คู่มือการใช้งาน Ansible

สารบัญ

เนื้อหา หน้า

1. บทนำ

1.1. ภาพรวมของการทดสอบ

เอกสารฉบับนี้จัดทำขึ้นเพื่อสรุปแนวทางการประเมินและการทดสอบการตั้งค่าความปลอดภัย (Security Configuration) ของระบบปฏิบัติการ Oracle Linux 8 ตามมาตรฐาน CIS (Center for Internet Security) Benchmark โดยใช้ Ansible Playbook ที่ถูกพัฒนาสำหรับดำเนินการตรวจสอบและปรับแก้ไขค่า (Remediation) แบบอัตโนมัติ

การดำเนินงานนี้ครอบคลุมจำนวน 40 รายการควบคุม (CIS 40 Task) ที่เกี่ยวข้องกับความปลอดภัยด้าน Filesystem, Authentication, SSH Configuration, Password Policy และ System Logging โดยมีเป้าหมายเพื่อให้มั่นใจว่าระบบมีการกำหนดค่าที่สอดคล้องกับแนวทางปฏิบัติที่ดีที่สุด (Best Practices) สามารถลดความเสี่ยงจากการโจมตี และเพิ่มความน่าเชื่อถือของระบบในการใช้งานจริง

1.2. วิธีการที่ใช้ในการทดสอบ

การทดสอบและประเมินผลจะดำเนินการตามแนวทางของ CIS Benchmark โดยมีขั้นตอนดังนี้:

1. การเตรียมระบบ
    - ติดตั้ง Ansible บนเครื่องควบคุม (Control Node)
    - กำหนด inventory.ini เพื่อระบุเครื่องเป้าหมาย (Target Host)
2. การใช้งาน Playbook
    - ใช้ Playbook ที่ถูกออกแบบแยกตามแต่ละข้อของ CIS Benchmark
    - ดำเนินการตรวจสอบ (Audit) และแก้ไขการตั้งค่า (Remediation) โดยอัตโนมัติ
3. การตรวจสอบผลลัพธ์ (Validation)
    - ใช้คำสั่ง Audit จาก CIS Benchmark เพื่อตรวจสอบผลลัพธ์หลังการปรับแก้
    - จัดเก็บสถานะของแต่ละ Control (Pass, Fail, Not Applicable) เพื่อรายงาน

1.3. วัตถุประสงค์ของการทดสอบ

1. ตรวจสอบการตั้งค่าความปลอดภัยของระบบ Oracle Linux 8 ให้สอดคล้องกับมาตรฐาน CIS Benchmark
2. ลดความเสี่ยงจากการโจมตีที่เกิดจากการกำหนดค่าระบบที่ไม่ปลอดภัย
3. จัดทำรายงานผลการทดสอบเพื่อเป็นคู่มือการตรวจสอบและการปรับแก้ในอนาคต
4. สนับสนุนการทำงานของฝ่ายความปลอดภัย (Security Team) และผู้ดูแลระบบ (System Administrator) ในการดำเนินงานด้าน Compliance

2. แนวทางการทดสอบ

2.1. การเตรียมเครื่องมือ

เพื่อให้การทดสอบและปรับตั้งค่าความปลอดภัยด้วย Ansible CIS 40 Task สามารถทำได้อย่างถูกต้อง จำเป็นต้องเตรียมเครื่องมือดังนี้:

2.1.1. Control Node (เครื่องควบคุม)

ระบบปฏิบัติการ: Linux (เช่น Ubuntu 22.04 หรือ Oracle Linux 8)

ติดตั้ง Ansible

```
sudo dnf install ansible -y    # สำหรับ Oracle Linux / RHEL
sudo apt install ansible -y    # สำหรับ Ubuntu / Debian
```

ตรวจสอบเวอร์ชัน

```
ansible --version
```

2.1.2. Target Node (เครื่องเป้าหมาย)

1. ระบบปฏิบัติการ: Oracle Linux 8
2. เปิดใช้งาน SSH และอนุญาตให้ Control Node เข้ามาได้
3. ผู้ใช้งานต้องมีสิทธิ์ root หรือ sudo
4. ต้องมี Python ในเครื่อง

