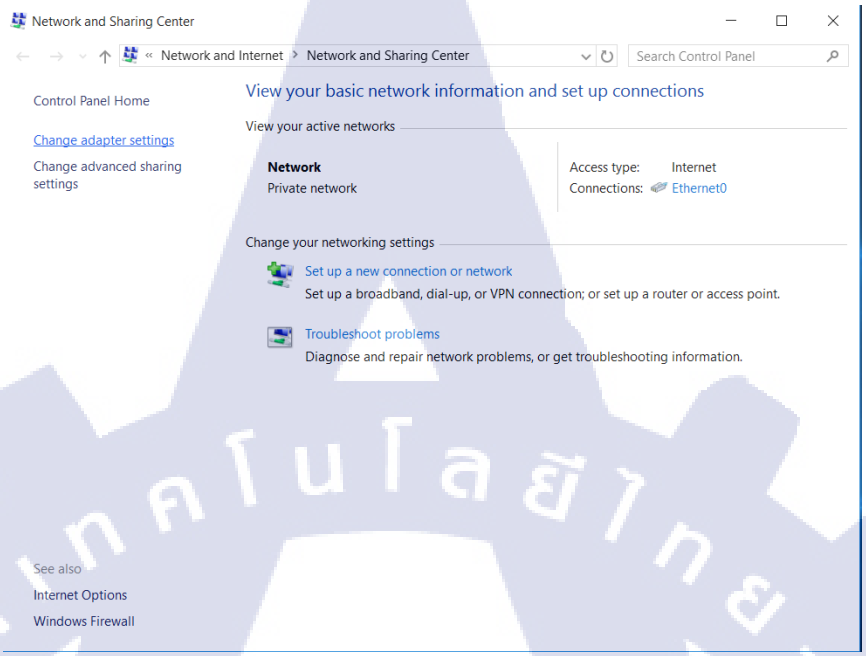
4.1.1.2.4 Network Configuration

- คลิกซ้ายที่ Network logo แล้ว เลือก Open Network and Sharing Center



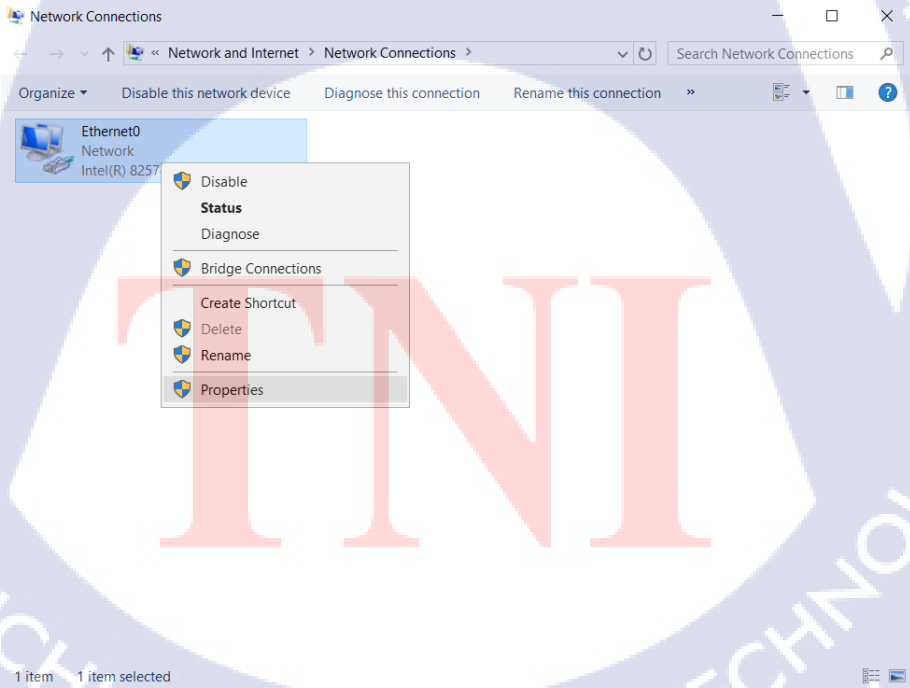
ภาพที่4.40 คลิกเปิด Network and Sharing Center

- เข้าไปที่ Change adapter settings



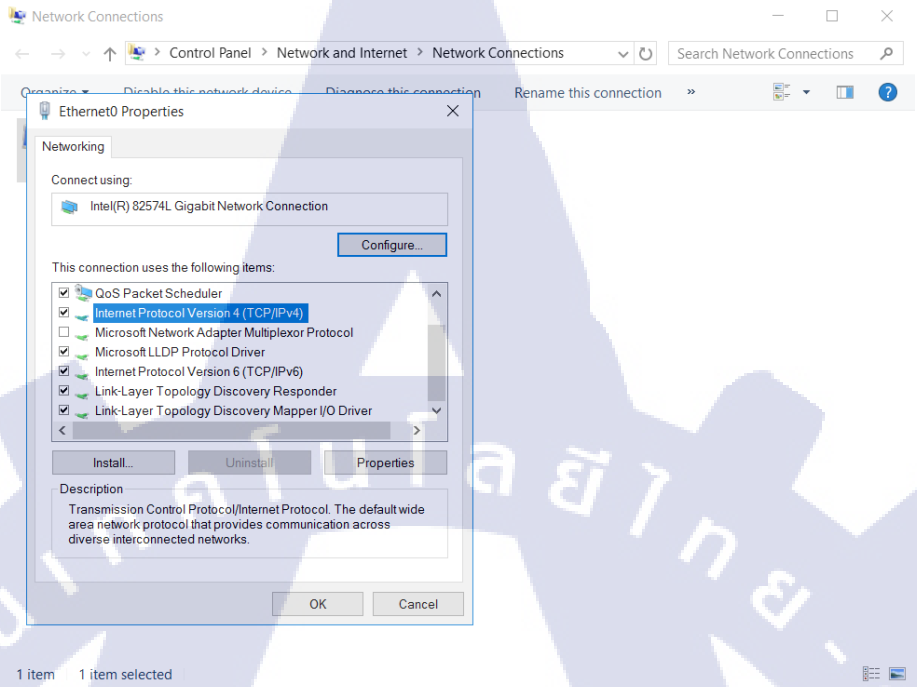
ภาพที่4.41 หน้า Network and Sharing Center

- เลือก Properties



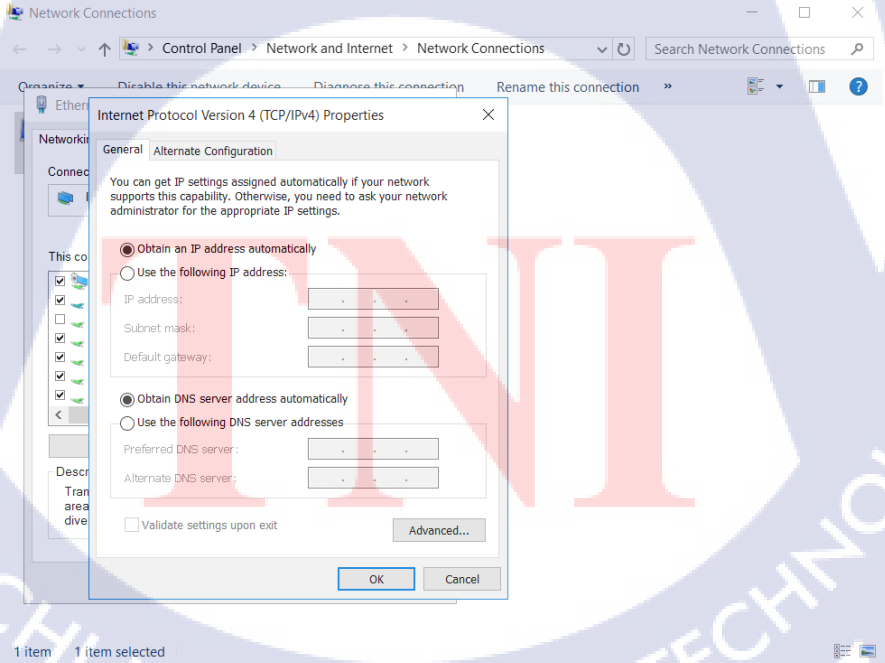
ภาพที่4.42 Network Connection

- เลือก IPV 4



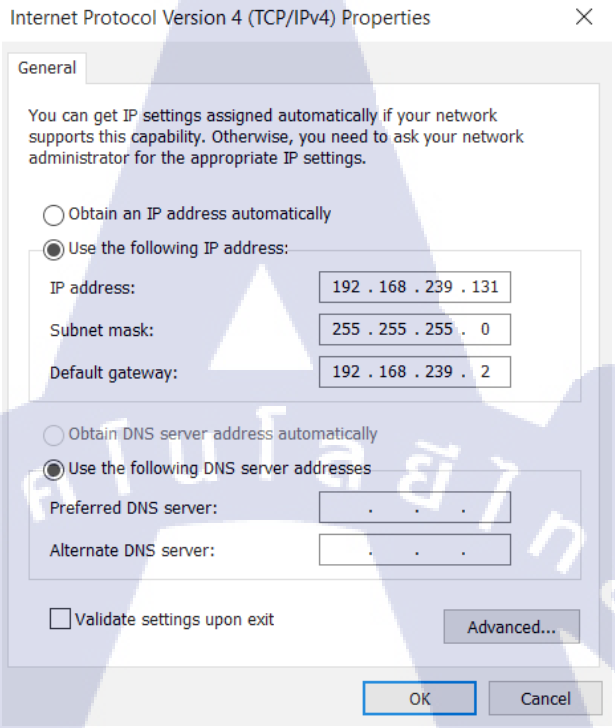
ภาพที่4.43 IP setting(1)

- เลือกใช้แบบใส่ IP เอง



ภาพที่4.44 IP setting(2)

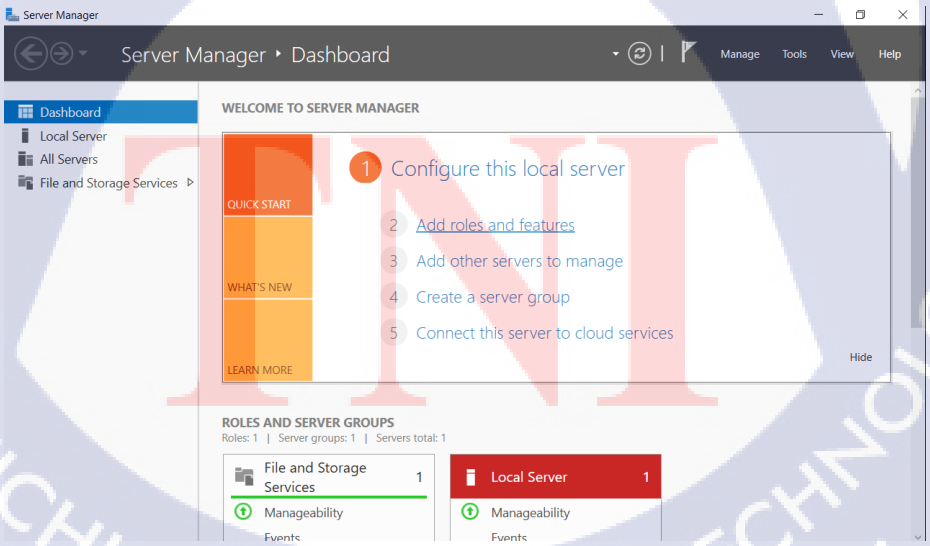
- ทำการตั้ง IP Address ที่เราต้องการเพื่อกำหนดช่องทางและดูแลการเชื่อมต่อ



ภาพที่4.45 IP setting(3)

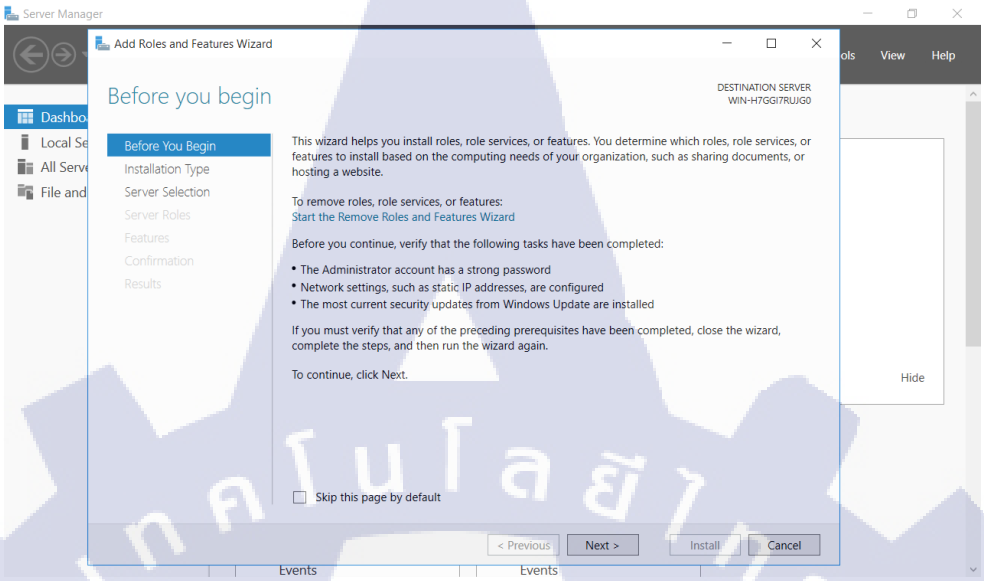
4.1.1.2.5 Features and Roles Configuration

- เลือก Add roles and Features



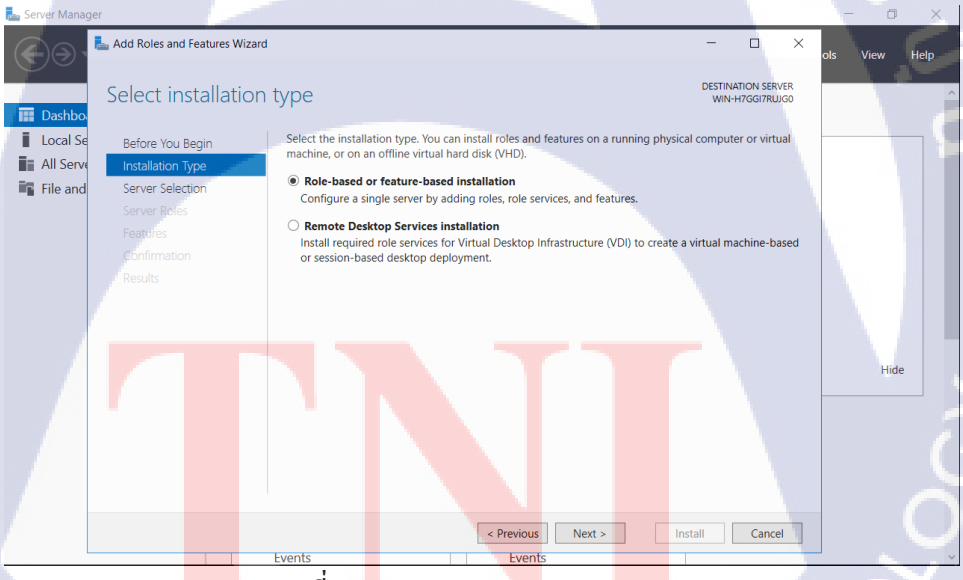
ภาพที่4.46 Add roles and features(1)

- กด Next



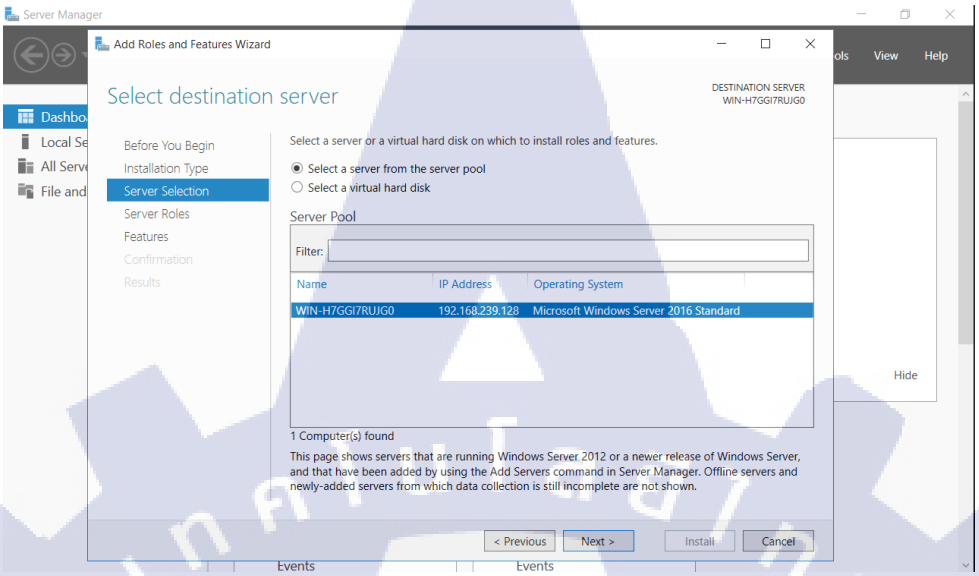
ภาพที่4.47 Add roles and features(2)

- เลือก Role-based or feature-based installation



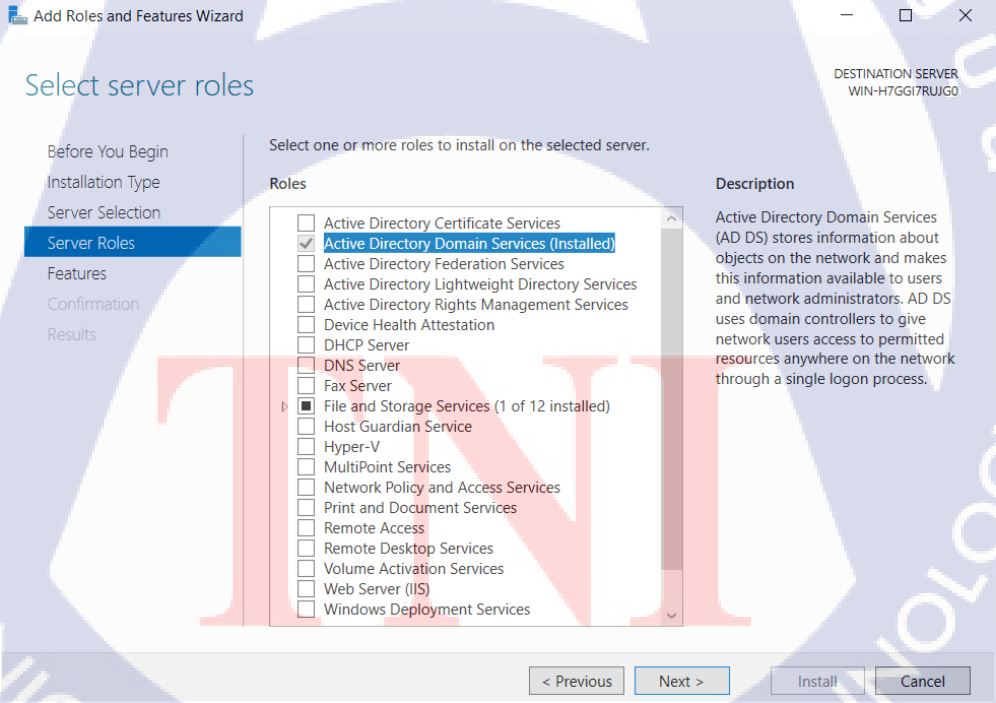
ภาพที่4.48 Add roles and features(3)

- เลือก Server จาก Server Pool



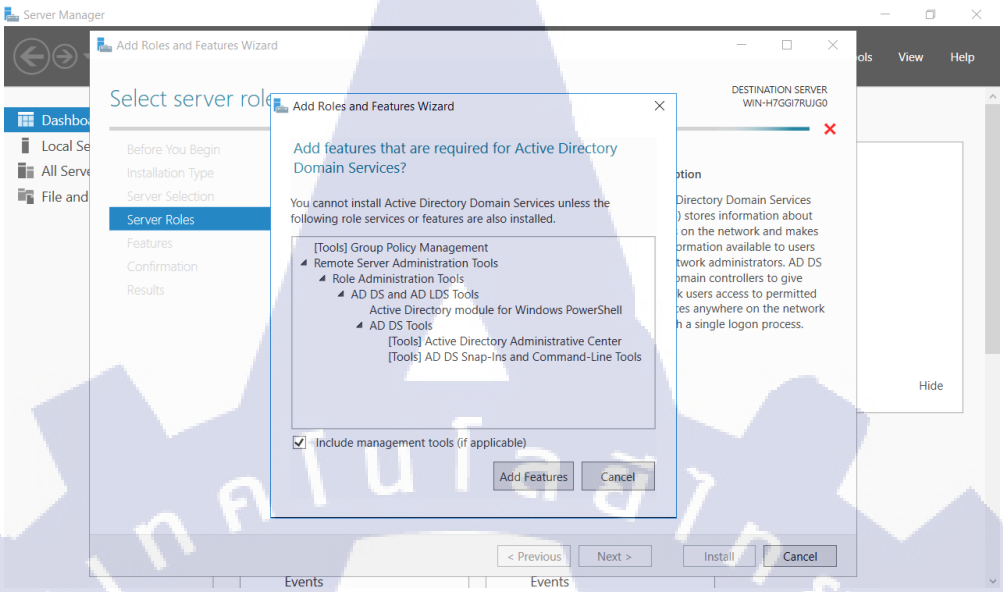
ภาพที่4.49 Add roles and features(4)

- ทำการเลือก Roles ที่ต้องการ



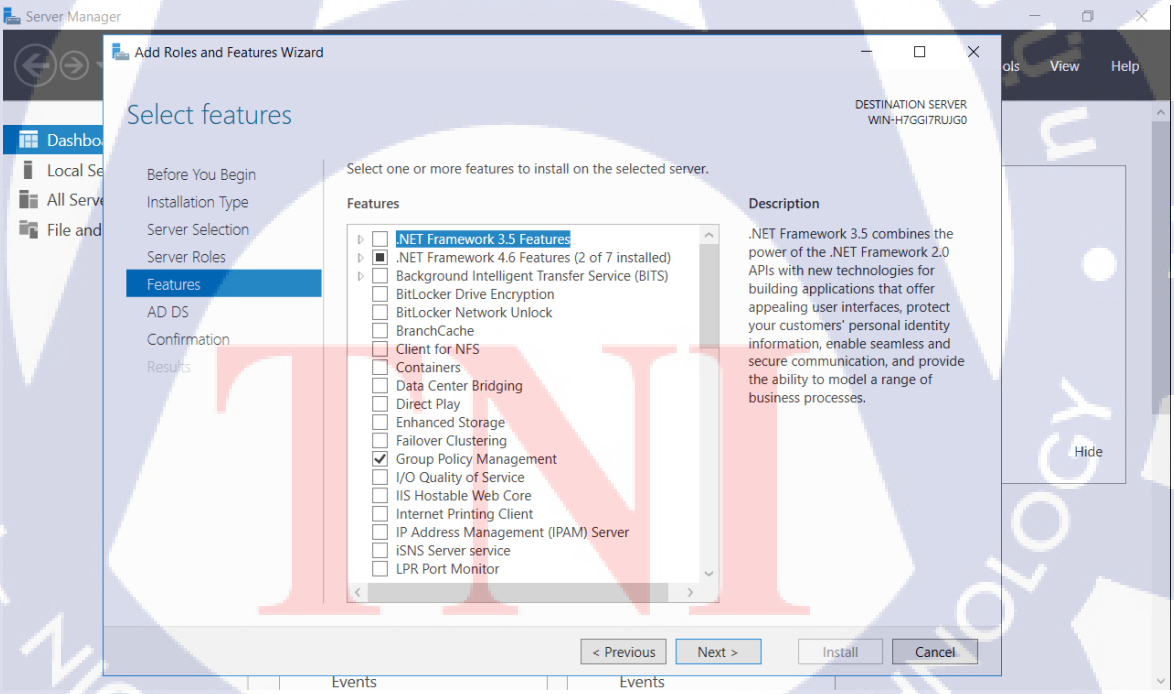
ภาพที่4.50 Add roles and features(5)

- ให้กด Add Features



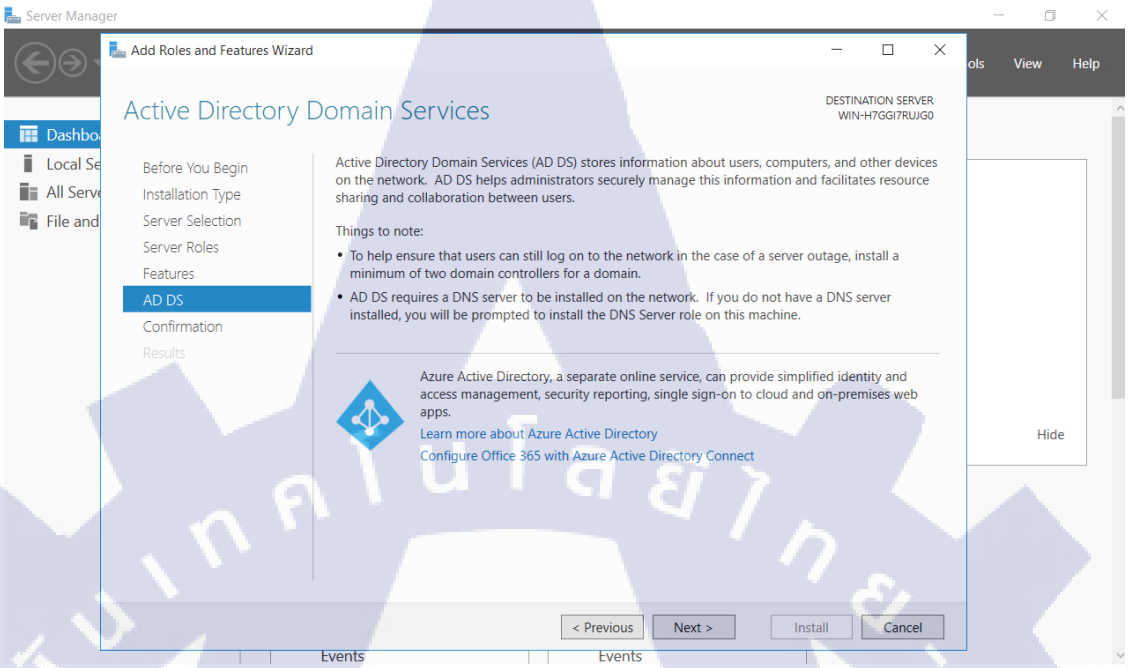
ภาพที่4.51 Add roles and features(6)

- ให้เลือก Feature ที่ต้องการ



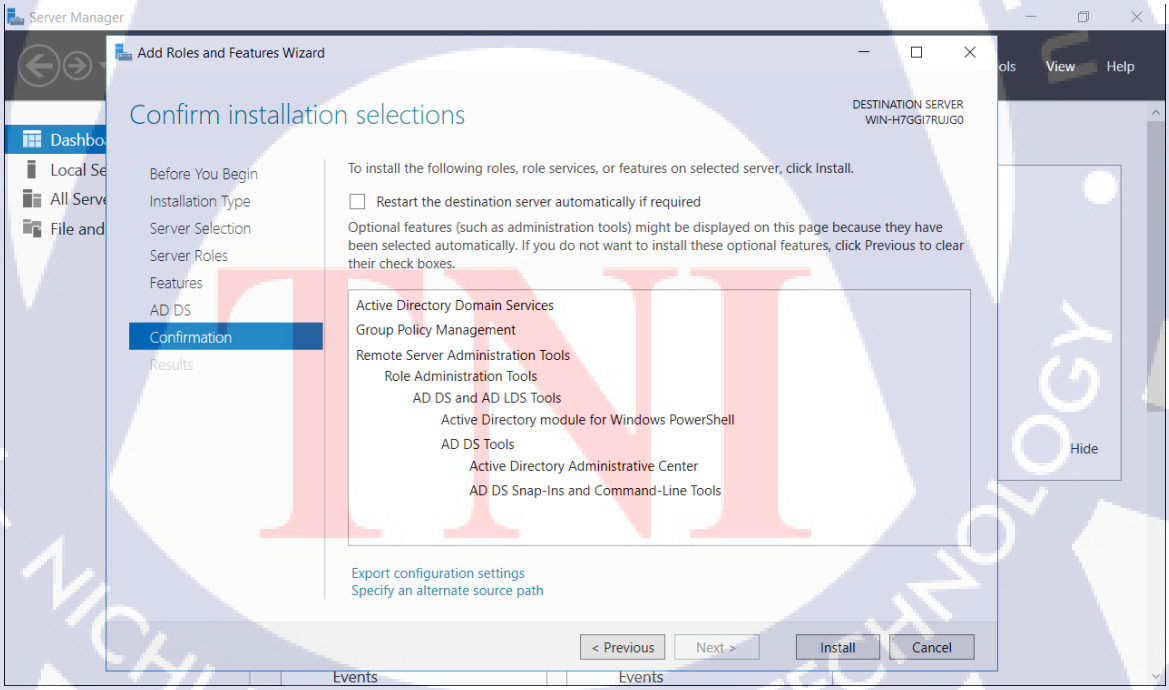
ภาพที่4.52 Add roles and features(7)

