**รายงานโครงงานการปฏิบัติงานสหกิจศึกษา**

**การทำ Hardening ของระบบ Red hat operating system โดยใช้ Ansible**

**นายทัตปิยะ จิระศักดิ์โรจน์ 5907101005**

**รายงานนี้เป็นส่วนหนึ่งของการศึกษาวิชา สหกิจศึกษา (**NC001**)**

**ภาค 2 ปีการศึกษา 2563**

**สาขาวิชาวิศวกรรมคอมพิวเตอร์และมัลติมีเดีย คณะวิศวกรรมศาสตร์**

**มหาวิทยาลัยหอการค้าไทย**

**รายงานโครงงานการปฏิบัติงานสหกิจศึกษา**

**การทำ Hardening ของระบบ Red hat operating system โดยใช้ Ansible**

**นายทัตปิยะ จิระศักดิ์โรจน์ 5907101005**

**รายงานนี้เป็นส่วนหนึ่งของการศึกษาวิชา สหกิจศึกษา (**NC001**)**

**ภาค 2 ปีการศึกษา 2563**

**สาขาวิชาวิศวกรรมคอมพิวเตอร์และมัลติมีเดีย คณะวิศวกรรมศาสตร์**

**มหาวิทยาลัยหอการค้าไทย**

**กิตติกรรมประกาศ**

รายงานโครงงานการปฏิบัติงานสหกิจศึกษาเล่มนี้สำเร็จได้ด้วยความกรุณาจากอาจารย์ที่ปรึกษา ผศ. ดร.ศุภฤกษ์ มานิตพรสุทธ์ ที่ให้ความช่วยเหลือ ให้คำชี้แนะ ตลอดจนช่วยแก้ปัญหา ทำให้เกิดความรู้และประสบการณ์ที่ดีแก่ข้าพเจ้า

ขอขอบพระคุณ นาย สุรยศ ศรีเจริญ ที่ได้กรุณาให้คำแนะนำตลอดจนข้อชี้แนะ จนในที่สุดทำให้รายงานโครงงานการปฏิบัติงานสหกิจศึกษาฉบับนี้สำเร็จลงได้

ทัตปิยะ จิระศักดิ์โรจน์



( ) (. นาย สุรยศ ศรีเจริญ )

………………………………………. ……………………………………….

อาจารย์ที่ปรึกษาสหกิจ ตำแหน่ง / Opensource Technology Specialist

**บทคัดย่อ**

จากการปฏิบัติการสหกิจศึกษา ข้าพเจ้านายทัตปิยะ จิระศักดิ์โรจน์ ได้ปฏิบัติงานสหกิจศึกษา ณ บริษัท เอ็มเอฟอีซี จำกัด (มหาชน) ในแผนก Information security โดยมีหน้าที่รับผิดชอบในการปฏิบัติงาน คือ ผู้ช่วยงานด้านระบบคอมพิวเตอร์ โดยระยะเวลาการปฏิบัติสหกิจศึกษาในครั้งนี้เริ่มตั้งแต่วันที่ 6 มกราคม พ.ศ. 2563 ถึง วันที่ 24 เมษายน พ.ศ. 2563 รวมระยะเวลาทั้งสิ้น 16 สัปดาห์

การปฏิบัติงานในครั้งนี้ได้รับมอบหมายให้ปฏิบัติงานในตำแหน่งผู้ช่วยงานด้านระบบคอมพิวเตอร์ โดยลักษณะงานที่นักศึกษาปฏิบัติคือ programing กับ implementation ได้แก่ การทำ amsible playbook สำหรับทำงานในรูปแบบต่างๆ เช่น playbook สำหรับการทำ backup ข้อมูล, playbook สำหรับการทำ reverse proxy เป็นต้น

ผลการศึกษาพบว่า 1.) ได้เรียนรู้เกี่ยวกับการใช้งานระบบปฏิบัตการLinux และ สามารถนำไปใช้ประกอบอาชีพได้ในอนาคต 2.) ได้เรียนรู้เกี่ยวกับการใช้งาน Ansible ที่สามารถนำไปใช้จัดการระบบ RedHat หรือ ระบบอื่นได้ 3.) จากการปฏิบัติการสหกิจศึกษา ทำให้ทราบว่าการทำ Hardening โดยใช้ Ansible นั้น ภายในบริษัท ยังไม่ได้รับการพัฒนา ทำให้เป็นที่มาของการทำรายงานในครั้งนี้

**สารบัญ**

หน้า

กิตติกรรมประกาศ ก

บทคัดย่อ ข

บทที่ 1 บทนำ

* 1. สถานประกอบการ 1
  2. ลักษณะงานและหน้าที่รับผิดชอบ 1
  3. วัตถุประสงค์ของการทำโครงงาน 2
  4. ประโยชน์ที่คาดว่าจะได้รับ 2

บทที่ 2 การทบทวนเอกสาร

2.1 Centos คืออะไร 3

2.2 RHEL คืออะไร 5

2.3 Ansible คืออะไร 6  
 2.4 Hardening คืออะไร 6

2.5 ตารางอธิบายตัวย่อหรือชื่อต่างๆที่ใช้ในการทำ Hardening 8

บทที่ 3 วิธีการทำโครงงาน

3.1 ติดตั้ง Ansible 11  
 3.2 ติดตั้ง Git 12  
 3.3 ติดตั้งระบบ RHEL และตั้งค่า 12  
 3.4 เริ่มการทำ Playbook 15  
 3.5 ทำPlaybook สำหรับตรวจสอบการทำ Hardening 25

บทที่ 4 ผลการทำโครงงาน

4.1 ผลการทำ Hardening โดยใช้ Ansible playbook 27  
 4.2 ผลการตรวจสอบการทำ Hardening โดยใช้ Ansible playbook 31

บทที่ 5 บทสรุปและข้อเสนอแนะ

5.1 สรุปผลการทำโครงงาน 32

5.2 ประโยชน์จากการทำโครงงาน 32

5.3 ปัญหา อุปสรรค และแนวทางการแก้ไขโครงงาน 32

5.4 ข้อเสนอแนะ 33

บรรณานุกรม 34

**บทที่ 1**

**บทนำ**

ข้าพเจ้านายทัตปิยะ จิระศักดิ์โรจน์ ได้ปฏิบัติงานสหกิจศึกษา ณ บริษัท เอ็มเอฟอีซี จำกัด (มหาชน) ในแผนก Information security โดยมีหน้าที่รับผิดชอบในการปฏิบัติงาน คือ ผู้ช่วยงานด้านระบบคอมพิวเตอร์ โดยระยะเวลาการปฏิบัติสหกิจศึกษาในครั้งนี้เริ่มตั้งแต่วันที่ 6 มกราคม พ.ศ. 2563 ถึง วันที่ 24 เมษายน พ.ศ. 2563 รวมระยะเวลาทั้งสิ้น 16 สัปดาห์

**1.1 สถานประกอบการ**

บริษัท เอ็มเอฟอีซี จำกัด(มหาชน) เป็นบริษัทที่ให้บริการให้คำปรึกษา พัฒนา และวางระบบคอมพิวเตอร์และเครือข่ายงานสารสนเทศอย่างครบวงจร