2.1.3.ไฟล์ที่ต้องเตรียม

inventory.ini – ระบุเครื่องเป้าหมาย เช่น

```
[Default]
Hostname_here ansible_host=(192.168.xxx.xxx)
```

playbook.yml – Playbook ที่รวม 40 Task ตามมาตรฐาน CIS Benchmark

2.2. ขั้นตอนการรัน Playbook

2.2.1. ตรวจสอบการเชื่อมต่อกับ Target Node

คำสั่ง

```
ansible -i inventory.ini all -m ping
```

2.2.2. คำสั่งในทดสอบ (ไม่มีผลต่อระบบ)

คำสั่ง

```
ansible-playbook -i <inventory.ini> <playbook.yaml> -u <user for login> --ask-pass --ask-become-pass --check --diff
```

2.2.3. รันจริงมีผลต่อระบบ Playbook CIS 40 Task

คำสั่ง

```
ansible-playbook -i <inventory.ini> <playbook.yaml> -u <user for login> --ask-pass --ask-become-pass
```

2.2.4. รันจริงแบบครบทุกข้อและมีผลต่อระบบ โดยใช้ Python

คำสั่ง

```
python3 automated.py –root>. -u <root> --ask-pass-once --ask-become-pass-once
```

2.3. เกณฑ์การพิจารณาผล

1. PASS (ผ่าน): การตั้งค่าตรงตาม CIS Benchmark
2. FAIL (ผิดพลาด): การตั้งค่าไม่ถูกต้อง ต้องปรับแก้เพิ่มเติม
3. N/A (Not Applicable) : ไม่เข้าข่าย เครื่องเป้าหมายไม่ได้มีไฟล์ดังกล่าวที่ต้องแก้ไข

2.4. ข้อควรระวัง

1. ควรทดสอบบน VM หรือเครื่องจำลอง ก่อนใช้งานจริง
2. การรัน Playbook อาจส่งผลต่อ Service บางตัว เช่น SSH, Logging
3. ควรสำรอง (Backup) ค่าคอนฟิกเดิมก่อนทุกครั้ง

3. การทดสอบตามมาตรฐาน CIS 40 ข้อ

3.1. หมวด: Filesystem Security

1.1.2.2.4 – Ensure noexec option set on /dev/shm partition

คำอธิบาย

- /dev/shm เป็นพื้นที่ shared memory ที่ใช้เก็บไฟล์ชั่วคราวใน RAM หากไม่ได้ใส่ noexec อาจทำให้ผู้โจมตีรันไฟล์อันตรายได้

ผลกระทบ

- เสี่ยงต่อการรัน malware หรือ script โดยตรงจากหน่วยความจำ (หลบ forensic/antivirus)

ผลกระทบเมื่อแก้ด้วยสคริปต์

- บางโปรแกรมที่ต้อง execute ใน /dev/shm อาจทำงานผิดพลาด เช่น Chromium headless, Java-based app

1..1.2.3.3 – Ensure nosuid option set on /home partition

คำอธิบาย

- การใส่ nosuid บน /home ป้องกันไม่ให้ไฟล์ที่มี SUID/SGID bit ใน home directory รันด้วยสิทธิ์สูงกว่าผู้ใช้ปกติ

ผลกระทบ

- ถ้าไม่กำหนด อาจมี user สร้างไฟล์ที่ยกระดับสิทธิ์เป็น root ได้

ผลกระทบเมื่อแก้ด้วยสคริปต์

- ไม่มีผลกระทบต่อการใช้งานทั่วไปของผู้ใช้ แต่ script ที่ใช้ SUID ใน home (หากมี) จะไม่ทำงาน

1.1.2.4.2 – Ensure nodev option set on /var partition

คำอธิบาย

- nodev ป้องกันการสร้างและใช้งาน device file บน /var ซึ่งเป็นที่เก็บ log และ data ของ service

ผลกระทบ

- ถ้าไม่มี nodev อาจมีผู้โจมตีสร้าง device พิเศษเพื่อเข้าถึงระบบไฟล์หรือ kernel

ผลกระทบเมื่อแก้ด้วยสคริปต์

- โดยทั่วไปไม่มีผลกระทบกับ service แต่บางระบบที่ map device ลง /var จะไม่ทำงาน

1.1.2.4.3 – Ensure nosuid option set on /var partition

คำอธิบาย

- nosuid ช่วยป้องกันไฟล์ใน /var ถูกใช้ยกระดับสิทธิ์

ผลกระทบ

- หากไม่ได้ตั้งค่า อาจถูกวางไฟล์ที่มี SUID เพื่อยกระดับสิทธิ์จาก log หรือ temp ของ service