- ในกรณีที่ Add เพิ่มเข้ามาจะมีการอธิบายให้กด Next



ภาพที่4.53 Add roles and features(8)

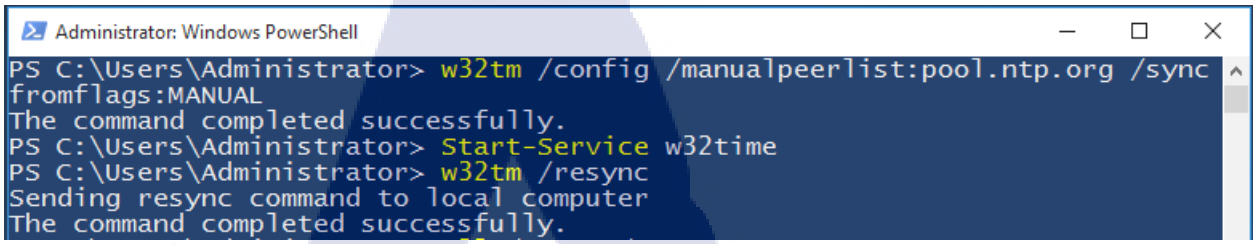
- กด Install



ภาพที่4.54 Add roles and features(9)

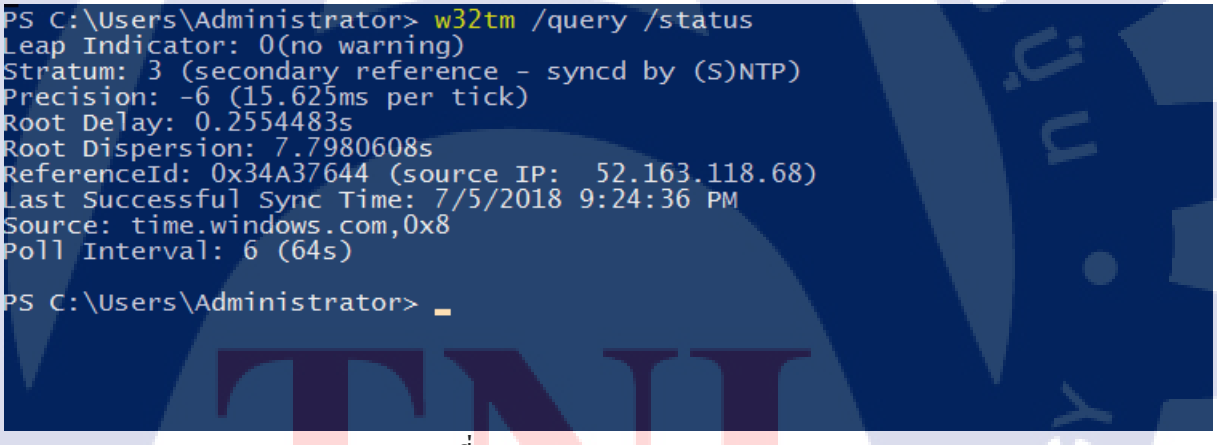
4.1.1.2.6 NTP Server Configuration

- NTP(Network Time Protocol)ใช้สำหรับ sync time ของ server ทุกเครื่องใน network ให้ตรงกัน ผ่าน packet-switch



ภาพที่4.55 NTP Setting(1)

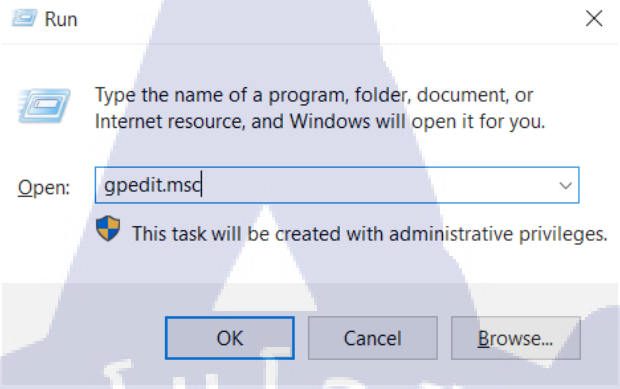
สาเหตุที่ต้องมี NTP นั้นก็เพราะ นาฬิกา หรือ clock ของ server, computer ใน network ไม่ได้ตรงเท่ากันหมด ถ้าเกิดการคลาดเคลื่อนกันเพียงหลักวินาทีก็อาจจะทำให้ application ที่ใช้งานสื่อสารกันผิดพลาดได้ และยิ่งในระบบ server ขนาดใหญ่ที่มีการ run ต่อเนื่องกันเป็นเวลานานหลายปี ย่อมมีความคลาดเคลื่อนไปบ้างอยู่แล้ว เพราะฉะนั้น NTP จึงเข้ามาช่วยในการทำ synchronize computer ในระบบ network เราให้แม่นยำในระดับ millisecond



ภาพที่4.56 NTP Setting(2)

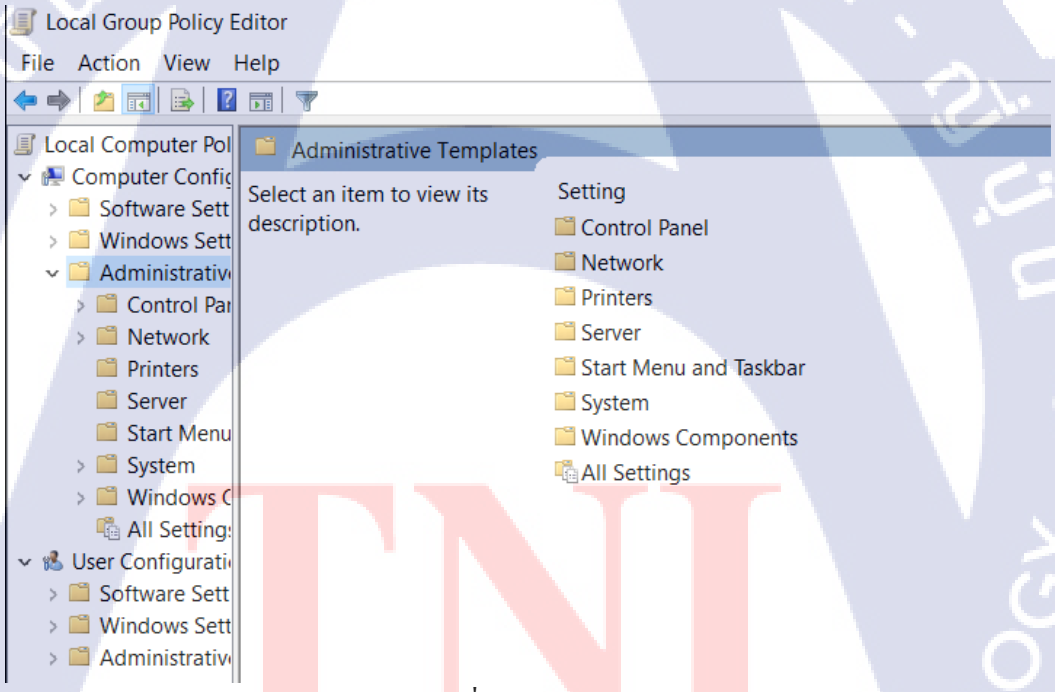
4.1.1.2.6.1 NTP Client Configuration

- เข้าไปที่ run แล้วใส่ gpedit.msc จากนั้นกด ok



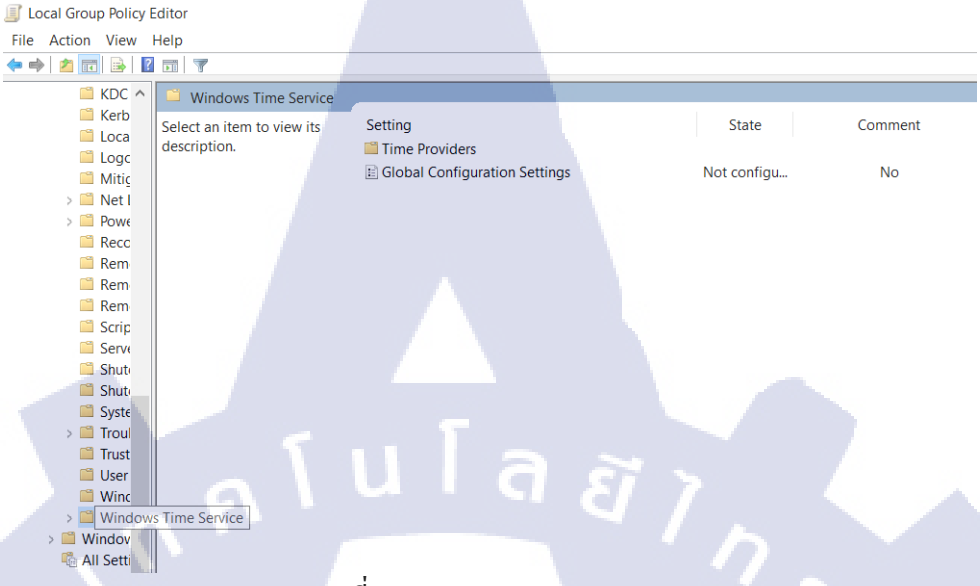
ภาพที่4.57 เข้า Run

- เข้าไปที่ Administrative Templates



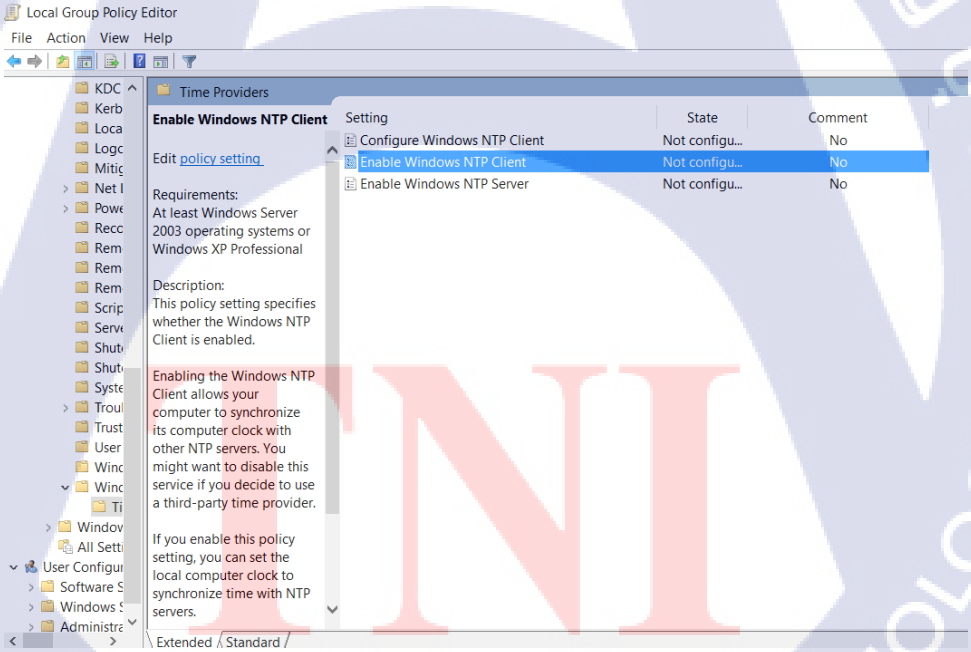
ภาพที่4.58 เลือก Config

- เข้าไปที่ Administrative Templates แล้วเลือก System



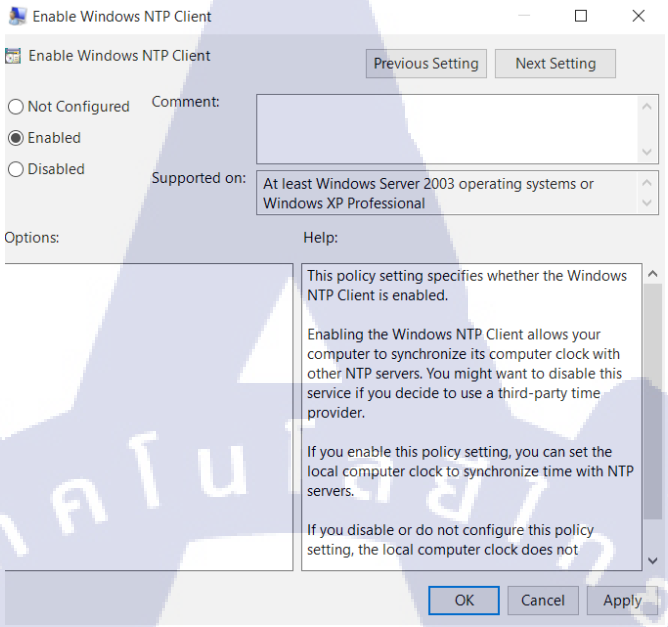
ภาพที่4.59 Client NTP Config(1)

- เลือก Windows Time Service แล้วเลือก Time Providers



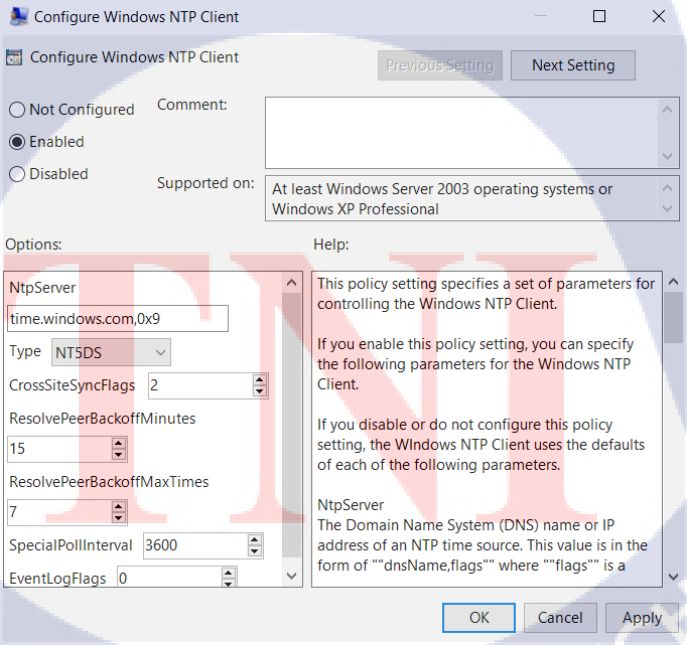
ภาพที่4.60 Client NTP Config(2)

- เข้าไปที่ Enable Windows NTP Client แล้วเลือกเป็น Enable



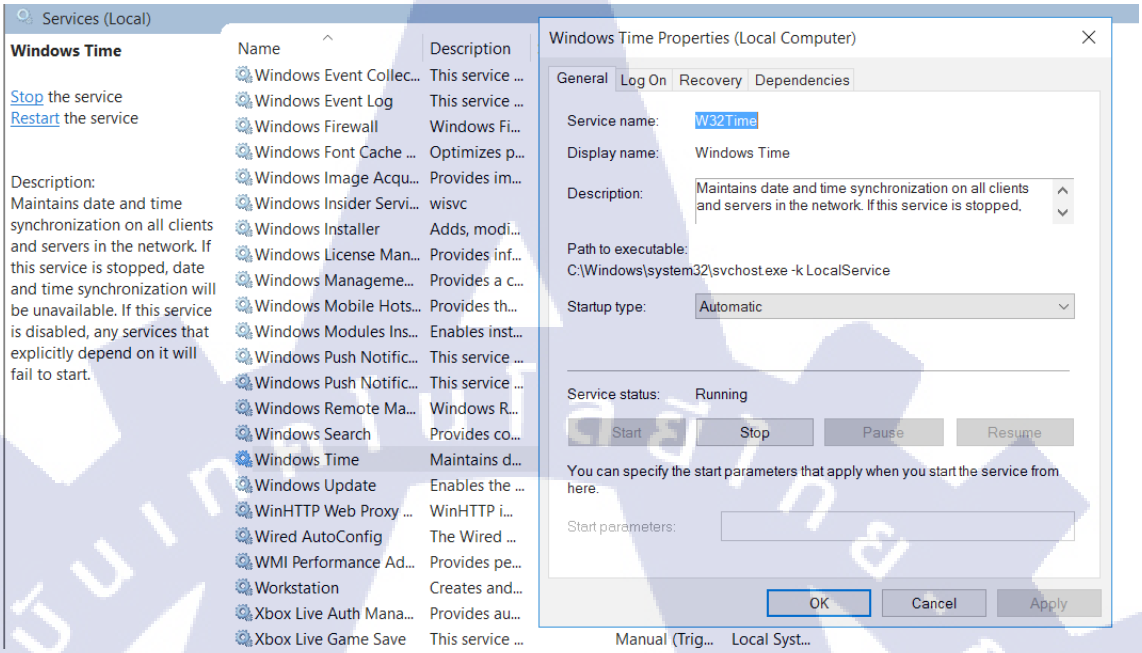
ภาพที่4.61 Client NTP Config(3)

- เข้าไปที่ Configure Windows NTP Client เลือก Enable แล้ว Setting ค่าเป็น Type=NTP,CrossSite=2,ResolvePeermin=15,max= 7,SpecialPolllnterval=3600



ภาพที่4.62 Client NTP Config(4)

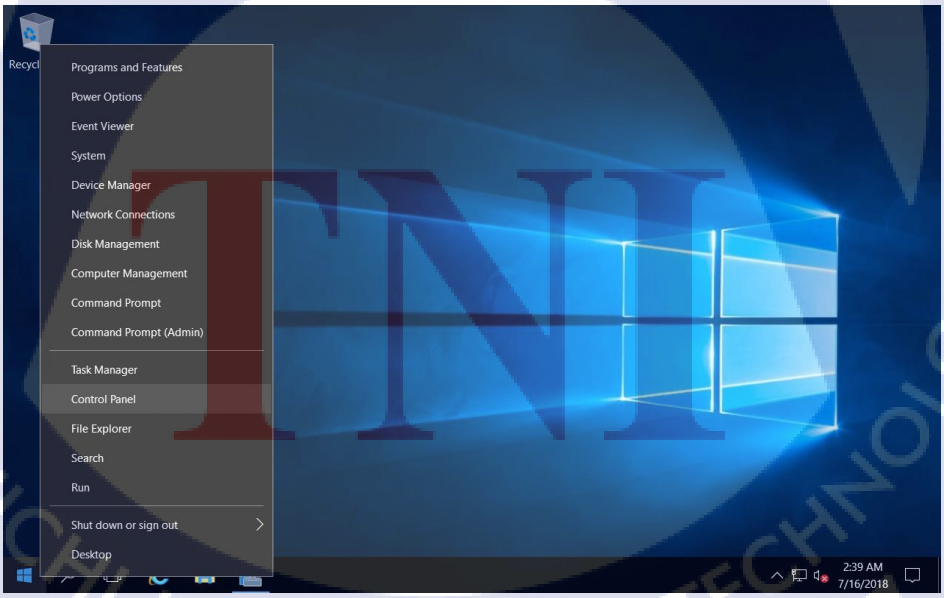
- เข้าไปที่ Server manager เลือก Tool แล้วไปที่ Service เลือก Windows Time ให้ Stop แล้ว Start ใหม่อีกที



ภาพที่4.63 Client NTP Config(5)

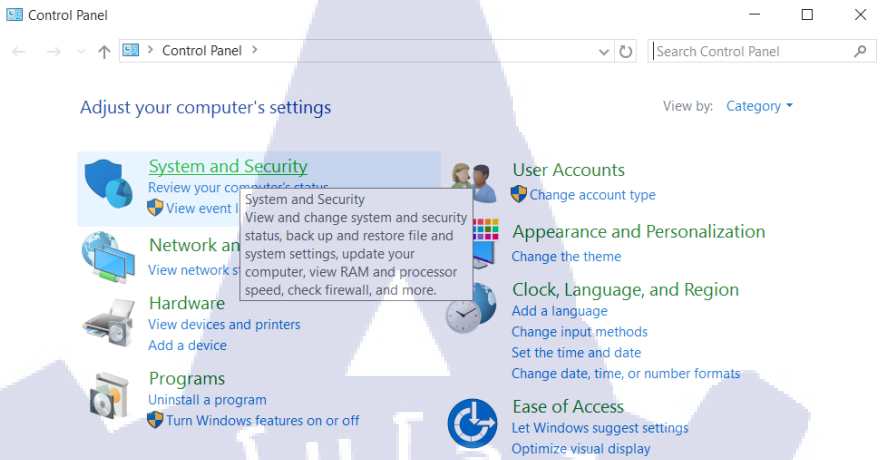
4.1.1.2.7 Firewall Configuration

- เข้าไปที่ Control Panel



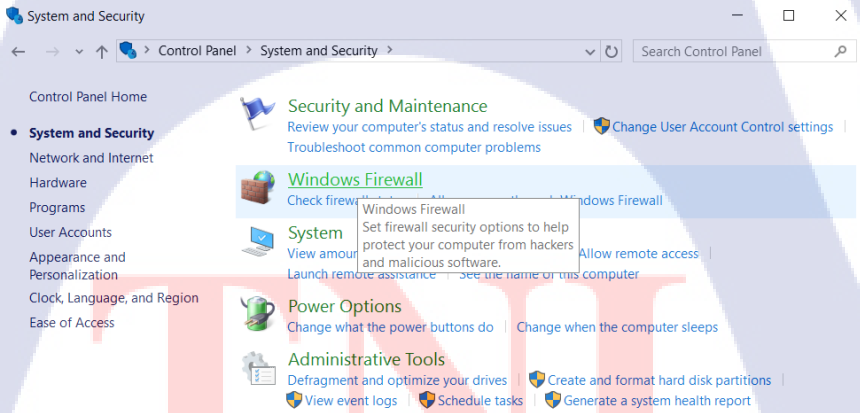
ภาพที่4.64 Fire wall Setting

- เข้าไปที่ System and Security



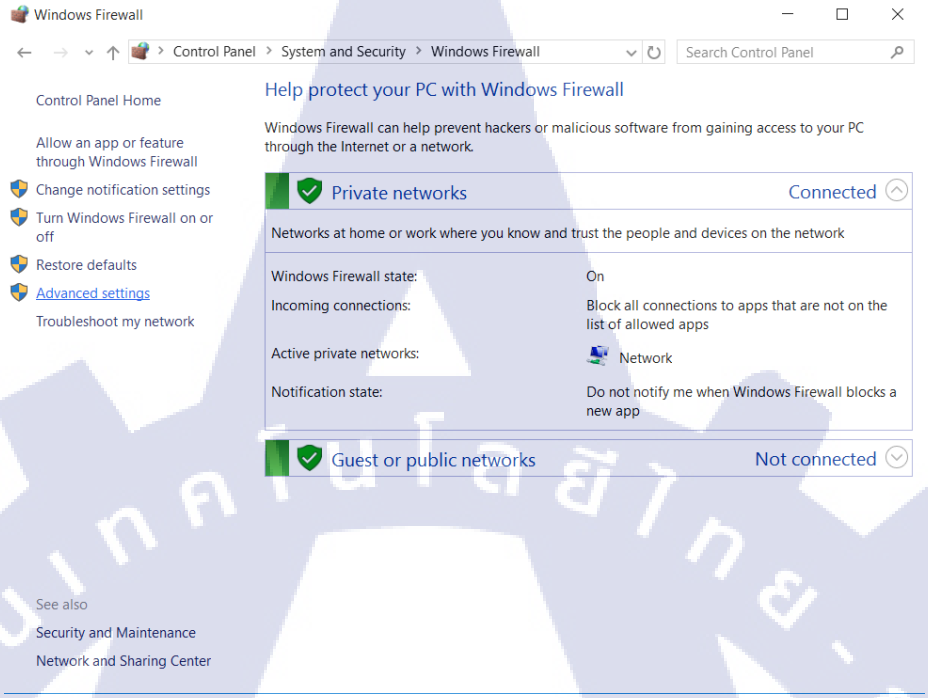
ภาพที่4.65 หน้า Control panel

- เลือก Windows Firewall



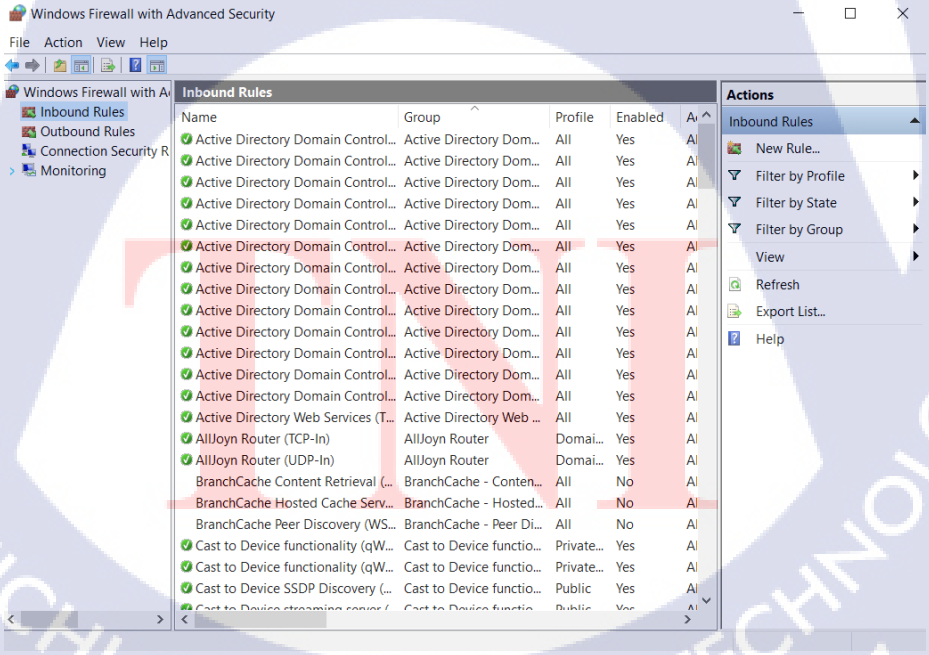
ภาพที่4.66 Fire wall Setting(1)

- เลือก Advanced settings



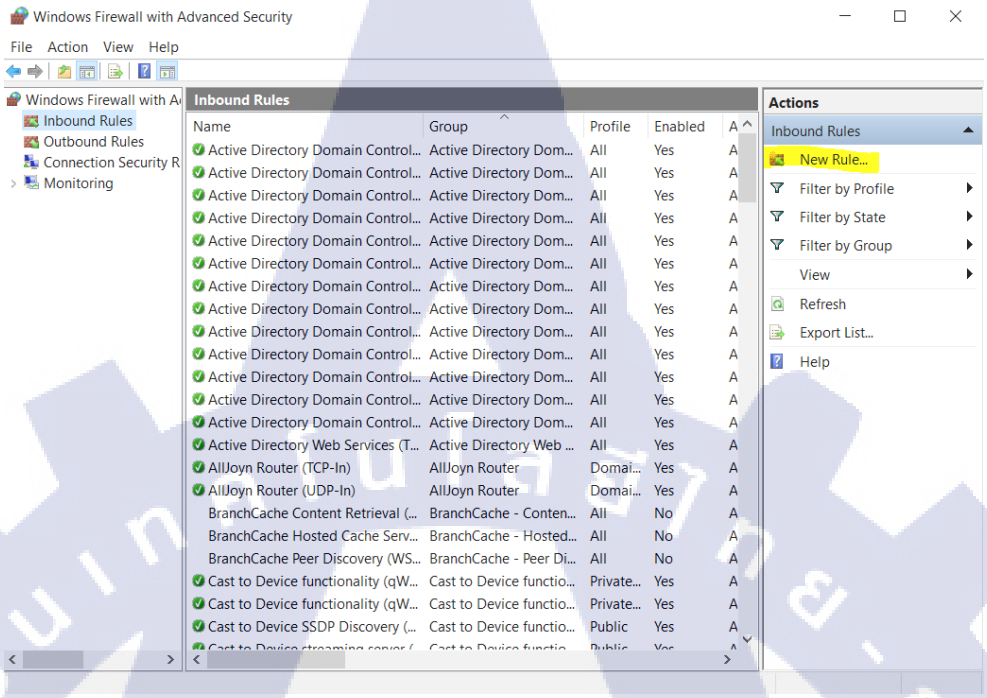
ภาพที่4.67 Fire wall Setting(2)