**1.2 ลักษณะงานและหน้าที่รับผิดชอบ**

การปฏิบัติงานในครั้งนี้ได้รับมอบหมายให้ปฏิบัติงานในตำแหน่งผู้ช่วยงานด้านระบบคอมพิวเตอร์ โดยลักษณะงานที่นักศึกษาปฏิบัติคือ programing กับ implementation ได้แก่ การทำ amsible playbook สำหรับทำงานในรูปแบบต่างๆ เช่น playbook สำหรับการทำ backup ข้อมูล, playbook สำหรับการทำ reverse proxy

**1.3 วัตถุประสงค์ของการทำโครงงาน**

เพื่อพัฒนา Playbook สำหรับการทำ Hardening ของระบบปฏิบัติการ RedHat และพัฒนา Playbook สำหรับใช้ตรวจสอบการทำ Hardening

**1.4 ประโยชน์ที่คาดว่าจะได้รับ**

1. ได้รับความรู้เกี่ยวกับการใช้งาน Ansible และการใช้งานระบบปฏิบัตการ RedHat
2. เพิ่มความรวดเร็วในการทำ Hardening

**บทที่ 2**

**การทบทวนเอกสาร**

บทที่ 2 เป็นการทบทวนเอกสารที่ใช้ในการทำรายงานโครงงานสหกิจเล่มนี้

**2.1 Centos คืออะไร**

CentOS เป็นลีนุกซ์ในระดับ Enterprise ที่มีเป้าหมายหลักในเรื่องของความ stable เพื่อให้ใช้กับงานในระดับองค์กร CentOS แตกต่างจากลีนุกซ์ตัวอื่นๆ ที่ค่อนข้างจะมีการเปลี่ยนแปลงบ่อยและมักจะใส่ feature ที่ยังไม่ stable ลงไป ดังนั้นการที่ CentOS ให้ความสำคัญในเรื่องของความ stable จึงทำให้ผู้ใช้งานสามารถมุ่งความสนใจในเรื่องของ application โดยลดความกังวลในส่วนของ OS ลงไป

CentOS ย่อมาจาก (Community ENTerprise Operating System) เป็นลีนุกซ์ที่พัฒนามาจากต้นฉบับ RedHat Enterprise Linux (RHEL) โดยที่ CentOS ได้นำเอาซอร์สโค้ดต้นฉบับของ RedHat มาทำการคอมไพล์ใหม่โดยการพัฒนายังเน้นพัฒนาเป็นซอฟต์แวร์ Open Source โดยเป็นลิขสิทธิ์แบบ GNU General Public License ในปัจจุบัน CentOS Linux ถูกนำมาใช้ในการทำ Web Hosting กันอย่างกว้างขวางเนื่องจากเป็นระบบปฏิบัติการที่มีต้นแบบจาก RedHat ที่มีความแข็งแกร่งสูง  การติดตั้งแพ็กเกจย่อยภายในสามารถใช้ได้ทั้ง RPM, TAR, APT หรือใช้คำสั่ง YUM ในการอัปเดทซอฟต์แวร์แบบอัตโนมัติ

**เหตุผลที่ควรเลือกใช้ CentOS**

สำหรับองค์กรเหมาะสมที่จะนำระบบตัวลีนุกซ์ตัวนี้มาทำเป็น เซิร์ฟเวอร์ใช้งานภายในองค์กร เหตุผลหลักในการนำระบบนี้มาใช้งานคือ

1. เพื่อประหยัดงบประมาณขององค์กร เนื่องจาก CentOS เป็นซอฟต์แวร์ Open Source องค์กรไม่จำเป็นต้องจ่ายค่าลิขสิทธ์ซอฟต์แวร์

2. เพื่อนำมาทำเซิร์ฟเวอร์บริการงานต่างๆ ในองค์กร ซึ่งภายใน CentOS มีแพ็กเกจย่อยที่นำมาใช้ทำเซิร์ฟเวอร์สำหรับใช้งานในองค์กรจำนวนมาก อาทิ เช่น

·       Web Server (Apache)

·       FTP Server (ProFTPd / VSFTPd)

·       Mail Server (Sendmail / Postfix / Dovecot)

·       Database Server (MySQL / PostgreSQL)

·       File and Printer Server (Samba)

·       Proxy Server (Squid)

·       DNS Server (BIND)

·       DHCP Server (DHCPd)

·       Antivirus Server (ClamAV)

·       RADIUS Server (FreeRADIUS)

·       Control Panel (ISPConfig)

3. เพื่อนำมาทำเป็นระบบเซิร์ฟเวอร์สำหรับจ่าย Private IP Address แจกเครื่องลูกข่ายในองค์กร รวมทั้งตั้งเป็นระบบเก็บ Log Files ผู้ใช้งาน เพื่อให้สอดคล้องกับพระราชบัญญัตว่าด้วยการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์ปี 2550

**การดาวน์โหลด**

สำหรับตัวติดตั้ง CentOS สามารถดาวน์โหลดตัวติดตั้งแบบ image file แล้วมาทำการเขียนใส่แผ่น CD/DVD CentOS เวอร์ชั่นที่ใช้ เวอร์ชั่นคือ 7 โดยสามารถดาวน์โหลดได้จากเว็บไซต์ [http://isoredirect.centos.org/centos/7/isos/x86\_64/](https://github.com/tatpiya1/Audit_Hardening_RHEL.git) (64 bit)

**หน่วยความจำที่ต้องการ**

หน่วยความจำขั้นต่ำ ของเครื่องที่จะติดตั้ง CentOS 6.3 ได้นั้น ต้องมีขนาด 392 MB สำหรับ Text mode ส่วนการติดตั้งใน Text mode จะไม่สามารถแก้ไขพาร์ทิชั่นของดิสก์และเลือกชุดซอฟต์แวร์ได้ ต้องเลือกติดตั้งในโหมด GUI เท่านั้น ซึ่งเป็นโหมดดีฟอลต์อยู่แล้วตอนบู๊ตจากแผ่นดีวีดี หน่วยความจำขั้นต่ำที่ต้องใช้เพื่อติดตั้งในโหมด GUI คือ 652 MB

**2.2 RHEL คืออะไร**

RHEL คือระบบปฏิบัติการที่เป็นต้นฉบับของ Centos โดยส่วนใหญ่แล้ว เหมือน Centos ทุกอย่าง แต่ RHEL นั้นเป็นระบบปฏิบัติการที่ต้องลงโปรแกรมแบบออฟไลน์ ถ้าอยากลงโปรแกรมแบบออนไลน์ จะเป็นจ่ายเงินซื้อ license เพื่อใช้งานในส่วนนี้

**2.3 Ansible คืออะไร**

Ansible คือ เครื่องมือที่ใช้สำหรับการจัดการ configuration โดยจะทำงานผ่านทาง ssh พัฒนาด้วย ภาษา python การทำงานจะงานในรูปแบบที่ต้องมี management node ที่ทำหน้าเป็น server หลังที่จะทำหน้าเป็น ผู้ที่จะต้องไปติดตั้ง package บน เครื่องserverในระบบ การทำงานจะประกอบด้วยfile ที่เกี่ยวข้อง 2 file คือ inventory file และ playbook

1. inventory file ทำหน้าเก่็บรายชื่อของ server หรือ ip ของ server ที่จะใช้สำหรับเป้าหมายสำหรับการติดตั้ง โดยdefault หากไม่มีการกำหนด ใน option -i ก็จะใช้ inventory คือ /etc/ansible/hosts เราสามารถที่จะแก้ไขค่านี้ได้โดยทำการแก้ไข file /etc/ansible/ansible.cfg
2. playbook.yml ไฟล์นี้จะเป็นตัวระบุว่า จะให้ ansible ทำอะไรบ้างในแต่ละ server การเขียนไฟล์จะใช้เป็น format ของ yaml format