ผลกระทบเมื่อแก้ด้วยสคริปต์

- ไม่มีผลกระทบกับ service ทั่วไป

1.1.2.6.2 – Ensure nodev option set on /var/log partition

คำอธิบาย

- ป้องกันการสร้าง device file ใน /var/log

ผลกระทบ

- เสี่ยงต่อการถูกสร้าง device พิเศษเพื่อโจมตี

ผลกระทบเมื่อแก้ด้วยสคริปต์

- ไม่กระทบการเก็บ log ปกติ

1.1.2.6.3 – Ensure nosuid option set on /var/log partition

คำอธิบาย

- nosuid ป้องกันไม่ให้ไฟล์ log ถูกใช้เพื่อยกระดับสิทธิ์

ผลกระทบ

- ถ้าไม่ตั้ง อาจมีการฝังไฟล์ที่ใช้ SUID ใน log

ผลกระทบเมื่อแก้ด้วยสคริปต์

- ไม่กระทบการทำงานของระบบ log

1.1.2.6.4 – Ensure noexec option set on /var/log partition

คำอธิบาย

- noexec ป้องกันการ execute ไฟล์ binary หรือ script ใน /var/log

ผลกระทบ

- ถ้าไม่ตั้ง อาจรันไฟล์ที่ฝังใน log ได้ (log injection → execution)

ผลกระทบเมื่อแก้ด้วยสคริปต์

- โดยทั่วไปไม่มีผลกระทบ แต่ script/debug tool ที่รันจาก log path จะทำงานไม่ได้

3.2. หมวด: Core Dumps

1.4.3 – Ensure core dump backtraces are disabled

คำอธิบาย

- การแสดง backtrace ของ core dump จะเปิดเผยรายละเอียดการทำงานของโปรเซส เช่น call stack และ memory address

ผลกระทบ

- หากเปิดใช้งาน อาจทำให้ attacker ใช้ข้อมูล stack trace เพื่อวิเคราะห์หาช่องโหว่หรือ reverse engineering โปรแกรมได้

ผลกระทบเมื่อแก้ด้วยสคริปต์

- นักพัฒนาอาจไม่สามารถใช้ข้อมูล backtrace อัตโนมัติในการ debug ได้ ต้องพึ่ง log หรือเครื่องมืออื่นแทน

1.4.4 – Ensure core dump storage is disabled

คำอธิบาย

- core dump คือ snapshot ของหน่วยความจำเมื่อโปรเซส crash หากมีการเก็บ core dump อาจทำให้ข้อมูลลับ เช่น password, key หรือ token รั่วไหลได้

ผลกระทบ

- attacker สามารถอ่านไฟล์ core เพื่อนำข้อมูลสำคัญไปใช้โจมตีต่อ เช่น privilege escalation หรือ data leakage

ผลกระทบเมื่อแก้ด้วยสคริปต์

- การ debug crash โดยใช้ไฟล์ core จะไม่สามารถทำได้ ต้องใช้วิธี trace หรือ logging ในสภาพแวดล้อมควบคุมแทน

3.3. หมวด: Network Security

3.3.5 – Ensure ICMP redirects are not accepted

คำอธิบาย

- ICMP redirect คือแพ็กเก็ตที่บอกให้โฮสต์เปลี่ยนเส้นทางการส่งข้อมูล หากเปิดใช้อาจถูก attacker ปลอมแพ็กเก็ตเพื่อบังคับให้ทราฟฟิกวิ่งผ่านเส้นทางที่ควบคุมได้ (MITM)

ผลกระทบ

- หากไม่ปิด ระบบอาจถูกโจมตีแบบ man-in-the-middle หรือ route manipulation ได้

ผลกระทบเมื่อแก้ด้วยสคริปต์

- โดยทั่วไปไม่มีผลกระทบกับการทำงานปกติของระบบ ยกเว้นในกรณีที่เครือข่ายพึ่งพา ICMP redirect ในการทำ routing ซึ่งถือว่ามีความเสี่ยงและไม่ปลอดภัยอยู่แล้ว

3.3.9 – Ensure suspicious packets are logged

คำอธิบาย

- การ log แพ็กเก็ตที่ผิดปกติ (เช่น fragmented, martian packets) ช่วยให้ผู้ดูแลสามารถตรวจจับพฤติกรรมที่บ่งชี้ถึงการโจมตีเครือข่ายหรือ probing