- เลือก Inbound



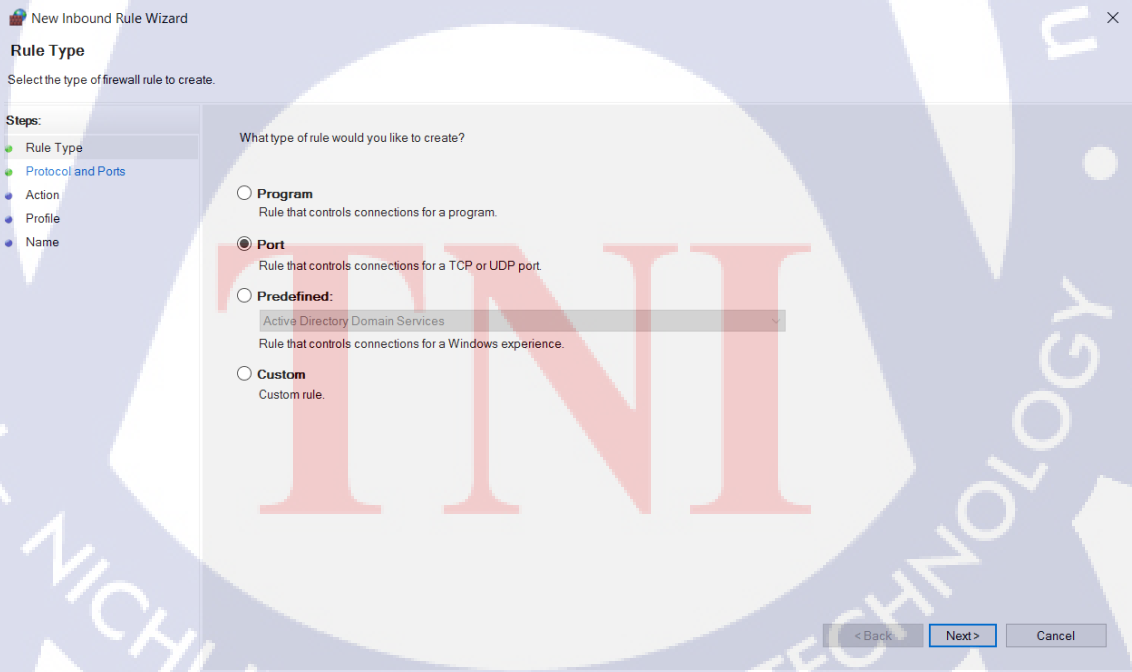
ภาพที่4.68 Fire wall Setting(3)

- เลือก New Rule



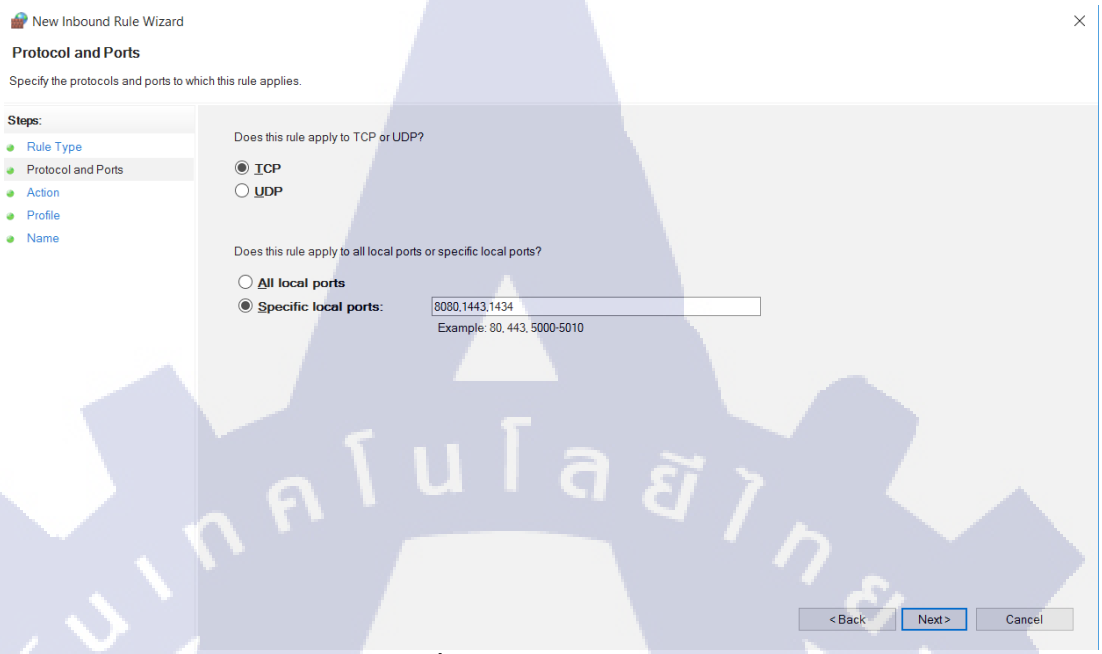
ภาพที่4.69 Fire wall Setting(4)

- เลือก Port แล้วกด Next



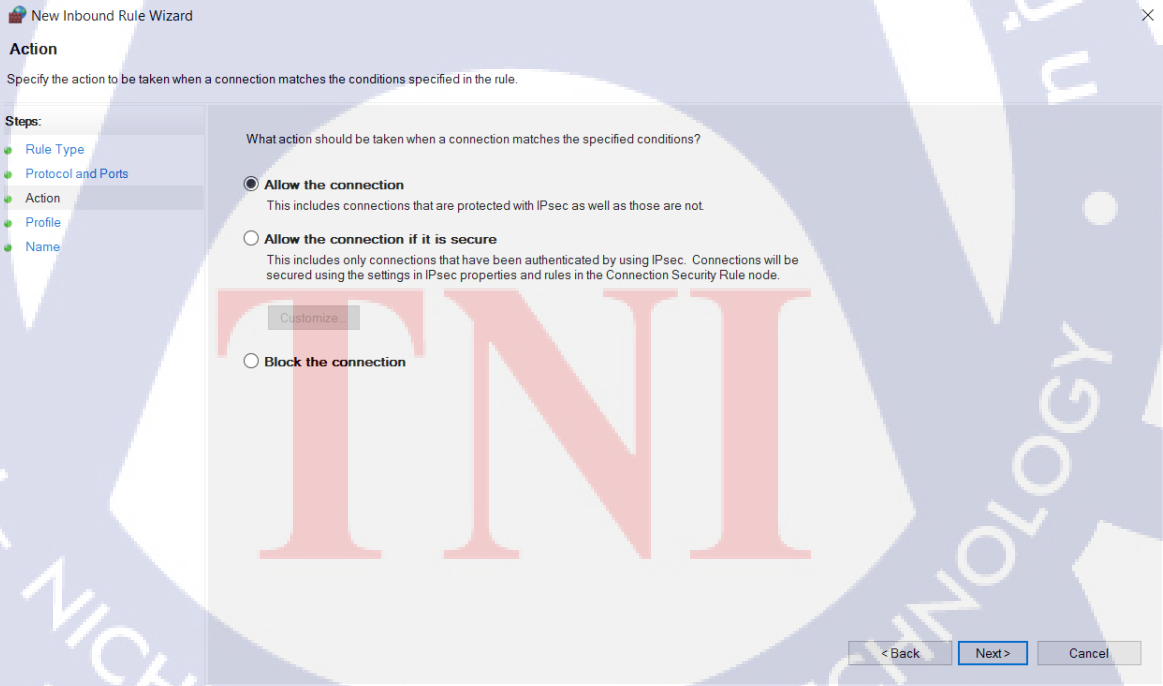
ภาพที่4.70 Fire wall Setting(5)

- ตั้งค่าให้ Inbound รับ Port ที่ตั้งค่าไว้เท่านั้น



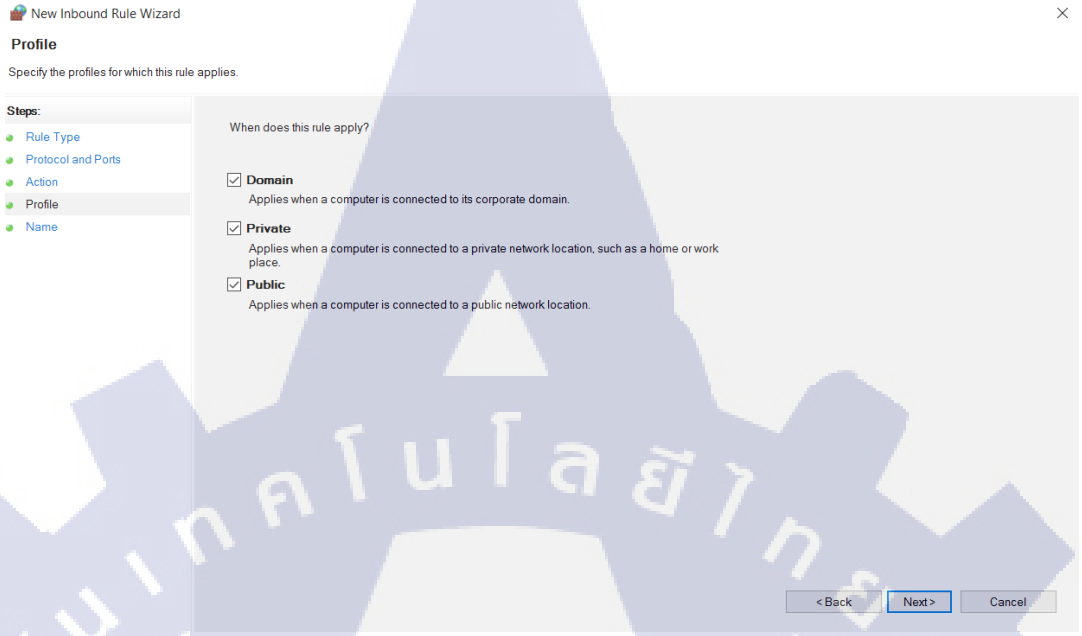
ภาพที่4.71 Fire wall Setting(6)

- เลือก Allow the connection



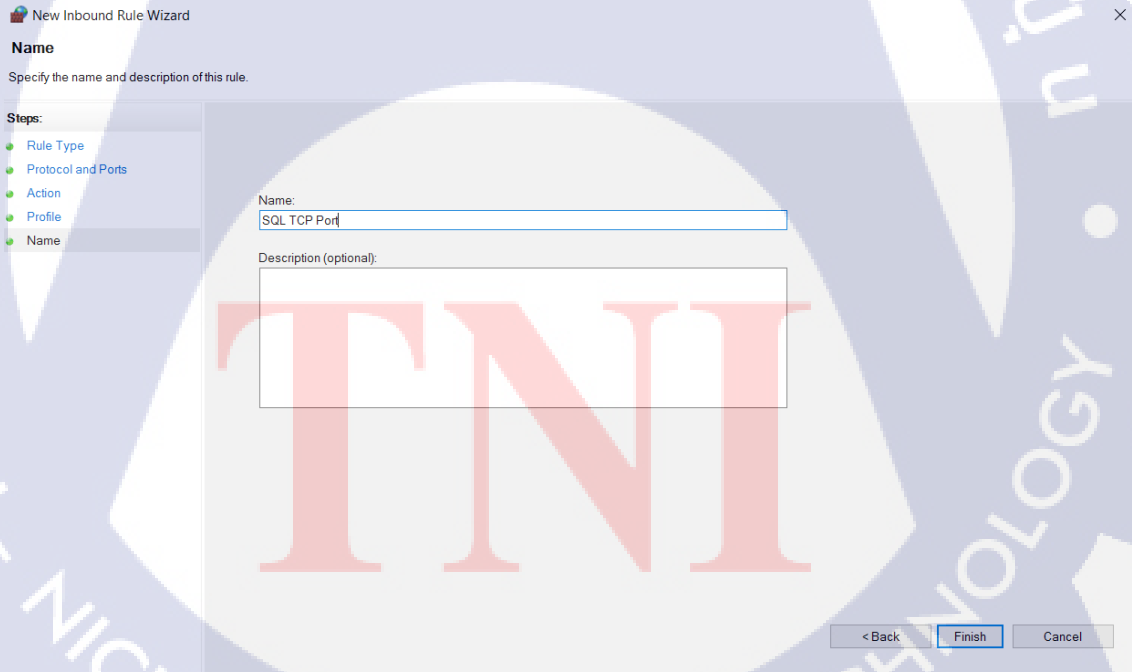
ภาพที่4.72 Fire wall Setting(7)

- เลือกให้ Rule ของเราแสดงมีผลที่ไหนบ้าง



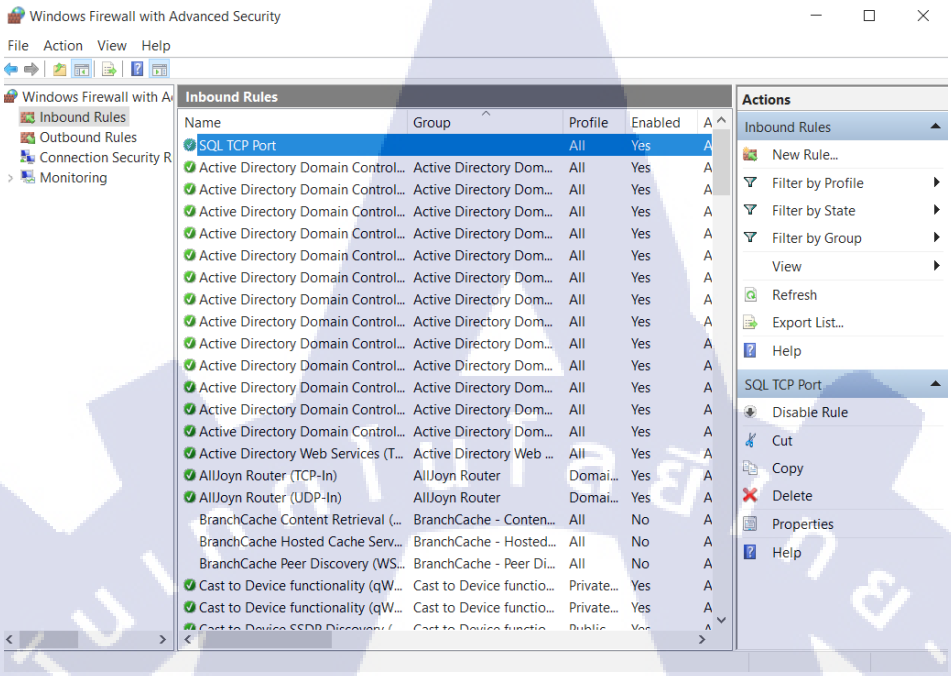
ภาพที่4.73 Fire wall Setting(8)

- ตั้งชื่อ Rule ที่สร้าง



ภาพที่4.74 Inbound name setting

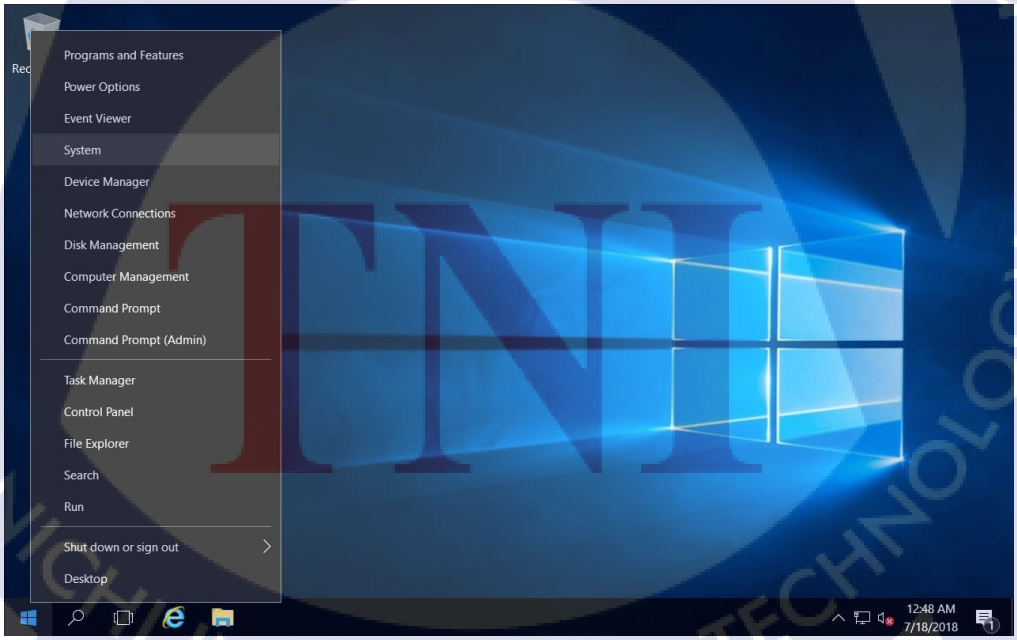
- จะเห็น Rule ที่สร้างโผล่ขึ้นมา



ภาพที่4.75 Rule ที่สร้าง

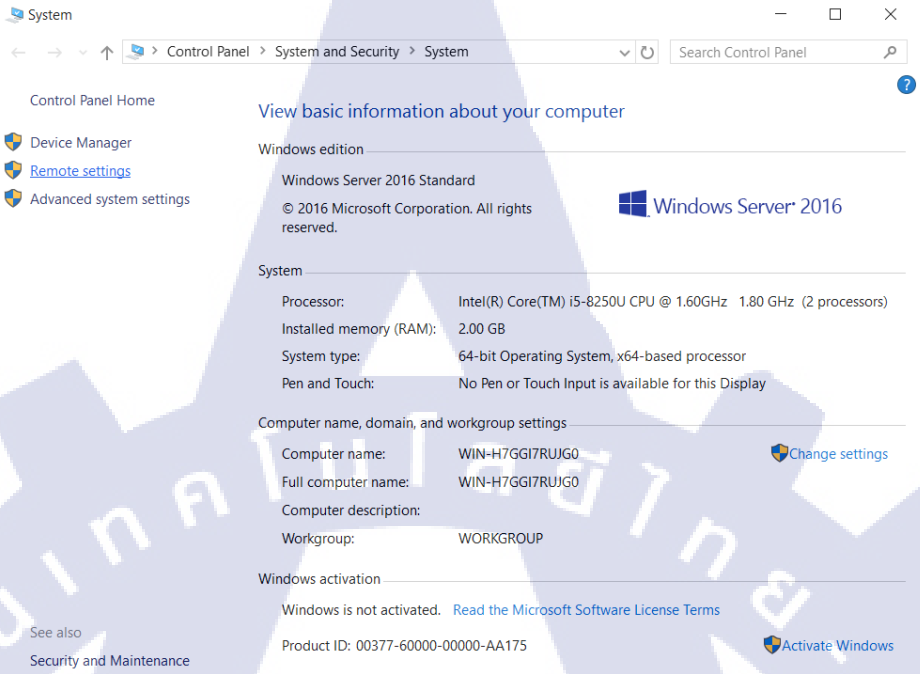
4.1.1.2.8 Remote Access Configuration

- เข้าไปที่ System



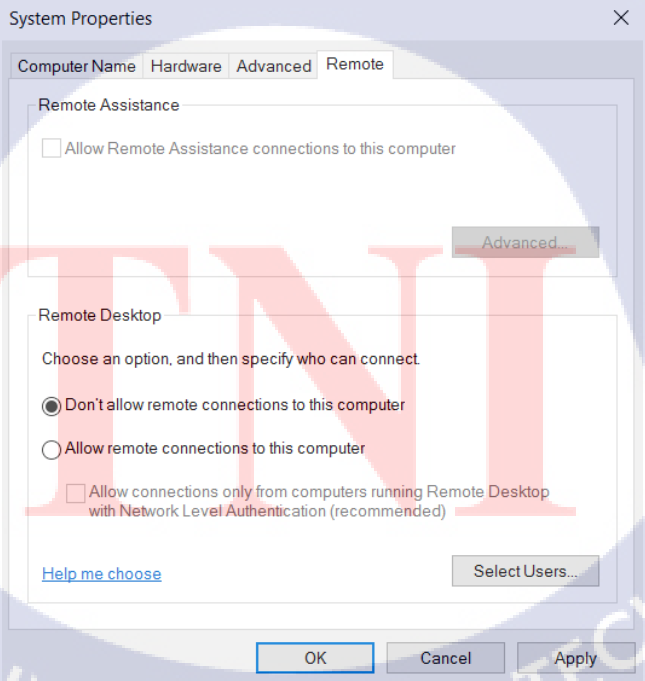
ภาพที่4.76 Remote access configuration(1)

- เลือก Remote settings



ภาพที่4.77 Remote access configuration(2)

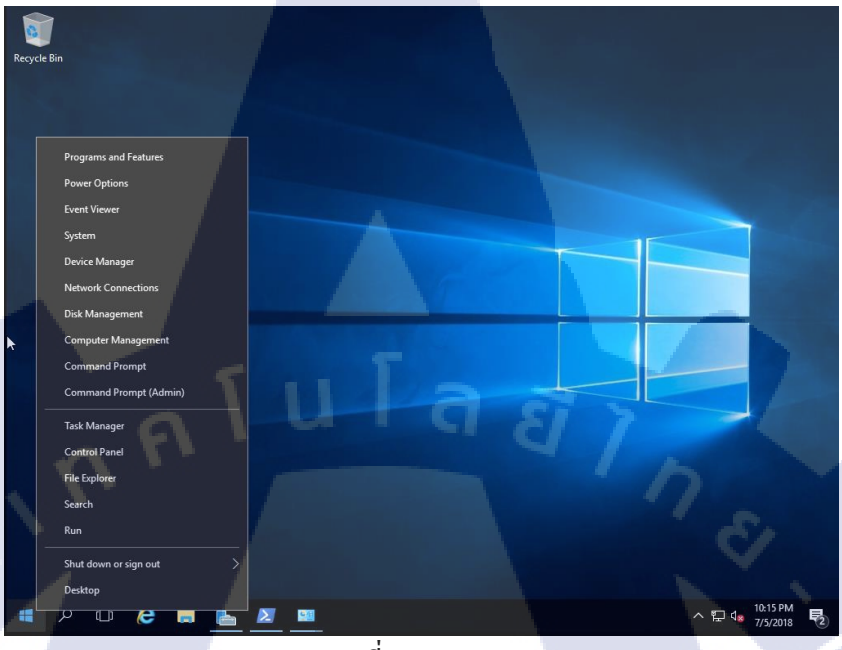
- เข้าไปที่ Remote แล้วเลือก Don’t allow remote connection to this computer



ภาพที่4.78 Remote access configuration(3)

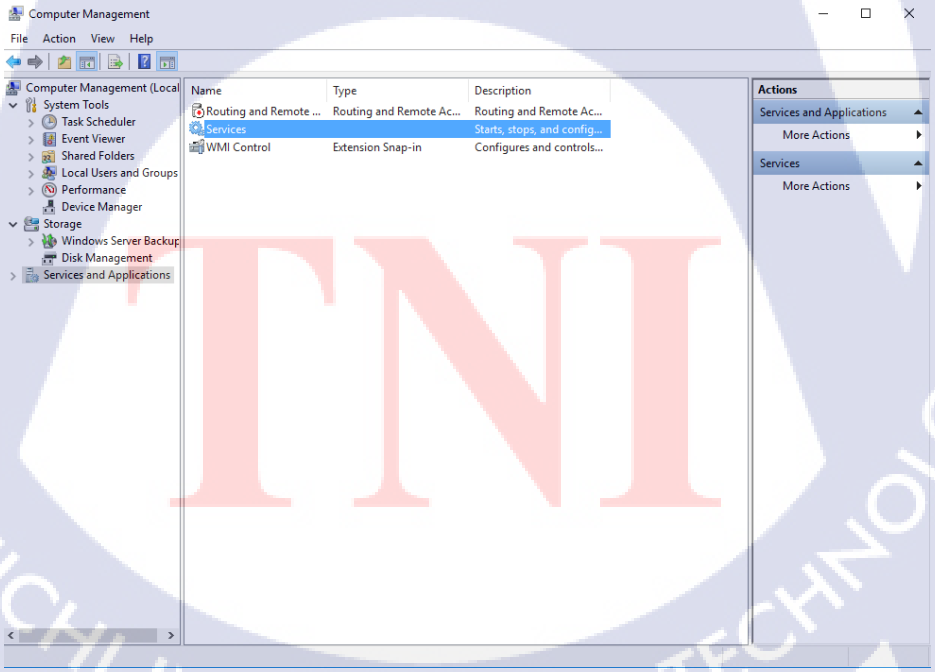
4.1.1.2.9 Service Configuration

- เลือก Computer Management



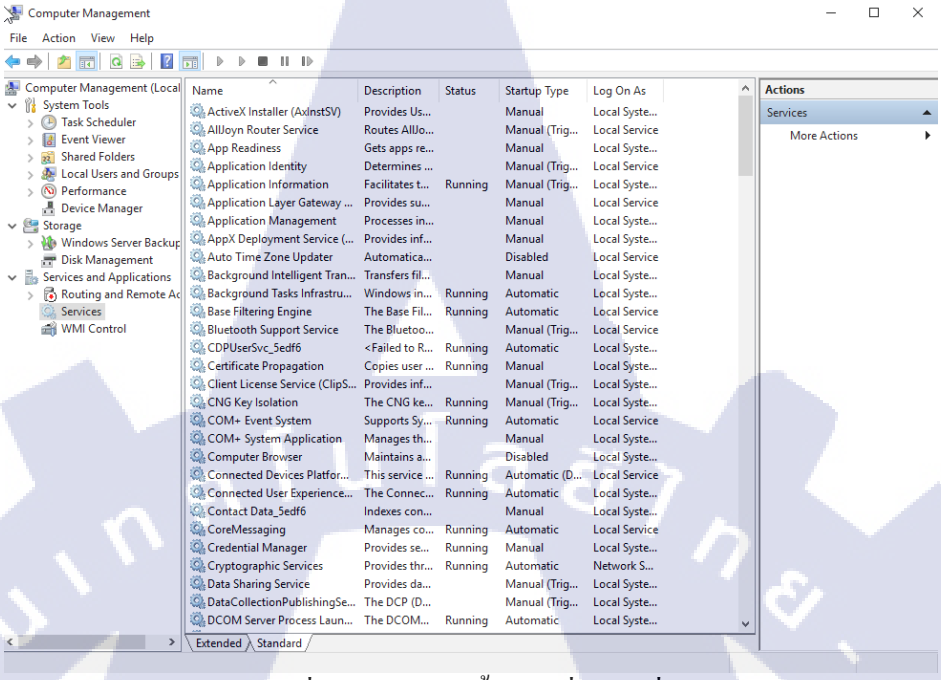
ภาพที่4.79 Service

- กดที่ Services



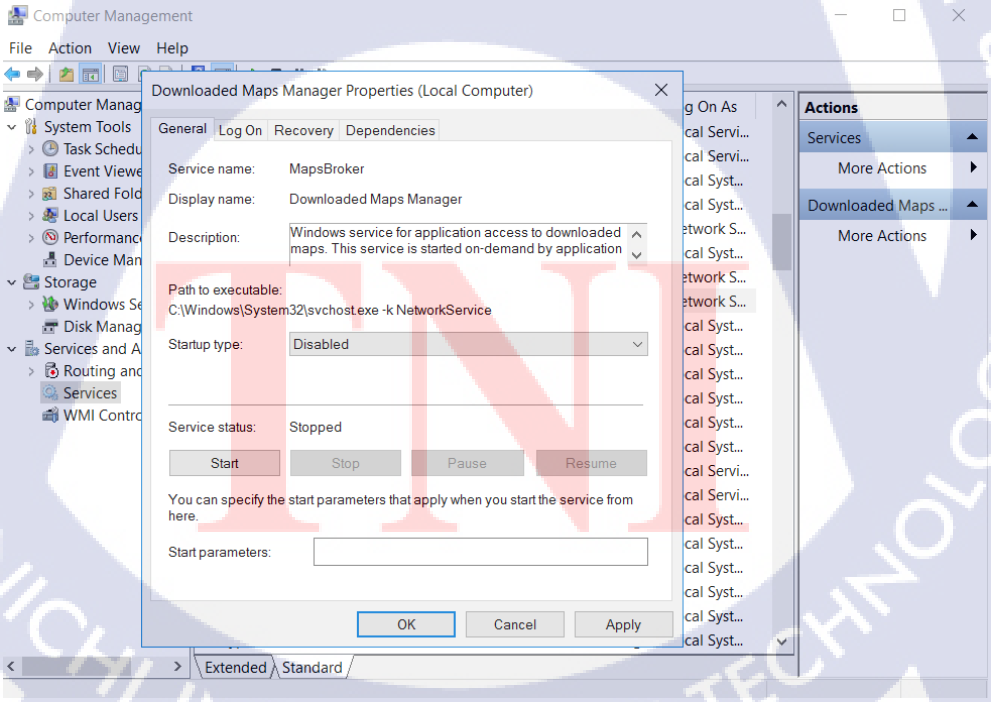
ภาพที่4.80 Computer management

- เข้าไปที่หมวด Standard ด้านล่าง



ภาพที่4.81 Service ทั้งหมดที่มีในเครื่อง

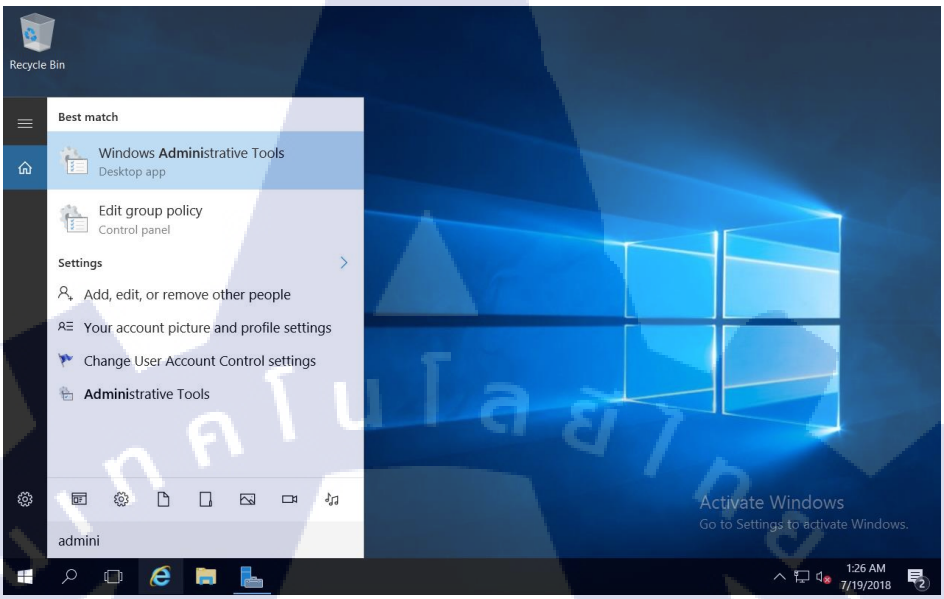
- ปิด Service ที่ไม่ใช้อย่าง Map Broker เรายังไม่มีความจำเป็นต้องไปใช้ก็ปิดทิ้งได้เลย