**2.4 Hardening คืออะไร**

การฮาร์ดเดนนิงระบบปฏิบัติการ (Operating System Hardening) เป็นกระบวนการของการกำหนดค่า (Parameter) บนระบบปฏิบัติการเพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต ป้องกันผู้บุกรุก แฮกเกอร์ และช่องโหว่ด้านความปลอดภัยอื่น ๆ OS Hardening ทำให้ระบบคอมพิวเตอร์เชื่อถือได้มากขึ้น มีความปลอดภัย และช่วยเพิ่มประสิทธิภาพการทำงานเนื่องจากใช้หลักการ "ลดสิ่งที่ไม่ได้ใช้ออกไปจากระบบ"

ดังนั้น วัตถุประสงค์หลักของการ Hardening คือการ ลดความเสี่ยงที่จะเกิดด้านความปลอดภัยให้ได้มากที่สุด

Hardening นั้นเป็นการเพิ่มความปลอดภัยให้ระบบปฏิบัติการที่เราใช้อยู่โดยมีต้นทุนค่าใช้จ่ายต่ำมาก ไม่ต้องซื้อ Hardware / Software ราคาแพงเราก็สามารถเพิ่มความปลอดภัยให้กับคอมพิวเตอร์ของเราได้เป็นอย่างดี เพียงแค่เราใส่ใจที่จะนำเอา Security Best Practice ของระบบปฏิบัติการที่เราใช้อยู่นำมาลงมือทำ (ซึ่งโดยส่วนใหญ่มักจะมีแจกจ่ายฟรีให้ผู้ใช้งานโดยบรรดาผู้ผลิตอยู่แล้ว)

หากจะมองในมุมมองขององค์กรด้วยแล้ว กระบวนการทำ Hardening เป็นหนึ่งในส่วนสำคัญในการสร้างมาตรฐานของการบริหารจัดการระบบรักษาความปลอดภัยข้อมูลอย่างเป็นระบบและมีประสิทธิภาพ

จากการอิงจากมาตรฐานของCIS นั้น การทำ Hardening จะมีทั้งหมด6ขึ้นตอนสำคัญโดยแต่ละขั้นตอนมีดังนี้  
**2.4.1 Initial setup**  
- disable filesystem ที่ไม่ใช้งาน,ตรวจสอบPartitionที่แบ่งไว้, ตรวจสอบoptionที่ตั้งไว้ของpartition,ตรวจสอบว่าได้ตั้งค่าSticky Bitไว้รึเปล่า, Disable Automounting  
- ตรวจสอบว่าเปิด gpgcheckไว้หรือไม่  
- ตรวจสอบว่าว่าได้ติดตั้ง AIDE ไว้รึเปล่า, ตรวจสอบว่ามีการตรวจสอบfilesystemเป็นประจำหรือไม่  
- ตรวจสอบว่าได้ตั้ง permission ของ bootloader ที่ให้ root, ตรวจสอบว่าได้ตั้ง password ของbootloader ไว้หรือไม่  
- ตรวจสอบว่าcore dumpsได้ถูกจำกัดไว้หรือไม่, เปิดaddress space layout randomization (ASLR), ปิดprelink  
- enable SELinux, setให้SELinuxอยู่ในสถานะenforcing, ตั้งpolicyให้SELinux, Remove SETroubleshoot, Remove MCS Translation Service (mcstrans), เช็คว่าไม่มีdeamonsที่ไม่ได้ตั้งค่าไว้  
- ตั้งค่าข้อความประจำวันให้เหมาะสม, ตั้งpermissionให้กับ/etc/issue, ตั้งค่า GDM login banner  
**2.4.2 Service**  
- Disable service ที่ไม่ใช้  
- ตั้งค่า ntp กับ chrony (ตั้งค่า Time Synchronization)  
- Remove service client ที่ไม่ใช้ได้แก่ ypbind(NIS), rsh, talk, telnet, openldap-clients(LDAP)  
**2.4.3 Network Configuration**  
- ตั้งค่า Firewalld   
**2.4.4 Logging and Auditing**  
- กำหนดขนาดlog, ตั้งค่าให้หยุดทำงานเมื่อlogเต็ม, ตั้งค่าให้ไม่ลบตัวเองอัติโนมัติ, ตั้งค่าให้auditdเริ่มทำงานตอนเปิดใช้งานระบบ, etc  
- ลง rsyslog กับsyslog-ng, เปิดใช้serviceของ rsyslog และ syslog-ng, ตั้งต่าเบื่องต้น, กำหนดpermissionของlogfiles  
**2.4.5 Access, Authentication and Authorization**  
- Enable crond, กำหนดpermissionเป็น 600 และกำหนดownerและgroupเป็นroot  
- Enable sshd และกำหนดpermissionเป็น 600 และกำหนดownerและgroupเป็นroot, เปลี่ยนprotocol ของ ssh เป็น protocol 2, ตั้ง LogLevel ของ ssh เป็นINFO, disable X11Forwarding, กำหนดจำนวนครั้งที่จะใส่พาสเวิร์ดผิดได้เป็น4ครั้งหรือน้อยกว่านั้น, Disable HostbasedAuthentication, กำหนดจำนวนที่ผู้ใช้ที่จะเข้าใช้งานsshได้พร้อมกัน  
- กำหนดเงื่อนไขในการสร้างพาสเวิร์ด, ตั้งค่าให้ล็อคระบบเมื่อใส่พาสเวิร์ดผิดครบจำนวนครั้งที่กำหนด, ตั้งค่าให้ระบบจดจำพาสเวิร์ดเก่าๆของuser เพื่อไม่ให้userใช้พาสเวิร์ดซ้ำ, เปลี่ยนการเข้ารหัสพาสเวิร์ดจากMD5เป็นSHA-512  
**2.4.6 System Maintenance**  
- กำหนดpermissionของdirectory /etc/passwd, /etc/shadow , /etc/group และ /etc/gshadow เป็น 644  
- กำหนดpermissionของdirectory /etc/passwd-, /etc/shadow-, /etc/group- และ /etc/gshadow- เป็น 600  
- ตรวจสอบข้อมูลเบื่องต้นเช่น หาว่ามีworld writable filesหรือไม่, หาว่ามีfileหรือdirectoryที่ไม่มีownerหรือgroupหรือไม่, หาuserที่ไม่พาสเวิร์ด,   
หาdirectory ที่ไม่มีgroup เป็นต้น