ผลกระทบ

- หากไม่เปิดใช้งาน log จะขาดหลักฐานเมื่อเกิดเหตุการณ์โจมตี ทำให้การ forensic และ incident response ทำได้ยากขึ้น

ผลกระทบเมื่อแก้ด้วยสคริปต์

- อาจทำให้มี log เพิ่มขึ้นเล็กน้อยในระบบ แต่ไม่ส่งผลกระทบต่อการทำงานของ network service

3.4. หมวด: Scheduled Tasks & Cron Permissions

4.1.1.3 – Ensure permissions on /etc/cron.hourly are configured

คำอธิบาย

- โฟลเดอร์ /etc/cron.hourly ใช้เก็บสคริปต์ที่รันทุกชั่วโมง ควรกำหนดสิทธิ์ให้เข้าถึงได้เฉพาะ root

ผลกระทบ

- หากสิทธิ์เปิดกว้าง ผู้ไม่หวังดีอาจวางสคริปต์อันตรายเพื่อให้รันอัตโนมัติทุกชั่วโมง

ผลกระทบเมื่อแก้ด้วยสคริปต์

- ไม่กระทบการทำงานของ cron หากสคริปต์เดิมเป็นของ root อยู่แล้ว

4.1.1.4 – Ensure permissions on /etc/cron.daily are configured

คำอธิบาย

- โฟลเดอร์ /etc/cron.daily เก็บสคริปต์ที่รันทุกวัน ต้องจำกัดสิทธิ์ให้ root เท่า

ผลกระทบ

- หากสิทธิ์ไม่ถูกต้อง attacker อาจแทรกสคริปต์เพื่อรันทุกวัน

ผลกระทบเมื่อแก้ด้วยสคริปต์

- ไม่กระทบงานประจำวันของ cron ที่ถูกต้องอยู่แล้ว

4.1.1.5 – Ensure permissions on /etc/cron.weekly are configured

คำอธิบาย

- /etc/cron.weekly ใช้สำหรับสคริปต์ที่รันสัปดาห์ละครั้ง ต้องป้องกันการเขียนโดยผู้ใช้ทั่วไป

ผลกระทบ

- หากไม่กำหนดสิทธิ์ attacker สามารถแทรกโค้ดที่จะรันทุกสัปดาห์โดยอัตโนมัติ

ผลกระทบเมื่อแก้ด้วยสคริปต์

- ไม่มีผลต่อ cron jobs ปกติ

4.1.1.6 – Ensure permissions on /etc/cron.monthly are configured

คำอธิบาย

- /etc/cron.monthly เก็บสคริปต์ที่รันทุกเดือน ต้องเป็นสิทธิ์ root เท่านั้น

ผลกระทบ

- สิทธิ์ที่ไม่ถูกต้องทำให้ผู้ไม่หวังดีวางสคริปต์รันอัตโนมัติทุกเดือน

ผลกระทบเมื่อแก้ด้วยสคริปต์

- ไม่มีผลกระทบกับงานที่รันปกติอยู่แล้ว

4.1.1.7 – Ensure permissions on /etc/cron.d are configured

คำอธิบาย

- /etc/cron.d ใช้เก็บไฟล์กำหนด cron jobs ที่มีความสำคัญมาก ต้องจำกัดสิทธิ์เฉพาะ root

ผลกระทบ

- หากสิทธิ์กว้างเกินไป อาจถูก attacker สร้าง cron job อันตรายเพื่อรันโดยอัตโนมัติ

ผลกระทบเมื่อแก้ด้วยสคริปต์

- ไม่มีผลกระทบกับ cron jobs ที่ถูกต้อง

4.1.1.8 – Ensure crontab is restricted to authorized users

คำอธิบาย

- cron.allow และ cron.deny ใช้ควบคุมว่าใครสามารถใช้งาน cron ได้ ควรอนุญาตเฉพาะผู้ใช้ที่จำเป็น

ผลกระทบ

- หากไม่จำกัด อาจทำให้ผู้ใช้ทั่วไปสร้าง cron job ที่เป็นอันตรายหรือสิ้นเปลืองทรัพยากร

ผลกระทบเมื่อแก้ด้วยสคริปต์

- ผู้ใช้ที่ไม่อยู่ในรายชื่ออนุญาตจะไม่สามารถใช้ cron ได้ แต่ผู้ใช้ที่จำเป็นยังใช้งานได้ตามปกติ