ภาพที่4.82 Disable Service

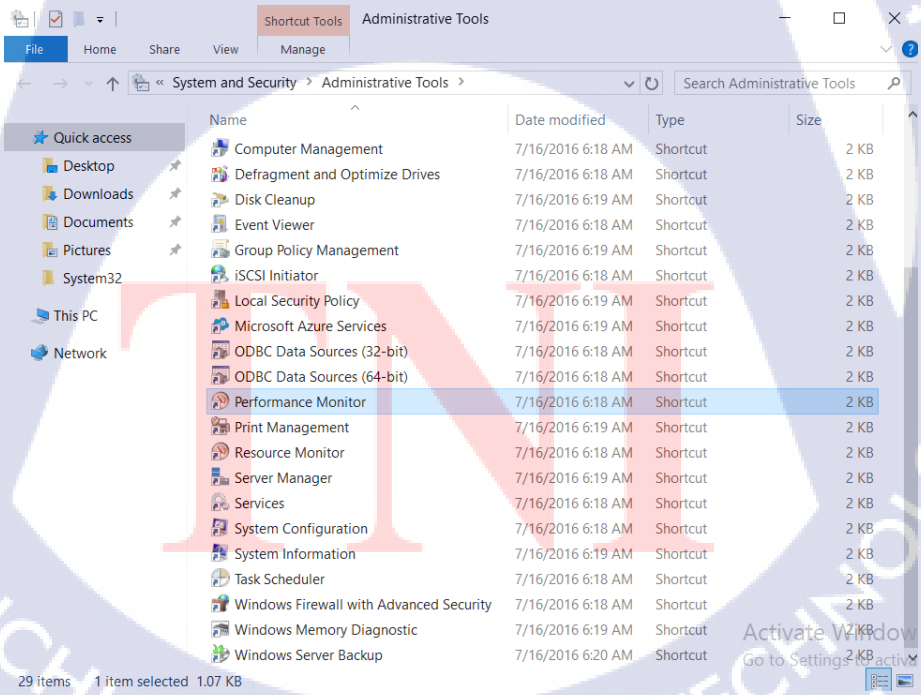
4.1.1.2.10 Log & Monitoring

- เข้าไปค้นหา Windows Administrative Tools



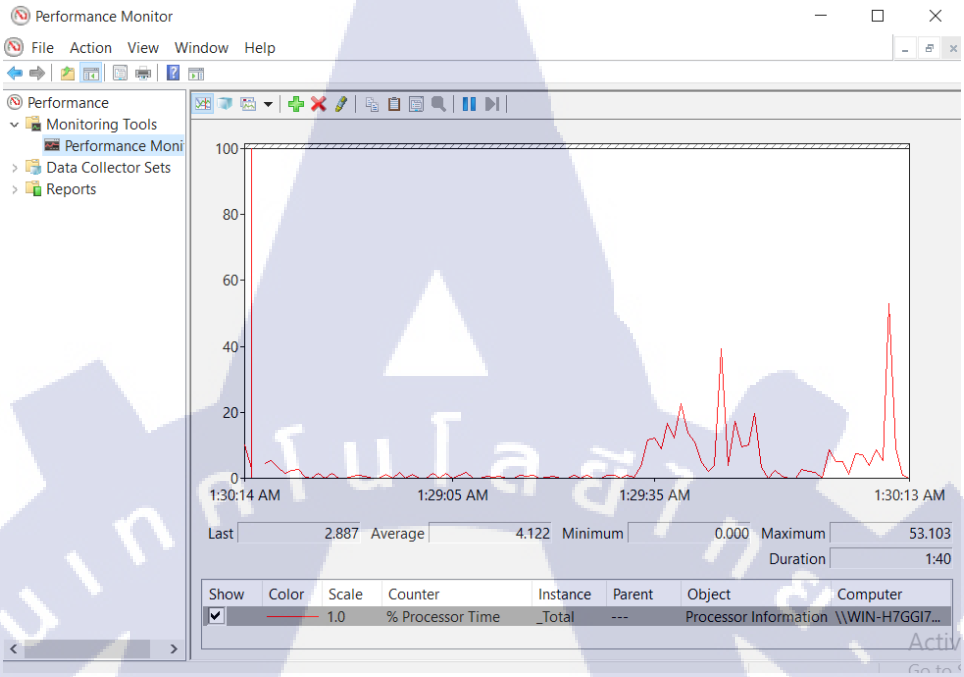
ภาพที่4.83 Windows Server Monitor(1)

- เข้าไปเลือก Performance Monitor



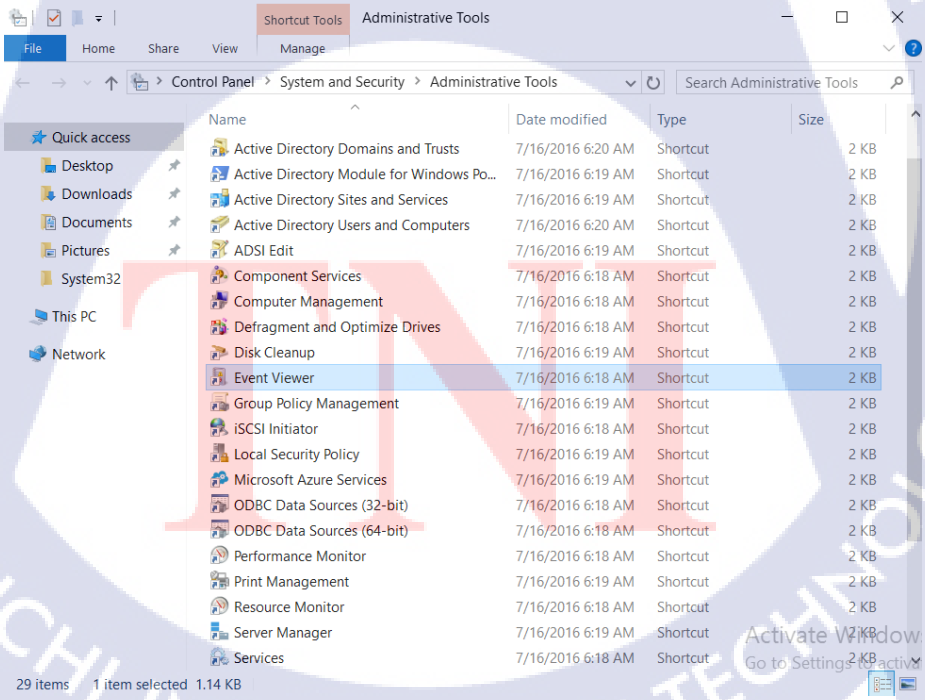
ภาพที่4.84 Windows Server Monitor(2)

- เข้ามาดูว่าตอนนี้เครื่องทำงานหนักเท่าไหร่



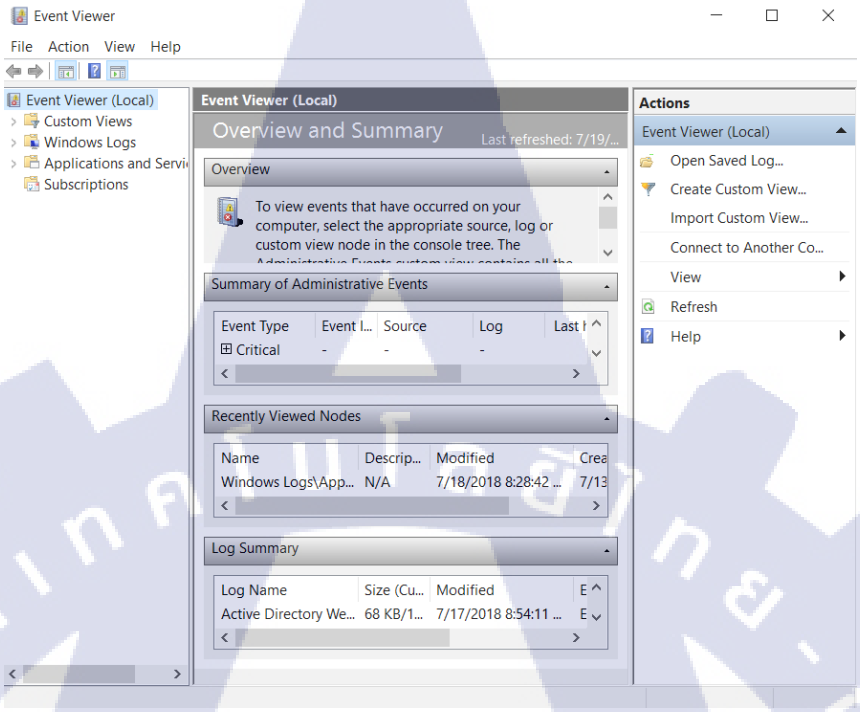
ภาพที่4.85 Windows Server Monitor(3)

- เข้าไปที่ Event Viewer



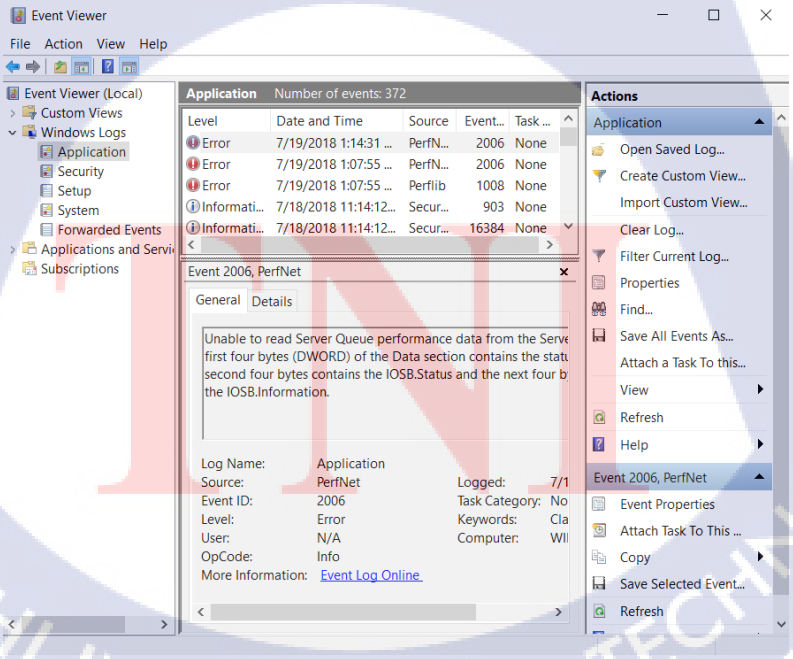
ภาพที่4.86 Windows Server Log(1)

- เลือก Windows Logs



ภาพที่4.87 Windows Server Log(2)

- เข้าไปที่ Application จะเห็นว่ามี log การใช้งานว่าทำอะไรไปบ้าง



ภาพที่4.88 Windows Server Log(3)

4.1.2 การติดตั้ง Linux

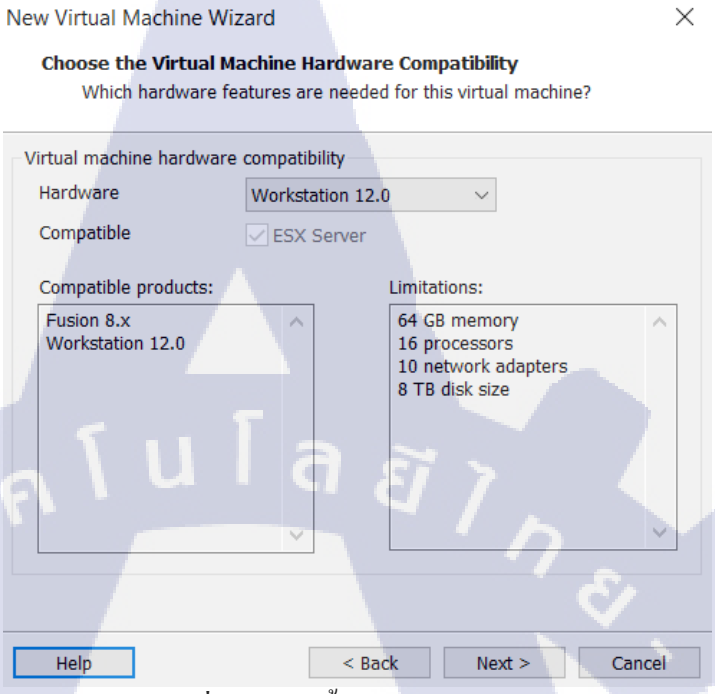
- ทำการสร้าง Virtual Machine ด้วยการกดปุ่ม Create a New Virtual Machine

ภาพที่4.89 การสร้าง Virtual Machine(1)

- เลือกแบบ Custom เพื่อทำการตั้งค่าต่างๆ

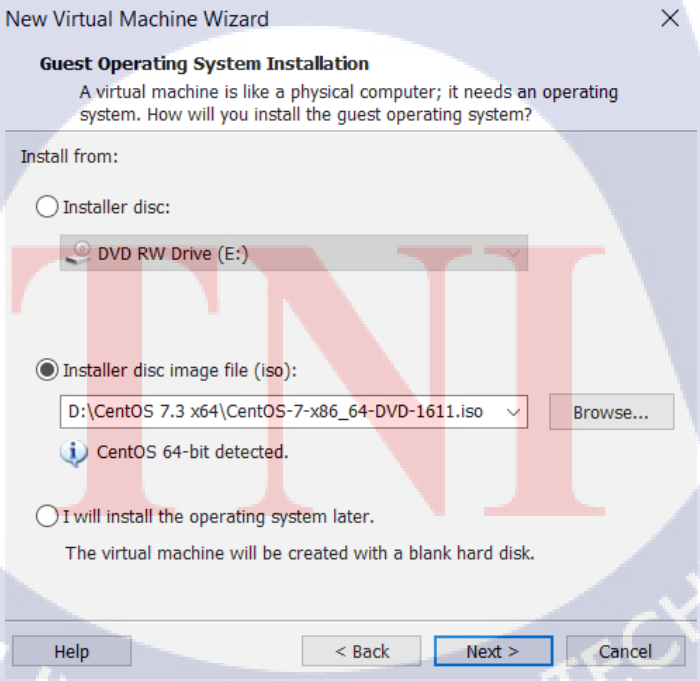
ภาพที่4.90 การสร้าง Virtual Machine(2)

- ให้เลือก Hardware เป็น Version ที่ตรงกับเราในที่นี้เลือกเป็น 12.0



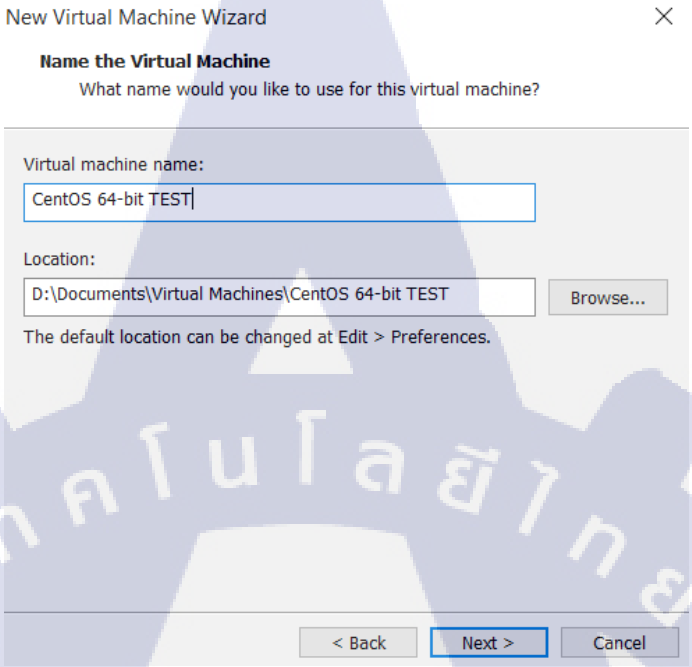
ภาพที่4.91 การตั้งค่า Virtual Machine

- ทำการเลือกแผ่นหรือไฟล์ที่เราเก็บ OS ที่จะลงไว้



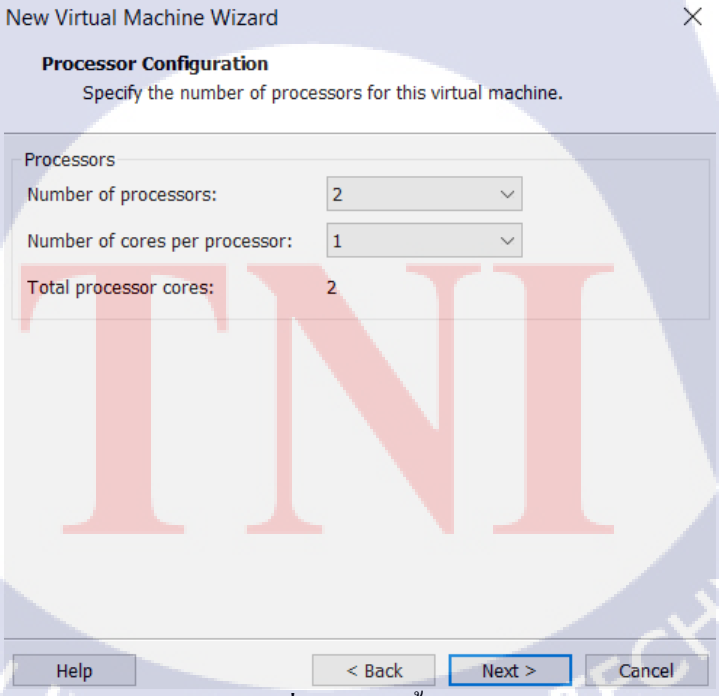
ภาพที่4.92 เลือกลง Linux

- ตั้งชื่อให้กับ VM ที่เราสร้าง



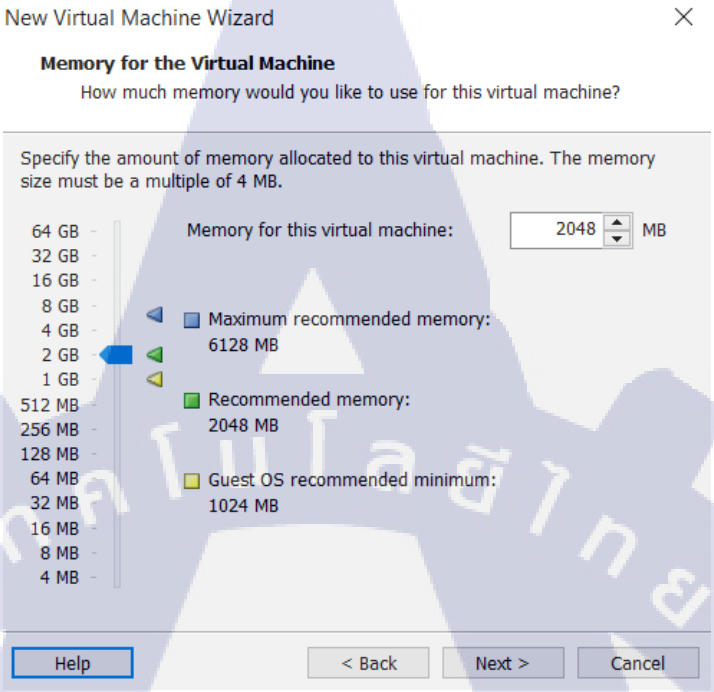
ภาพที่4.93 การระบุที่อยู่ของไฟล์ Virtual Machine