**2.5 ตารางอธิบายตัวย่อหรือชื่อต่างๆที่ใช้ในการทำ Hardening**

|  |  |
| --- | --- |
| ชื่อ | ความหมาย |
| AIDE | Software ที่เอาไว้ตรวจสอบไฟล์หรือ directory |
| ASLR | address space layout randomization เป็นกลไกด้านความมั่นคงปลอดภัยของระบบปฏิบัติการ ซึ่งจะทำการสุ่มตำแหน่งของ Memory ที่ถูกใช้โดย Process ต่างๆ ส่งผลให้แฮ็คเกอร์ไม่สามารถรู้ได้ว่าจะทำการ Exploit Shellcode ที่ตำแหน่งไหนบน Memory  โดยแฮ็คเกอร์จะใช้ช่องโหว่บน Branch Target Buffer (BTB) ซึ่งเป็นกลไกการทำ Caching ของ Branch Target Predictor บน CPU การทำ Branch Prediction นี้ถูกใช้ใน CPU สมัยใหม่ (เช่น Haswell CPU) เพื่อเพิ่มขีดความสามารถของประสิทธิภาพ ซึ่งช่องโหว่ดังกล่าวช่วยให้สามารถดึงข้อมูลตำแหน่ง ASLR ออกมาได้ โดยอาศัยการทำ BTB Collision ระหว่าง Process ของผู้ใช้ที่แตกต่างกัน หรือระหว่าง Process กับ Kernel |
| SELinux | ย่อมาจาก Security-Enhanced Linux เป็นกลไกภาคบังคับที่ใช้เพื่อควบคุมการเข้าถึงการใช้งานระบบ ที่อยู่ใน Kernel ของ Linux ช่วยเพิ่มประสิทธิภาพการรักษาความปลอดภัยให้กับลินุกซ์ที่ช่วยให้ผู้ใช้ และผู้ดูแลระบบทำการควบคุมการเข้าถึงการใช้งานระบบ ซึ่ง SELinux นี้เป็นผลงานการวิจัยของ National Security Agency ของประเทศสหรัฐอเมริกาที่พัฒนาระบบรักษาความปลอดภัยขึ้นมาใช้เป็นการภายใน       ระบบรักษาความปลอดภัยของ [Linux](https://www.mindphp.com/คู่มือ/73-คืออะไร/2098-linux-คืออะไร.html) เป็น OS ตัวหนึ่งที่มีโปรแกรมพื้นฐานทางด้านความปลอดภัยที่ดีมากนั่นคือมี [Firewall](https://www.mindphp.com/คู่มือ/73-คืออะไร/3021-firewall-คืออะไร.html) ที่ติดมากับระบบ โดยที่เราไม่จำเป็นต้องลงโปรแกรมเพิ่มเติม |
| ntp | ย่อมาจาก Network Time Protocol 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 |
| chrony | เป็น Client ของ ntp |
| ypbind(NIS) | เป็นsoftwareที่ทำงานกับ RPC Program ซึ่งจำเป็นต้องใช้software portmap ในการ map หมายเลขพอร์ตเข้ากับหมายเลข RPC Program |
| rsh | ย่อมาจาก remote shell ทำหน้าทีเหมือนssh แต่ไม่ปลอดภัยเท่า ssh โดยจะทำหน้าที่เห็นชุดคำสั่งสำหรับใช้เชื่อมต่อกับระบบผ่านเครือข่ายอินเตอร์เน็ต ซึ่งจะเชื่อมต่อผ่าน port 514 |
| talk | เป็นservice ที่เอาไว้ใช้พูดคุยกับuser ที่ login อยู่ |
| telnet | บริการที่ช่วยให้คุณสามารถเชื่อมต่อกับคอมพิวเตอร์อีกเครื่องหนึ่งโดยการใช้ [Internet](https://www.mindphp.com/คู่มือ/73-คืออะไร/2021-internet-คืออะไร.html) หากคุณได้รับสิทธิ์ในการเชื่อมต่อกับเครื่องคอมพิวเตอร์เครื่องอื่นจากเจ้าของเครื่องหรือผู้ดูแล Telnet จะยินยอมให้คุณพิมพ์คำสั่งที่ใช้สำหรับการเข้าถึงโปรแกรมและการบริการต่างๆ ที่อยู่บนเครื่องคอมพิวเตอร์ระยะไกล ราวกับว่าคุณนั่งอยู่ตรงข้างหน้าเครื่องดังกล่าว สามารถใช้ Telnet ทำงานได้หลายอย่าง ซึ่งรวมถึงการเข้าถึงอีเมล ฐานข้อมูล หรือแฟ้ม ซึ่งบริการ Telnet นี้จะทำงานในเครื่องบริการที่ติดตั้งระบบปฏิบัติการ Unix หรือ [Linux](https://www.mindphp.com/คู่มือ/73-คืออะไร/2098-linux-คืออะไร.html) ตัวอย่างโปรแกรม เช่น NCSA Telnet |
| LDAP | protocol ที่ใช้สำหรับค้นหาข้อมูลในฐานข้อมูล ก่อนที่จะลงลึกว่า LDAP คืออะไร มาดูที่มากันก่อนครับ Directory Access Protocol (DAP) คือมาตราฐาน X.500 ของ directory ในระบบ network ซึ่ง LDAP เป็น “lightweight” นั้นหมายถึง มีขนาดเล็กลง เพราะ version เริ่มต้นไม่ได้มีระบบ security มาด้วย ส่วนใหญ่นำเอามาใช้กับข้อมูลจำพวก รายระเอียดพนักงาน เช่น ชื่อ,นามสกุล,ตำแหน่ง,ที่อยู่ |
| rsyslog | โปรแกรมใช้เก็บข้อมูล log file ของ kernel และ application บนระบบunixและlinux เป็น daemon ที่ถูกติดตั้งให้มาพร้อมกับระบบปฏิบัตการในเกือบทุกระบบ โดยสามารถปรับแต่งไฟล์ กำหนดค่าเพื่อควบคุมการทำงานของ rsyslog ได้ เช่น ให้ rsyslog เก็บข้อมูลไปไว้ที่ใดหรือให้ส่งข้อมูล log file ไปเก็บไว้ยังคอมพิวเตอร์เครื่องอื่น |
| syslog-ng | ทำหน้าทีเหมือน rsyslog |
| crond | cron เป็น utilities ตัวหนึ่งทำงานบนระบบปฏิบัติการ linux ทําหน้าที่ช่วยจัดการให้ software ของเรารันโดยอัตโนมัติ ตาม scheduling ที่ config ไว้ |
| sshd | SSH (Secure Shell) คือ Network Protocal ที่สามารถแลกเปลี่ยนข้อมูลโดยช่องทางที่ปลอยภัย (Secure Channel) ระหว่างอุปกรณ์เครือข่ายสองตัว ใช้ Linux หรือ Unix เป็นระบบปฏิบัตการพื้นฐานในการเข้าถึงบัญชีผู้ใช้ (Shell Accounts) ซึ่ง SSH ได้รับการออกแบบให้มาแทนการ Telnet, Rlogin, RSH (The remote shell) ด้วยเหตุผลทางด้านความปลอดภัย การส่งข้อมูลจะอยู่ในรูปแบบตัวอักษร (Plaintext) ที่มีการเข้ารหัสข้อมูล (Encryption) เพื่อให้ข้อมูลเป็นความลับและให้สามารถส่งข้อมูลผ่านเครือข่าย Internet ได้อย่างสมบูรณ์ สามารถใช้งาน SSH ผ่านโปรแกรมประยุกต์ (Applications) ได้มากมายบนระบบปฏิบัติการ UNIX, Microsoft Windows, Apple Mac และ Linux โปรแกรมประยุกต์ (Applications) |

**บทที่ 3**

**วิธีการทำโครงงาน**

บทที่ 3 เป็นการอธิบายขั้นตอนการทำโครงงาน

**3.1 การติดตั้ง Ansible**

การติดตั้ง Ansible เราจะลงบนระบบ Centos โดยใช้คำสั่งดังนี้

- sudo yum install epel-release เพื่อติดตั้ง epel   
ซึ่ง epel นั้นคือ แพคเกจพิเศษที่สร้างโดย Fedora ที่สร้างรักษาและจัดการชุดแพ็คเกจเพิ่มเติมคุณภาพสูงสำหรับ Enterprise Linux โดย EPEL ไม่จำกัดเพียงแค่ Red Hat Enterprise Linux (RHEL) , CentOS และ Scientific Linux (SL), Oracle Linux (OL)