3.5. หมวด: SSH Server Configuration

4.2.4 – Ensure SSH access is configured

คำอธิบาย

- ควรกำหนดการเข้าถึง SSH ด้วย AllowUsers, AllowGroups หรือ DenyUsers เพื่อลดสิทธิ์เฉพาะบัญชีที่จำเป็น

ผลกระทบ

- หากไม่จำกัด อาจทำให้ผู้ไม่หวังดีพยายาม brute force SSH กับทุกบัญชีในระบบได้

ผลกระทบเมื่อแก้ด้วยสคริปต์

- ผู้ใช้ที่ไม่ได้อยู่ในกลุ่มที่อนุญาตจะไม่สามารถเข้า SSH ได้

4.2.11 – Ensure KexAlgorithms is configured

คำอธิบาย

- KexAlgorithms (Key Exchange) ต้องกำหนดให้ใช้เฉพาะอัลกอริทึมที่ปลอดภัย เช่น diffie-hellman-group14-sha256 หรือ ecdh-sha2-nistp256

ผลกระทบ

- หากปล่อยค่า default ที่ไม่ปลอดภัย อาจถูก downgrade attack หรือถอดรหัส session ได้

ผลกระทบเมื่อแก้ด้วยสคริปต์

- เครื่อง client เก่าที่ไม่รองรับอัลกอริทึมที่ปลอดภัยอาจเชื่อมต่อ SSH ไม่ได้

4.2.12 – Ensure LoginGraceTime is configured

คำอธิบาย

- LoginGraceTime คือเวลาที่อนุญาตให้ผู้ใช้ใส่รหัสผ่านหลังเชื่อมต่อ หากไม่ใส่ภายในเวลาที่กำหนดจะถูกตัดการเชื่อมต่อ ค่าแนะนำคือไม่เกิน 60 วินาที

ผลกระทบ

- หากค่าเวลายาวเกินไป อาจเปิดโอกาสให้ brute force attack ใช้เวลามากขึ้น

ผลกระทบเมื่อแก้ด้วยสคริปต์

- ผู้ใช้ที่ใส่รหัสช้ากว่ากำหนดจะถูกตัดการเชื่อมต่อ ต้องเชื่อมใหม่

4.2.15 – Ensure MaxAuthTries is configured

คำอธิบาย

- MaxAuthTries กำหนดจำนวนครั้งสูงสุดที่อนุญาตให้ใส่รหัสผิดก่อนเชื่อมต่อถูกตัด ค่าแนะนำคือ 4 หรือน้อยกว่า

ผลกระทบ

- หากไม่จำกัด อาจทำให้ brute force password ได้ง่ายขึ้น

ผลกระทบเมื่อแก้ด้วยสคริปต์

- ผู้ใช้ที่พิมพ์รหัสผิดเกินค่าที่กำหนดจะถูกตัดการเชื่อมต่อ ต้องเปิด session ใหม่

3.6. หมวด: Privilege Escalation

4.3.2 – Ensure sudo commands use pty

คำอธิบาย

- การบังคับให้ sudo ใช้ pseudo-terminal (pty) ทำให้ทุกคำสั่งที่รันผ่าน sudo ถูกบันทึกลงใน log ได้ง่ายขึ้น และลดโอกาสที่ attacker จะรันคำสั่งโดยไม่มีการตรวจสอบ

ผลกระทบ

- หากไม่กำหนด บางคำสั่งที่รันผ่าน sudo อาจไม่ถูกบันทึก ทำให้ forensic หรือ audit ยากขึ้น

ผลกระทบเมื่อแก้ด้วยสคริปต์

- ไม่มีผลกระทบกับผู้ใช้ทั่วไป ยกเว้นระบบ logging จะมีข้อมูลละเอียดขึ้น

4.3.3 – Ensure sudo log file exists

คำอธิบาย

- sudo log ช่วยบันทึกคำสั่งที่ถูกสั่งผ่านสิทธิ์ root เพื่อใช้ตรวจสอบย้อนหลังและทำ forensic analysis ได้

ผลกระทบ

- หากไม่มี log อาจไม่สามารถหาหลักฐานเมื่อเกิด misuse หรือ privilege escalation attack