- เลือก Cores ที่จะให้นำไปงาน



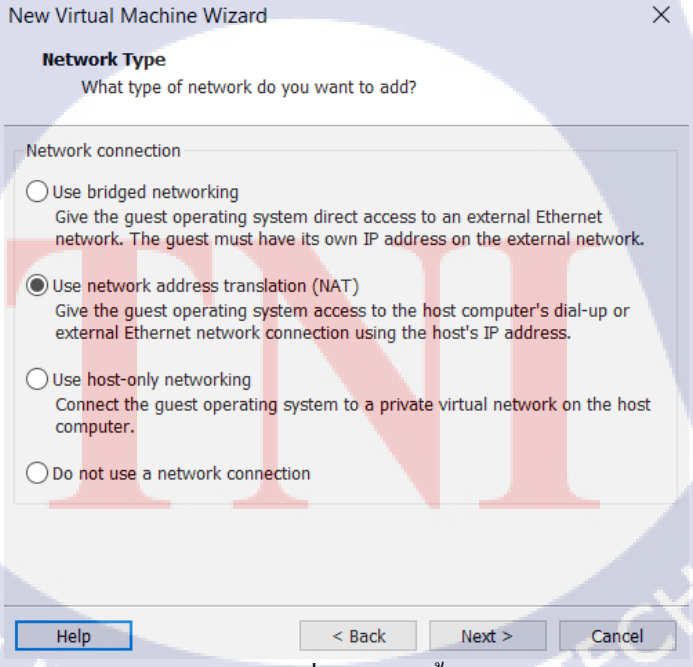
ภาพที่4.94 การตั้งค่า Linux

- เลือกจำนวน Ram ให้กับ VM



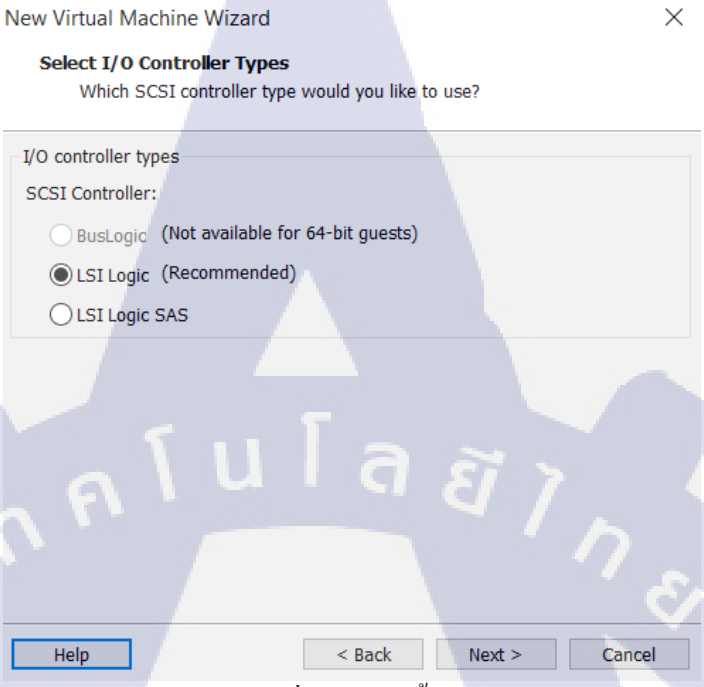
ภาพที่4.95 การให้ Memory กับ VM

- เลือก Network แบบ NAT



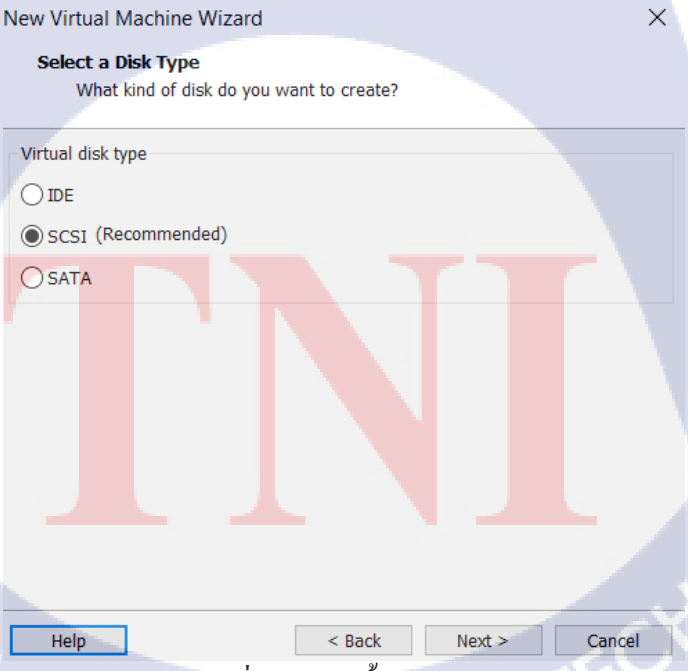
ภาพที่4.96 การตั้งค่า Network

- เลือก LSI Logic



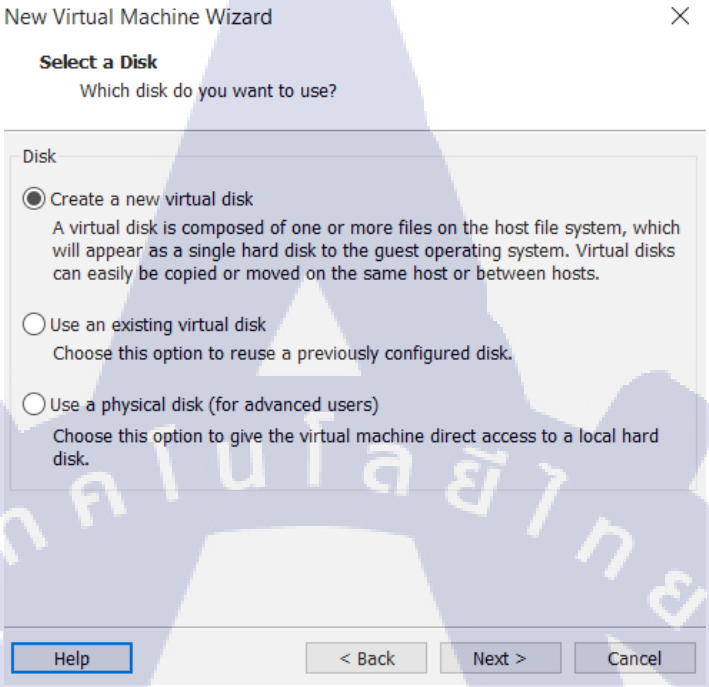
ภาพที่4.97 การตั้งค่า I/O

- เลือก SCSI



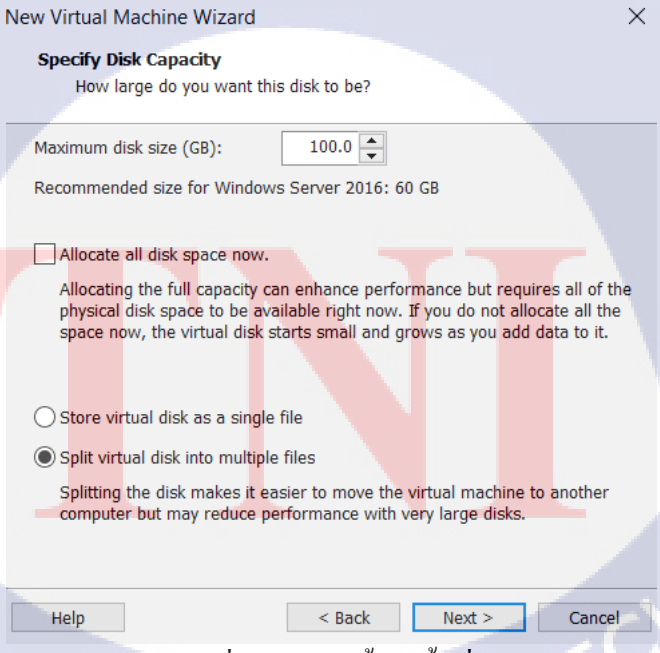
ภาพที่4.98 การตั้งค่า Disk type

- เลือก Create a new virtual disk เพื่อสร้าง



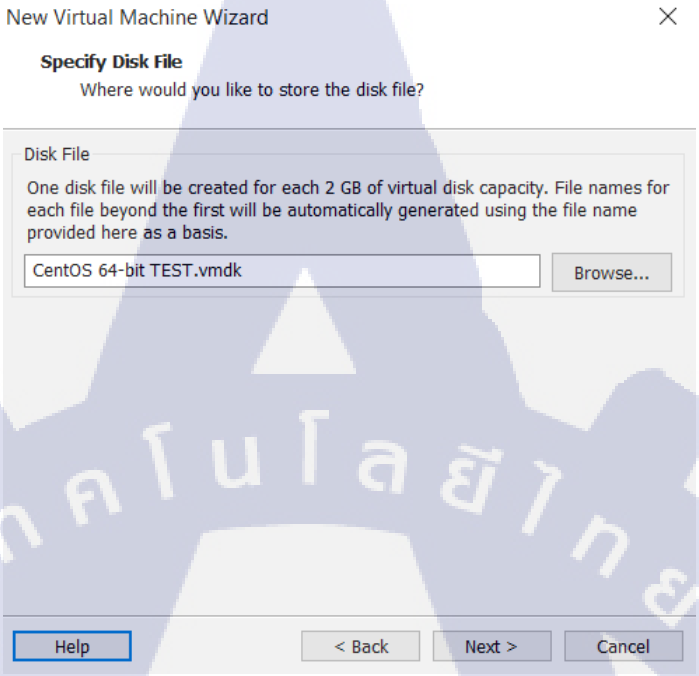
ภาพที่4.99 การสร้าง VM

- เลือกพื้นที่ให้กับ VM เป็นแบบ Split disk



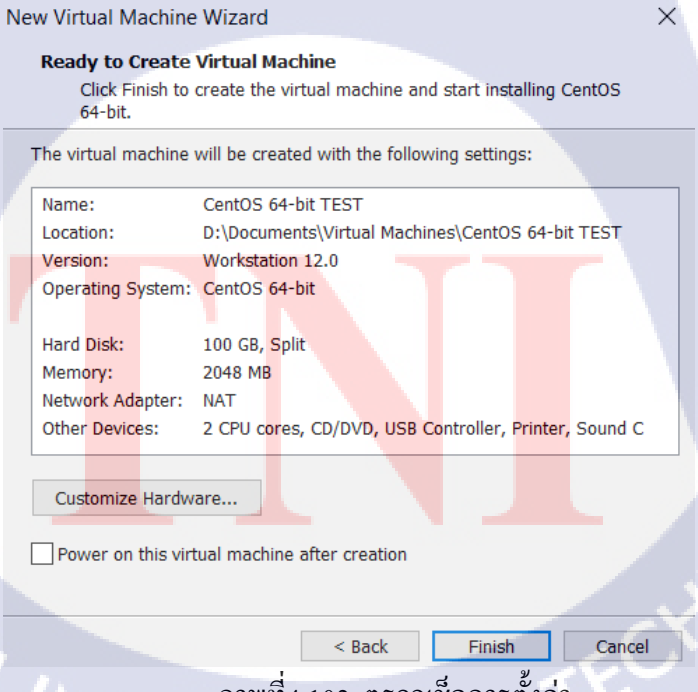
ภาพที่4.100 การตั้งค่าพื้นที่ให้ Linux

- ตั้งชื่อ Disk



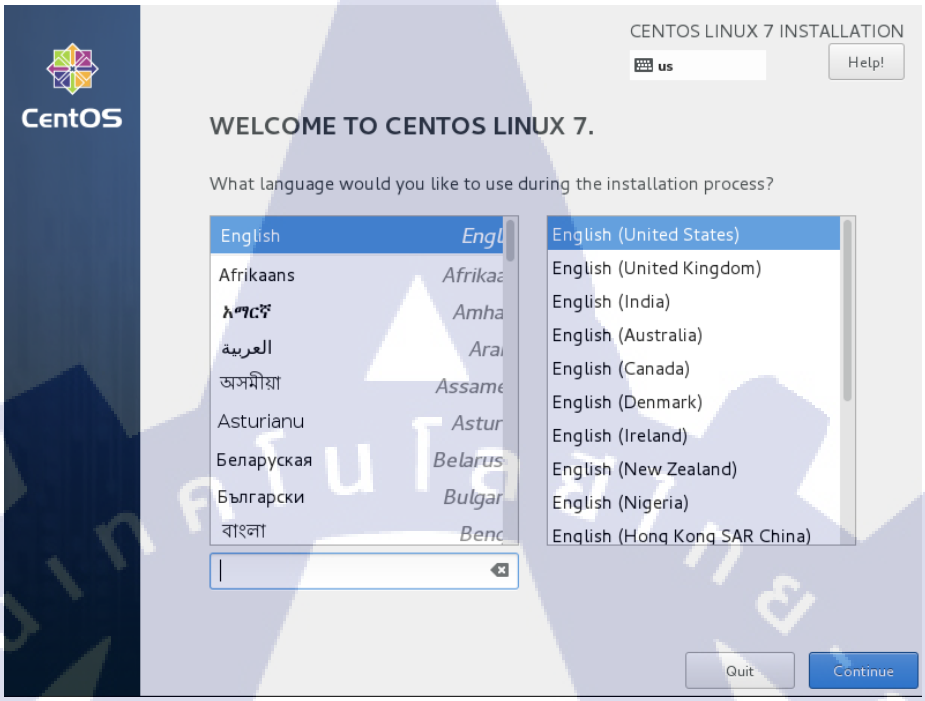
ภาพที่4.101 การตั้งชื่อให้กับ VM

- เช็คดูว่าตรงกับที่เราตั้งค่าไว้ไหมแล้วไปกดเปิด VM



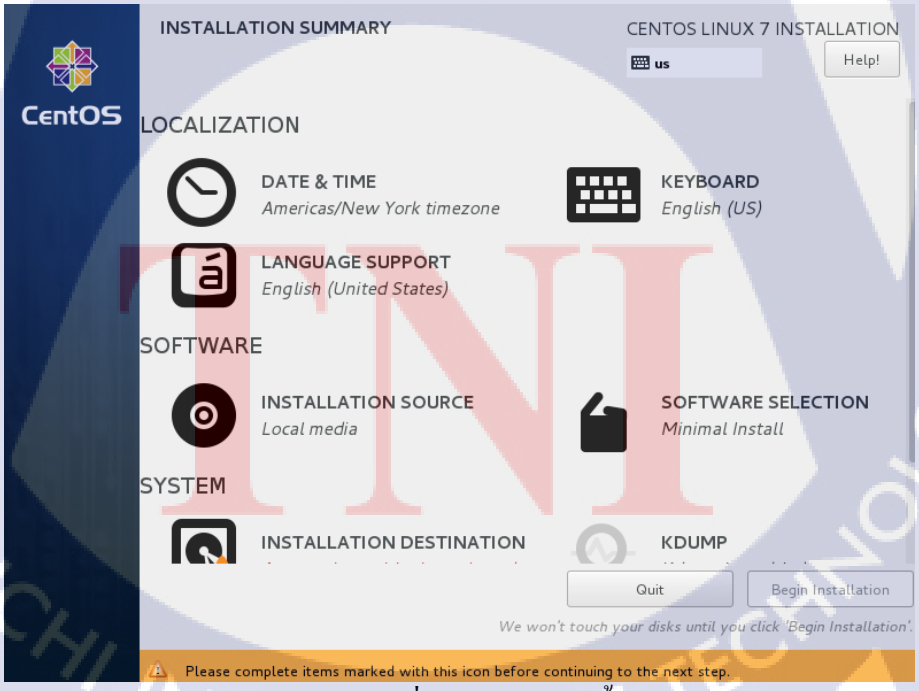
ภาพที่4.102 ตรวจเช็คการตั้งค่า

- เลือกภาษาที่ต้องการ



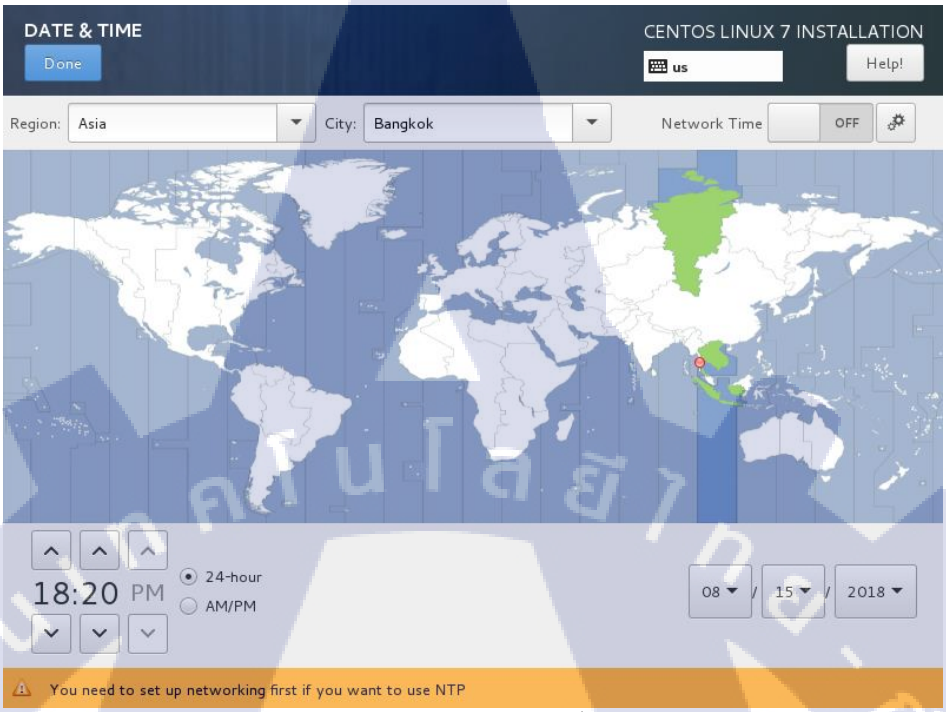
ภาพที่4.103 เลือกภาษา

- เลือก Date & Time



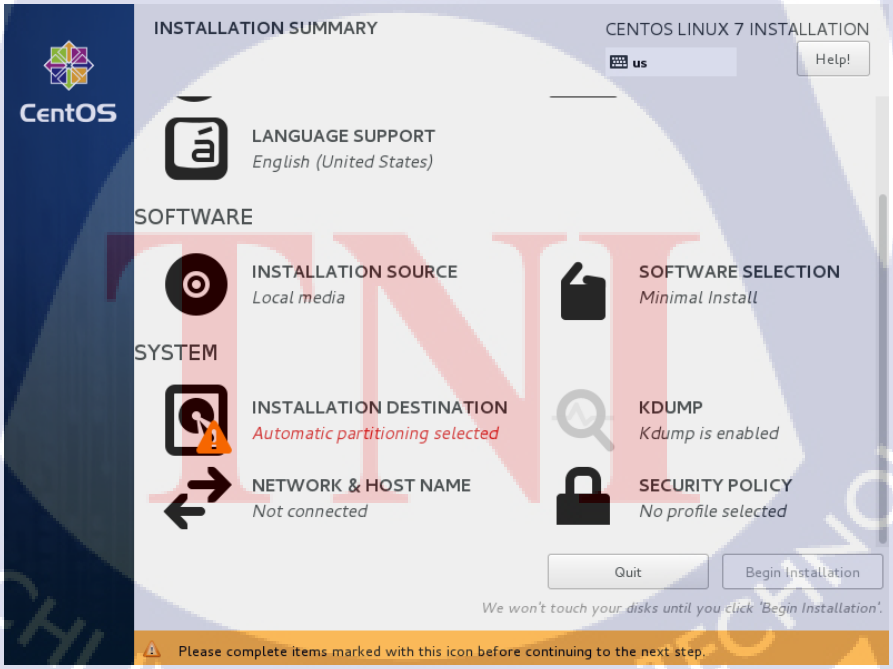
ภาพที่4.104 หน้าการตั้งค่าต่างๆ

- เลือก Time zone ที่เราอยู่



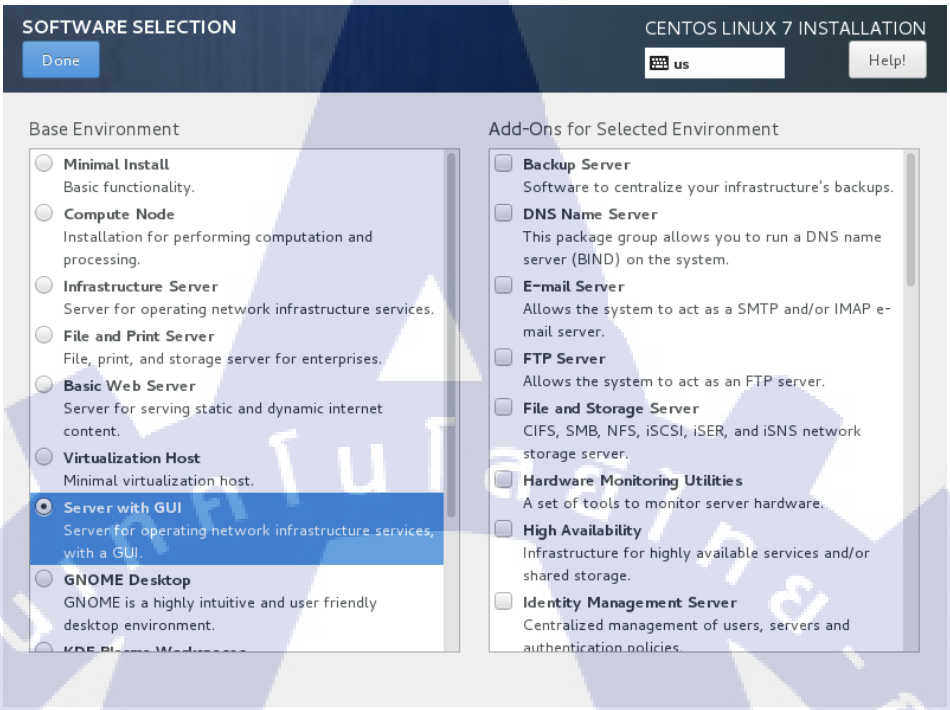
ภาพที่4.105 ตั้งค่าเวลา

- เลือก Software Selection



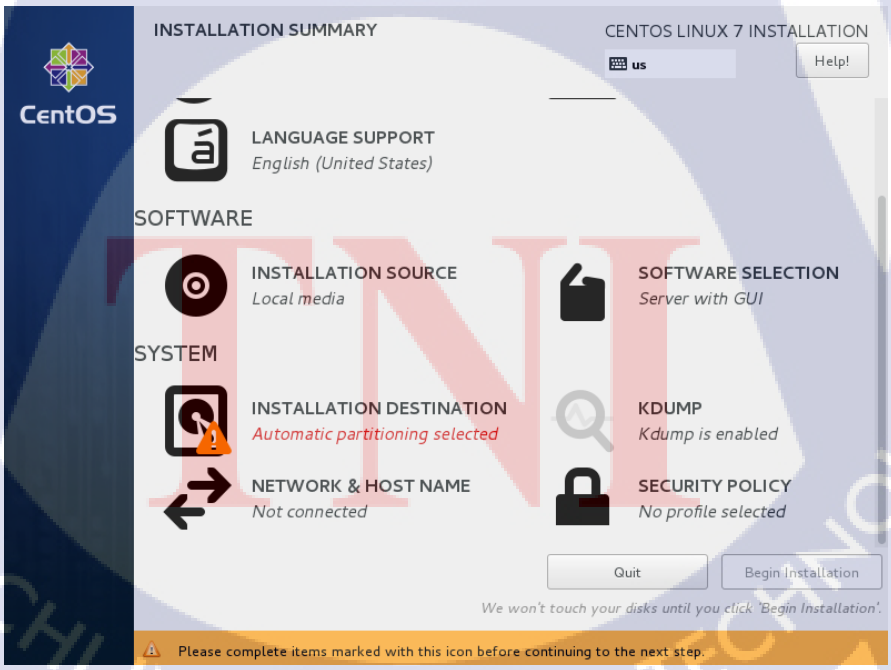
ภาพที่4.106 เข้าไปที่ Software Selection

- เลือก Server with GUI แล้วเลือก Add-On ตามที่ต้องการ



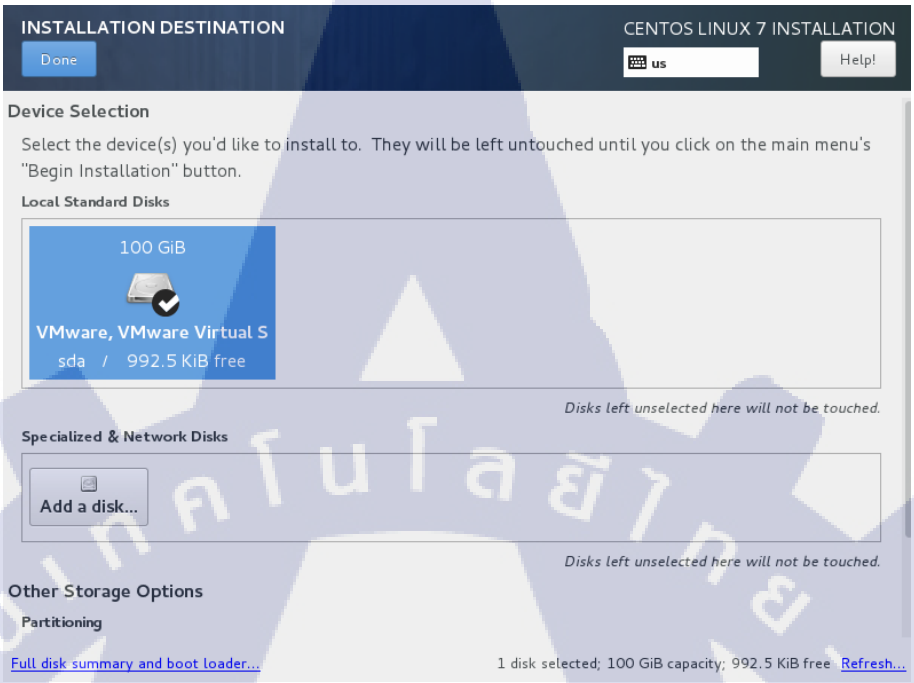
ภาพที่4.107 เลือก Environment ที่ต้องการ

- เลือก Installation Destination



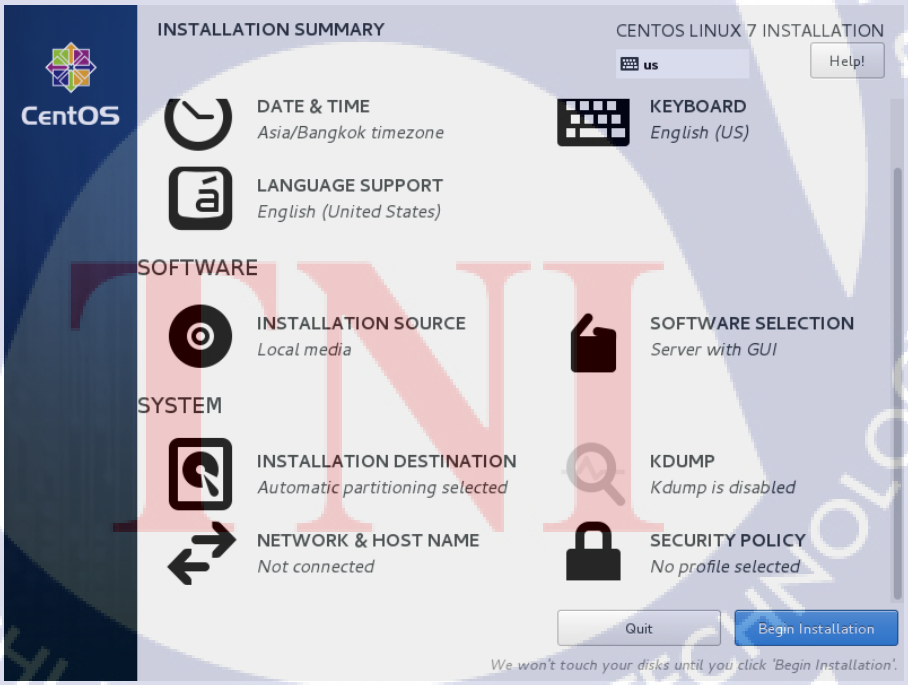
ภาพที่4.108 เข้าไปที่ Installation Destination

- เลือก Disk ที่เราตั้งไว้ตั้งแต่ตอนสร้าง VM



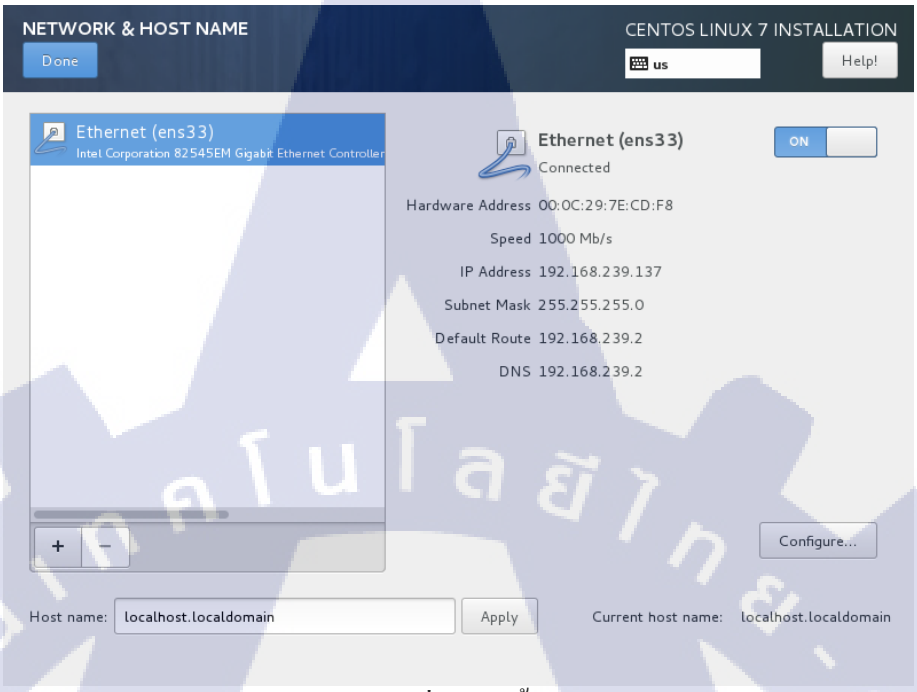
ภาพที่4.109 ตั้งค่า Disk ให้กับ Os Linux