โครงการ EPEL เกิดขึ้นเมื่อ ผู้ดูแล Fedora ตระหนักว่าโครงสร้างพื้นฐานแบบเดียวกันกับที่สร้างและดูแลแพ็คเกจสำหรับ Fedora นั้นยอดเยี่ยมสำหรับการบำรุงรักษาเพิ่มบนแพ็คเกจสำหรับ Enterprise Linux ความต้องการเริ่มต้นส่วนใหญ่ได้รับแรงหนุนจากโครงสร้างพื้นฐานของ Fedora ที่ต้องการบนเครื่อง RHEL ที่สร้างและดูแล Fedora จากนั้นสิ่งต่าง ๆ ได้เติบโตขึ้นไปเป็นกลุ่มของแพ็คเกจที่หลากหลาย ดูหน้าประวัติและปรัชญาของเราสำหรับข้อมูลเพิ่มเติมEPEL ได้ริเริ่มขึ้นเนื่องจากผู้ให้ข้อมูล Fedora หลายคนต้องการใช้แพ็คเกจ Fedora ที่ดูแลบน Red Hat Enterprise Linux (RHEL) เพื่อให้ประยุกเข้ากันได้

แพคเกจ EPEL นั้นมักจะอิงกับ Fedora และจะไม่ขัดแย้งหรือแทนที่แพ็คเกจใน Enterprise Linux พื้นฐาน โดย EPEL ใช้โครงสร้างพื้นฐานส่วนใหญ่เช่นเดียวกับ Fedora รวมถึง buildsystem, bugzilla instance, manager manager, mirror manager และอีกมากมาย

- sudo yum install ansible เพื่อติดตั้ง ansible

**3.2 ติดตั้ง git**

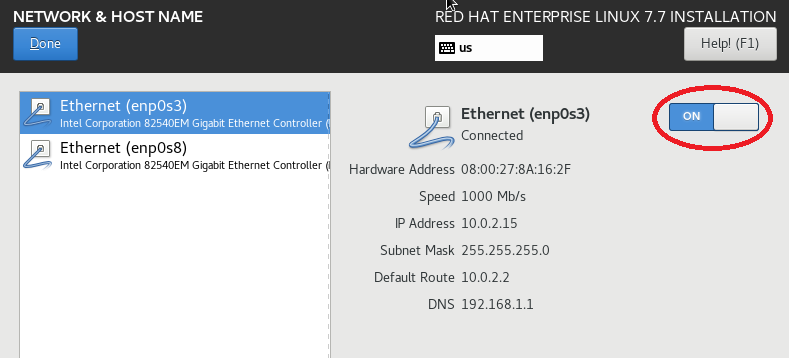
git นั้นติดตั้งไว้เพื่อดาวน์โหลดและอัพโหลด Code ที่อยู่ใน Github โดยใช้คำสั่งดังนี้

- sudo yum install git

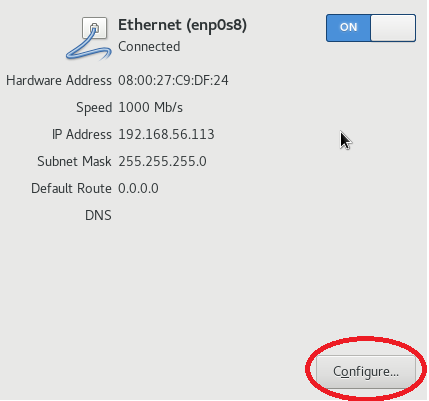
**3.3 ติดตั้งระบบ RHEL และตั้งค่า**

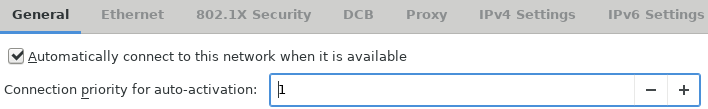
สิ่งที่ต้องทำการที่จะเริ่มทำ Hardening นั้น คือการติดตั้งระบบ RHEL และตั้งค่าเบื้องต้นโดยสามารถทำตามขั้นตอนดังนี้

**3.3.1 ตั้งค่าNetwork**  
สำหรับระบบ RHEL จะมีวิธีเชื่อมต่ออินเตอร์เน็ตอยู่2วิธี โดยที่วิธีแรกทำได้ตอนก่อนติดตั้งระบบRHEL และวิธีที่2ทำได้หลังจากติดตั้งระบบเสร็จแล้ว ซึ่งทำได้ดังนี้

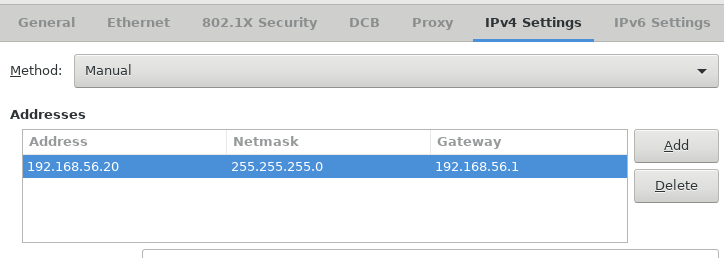
- ตั้งค่า Network ก่อนติดตั้งระบบ  


จากรูปให้กดปุ่มที่อยู่ในวงกลมสีแดง โดยที่ตอนแรกนั้นจะขึ้นว่า OFF อยู่หลังจากกดจะเปลี่ยนเป็น ON ให้กดเปิดทั้ง 2 Interface โดยที่ Interface แรก enp0s3 เป็น interface ที่เอาเชื่อมต่ออินเตอร์เน็ต  
Interface ที่2 enp0s8 เป็น interface ที่เอาใช้ในการเชื่อมต่อแบบ SSH และเป็น interface ที่ต้องตั้งค่าเพิ่มเติมดังนี้ 1.) ให้เลือก enp0s8 และกดปุ่มที่อยู่ในวงกลมสีแดงให้ขึ้นว่า ON และกดปุ่ม Configure

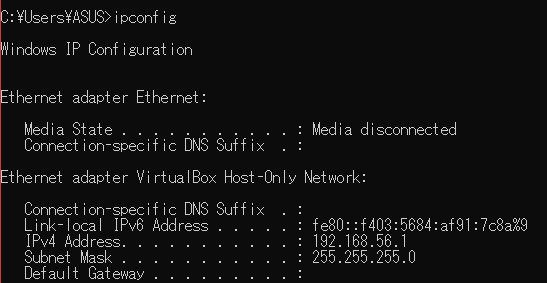


2.) ให้ตั้งค่าดังนี้  


ตั้งให้เชื่อมอัตโนมัติตอนเปิดระบบโดยของenp0s3 ค่า priority เป็น 0 และ enp0s8 เป็น1



Method ให้ตั้งเป็น Manual และไอพีก็ตั้งตามไอพีของInterface ที่เชื่อมต่อกับระบบนี้ โดยเช็คได้โดยใช้Command Prompt และใช้คำสั่ง ipconfig



- ตั้งค่าการแบ่งPartition โดยให้แบ่งpartitionดังนี้  
/tmp  
/var  
/var/tmp  
/var/log  
/var/log/audit  
/home  
/dev/shm  
/  
/boot  
swap  
โดยความจุและLVM Group ก็ตั้งได้ตามสบายหรือตามระเบียบที่กำหนดไว้