ผลกระทบเมื่อแก้ด้วยสคริปต์

- จะมี log file เพิ่มขึ้นเล็กน้อยในระบบ แต่ไม่กระทบการใช้งาน

4.3.7 – Ensure access to the su command is restricted

คำอธิบาย

- ควรจำกัดสิทธิ์การใช้คำสั่ง su ให้เฉพาะผู้ใช้ที่อยู่ในกลุ่มที่กำหนด (เช่น wheel) เพื่อบังคับให้ผู้ใช้ทั่วไปใช้ sudo ซึ่งมีการควบคุมและ logging ที่ดีกว่า

ผลกระทบ

- หากไม่จำกัด ผู้ใช้ทุกคนสามารถพยายามเข้าสู่ root ด้วย su ได้ ทำให้เพิ่มความเสี่ยงจาก brute force หรือ misuse

ผลกระทบเมื่อแก้ด้วยสคริปต์

- ผู้ใช้ที่ไม่ได้อยู่ในกลุ่มที่กำหนดจะไม่สามารถใช้ su ได้ แต่ยังคงใช้ sudo ได้ตามสิทธิ์

3.7. หมวด: Password Policy & Authentication

4.4.3.1.1 – Ensure password failed attempts lockout is configured

คำอธิบาย

- กำหนดให้ล็อกบัญชีผู้ใช้ชั่วคราวหลังจากใส่รหัสผ่านผิดตามจำนวนครั้งที่กำหนด (เช่น 5 ครั้ง)

ผลกระทบ

- หากไม่กำหนด ผู้โจมตีสามารถ brute force รหัสผ่านได้ไม่จำกัด

ผลกระทบเมื่อแก้ด้วยสคริปต์

- ผู้ใช้ที่พิมพ์รหัสผิดหลายครั้งจะถูกล็อกชั่วคราว ต้องรอหรือให้ผู้ดูแลปลดล็อก

4.4.3.1.2 – Ensure password unlock time is configured

คำอธิบาย

- กำหนดระยะเวลาที่บัญชีจะถูกล็อกหลังจากใส่รหัสผิดครบจำนวนครั้ง เช่น 15 นาที

ผลกระทบ

- หากไม่กำหนด บัญชีอาจถูกล็อกถาวรจนต้องให้ผู้ดูแลแก้ไขเอง หรือเปิดโอกาสให้ brute force ต่อเนื่อง

ผลกระทบเมื่อแก้ด้วยสคริปต์

- ผู้ใช้ต้องรอครบเวลาที่ตั้งไว้ก่อนจะล็อกอินได้อีกครั้ง

4.4.3.2.1 – Ensure password number of changed characters is configured

คำอธิบาย

- กำหนดให้เมื่อผู้ใช้เปลี่ยนรหัส ต้องเปลี่ยนจำนวนตัวอักษรขั้นต่ำจากรหัสเก่า (เช่น 3 ตัว)

ผลกระทบ

- หากไม่กำหนด ผู้ใช้สามารถเปลี่ยนรหัสผ่านโดยเปลี่ยนเพียงเล็กน้อย (เช่น เพิ่มตัวเลขท้าย 1 หลัก) ทำให้รหัสเดาง่าย

ผลกระทบเมื่อแก้ด้วยสคริปต์

- ผู้ใช้อาจไม่สะดวกเพราะต้องเปลี่ยนรหัสมากกว่าขั้นต่ำ แต่ได้ความปลอดภัยสูงขึ้น

4.4.3.2.4 – Ensure password same consecutive characters is configured

คำอธิบาย

- ป้องกันการตั้งรหัสผ่านที่มีตัวอักษรซ้ำติดกันเกินค่าที่กำหนด เช่น "aaaa1111"

ผลกระทบ

- หากไม่กำหนด รหัสผ่านอาจอ่อนแอและคาดเดาได้ง่าย

ผลกระทบเมื่อแก้ด้วยสคริปต์

- ผู้ใช้จะถูกปฏิเสธหากพยายามตั้งรหัสผ่านที่มีตัวซ้ำกันต่อเนื่อง

4.4.3.2.5 – Ensure password maximum sequential characters is configured

คำอธิบาย

- ป้องกันการใช้ตัวอักษรหรือตัวเลขเรียงลำดับเกินค่าที่กำหนด เช่น "12345" หรือ "abcd"