- เลือก Network & Host name



ภาพที่4.110 เข้าไปที่ Network & Host name

- เลือกเปิด

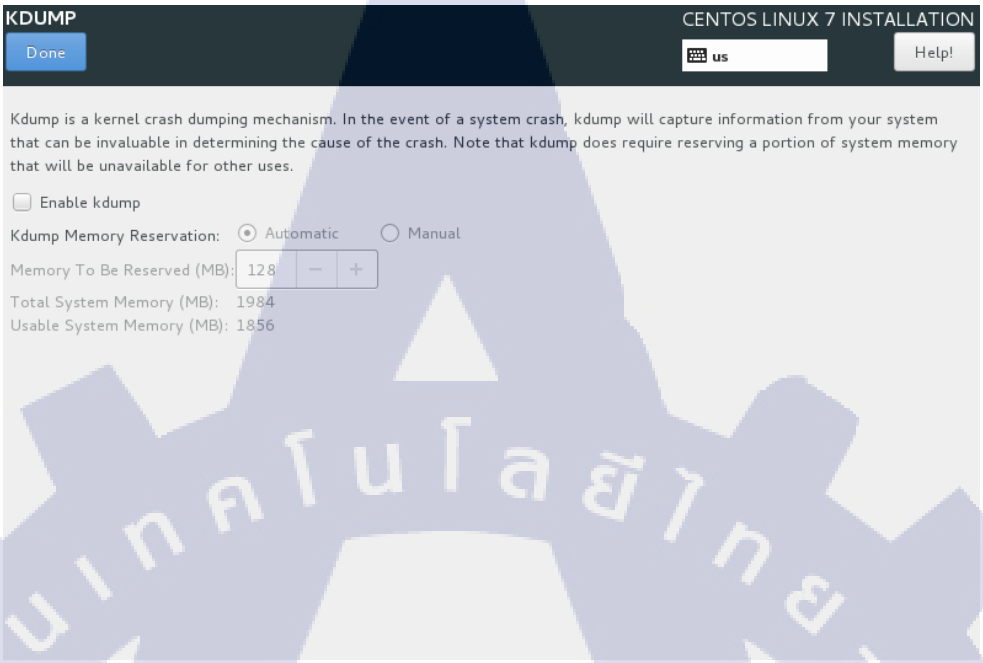


ภาพที่4.111 ตั้งค่า Network

- เลือก KDUMP

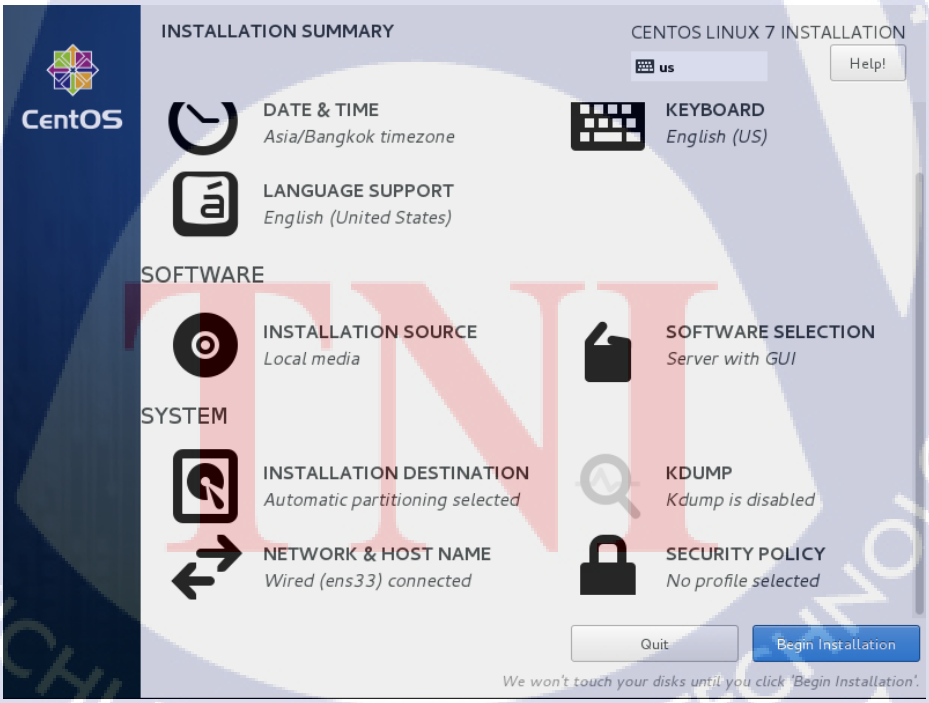
ภาพที่4.112 เข้าไปที่ KDUMP

- เข้าไปปิด KDUMP



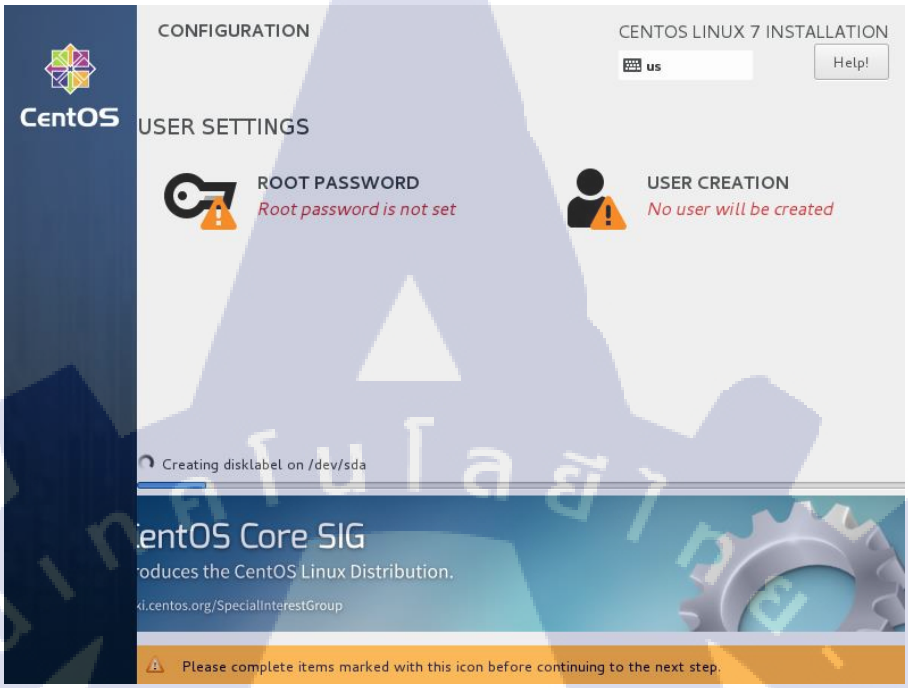
ภาพที่4.113 ตั้งค่า KDUMP

- กด Begin Installation



ภาพที่4.114 เลือก Begin Installation

- เข้าไปตั้งรหัสที่ Root password

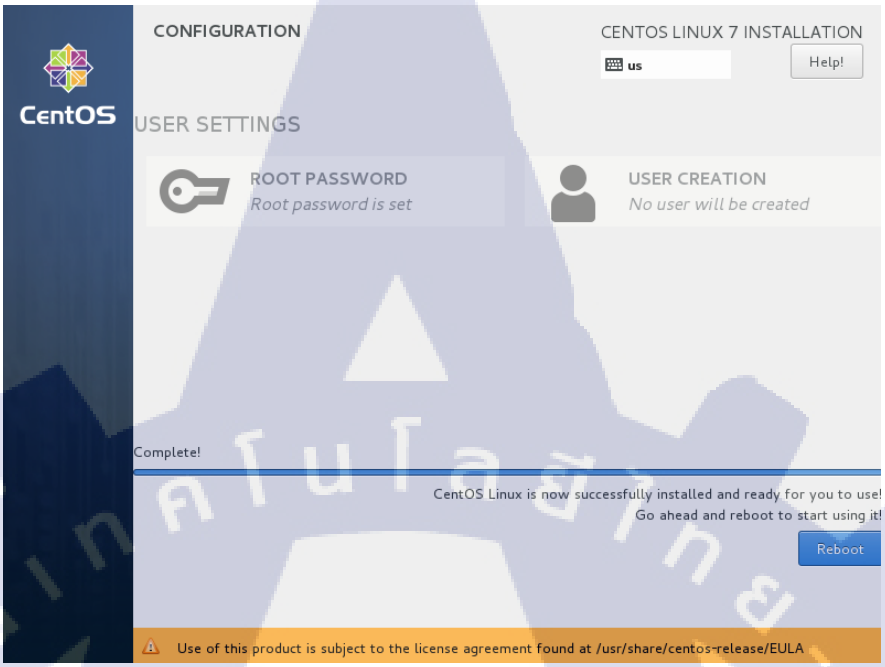


ภาพที่4.115 เข้าไปที่ Root password

- ตั้งรหัสตามที่ต้องการ

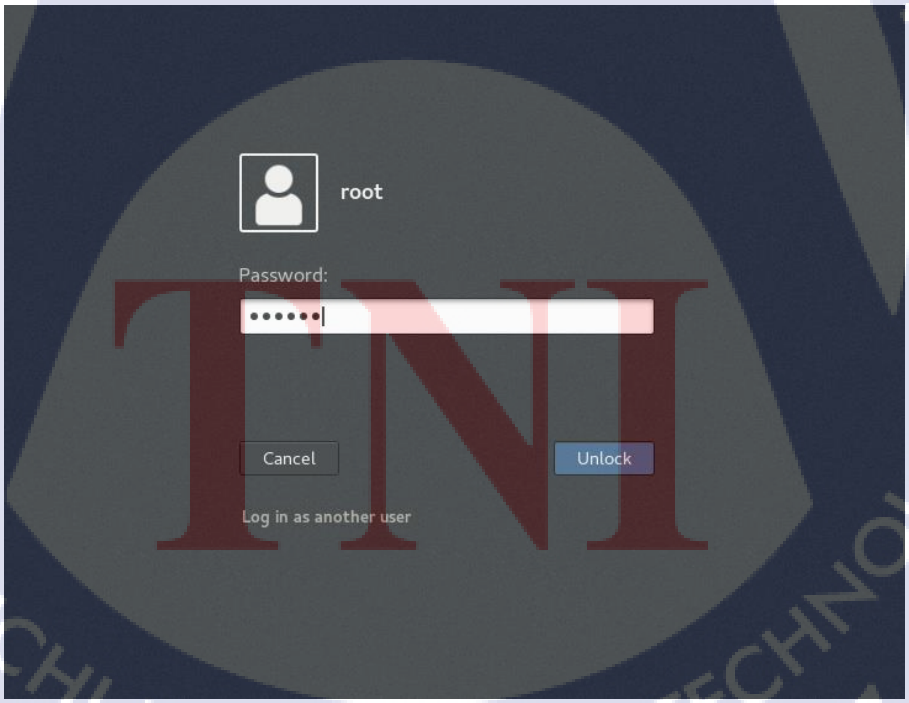
ภาพที่4.116 ตั้งค่า Root password

- ติดตั้งเสร็จแล้วจะมีปุ่มขึ้นมาให้กด Reboot ด้วย



ภาพที่4.117 ทำการ Reboot

- Login ด้วย Root และรหัสที่เราตั้งไว้



ภาพที่4.118 หน้า Login

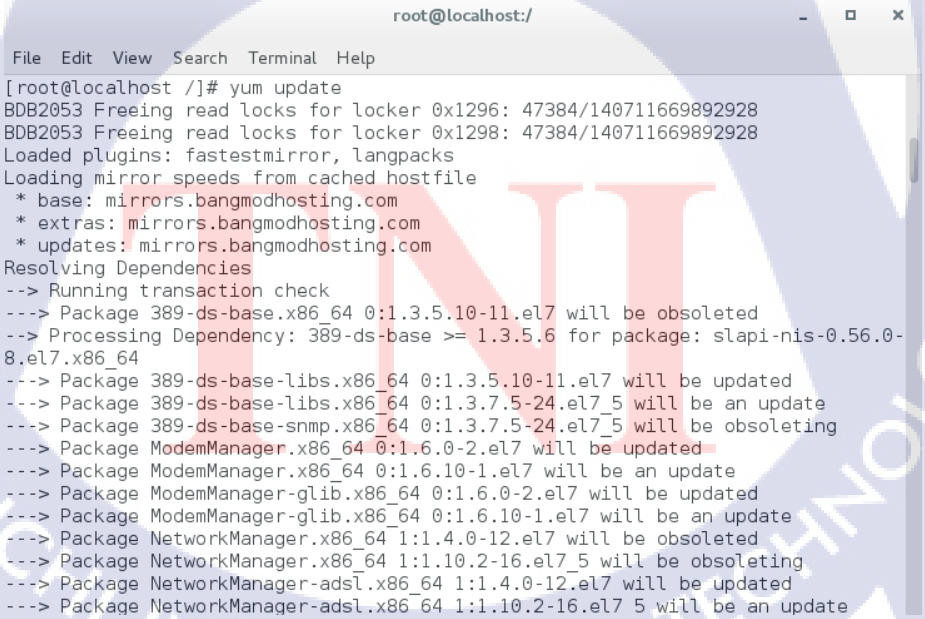
- เข้าหน้า CentOS พร้อมใช้งาน

ภาพที่4.119 หน้า CentOS 7

4.1.2.1 การทำ Linux Hardening

4.1.2.1.2 Yum update

- ใช้คำสั่ง yum update



ภาพที่4.120 Yum update(1)

- เพื่อทำให้ระบบทุกๆอย่างในเครื่องเรา update เป็นตัวล่าสุด

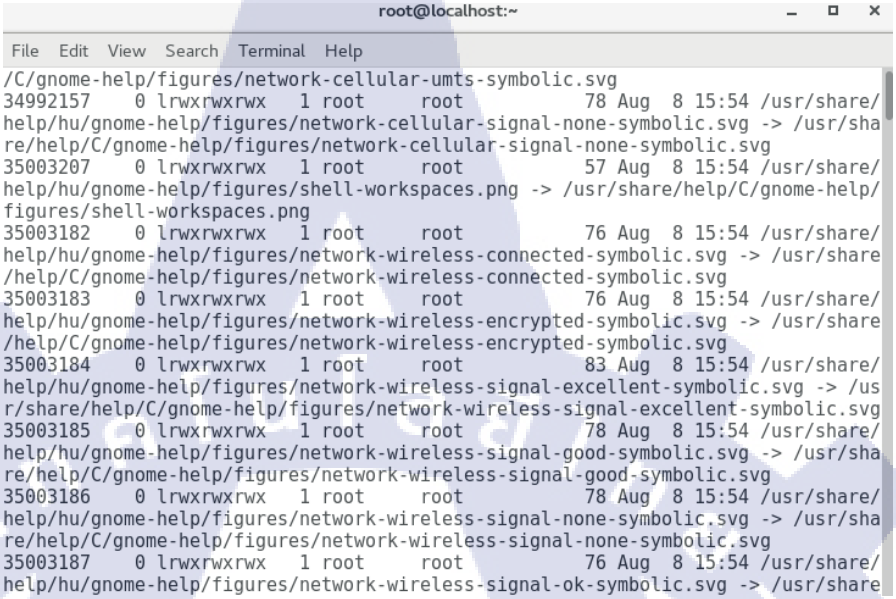
ภาพที่4.121 Yum update(2)

4.1.2.1.3 World-writable Files

- ใช้คำสั่ง find เพื่อเรียกดูไฟล์ทั้งหมดของ Linux Server

ภาพที่4.122 World-writable Files

- ใช้คำสั่งนี้เป็นระยะๆ เพื่อตรวจดูว่าช่วงที่ผ่านมามีไฟล์ที่ World-writable หรือ World-executable อะไรเพิ่มขึ้นมาบ้างมีไฟล์ไหนแปลกปลอมไหม



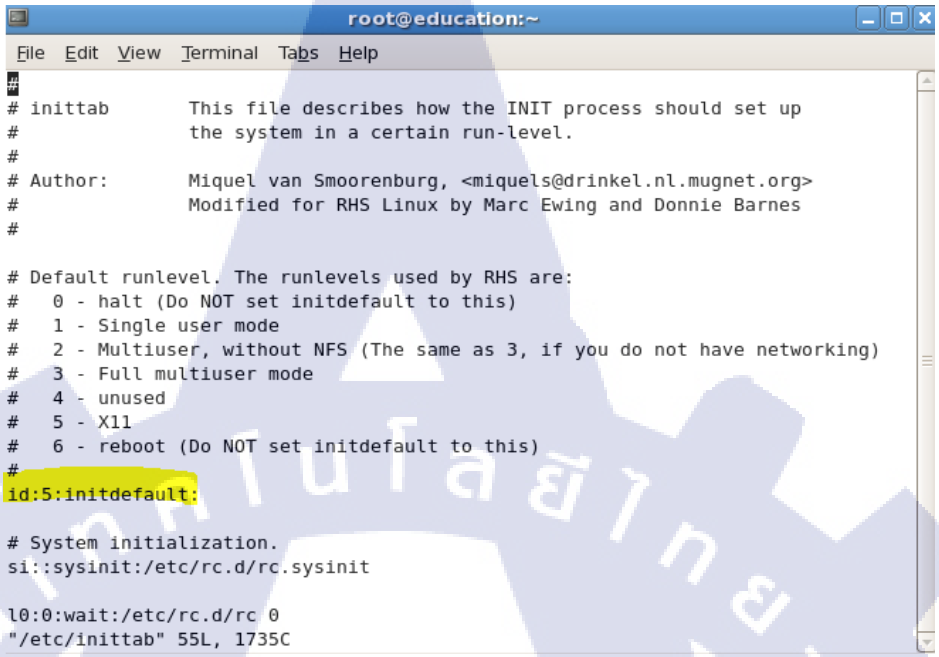
ภาพที่4.123 ตรวจเช็คไฟล์

4.1.2.1.4 Window X disable

- ใช้คำกสั่ง vi เข้าไปแก้ไขไฟล์

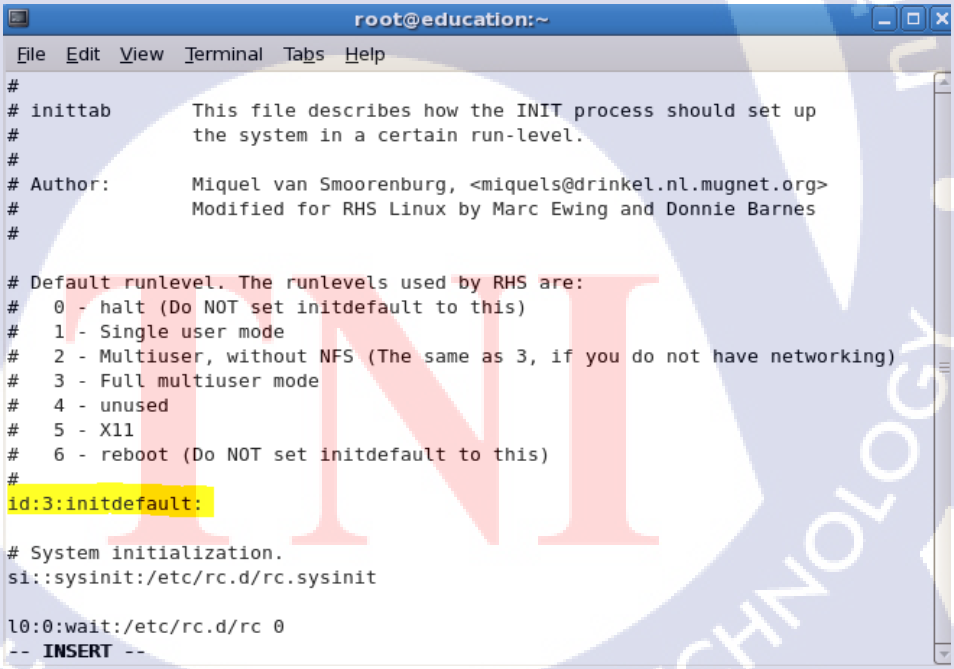
ภาพที่4.124 การปิด GUI (1)

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



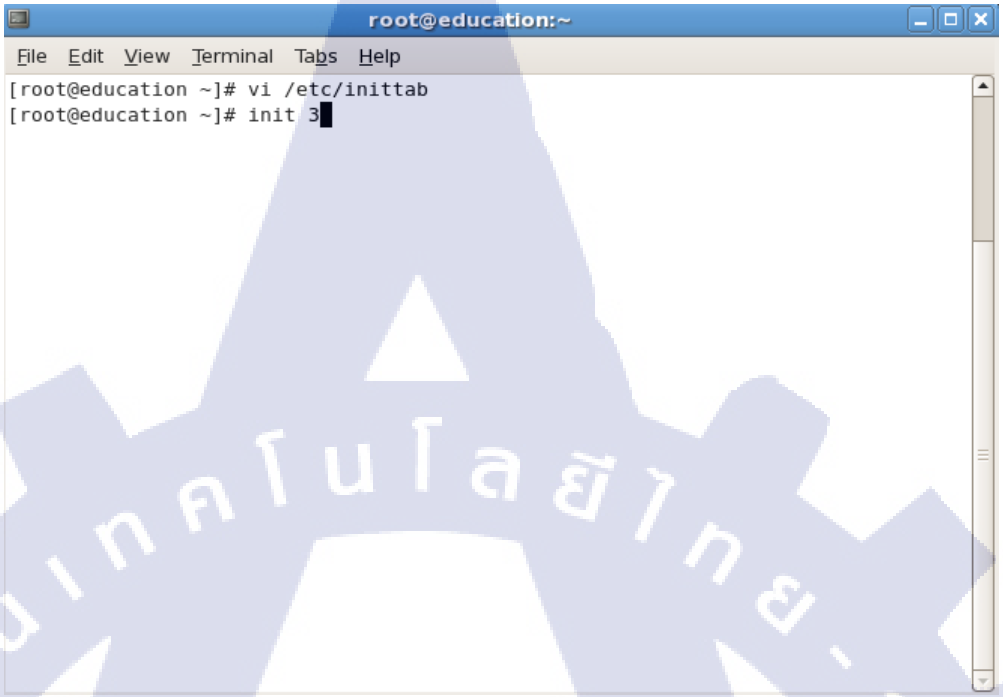
ภาพที่4.125 การปิด GUI (2)

- จากนั้นใช้กด esc แล้วกด : แล้วใช้คำสั่ง wq เพื่อบันทึกแล้วออก



ภาพที่4.126 การปิด GUI (3)

- ใช้คำสั่ง init 3 เพื่อเป็นการปิด GUI



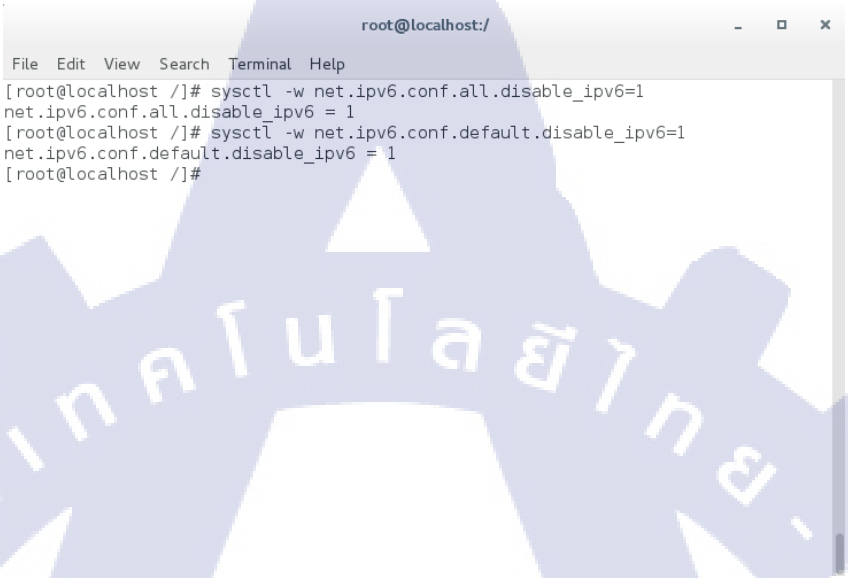
ภาพที่4.127 การปิด GUI (4)

- หน้าจอ GUI จะหายไปกลายเป็นหน้า command line

ภาพที่4.128 การปิด GUI (5)

4.1.2.1.5 Turn off IPv6

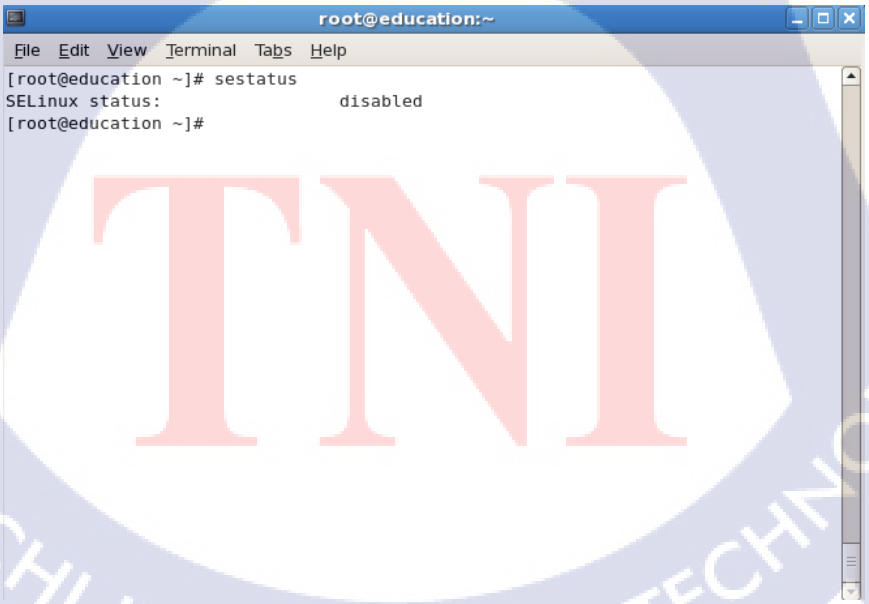
- ปิด ipv6 ด้วยคำสั่ง *sysctl -w net.ipv6.conf.all.disable_ipv6=1* และ *sysctl -w net.ipv6.conf.default.disable_ipv6=1* ถ้าจะเปิดก็ให้เซ็ตกลับมาเป็น *0*



ภาพที่4.129 การปิด IPv6 ใน Linux

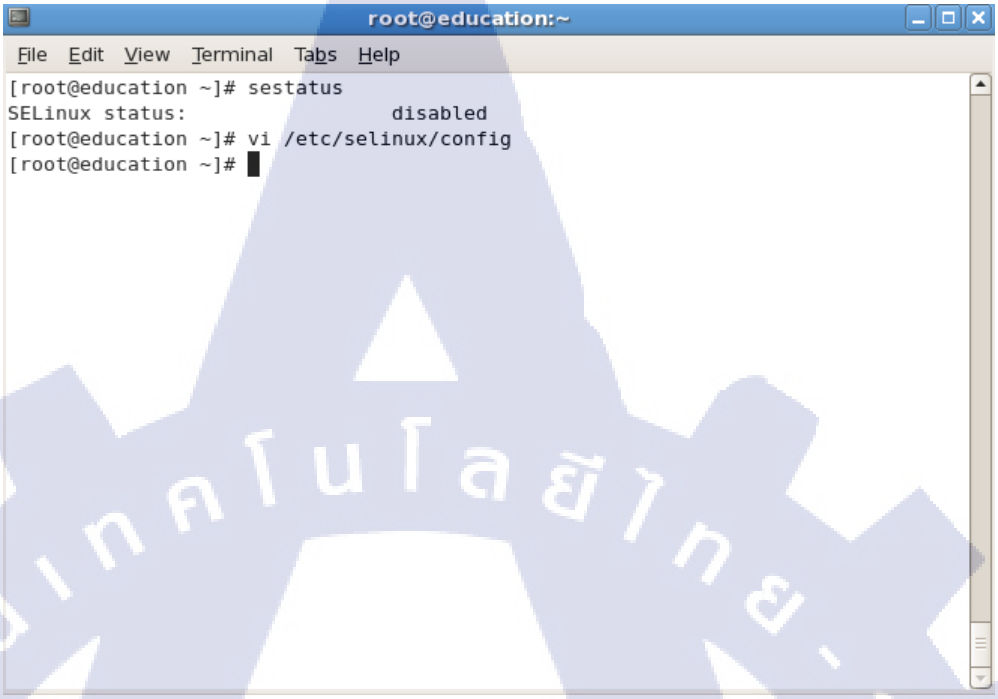
4.1.2.1.6 Selinux

- ใช้คำสั่ง sestatus เพื่อเช็คว่า Selinux เปิดหรือปิดอยู่



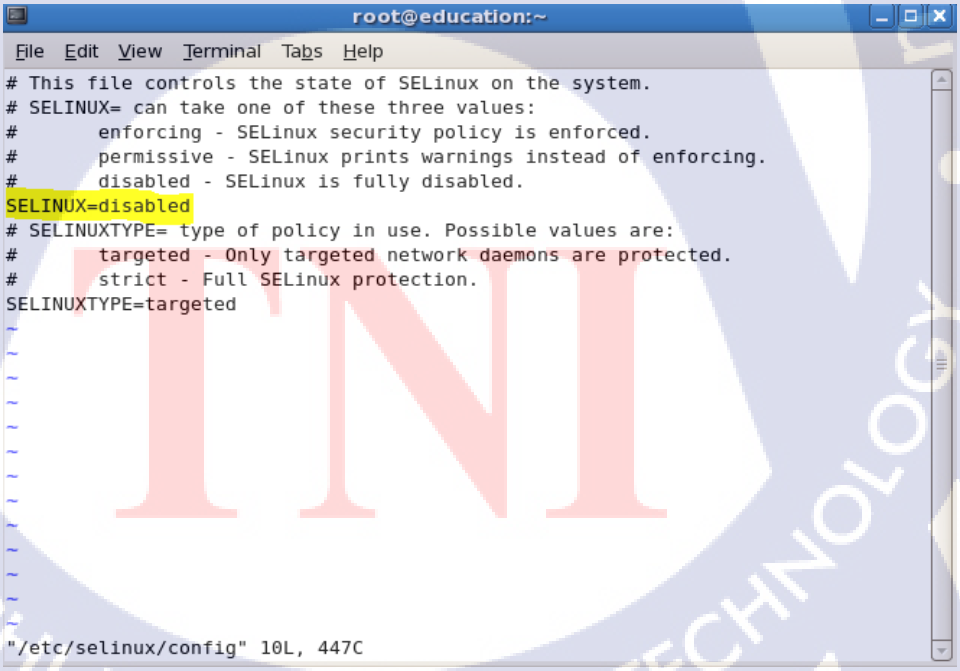
ภาพที่4.130 การเปิด Security-Enhanced Linux(1)

- ใช้คำสั่ง Vi เข้าไปแก้ไขไฟล์



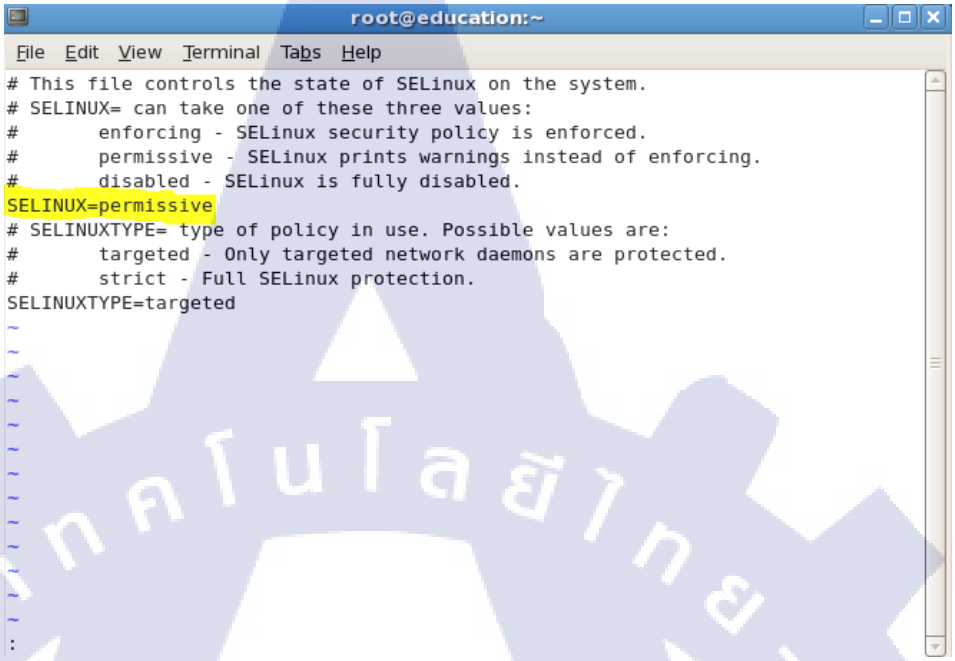
ภาพที่4.131 การเปิด Security-Enhanced Linux(2)

- แก้ไข SELIINUX=disable เป็น permissive



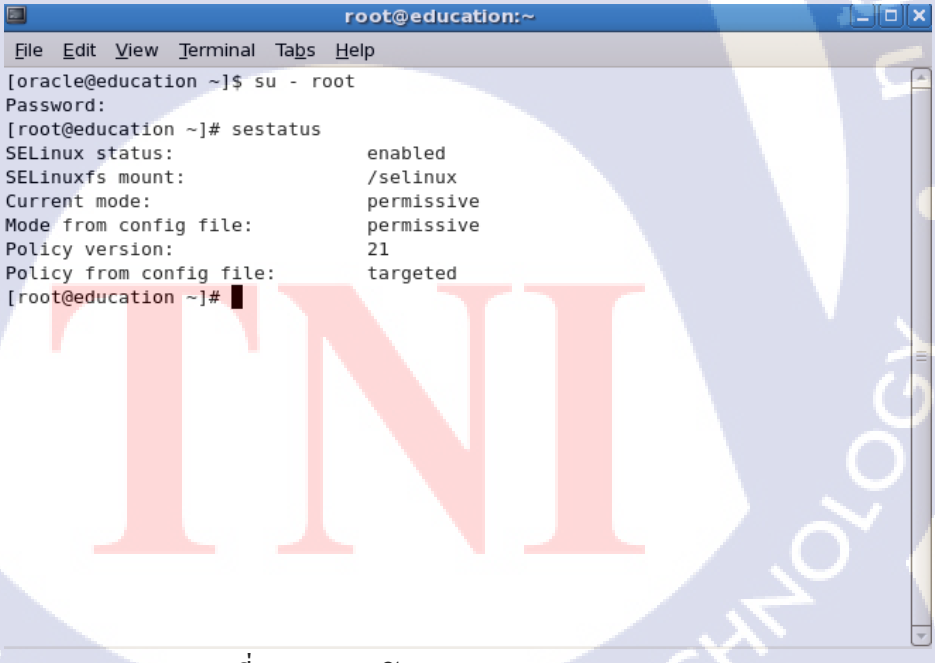
ภาพที่4.132 การเปิด Security-Enhanced Linux(3)

- จากนั้น save แล้วออกด้วย :wq



ภาพที่4.133 การเปิด Security-Enhanced Linux(4)

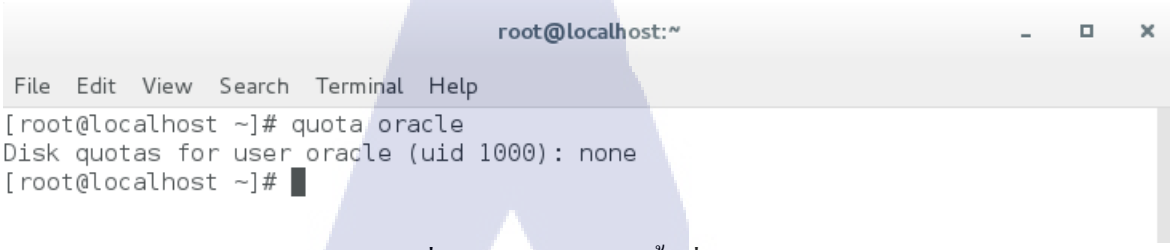
- ใช้คำสั่ง sestatus เพื่อเช็คคราวนี้จะขึ้นเป็น enable แล้ว