- Software selection ให้เลือกตามต้องการ

**3.4 เริ่มการทำPlaybook**

โดยจะใช้โปรแกรม Microsoft VS Code ในการเขียนCode เป็นหลัก และให้ลง Extension Ansible ในโปรแกรมนี้ด้วย

โดยที่Codeที่ทำเสร็จแล้วสามารถดูได้ในนี้  
[https://github.com/tatpiya1/CO-OP-Project.git](https://github.com/tatpiya1/Audit_Hardening_RHEL.git)

โดยจะทำเป็น Ansible Role ซึ่ง Ansible Role จะมี Directory หลายๆ Directory   
Directory หลักๆที่ใช้จะมี defaults ,files ,handlers ,tasks ,templates ซึ่ง Directory ต่างๆ จะทำหน้าที่ดังนี้  
- defaults เก็บค่าdefaults ของ Roles ชุดนี้เอาไว้  
- files เก็บไฟล์ที่เอาไว้ใช้ใน Roles ชุดนี้ไว้  
- handlers เก็บ playbook ที่เอาไว้รับค่าจาก tasks แล้วจะเริ่มทำงาน ตัวอย่างเช่น เมื่อรับค่ามาจาก tasks แล้วให้playbookในhandlerทำการRestart Service ที่กำหนดไว้  
- tasks เก็บ playbook ที่เอาไว้ใช้ทำงานทั้งหมด โดยจะรับค่า defaults จาก defaults, ส่งค่าบางค่าไปที handlers, นำไฟล์จาก files และ templates มาใช้งาน  
- templates เก็บ template ที่เอาไว้ใช้ใน Role ชุดนี้ไว้

ตัวอย่างของplaybookที่ทำเสร็จแล้ว

- playbook สำหรับเรียกใช้งาน role  
  
- playbook ของ section 1  


- playbook ของ section 2  


- playbook ของ section 3  
- playbook ของ section 4  


- playbook ของ section 5  


- playbook ของ section 6  


วิธีใช้Playbook  
จาก playbook สำหรับเรียกใช้งาน role  


จะเห็นว่าจะบรรทัดที่ขึ้นต้นด้วย vars: ตรงนี้จะเป็นส่วนที่จะใช้ในการกำหนดสิ่งต่างๆในการใช้playbookนี้ โดย vars นั้นคือตัวแปร โดยสามารถหาตัวแปรได้จาก defaults ซึ่งตัวแปรมีดังนี้  


สมมติว่าต้องการจะไม่ทำ Hardening เฉพาะบางSection เช่น section ที่ 3 ก็ทำได้โดย นำค่า rhel7cis\_section3: มาใส่ใน vars: แล้วเติม false ตามหลัง ซึ่งจะออกมาดังนี้  
  
และผลที่ออกมาก็คือเวลาใช้playbook ก็จะskip เฉพาะ section 3

**3.5 ทำPlaybook สำหรับตรวจสอบการทำHardening**

การทำPlaybook นี้จะอ้างอิงจากหนังสือ CIS Red Hat Enterprise Linux 7 Benchmark v2.1.1-01-31-2017

โดยCode ที่เสร็จแล้วดูได้ในนี้  
<https://github.com/tatpiya1/Audit_Hardening_RHEL.git>

ตัวอย่างของplaybookที่ทำเสร็จแล้ว



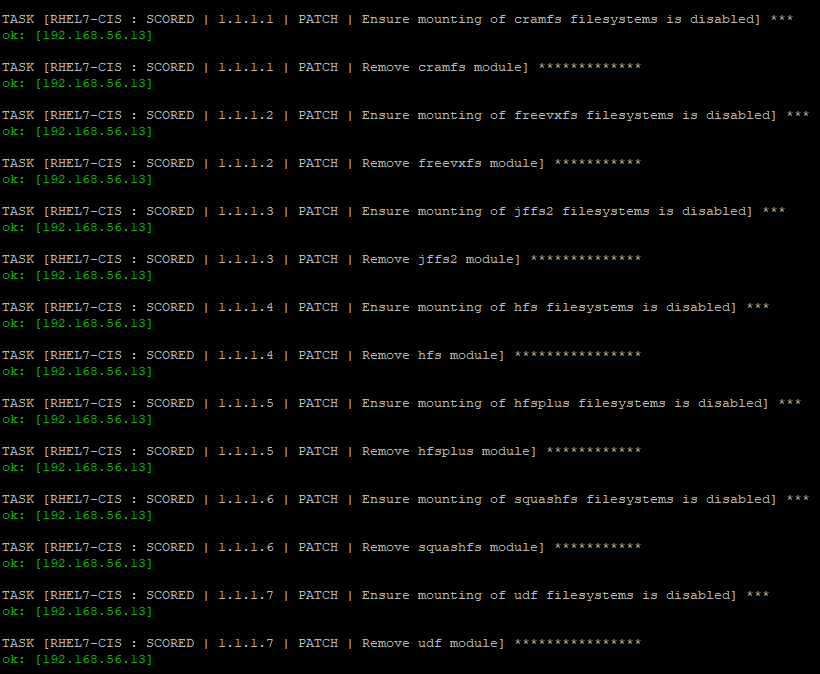
**บทที่ 4**

**ผลการทำโครงงาน**

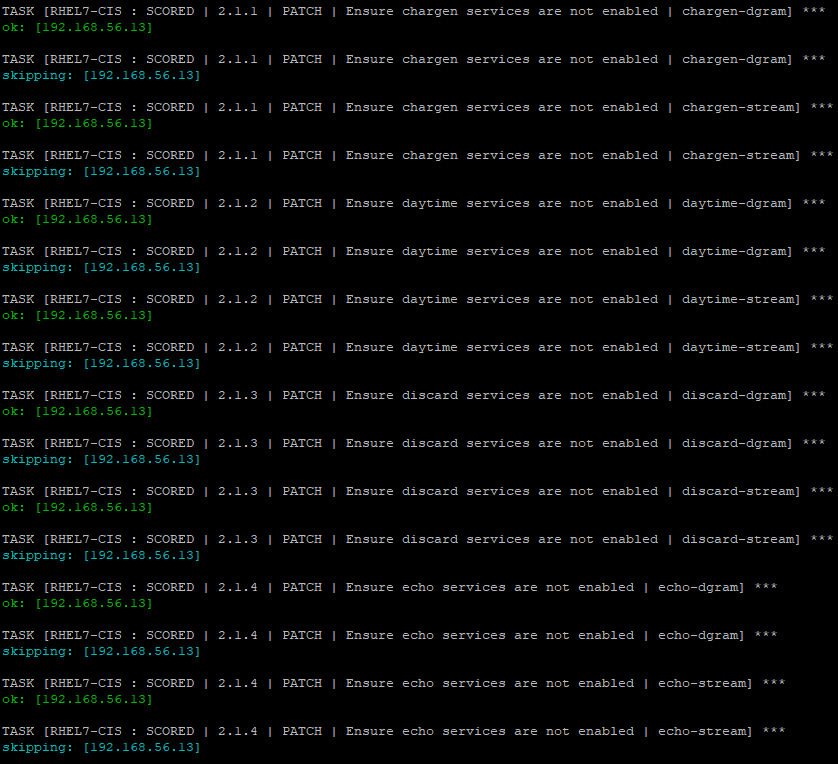
หลังจากทำการทดลองแล้ว ได้ผลการทำโครงออกมาได้ดังนี้