ผลกระทบ

- หากไม่กำหนด ผู้ใช้สามารถสร้างรหัสผ่านที่เดาง่ายและเสี่ยงต่อ brute force

ผลกระทบเมื่อแก้ด้วยสคริปต์

- ผู้ใช้จะไม่สามารถใช้รหัสผ่านที่เป็นลำดับเรียงกันยาวๆ ได้

4.4.3.2.7 – Ensure password quality is enforced for the root user

คำอธิบาย

- บังคับใช้กฎรหัสผ่านที่เข้มงวดกับ root เช่น ความยาวขั้นต่ำ ตัวอักษรพิเศษ ตัวเลข และตัวพิมพ์ใหญ่/เล็ก"

ผลกระทบ

- หากไม่กำหนด root อาจใช้รหัสผ่านที่ง่ายต่อการเดา ซึ่งเป็นความเสี่ยงสูง

ผลกระทบเมื่อแก้ด้วยสคริปต์

- root ต้องตั้งรหัสที่ซับซ้อนขึ้น แต่เพิ่มความปลอดภัยของระบบ

4.4.3.3.1 – Ensure password history remember is configured

คำอธิบาย

- บังคับให้ระบบจำรหัสผ่านเก่าจำนวนหนึ่ง (เช่น 5 ชุด) เพื่อป้องกันไม่ให้ผู้ใช้ตั้งรหัสเดิมซ้ำq

ผลกระทบ

- หากไม่กำหนด ผู้ใช้อาจใช้รหัสผ่านเดิมซ้ำ ทำให้เสี่ยงต่อการรั่วไหล

ผลกระทบเมื่อแก้ด้วยสคริปต์

- ผู้ใช้ต้องตั้งรหัสใหม่ที่แตกต่างจากรหัสก่อนหน้าในรอบที่กำหนด

4.4.3.3.2 – Ensure password history is enforced for the root user

คำอธิบาย

- ใช้การบังคับจำรหัสผ่านเดิมกับ root เช่นเดียวกับผู้ใช้ทั่วไป เพื่อป้องกันการใช้รหัสผ่านซ้ำ

ผลกระทบ

- หากไม่กำหนด root อาจตั้งรหัสผ่านซ้ำเดิม ทำให้ความปลอดภัยต่ำ

ผลกระทบเมื่อแก้ด้วยสคริปต์

- root ต้องตั้งรหัสใหม่ที่ไม่เหมือนกับรหัสก่อนหน้าในรอบที่กำหนด

3.8. หมวด: Session Management

4.5.1.2 – Ensure password expiration is 365 days or less

คำอธิบาย

- กำหนดให้อายุรหัสผ่านไม่เกิน 365 วัน เพื่อบังคับให้ผู้ใช้เปลี่ยนรหัสตามรอบเวลา

ผลกระทบ

- หากไม่กำหนด รหัสผ่านอาจถูกใช้นานเกินไปจนมีโอกาสรั่วไหลหรือถูก brute force ได้

ผลกระทบเมื่อแก้ด้วยสคริปต์

- ผู้ใช้ต้องเปลี่ยนรหัสผ่านตามรอบเวลาที่กำหนด อาจไม่สะดวกแต่เพิ่มความปลอดภัย

4.5.3.2 – Ensure default user shell timeout is configured

คำอธิบาย

- TMOUT ใช้กำหนดเวลา inactivity ของ shell session เมื่อครบเวลาจะ logout อัตโนมัติ ค่าแนะนำคือ 900 วินาที (15 นาที) หรือน้อยกว่า

ผลกระทบ

- หากไม่กำหนด Session ที่ค้างไว้โดยไม่มีการใช้งานอาจถูกผู้ไม่หวังดีเข้ามาใช้ต่อได้

ผลกระทบเมื่อแก้ด้วยสคริปต์

- ผู้ใช้จะถูกบังคับ logout อัตโนมัติเมื่อไม่ใช้งานตามเวลาที่ตั้งไว้ ต้อง login ใหม่

4.5.3.3 – Ensure default user umask is configured

คำอธิบาย

- umask กำหนด permission พื้นฐานเมื่อสร้างไฟล์หรือโฟลเดอร์ใหม่ ค่าแนะนำคือ 027 หรือ 0277 เพื่อไม่ให้สิทธิ์ world-writable

ผลกระทบ

- หากไม่กำหนด ไฟล์ใหม่อาจถูกสร้างด้วย permission ที่เปิดกว้างเกินไป เช่น 644 หรือ 666 ซึ่งเสี่ยงต่อการรั่วไหลข้อมูล