ภาพที่4.134 การเปิด Security-Enhanced Linux(5)

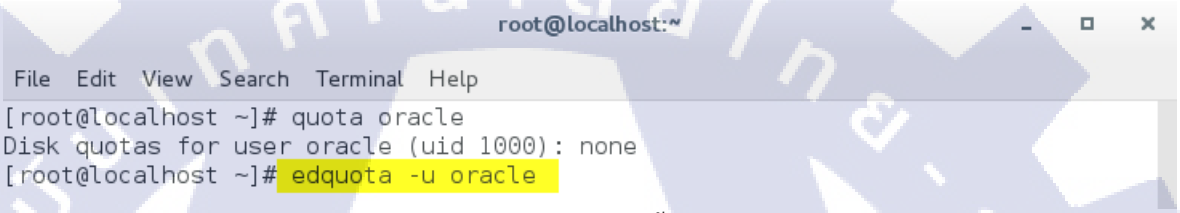
4.1.2.1.7 Quotas

- ใช้คำสั่ง quota แล้วตามด้วย user ที่จะเช็ค ในที่นี้จะให้ user เป็น oracle



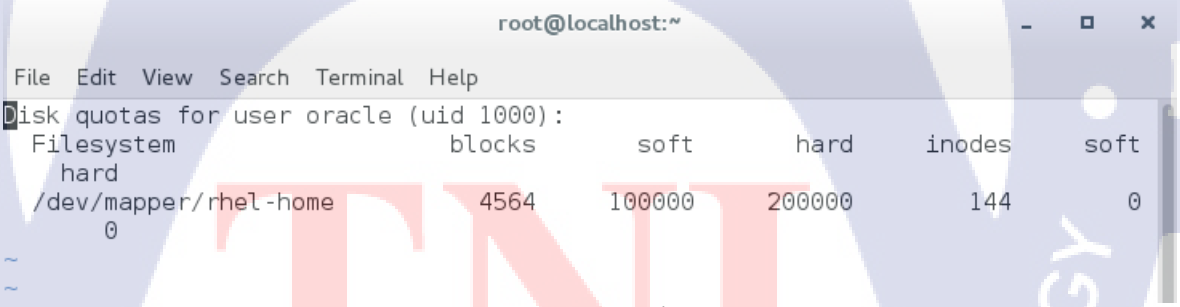
ภาพที่4.135 การกำหนดพื้นที่ Disk ให้ User(1)

- ใช้คำสั่ง edquota เพื่อเข้าไปแก้ไข quotas disk ของ user oracle



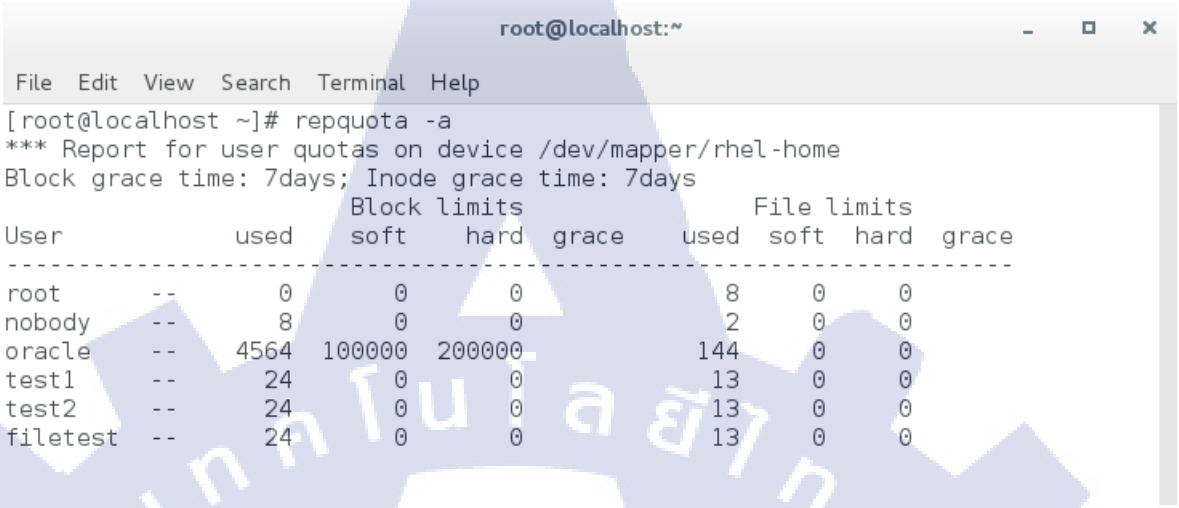
ภาพที่4.136 การกำหนดพื้นที่ Disk ให้ User(2)

- เข้าไปเพิ่มพื้นที่ให้กับ user oracle ในช่อง soft และ hard จากนั้น save แล้วออก ด้วยคำสั่ง :wq



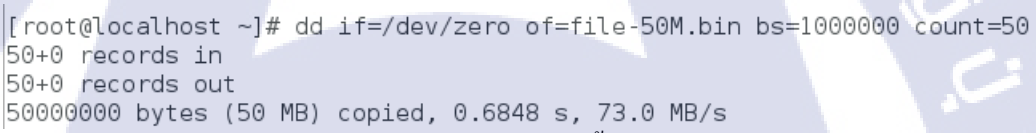
ภาพที่4.137 การกำหนดพื้นที่ Disk ให้ User(3)

- ใช้คำสั่ง repquota -a เพื่อเช็คค่า quota ของทุก user จะเห็นว่า user oracle มีพื้นที่ในส่วนที่เราเพื่อโผล่ขึ้นมาแล้ว



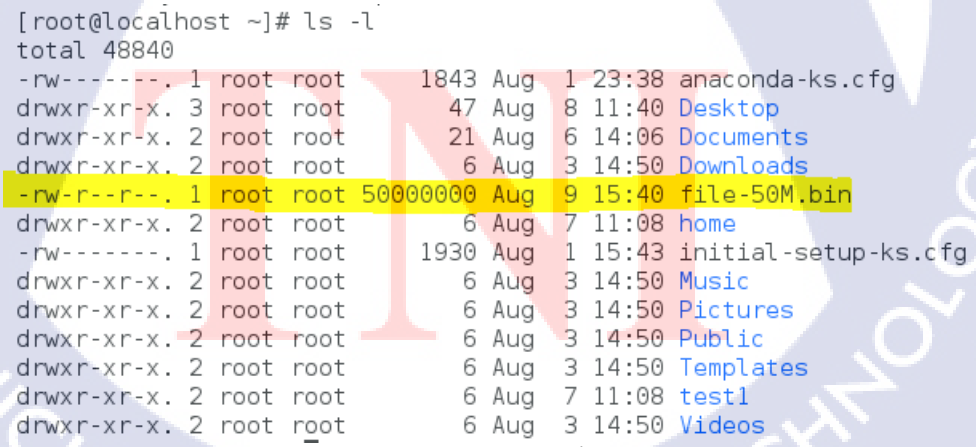
ภาพที่4.138 การกำหนดพื้นที่ Disk ให้ User(4)

- ทำการลอง add ค่าเข้าไปที่ root



ภาพที่4.139 การกำหนดพื้นที่ Disk ให้ User(5)

- ใช้คำสั่ง ls -l เพื่อดูไฟล์ที่พึ่ง add เข้าไปว่ามีพื้นที่เท่าไหร่



ภาพที่4.140 การกำหนดพื้นที่ Disk ให้ User(6)

- ลองมา add ให้ user oracle บ้างโดย add ตั้งแต่ 50,60,70,80 จะเห็นได้ว่าพอ add 80 เข้าไปจะมีข้อความขึ้นมาแจ้งว่าพื้นที่เต็มแล้วไม่สามารถเพิ่มได้อีก 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)

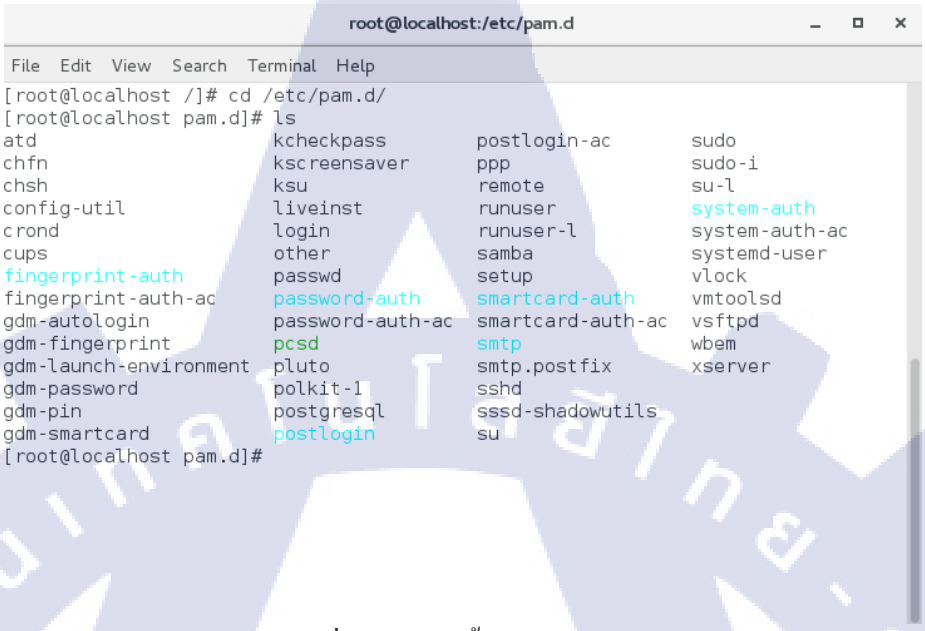
- พื้นที่ของ user oracle หลังจากทำการ add เข้าไปจนเต็ม

```
[oracle@localhost ~]$ quota
Disk quotas for user oracle (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)

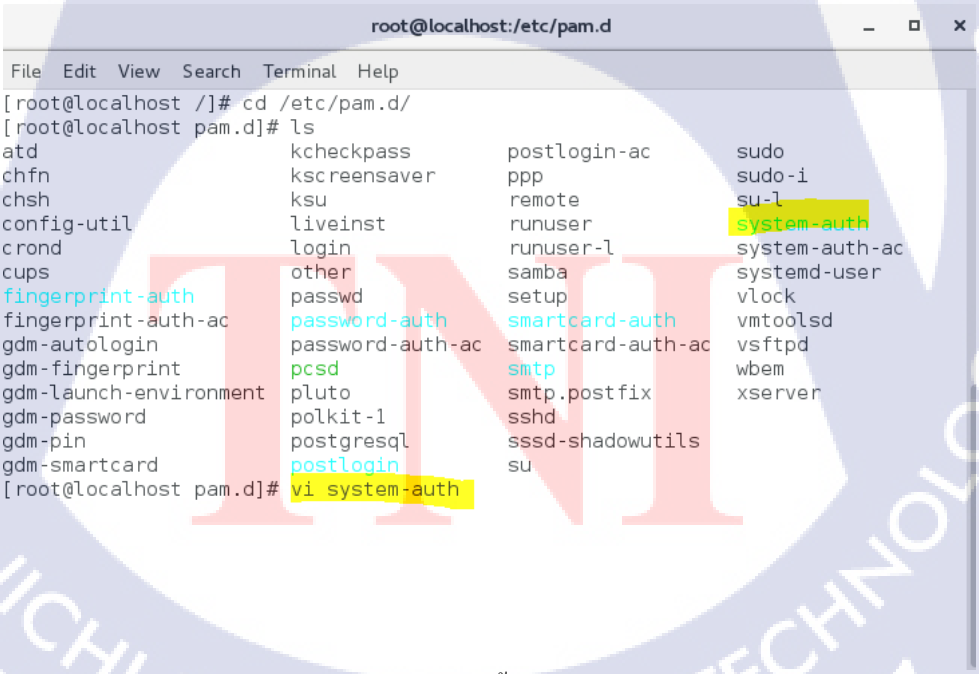
4.1.2.1.8 Password Remember

- ใช้คำสั่ง cd เข้าไปที่ /etc/pam.d



ภาพที่4.143 การตั้งค่า Password Remember(1)

- ใช้คำสั่ง vi เข้าไปแก้พไขไฟล์ system-auth



ภาพที่4.144 การตั้งค่า Password Remember(2)

- หา password sufficient pam_unix.so sha512 shadow nullok try_first_pass use_authtok ให้เพิ่ม remember เข้าไป

ภาพที่4.145 การตั้งค่า Password Remember(3)

- ให้ remember = 2 จากนั้น save ด้วยคำสั่ง :wq

ภาพที่4.146 การตั้งค่า Password Remember(4)

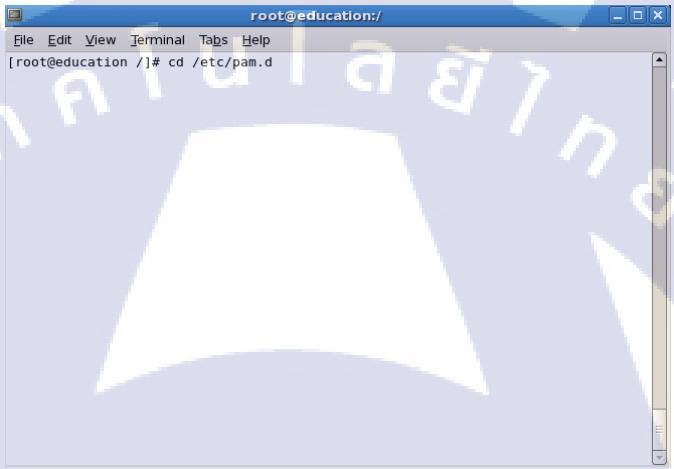
- ทีนี้ถ้า User ที่เคยตั้งรหัสไปแล้วจะไม่สามารถใช้รหัสเดิมมาตั้งได้อีก

```
[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:
```

ภาพที่4.147 การตั้งค่า Password Remember(5)

4.1.2.1.9 Password auth

- ใช้คำสั่ง cd เข้าไปที่ /etc/pam.d

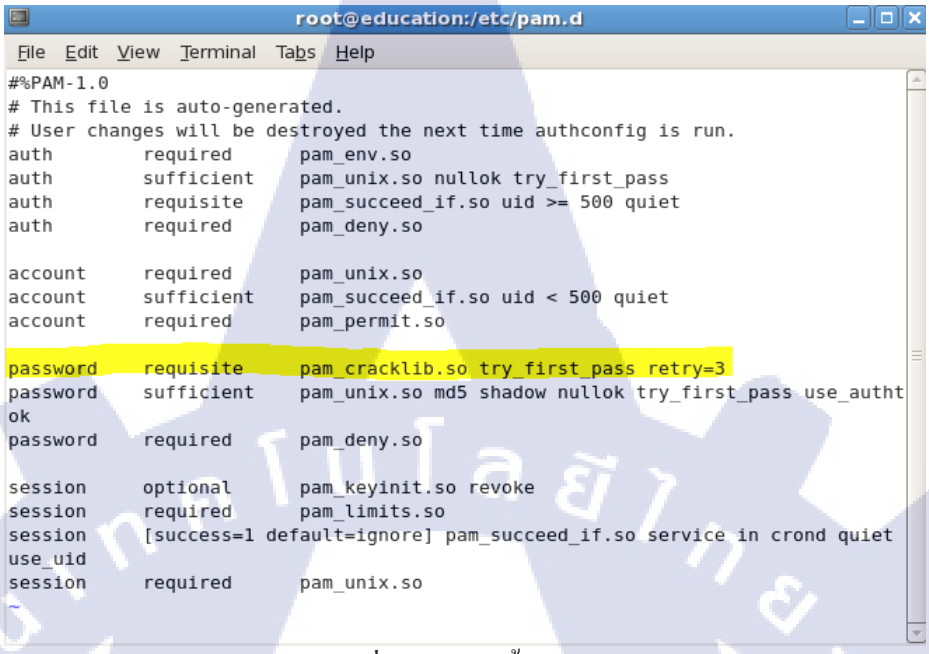


ภาพที่4.148 การตั้งค่า Password auth(1)

- ใช้คำสั่ง Vi เข้าไปแก้ไขไฟล์ system-auth

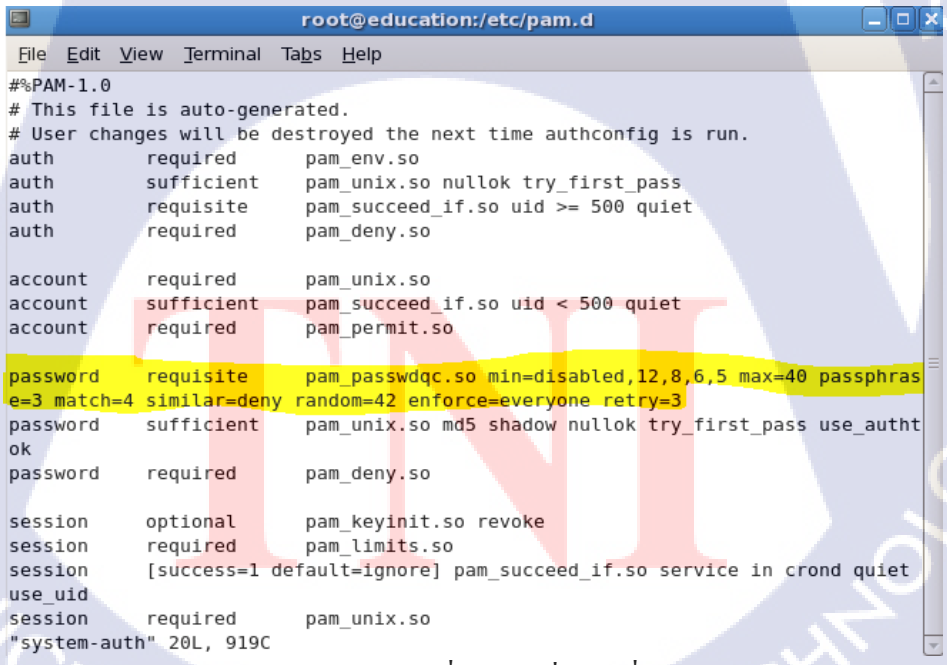
ภาพที่4.149 การตั้งค่า Password auth(2)

- เปลี่ยนเงื่อนไขในการตั้งรหัสผ่านในบรรทัดที่ดไว้



ภาพที่4.150 การตั้งค่า Password auth(3)

- แก้ไขและเพิ่มเงื่อนไขเข้าไป ทำให้การตั้งรหัสผ่านมีข้อแม้มากขึ้นละปลอดภัยยิ่งขึ้น

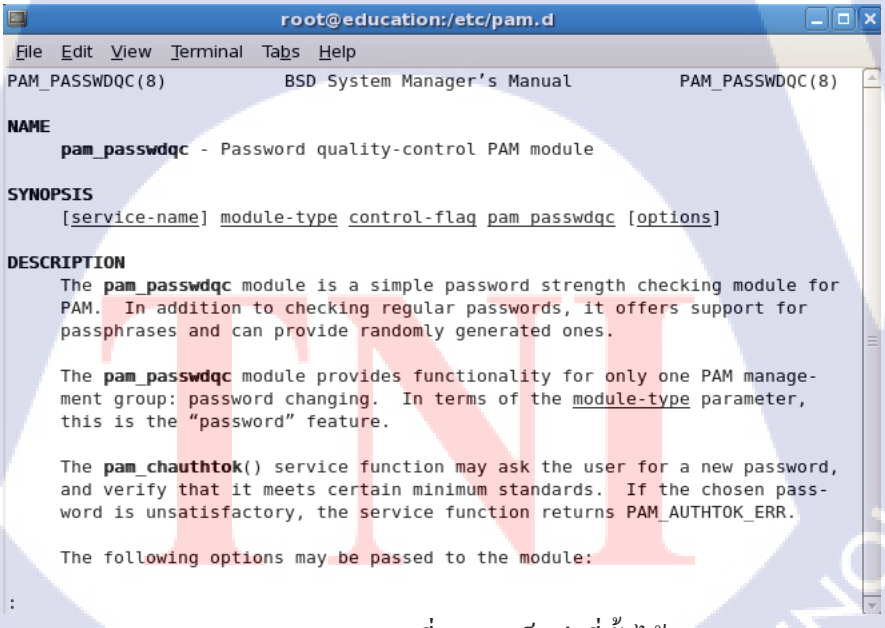


ภาพที่4.151 เพิ่มเติมเงื่อนไข

- ใช้คำสั่ง man pam_passwdqc เพื่อเข้าไปตรวจสอบว่าที่เราตั้งไว้ขึ้นไหม

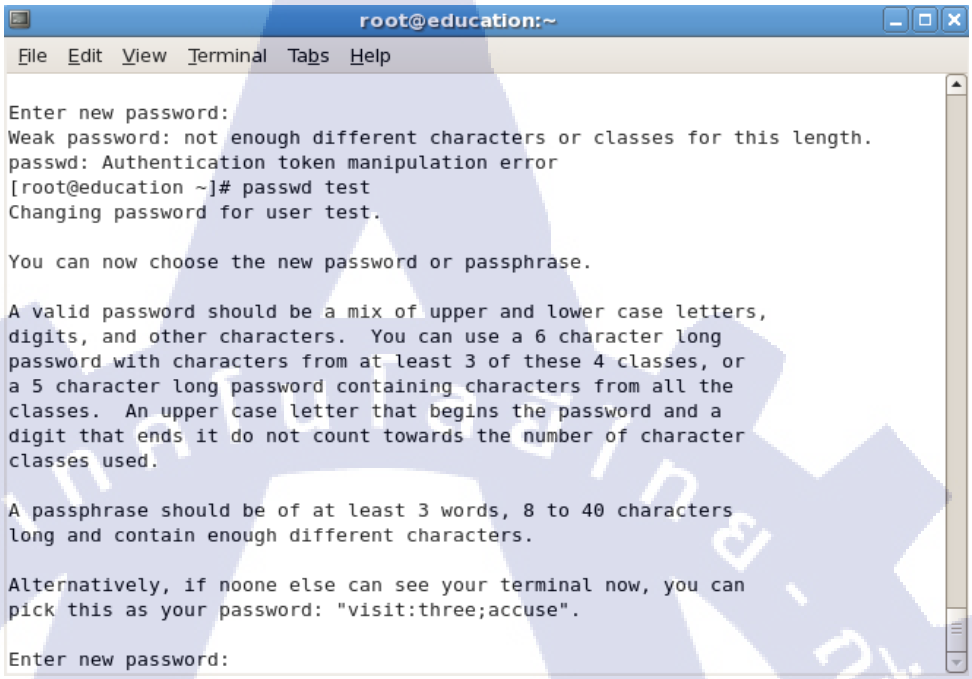
ภาพที่4.152 คำสั่งเช็คค่า

- เข้ามาตรวจสอบว่าถูกไหม



ภาพที่4.153 เช็คค่าที่ตั้งไว้

- ลองตั้ง password ให้ user test จะเห็นว่ารหัสที่ระบบทำการสุ่มตัวอย่างมาให้ดูนั้นยากขึ้นยาวขึ้นมีตัวอักษรพิเศษอยู่ด้วยทำให้รหัสยากแก่การขาดเดาอย่างมาก



ภาพที่4.154 ลองตั้ง Password

4.1.2.1.10 Password aging

- ใช้คำสั่ง chage -l เพื่อเช็คว่าตั้งค่าไว้ยังไงบ้าง

ภาพที่4.155 เช็คค่า

- 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)

- คำสั่ง 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 expires       : 7
```

ภาพที่4.157 ตั้งค่า Password aging(2)

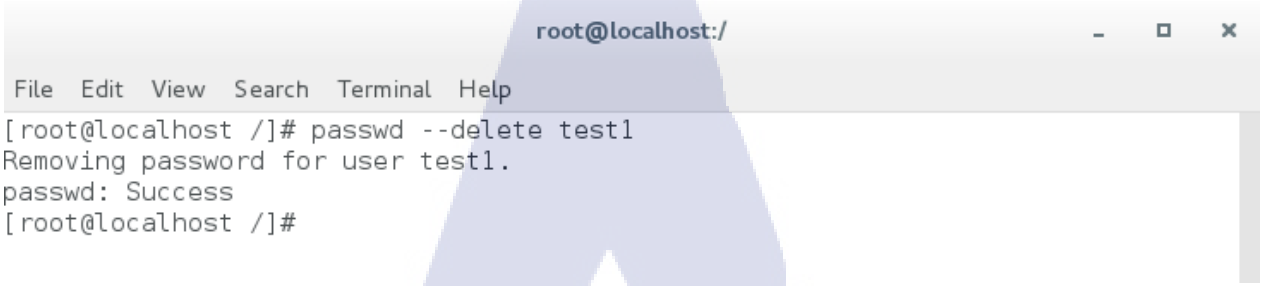
4.1.2.1.11 No Password

- ใช้คำสั่งเพื่อเช็คดูว่ามี user คนไหนในระบบไม่มีรหัสบ้าง

```
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
[root@localhost /]#
```

ภาพที่4.158 เช็คค่า Password(1)

- ลองลบรหัสของ user test1 ออกดูว่าจะเป็นยังไง



ภาพที่4.159 ลบ Password

- ใช้คำสั่งพื่อหา user ที่ไม่มีรหัสอีกทีและจะพบว่ามี user test1 โผล่ขึ้นมา

ภาพที่4.160 เช็คค่า Password(2)

4.1.2.1.12 No owner file

- ใช้คำสั่งเช็คดูว่าไฟล์เจ้าของเป็นใครมีสิทธิอะไรในไฟล์บ้าง

ภาพที่4.161 เช็คสิทธิของไฟล์(1)

- ใช้สิทธิ Root เปลี่ยนเจ้าของไฟล์ให้เป็น nobody:nobody

ภาพที่4.162 ตั้งค่าสิทธิ

- ใช้คำสั่งดูอีกทีจะเห็นว่าเจ้าของไฟล์และกลุ่มเปลี่ยนไปเป็น 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)