**4.1 ผลการทำ Hardening โดยใช้ Ansible playbook**

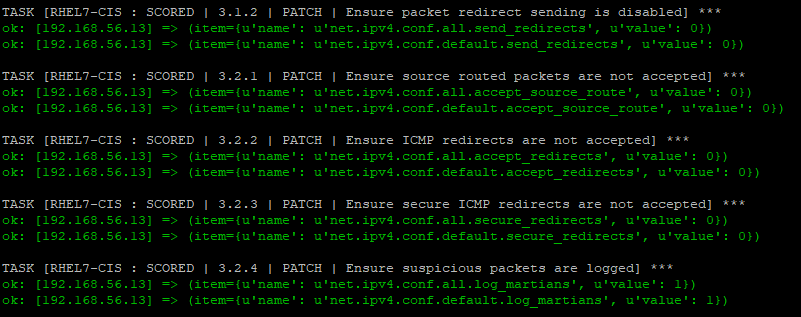
ตัวอย่างผลการรันจาก section 1

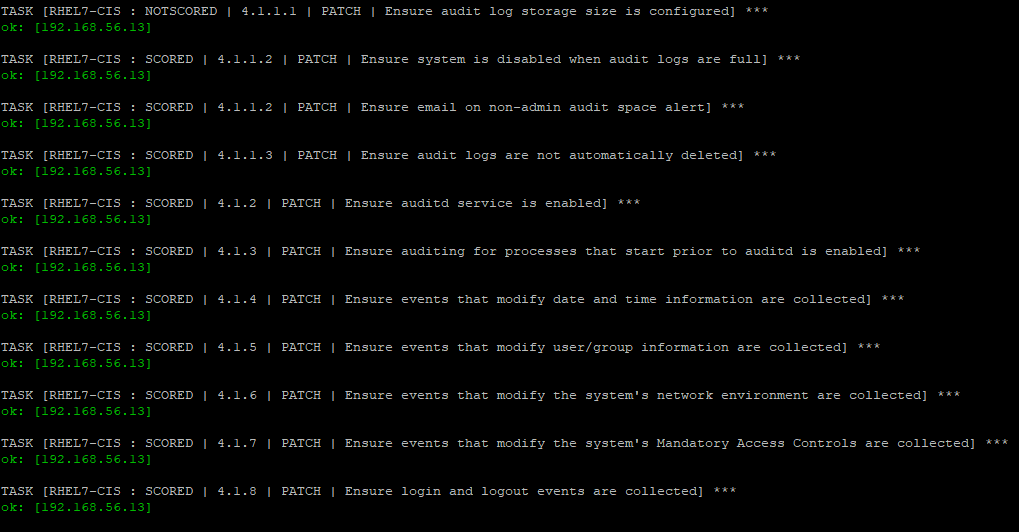


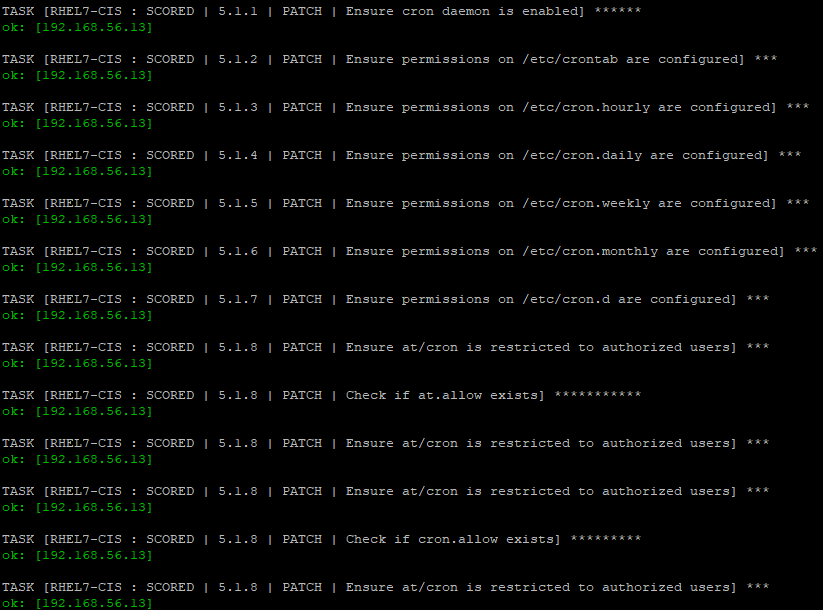
ตัวอย่างผลการรันจาก section 2

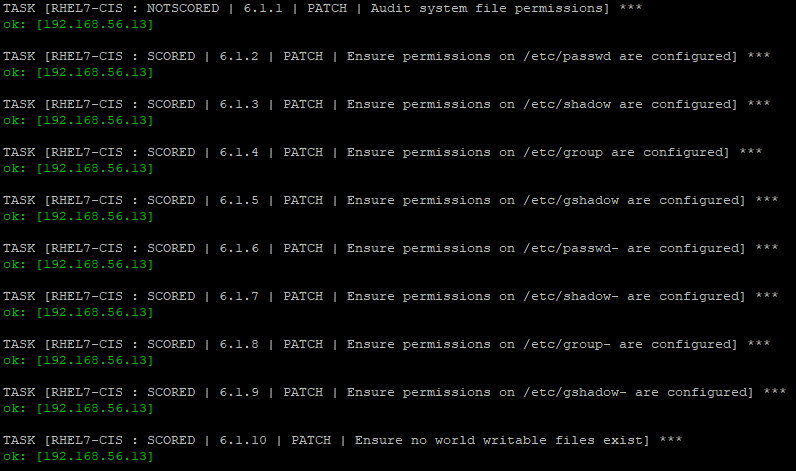


ที่เห็นว่า skip เพราะก่อนหน้านี้ มีการเช็คว่ามีservice นั้น ลงไว้หรือไม่ ถ้าไม่มีก็ให้skip