ผลกระทบเมื่อแก้ด้วยสคริปต์

- ไฟล์และโฟลเดอร์ใหม่จะถูกสร้างด้วย permission ที่เข้มงวดขึ้น อาจทำให้บางผู้ใช้ไม่มีสิทธิ์อ่าน/เขียนหากไม่ถูกกำหนดชัดเจน

3.9. หมวด: Logging

5.1.1.4 – Ensure rsyslog default file permissions are configured

คำอธิบาย

- ต้องกำหนดสิทธิ์ไฟล์ log ที่สร้างโดย rsyslog ให้ปลอดภัย เช่น 0640 เพื่อให้ root และกลุ่มที่กำหนดเท่านั้นเข้าถึงได้

ผลกระทบ

- หากไม่กำหนด ไฟล์ log อาจถูกผู้ใช้ทั่วไปอ่านได้ ทำให้ข้อมูลภายในระบบรั่วไหล

ผลกระทบเมื่อแก้ด้วยสคริปต์

- log ใหม่จะถูกสร้างด้วยสิทธิ์ที่เข้มงวดขึ้น อาจทำให้บางโปรแกรมที่ต้องการอ่าน log โดยตรงไม่สามารถเข้าถึงได้

5.1.2.3 – Ensure journald is configured to compress large log files

คำอธิบาย

- journald สามารถบีบอัด log ขนาดใหญ่เพื่อลดการใช้พื้นที่ดิสก์ ควรเปิดใช้งานตัวเลือก Compress=yesกำหนดเท่านั้นเข้าถึงได้

ผลกระทบ

- หากไม่เปิดใช้งาน พื้นที่เก็บ log อาจเต็มเร็ว และอาจต้องลบ log เก่าออกก่อนเวลา ทำให้ข้อมูลสูญหา

ผลกระทบเมื่อแก้ด้วยสคริปต์

- log ที่บีบอัดอาจใช้เวลามากขึ้นเล็กน้อยในการอ่าน แต่ช่วยประหยัดพื้นที่เก็บข้อมูล

5.1.2.4 – Ensure journald is configured to write logfiles to persistent disk

คำอธิบาย

- journald โดยค่าเริ่มต้นอาจเก็บ log แค่ใน memory ซึ่งจะหายไปเมื่อรีบูต ควรกำหนด Storage=persistent เพื่อเก็บในดิสก์

ผลกระทบ

- หากไม่กำหนด Log จะสูญหายทุกครั้งที่เครื่องถูกรีบูต ทำให้ forensic และ audit ย้อนหลังทำไม่ได้

ผลกระทบเมื่อแก้ด้วยสคริปต์

- log จะถูกเก็บถาวรบนดิสก์ ใช้พื้นที่มากขึ้น แต่เพิ่มความสามารถในการตรวจสอบย้อนหลัง

3.10. หมวด: User Environment

6.2.8 – Ensure root path integrity

คำอธิบาย

- ต้องตรวจสอบให้แน่ใจว่า PATH ของ root ไม่มี directory ที่ไม่ปลอดภัย เช่น . (current directory) หรือ directory ที่เขียนได้โดยผู้ใช้ทั่วไป

ผลกระทบ

- หาก PATH ของ root มีโฟลเดอร์ที่ไม่ปลอดภัย ผู้ไม่หวังดีสามารถวางไฟล์ binary ปลอมใน path นั้น ทำให้ root รัน

ผลกระทบเมื่อแก้ด้วยสคริปต์

- root อาจต้องปรับ command search path ให้ปลอดภัยขึ้น แต่ไม่มีผลกับการใช้งานทั่วไป

6.2.11 – Ensure local interactive user dot files access is configured

คำอธิบาย

- ไฟล์ dot files (เช่น .bashrc, .profile, .ssh/authorized_keys) ของผู้ใช้ควรถูกจำกัดสิทธิ์ไม่ให้ผู้อื่นเข้าถึง เพื่อป้องกันการแก้ไขค่า environment หรือ config สำคัญ

ผลกระทบ

- หากสิทธิ์เปิดกว้าง ผู้ไม่หวังดีสามารถแก้ไข dot files เพื่อฝัง backdoor, alias อันตราย หรือเพิ่ม key สำหรับ SSH

ผลกระทบเมื่อแก้ด้วยสคริปต์

- ผู้ใช้อาจไม่สามารถแชร์ไฟล์ config ของตนกับผู้ใช้อื่นได้ แต่ช่วยเพิ่มความปลอดภัยของ session