- ใช้คำสั่ง vi โดยใช้ user test1 เข้าไปดูไฟล์ public.txt

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

ภาพที่4.164 เข้าไปแก้ไขไฟล์

- จะมีข้อความขึ้นมาข้างล่างว่าเราไม่มีสิทธิที่จะทำอะไรกะไฟล์นี้เลย

ภาพที่4.165 ไม่มีสิทธิเข้าถึง

- ใช้คำสั่ง chmod 777 กับไฟล์ public.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
```

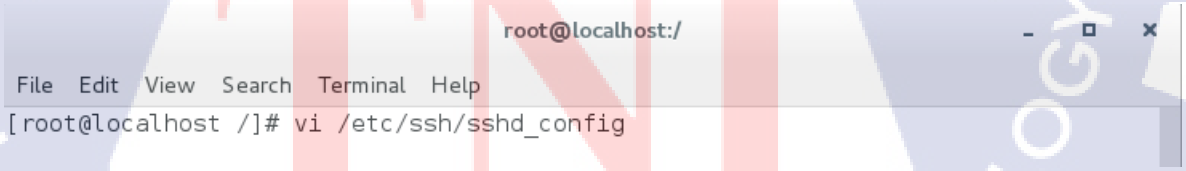
ภาพที่4.167 เข้าไปเช็คสิทธิการเข้าถึง

- รอบนี้จะเห็นข้องความที่อยู่ด้านในแล้วและยังสามารถแก้ไขได้อีกด้วยโดยที่ทุกๆ user ก็สามารถทำได้เช่นกัน

ภาพที่4.168 ข้อความที่ตอนแรกไม่เห็น

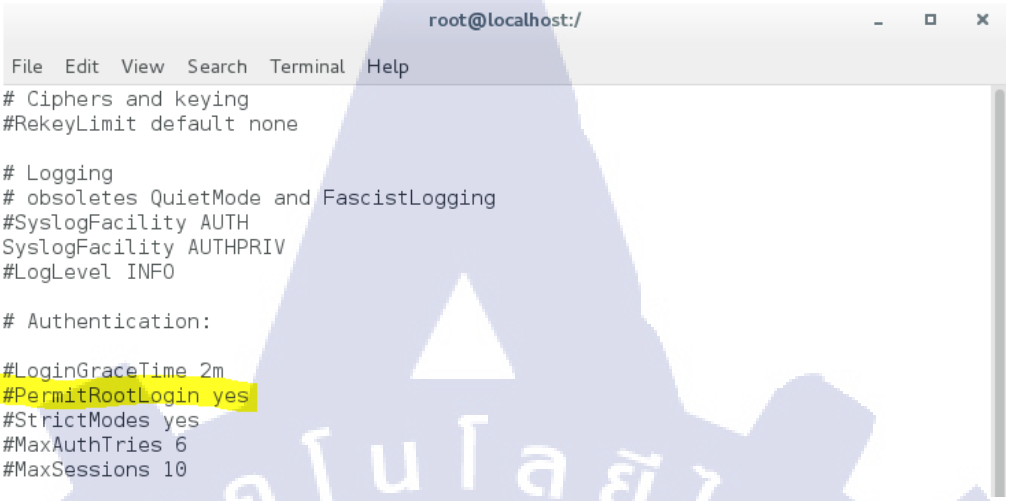
4.1.2.1.13 Disable root login

- ใช้คำสั่ง vi เข้าไปแก้ไขไฟล์ sshd_config



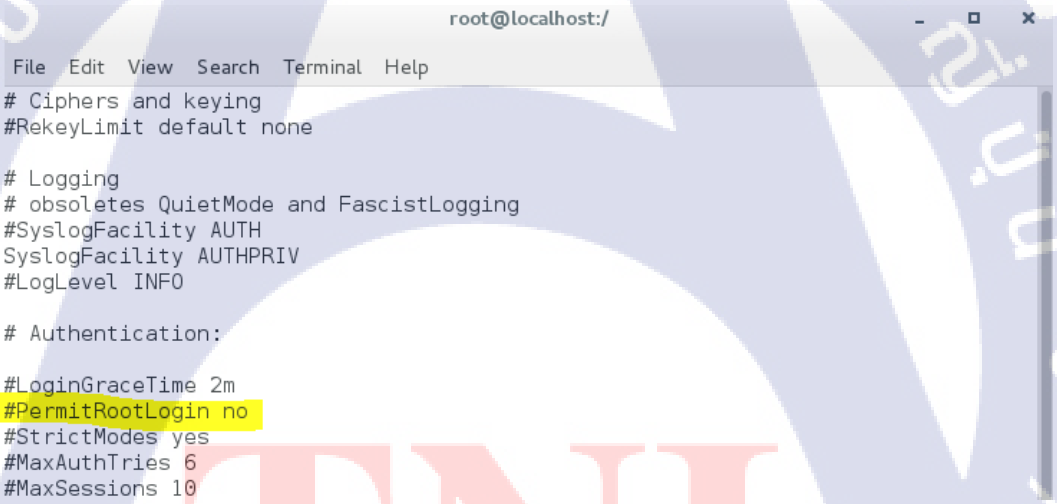
ภาพที่4.169 Disable Root login(1)

- เข้าไปเปลี่ยน PermitRootLogin จาก yes เป็น no



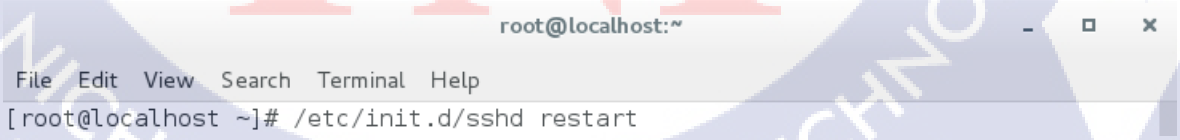
ภาพที่4.170 Disable Root login(2)

- ใช้คำสั่ง :wq เพื่อ save



ภาพที่4.171 Disable Root login(3)

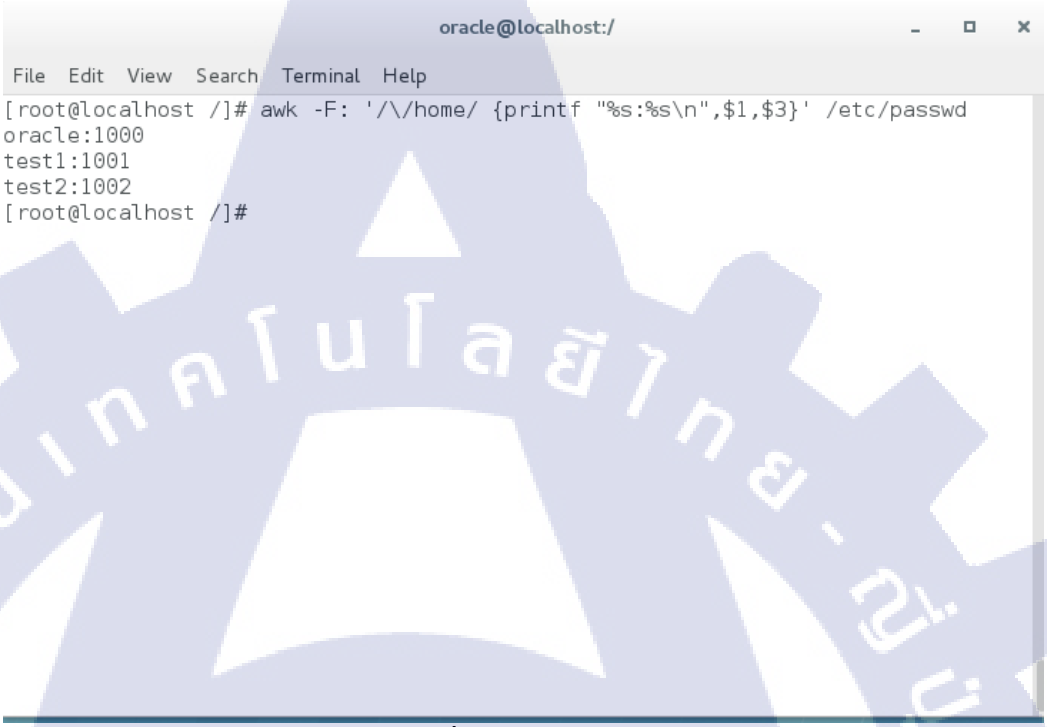
- จากนั้น restart



ภาพที่4.172 Restart sshd

4.1.2.1.14 User UID not set to 0

- ใช้คำสั่งเพื่อเช็คว่ามี user คนไหนในระบบมี UID 0 ไหมถ้ามีจะต้องเปลี่ยนให้เป็น UID อื่น



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
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
#PrintMotd yes
#PrintLastLog yes
#TCPKeepAlive yes
#UseLogin no
UsePrivilegeSeparation sandbox          # Default for new installations.
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#ShowPatchLevel no
#UseDNS yes
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
```

ภาพที่4.177 ตั้งค่า ClientAlive(1)

- แก้เป็น #ClientAliveInterval 360 และ #ClientAliveCountMax 0

```
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
#PrintMotd yes
#PrintLastLog yes
#TCPKeepAlive yes
#UseLogin no
UsePrivilegeSeparation sandbox          # Default for new installations.
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 360
#ClientAliveCountMax 0
#ShowPatchLevel no
#UseDNS yes
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
```

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 นั้นเก่ากว่าและปลอดภัยน้อยกว่ามากจึงจำเป็นต้องเปลี่ยนให้ใช้แค่ Protocal ที่ 2

- เปลี่ยน #Protocal ให้เหลือแค่ 2

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

ภาพที่4.180 ตั้งค่าการใช้ Protocol(1)

- จากนั้นลบ # แล้วใช้คำสั่ง :wq เพื่อ save แล้วทำการ restart ด้วยคำสั่ง service sshd restart

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

ภาพที่4.181 ตั้งค่าการใช้ Protocol(2)

4.1.2.1.16 Audit

- ใช้คำสั่งเพื่อเปิดใช้งาน auditd

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

ภาพที่4.182 Audit Setting(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
```

ภาพที่4.184 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
```

ภาพที่4.185 Audit Setting(4)

- แก้ไข flush = INCREMENTAL_ASYNC เป็น INCREMENTAL max_log_file = 8 เป็น 6 และ freq = 50 เป็น 20

```
log_file = /var/log/audit/audit.log
log_group = 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
```

ภาพที่4.186 Audit Setting(5)

- แก้ไข tcp_listen_port = 60 เป็น ไม่มี

```
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
use_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
```

ภาพที่4.187 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
 * extras: mirror2.totbb.net
 * 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 be an update
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package        Arch          Version                Repository        Size
================================================================================
Updating:
 gnupg2         x86_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: keyring `/root/.gnupg/pubring.gpg' created
```

ภาพที่4.189 สร้างไฟล์

- ใช้คำสั่ง ls ที่ Desktop เพื่อดูไฟล์ที่เราสร้างไว้

```
[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/license
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

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 เช็คไฟล์

- ข้อความในไฟล์ test.txt

```
Hello
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
-- INSERT --
```

ภาพที่4.193 ดูข้อความในไฟล์

- ใช้คำสั่ง cat ดพื่อดูข้อความที่อยู่ในไฟล์

```
[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 ทำการลบไฟล์

- ใช้คำสั่ง cat เพื่อดูไฟล์ test.txt.gpg ที่ได้ทำการ Encrypt ไว้จะเห็นได้ว่าข้อความจะนั้นจะไม่แสดงออกมาให้เห็นแต่จะออกมาในรูปแบบข้อความที่ถูกเข้ารหัสเอาไว้แล้ว

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

ภาพที่4.196 เรียกดูไฟล์ที่ทำการ Encrypt ไว้

- ใช้คำสั่งเพื่อ Decrypt ไฟล์ gpg แต่เราจำต้องรู้รหัสที่ถูกตั้งไว้ตอน Encrypt ถึงจะสามารถ 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: new3.txt (stored 0%)
```

ภาพที่4.198 zip ไฟล์

- ใช้คำสั่ง ls เพื่อดูไฟล์ที่ได้ทำการ zip ไว้

```
[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

- ใช้คำสั่ง 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: new.txt
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
```

ภาพที่4.200 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

- เพิ่มคำสั่งเข้าไปในไฟล์ httpd.conf

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

ภาพที่4.204 เพิ่มคำสั่ง

- ใช้คำสั่ง systemctl 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: 5760 (vsftpd)
   CGroup: /system.slice/vsftpd.service
           └─5760 /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.
```

ภาพที่4.206 Check Status

- ใช้คำสั่ง vsftpd stop เพื่อหยุดหารทำงานของ FTP เพื่อเป็นการปิดสิ่งที่เราไม่ได้ใช้งาน

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

ภาพที่4.207 Stop service

4.1.2.1.21 Stop unused services

- ใช้คำสั่ง ps ax เพื่อทำการเช็ค Service ที่ทำงานอยู่บนเครื่อง

```
2840 ?        S      0:00 /sbin/dhclient -d -q -sf /usr/libexec/nm-dhcp-helper
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]
6365 ?        S      0:00 [kworker/0:0]
6397 ?        S<     0:00 [kworker/1:1H]
6414 ?        S      0:00 [kworker/1:0]
6458 ?        R      0:00 [kworker/1:1]
6565 ?        S<     0:00 [kworker/1:2H]
6583 ?        S      0:00 [kworker/0:2]
6594 ?        S      0:00 [kworker/1:2]
6605 ?        S      0:00 pickup -l -t unix -u
6650 ?        Ss     0:00 /usr/sbin/httpd -DFOREGROUND
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/httpd -DFOREGROUND
6657 ?        S      0:00 /usr/sbin/httpd -DFOREGROUND
6658 ?        S      0:00 /usr/sbin/httpd -DFOREGROUND
6659 ?        S      0:00 /usr/sbin/httpd -DFOREGROUND
6682 ?        S<     0:00 [kworker/1:0H]
6691 ?        S      0:00 sleep 60
6693 pts/0    R+     0:00 ps ax
```

ภาพที่4.208 ดู Service ต่างๆ

- ใช้คำสั่ง ps ax | grep httpd เพื่อทำการดู Service ที่ทำงานอยู่และชื่อตรงกับที่เรากำหนดทั้งหมดออกมา

```
[root@localhost Desktop]# ps ax | grep httpd
  6650 ?        Ss     0:00 /usr/sbin/httpd -DFOREGROUND
  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/httpd -DFOREGROUND
  6657 ?        S      0:00 /usr/sbin/httpd -DFOREGROUND
  6658 ?        S      0:00 /usr/sbin/httpd -DFOREGROUND
  6659 ?        S      0:00 /usr/sbin/httpd -DFOREGROUND
  6998 pts/0    R+     0:00 grep --color=auto httpd
```

ภาพที่4.209 เช็ค httpd service

- ใช้คำสั่ง systemctl stop httpd เพื่อเป็นการหยุดการทำงานของ httpd

```
[root@localhost Desktop]# systemctl stop httpd
```

ภาพที่4.210 Stop httpd service

- ใช้คำสั่ง ps ax และ ps ax | grep httpd เพื่อทำการเช็คว่า Service httpd ที่ปิดไปยังทำงานอยู่อีกไหม

```
  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 unix -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@localhost Desktop]# ps ax | grep httpd
  7028 pts/0    R+     0:00 grep --color=auto httpd
[root@localhost Desktop]#
```

ภาพที่4.211 เช็ค Service

4.1.2.1.22 Physical Security

4.1.2.1.22.1 แนวทางการป้องกันความปลอดภัยทางกายภาพของระบบ

1. แบ่งแยกพื้นที่ควบคุมความปลอดภัยอย่างชัดเจน เช่น การแยกห้องที่เก็บเครื่องเซิร์ฟเวอร์และอนุญาตให้เฉพาะผู้ดูแลระบบเท่านั้นที่เข้าถึงได้
2. ใช้ระบบป้องกันและตรวจสอบการเข้าออกพื้นที่ควบคุมความปลอดภัย เช่น การใช้ key card ที่สามารถบันทึกได้ว่าใครเข้าออกได้ หรือการใช้กล้องวิดีโอ เป็นต้น
3. เก็บรักษาระบบและอุปกรณ์ต่างๆ เช่น backup tape, เซิร์ฟเวอร์ ในพื้นที่ควบคุมความปลอดภัยและอนุญาตให้เข้าถึงได้เฉพาะผู้ดูแลระบบเท่านั้น
4. ใช้เครื่องจ่ายกำลังไฟฟ้าสำรองหรือ UPS เพื่อให้ระบบสามารถใช้ไฟฟ้าได้อย่างต่อเนื่อง
5. วางแผนสำหรับการกู้ระบบคืนเมื่อมีเหตุการณ์เลวร้ายเกิดขึ้น
6. ตรวจสอบข้อมูลของเจ้าหน้าที่จากภายนอกที่เข้ามาให้คำปรึกษาหรือปฏิบัติงานภายในพื้นที่ควบคุมความปลอดภัย ถ้าหากเจ้าหน้าที่ผู้นั้นต้องการใช้สิทธิของ root ในการทำงานกับระบบ ผู้ดูแลระบบจะต้องทำการ login ให้ด้วยตนเอง หลังจากนั้นต้องคอยติดตามดูว่าผู้นั้นทำอะไรกับระบบบ้าง และเมื่อเสร็จภารกิจแล้วให้ทำการเปลี่ยนรหัสผ่านของ root ทันที

4.1.2.1.22.2 แนวทางการป้องกันความปลอดภัยทางกายภาพภายในเครื่องคอมพิวเตอร์

1. การล็อคเครื่องคอมพิวเตอร์ (Computer Lock) เช่น การใช้กุญแจล็อคที่ตัวเครื่อง เพื่อช่วยในการป้องกันเครื่องและอุปกรณ์ภายในเครื่องจากการถูกลักขโมย หรือทำการเปิดเครื่องเพื่อสร้างความเสียหายต่อฮาร์ดแวร์ภายในได้ และเป็นการป้องกันการรีบูตเครื่องด้วยแผ่นดิสก์หรือฮาร์ดแวร์อื่นๆด้วย
2. การรักษาความปลอดภัยใน BIOS (BIOS Security) เนื่องจาก BIOS มีความสำคัญต่อโปรแกรมที่ใช้บูตเข้าระบบ เช่น LILO ดังนั้นจึงควรปรับแต่งค่าใน BIOS เพื่อป้องกันผู้โจมตีทำการรีบูตเครื่อง มีวิธีการโดยสรุปดังนี้

    2.1 ปรับแต่งให้ป้อนรหัสผ่านตอนที่บูตเครื่อง ซึ่งอาจจะไม่สามารถป้องกันได้ 100% เนื่องจากผู้โจมตีสามารถทำการรีเซ็ตที่ BIOS ได้ แต่ก็เป็นการชะลอเวลาของผู้โจมตี

    2.2 ปรับแต่งให้เครื่องไม่สามารถใช้แผ่นดิสก์ในการบูตเครื่อง

2.3 ปรับแต่งให้ป้อนรหัสผ่านทุกครั้งก่อนที่จะทำการปรับแต่ง BIOS

หมายเหตุ การตั้งรหัสผ่านตอนบูตมีข้อเสียคือ ถ้าเกิดเหตุขัดข้องบางประการ เช่น ไฟฟ้าดับเป็นเวลานาน ส่งผลให้ต้องมีการบูตใหม่ ผู้ดูแลระบบเองจะต้องอยู่ใกล้เครื่องเพื่อที่จะป้อนรหัสผ่าน มิฉะนั้นระบบจะไม่สามารถทำงานต่อไปได้

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 เมื่อมีการเพิ่มค่าพารามิเตอร์ที่ LILO prompt (เช่น single) นอกจากนี้ยังมี prompt ที่จะใช้ระบุว่าทุกครั้งที่เปิดเครื่องต้องมีการเข้าสู่ boot prompt ก่อน และ timeout นั้นใช้บอกเวลาในหน่วยวินาทีที่ใช้รอรับอินพุตจากคีย์บอร์ดว่าจะเลือกบูตไฟล์ image ใด และการปรับแต่งให้ป้อนรหัสผ่านยังคงไม่สามารถป้องกันการบูตจากแผ่นดิสก์ และการ mount root partition ดังนั้นควรที่จะใช้ BIOS Security ควบคู่ไปกับ Boot Loader Security เช่น การปรับแต่งให้ไม่สามารถบูตจากแผ่นดิสก์ และให้ป้อนรหัสผ่านก่อนเข้าใช้งาน BIOS
4. การล็อคหน้าจอมอนิเตอร์ (Screen Lock) ในขณะที่ผู้ดูแลระบบใช้งานเครื่องค้างอยู่ และต้องหยุดการใช้งานดังกล่าวก่อนชั่วคราว แต่ยังไม่ต้องการที่จะ Logout ออกจากระบบ ก็ใช้คำสั่งในการล็อคหน้าจอเพื่อป้องกันผู้อื่นที่ไม่รู้รหัสผ่านของผู้ดูแลระบบเข้ามาใช้งานเทอร์มินัลที่ทำงานค้างไว้ได้ ตัวอย่างโปรแกรมดังกล่าวเช่น xlock สำหรับ X-windows และ vlock สำหรับ Text-mode
5. การตรวจสอบการเปลี่ยนแปลงของความปลอดภัยทางกายภาพ (Detecting Physical Security Compromises) วิธีที่ง่ายที่สุดในการตรวจสอบว่าเครื่องถูกผู้บุกรุกแก้ไขการทำงานใดๆ ภายในเครื่องหรือไม่ สามารถทำได้โดยการตรวจสอบจากล็อกไฟล์ที่สร้างขึ้นจากโปรแกรม syslog daemon ที่ถูกติดตั้งใน linux ซึ่งจะทำการเก็บล็อกไฟล์ไว้ ภายในล็อกไฟล์ดังกล่าวจะเก็บข้อมูลสถานะการทำงานของเครื่องตั้งแต่เริ่มบูตเครื่อง อย่างไรก็ตาม ถ้าผู้บุกรุกทราบว่าล็อกไฟล์เก็บไว้ที่ใด ก็สามารถที่จะเข้าไปแก้ไขหรือสร้างล็อกไฟล์ได้ ดังนั้นมีอีกทางเลือกหนึ่งคือการตั้งเซิร์ฟเวอร์ที่ใช้เก็บล็อกไฟล์ (Log Server) โดย syslog daemon สามารถปรับแต่งให้ส่งข้อมูลล็อกไฟล์ไปเก็บไว้ยังเซิร์ฟเวอร์ที่ใช้เก็บล็อกไฟล์ได้ แต่ข้อมูลนั้นยังไม่ได้เข้ารหัส ผู้บุกรุกสามารถดูข้อมูลดังกล่าว

ขณะที่ทำการส่งได้ เพราะฉะนั้นเซิร์ฟเวอร์ที่ใช้เก็บล็อกไฟล์ควรตั้งอยู่ภายในองค์กร

ข้อมูลของล็อกไฟล์โดยทั่วไปที่ควรตรวจสอบ

5.2 ล็อกไฟล์ที่ไม่สมบูรณ์หรือที่มีข้อมูลขาดหายไป

5.3 ล็อกไฟล์ที่มี timestamp ผิดปกติ

5.4 ล็อกไฟล์ทีมี permission หรือ เจ้าของล็อกไฟล์ผิดจากที่ควรเป็น เช่นล็อกไฟล์ของระบบแต่เจ้าของนั้นเป็น user

5.5 ข้อมูลของการรีบูตเครื่องหรือรีสตาร์ท service

5.6 การใช้คำสั่ง su หรือการ login เข้ามาจากต้นทางที่ผิดปกติ

4.2 ผลการวิเคราะห์ข้อมูล

ตามที่ได้ทำการศึกษา Hardening โดยมีวัตถุประสงค์ให้ระบบมีความปลอดภัยและมีความน่าเชื่อถือมากขึ้น ซึ่งในขณะนี้โครงการได้ดำเนินการจนแล้วเสร็จตามวัตถุประสงค์เป็นที่เรียบร้อยแล้ว โดยสามารถวิเคราะห์ได้จากการทำงานจากผลการทดสอบซึ่งได้ผลดังนี้

4.2.1 สามารถเข้าไปแก้ไขไฟล์ใน Linux ทำให้ user ไม่สามารถตั้งรหัสซ้ำได้อีก

4.2.2 สามารถเช็ค Log ของการใช้งานใน windows server ได้

4.2.3 สามารถกำหนดสิทธิการเข้าถึงไฟล์ต่างๆได้

4.2.4 สามารถ set inbound ของ firewall เพื่อกำหนด port ที่จะเข้ามาได้

สรุปได้ว่าการทำ Hardening มีประโยชน์จริงทั้งในด้านการเพิ่มความปลอดภัยและลดการใช้ทรัพยากรเครื่องอีกทั้งยังประหยัดค่าใช้จ่ายได้มากเพราะการทำ Hardening ไม่จำเป็นต้องไปซื้อ software และ hardware มาเพิ่มในการทำ Hardening อีกด้วย

4.3 วิจารณ์ข้อมูลโดยเปรียบเทียบผลที่ได้รับกับวัตถุประสงค์การจัดทำโครงการ

จากวัตถุประสงค์เพื่อเพิ่มความปลอดภัยและลดการใช้ทรัพยากรในเครื่องรวมถึงการลดค่าใช้จ่ายต่างๆ

จากการที่ทดสอบการทำ Hardening สามารถป้องกันช่องโหว่ต่างๆได้ไม่ว่าจะเป็นการเช็คว่ามี User คนไหนมี UID 0 นอกจาก Root ไหม หรือ ปิดการใช้งาน Service ต่างๆที่ไม่ได้มีการใช้งานหรือม่จำเป็นต่อระบบออกไปเพื่อไม่ใช่เกิดช่องโหว่และยังลดทรัพยากรการใช้งานในเครื่องไปได้มากทำให้เครื่องมีประสิทธิภาพในการทำงานสูงขึ้น หรือ การตั้งค่าแจ้งเตือนการหมดอายุของรหัส User เพื่อให้มาทำการเปลี่ยนใหม่เพื่อเพิ่มความปลอดภัยให้แก่ผู้ใช้งานและระบบของเราให้มากยิ่งขึ้นและการทำ Hardening นั้นสามารถนำมาใช้งานในองค์กรต่างๆเพื่อเพิ่มความปลอดภัยและความน่าเชื่อถือขององค์กรนั้นมากขึ้น

บทที่ 5
บทสรุปและข้อเสนอแนะ

5.1 สรุปผลการดำเนินงาน

จากการที่ได้ศึกษาและทดลองทำการ Hardening เพื่อนำไปเพิ่มความปลอดภัยให้แก่เครื่องและ 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 ได้สำเร็จ

5.1.4 สามารถปิด Service ต่างๆที่ไม่ได้ใช้งานใน Linux และ Windows Server ได้สำเร็จ

5.1.5 สามารถเช็คได้ว่าไม่มีผู้ใช้คนใดมีเลข UID = 0

จากผลลัพธ์ สารมารถสรุปได้ว่าการทำ Hardening สามารถตอบสนองความต้องการในด้านความน่าเชื่อถือ ความรวดเร็วและความปลอดภัยได้เป็นอย่างดี

5.2 แนวทางการแก้ไขปัญหา

ปัญหาที่พบในระหว่างการศึกษา Hardening ส่วนแรกจะเป็นปัญหาเรื่องการหาข้อมูลและทำความเข้าใจซึ่งข้อมูลเกือบทั้งหมดนั้นเป็นภาษาอังกฤษและบางเรื่องข้อมูลค่อนข้างน้อย ส่วนอีกปัญหาคือควยุ่งยากในการทำ ไม่ว่าจะเป็นการใช้คำสั่งต่างๆ การแก้ไขไฟล์ หากแก้ไขไม่ถูกต้องอาจจะต้องทำการลงระบบใหม่ทั้งหมดเลยเนื่องจากไปแก้ไขไฟล์ในระบบแล้วเกิดการผิดพลาดขึ้นซึ่งแนวทางการแก้ปัญหาคือทำการ Snapshot เอาไว้ก่อนจะเข้าไปแก้ไขไฟล์ทุกครั้งเพื่อที่จะสามารถย้อนกลับมาก่อนที่จะเกิดความเสียหายขึ้นเนื่องจากการเข้าไปทำการแก้ไขไฟล์ในระบบ

5.3 ข้อเสนอแนะจากการดำเนินงาน

5.3.1 ควรมีพื้นฐานในการใช้ระบบปฏิบัติการ Linux ในการใช้คำสั่งต่างๆ

5.3.2 ในการทำงานควรจะระมัดระวังในการเข้าไปแก้ไขไฟล์ต่างๆควรมีการ Snapshot ไว้เสมอก่อนจะลงมือทำ

5.3.3 ในการทำงานต้องหาข้อมูลเพื่อเตรียมความพร้อมก่อนลงมือทำและวางแผนในการทำงานเสมอเพราะการแก้ไขบางอย่างอาจจะส่งผลต่อการทำงานขั้นต่อๆไป

5.3.4 การติดต่อประสานงานกันภายในทีม เป็นส่วนสำคัญในการทำงานจริงที่จะส่งผลกระทบที่ดีหรือไม่ดีต่องานที่ได้รับมอบหมาย ซึ่งจะต้องอาศัยความร่วมมือของทุกฝ่ายที่จะทำให้งานสำเร็จลุล่วงไปได้ด้วยดี

5.3.5 การทำงานที่สามารถตรวจสอบได้ จะทำให้ผู้ปฏิบัติงานสามารถตรวจสอบข้อมูลหรือข้อผิดพลาดที่ได้เกิดขึ้นได้อย่างง่ายดาย และสามารถเข้าไปแก้ไขปัญหาได้ตรงจุดมากที่สุด

5.3.6 ในการทำงานจริง มีความจำเป็นอย่างยิ่งที่จะต้องศึกษาหาความรู้เพิ่มเติมอยู่ตลอดเวลา ซึ่งความรู้บางอย่างไม่สามารถเรียนรู้ได้จากในห้องเรียน

5.3.7 ความอดทนถือเป็นส่วนสำคัญอีกอย่าง ที่ทำให้การทำงานเป็นไปได้ด้วยดีและประสบผลสำเร็จ ซึ่งจะต้องขึ้นอยู่กับรูปแบบของงาน, ระยะเวลาของงานและผู้ร่วมงานด้วย

5.3.8 ความรับผิดชอบในหน้าที่ ถือเป็นสิ่งที่ดีอย่างมากที่ได้รับจากการทำงานจริงซึ่งสามารถนำมาใช้ในการพัฒนาตนเองได้อย่างดีเยี่ยม ทำให้มีความรับผิดชอบมากขึ้นและสามารถตัดสินใจได้เอง

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:https://www.tecmint.com/linux-password-protect-files-with-encryption/

[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:https://spalinux.com/2009/03/configure_linux_disk_quota_part_2

[5.] How to prevent users from reusing old passwords in Linux

Available:https://www.internetblog.org.uk/post/886/how-to-prevent-users-from-reusing-old-passwords-in-linux/

[6.] 40 Linux Server Hardening Security Tips [2017 edition]

Available:https://www.cyberciti.biz/tips/linux-security.html

ภาคผนวก

(รายงานประจำสัปดาห์)

ประวัติผู้จัดทำโครงงาน

ชื่อ – นามสกุล นายพิรษร อัครวุฒิ

วัน เดือน ปีเกิด 9 มกราคม 2540

ประวัติการศึกษา

ระดับประถมศึกษา โรงเรียนสี่พี่น้อง

ระดับมัธยมศึกษา โรงเรียนเซนต์ดอมินิก

ระดับอุดมศึกษา คณะเทคโนโลยีสารสนเทศ สาขาเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีไทย-ญี่ปุ่น

ทุนการศึกษา -

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

ผลงานที่ได้รับการตีพิมพ์ - ไม่มี -