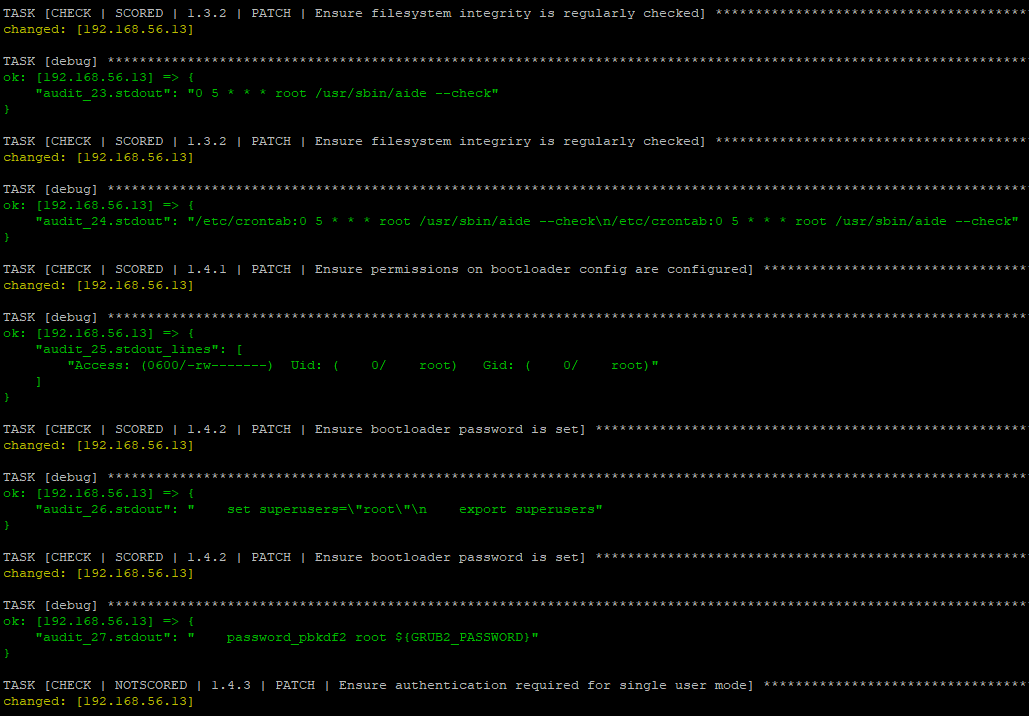
ตัวอย่างผลการรันจาก section 3  


ตัวอย่างผลการรันจาก section 4  


ตัวอย่างผลการรันจาก section 5  


ตัวอย่างผลการรันจาก section 6  


**4.2 ผลการตรวจสอบการทำ Hardening โดยใช้ Ansible playbook**

ตัวอย่างผลการรัน playbook  


**บทที่ 5**

**บทสรุปและข้อเสนอแนะ**

**5.1 สรุปผลการทำโครงงาน**

โดยรวมแล้วผลการทำโครงงานมีดังนี้ 1.)ที่skip นั้นเพราะว่ากำหนดไว้ให้ skip หรือว่า กรณีตัวอย่างเช่น skip เพราะตรวจสอบ service ที่กำหนดไว้ ถ้าไม่มีก็ให้ skip ถ้ามีก็ให้ disable service นั้นๆ 2.) ในส่วนของการตรวจสอบการทำ Hardening นั้น จะมี error แต่กำหนดไว้ว่า ถ้า error ก็ให้ skip ซึ่งสาเหตุที่ error นั้น เพราะว่า เครื่องนั้นไม่ได้ลง software ที่กำหนดไว้ เช่น   
syslog-ng เป็นต้น 3.) การใช้ansible ในการทำ Hardening นั้น ทำให้ประหยัดเวลาในการทำ Hardening ไปได้มาก จากที่ใช้เวลาทำประมาณ 1 ชั่วโมงหรือมากกว่านั้น การใช้ ansible นั้นใช้เวลาขั้นต่ำประมาณ20นาทีเท่านั้น

**5.2 ประโยชน์จากการทำโครงงาน**

5.2.1 ได้เรียนรู้การใช้งาน option ใหม่ๆของ ansible ที่ยังเคยใช้

5.2.2 ได้เรียนรู้เกี๋ยวกับเรื่อง umask ที่ต้องใส่ค่าที่ผลตรงข้ามกับ sticky bit เช่น sticky bit คือ 750 วิธีคิดumaskก็คือ ให้นำค่า777ไปลบกับsticky bit จะได้ผลดังนี้ 777-750 = 027

5.2.3 ในการทำโครงงานครั้งทำให้ได้ความรู้ในการทำplaybook กับ ansible role และสามารถนำความรู้ที่ได้ไปประยุกต์ใช้ในการทำ playbook กับ ansible role แบบอื่นได้ในอนาคต

**5.3 ปัญหา อุปสรรค และแนวทางการแก้ไขโครงงาน**

ปัญหาที่เจอจะเป็นการskipของขั้นตอนการทำงานที่ไม่ทราบสาเหตุ จากการศึกษาcodeที่ใช้นั้นทำให้ทราบสาเหตุและแก้ไข้ปัญหาได้

**5.4 ข้อเสนอแนะ**

**สำหรับสถานประกอบการ**

โดยรวมแล้วไม่มีข้อเสนอแนะอะไรสำหรับสถานประกอบการ

**สำหรับนักศึกษาสหกิจศึกษา**

นักศึกษาก่อนที่จะมาปฏิบัติงานสหกิจที่บริษัทนี้ หรือที่บริษัทไหนก็ตาม นักศึกษาควรศึกษาการใช้งานโปรแกรมหรือระบบปฏิบัติการที่ใช้ในการทำงานของบริษัทนั้นๆ

**สำหรับมหาวิทยาลัย**

จัดการเรียนการสอนเพิ่มเติมสำหรับการใช้งานระบบCentOS หรือก็ใช้งานAnsible

**บรรณานุกรม**

Ansible Configuration Management. (2559).

สืบค้นจาก http://itbakery.net/2016/08/22/ansible-configuration-management/

ฮาร์ดเดนนิง (Hardening). (2554)  
 สืบค้นจาก http://mmi55.blogspot.com/2011/05/hardening.html  
CentOS Introduction. (2555).  
 สืบค้นจาก https://www.etda.or.th/content/1344.html

พบช่องโหว่บายพาส ASLR บน Intel Haswell CPU เสี่ยงถูก Code Injection. (2559).  
 สืบค้นจาก https://www.techtalkthai.com/aslr-bypass-found-on-intel-haswell-cpu/

SELinux (ซีลีนุกซ์) คืออะไร เป็นกลไกภาคบังคับที่ใช้เพื่อควบคุมการเข้าถึงการใช้งานระบบ. (2560).  
 สืบค้นจาก https://www.mindphp.com/คู่มือ/73-คืออะไร/4168-what-is-selinux.html

NTP คืออะไร NTP คือ network protocol ที่ใช้เทียบเวลา. (2561).  
 สืบค้นจาก https://saixiii.com/what-is-ntp/

NIS/NIS+. (2552).  
 สืบค้นจาก https://blogitknowledge.wordpress.com/category/system-services/nisnis/

คำสั่ง Linux ขั้น Advance สำหรับ Programmers. (2561).  
 สืบค้นจาก https://www.techstarthailand.com/blog/detail/Important-Advanced-Linux-Commands-For-Programmers/665

Telnet คืออะไร แทลเน็ต คือ บริการที่ช่วยให้เราสามารถใช้คอมพิวเตอร์เครื่องอื่นราวกับไปนั่งใช้เครื่องคอมพิวเตอร์ของที่นั่น. (2560).  
 สืบค้นจาก https://www.mindphp.com/คู่มือ/73-คืออะไร/2078-telnet-คืออะไร.html

LDAP คืออะไร แอลแดป เป็นโปรโตรคอลที่ใช้สำหรับเข้าถึงข้อมูล. (2560).  
 สืบค้นจาก https://saixiii.com/what-is-ldap/

การใช้งาน crontab เพื่อรัน script ตามเวลาที่กําหนด. (2560).  
 สืบค้นจาก https://thiti.dev/blog/740/

ทำความรู้จักกับ SSH (Secure Shell) คืออะไร Protocol สำหรับติดต่อ. (2562).  
 สืบค้นจาก https://www.mindphp.com/คู่มือ/73-คืออะไร/3329-ทำความรู้จักกับ-ssh-secure-shell.html  
EPEL (Extra Packages for Enterprise Linux) คืออะไร. (2562).  
 สืบค้นจาก https://aoostudio.com/single-blog.php?id=57&EPEL%20(Extra%20Packages%20for%20Enterprise%20Linux)%20%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3

CIS Red Hat Enterprise Linux 7 Benchmark v2.1.1-01-31-2017. (2560)  
 สืบค้นจาก http://www.itsecure.hu/library/image/CIS\_Red\_Hat\_Enterprise\_Linux\_7\_Benchmark\_v2.1.1.pdf