



1. พิมพ์คำสั่ง, พิมพ์ keyboard

2. พิมพ์คำสั่ง (พิมพ์ คอมพิวเตอร์) (Text base)

3. Text file

มี type เดียว กับ binary file เป็น universal format

file association หาก zip, rar เมื่อแล้ว 9 ใน 10 ครั้ง อีก 1 ครั้ง / 10 ครั้ง พิมพ์คำสั่ง } เพื่อตรวจสอบความถูกต้อง
- extension

Command Unix

cd etc/issue | head → ดูบรรทัดแรกๆ ให้เห็น หัวข้อ
→ pipe

cd etc/issue | more → ดูทีละหน้า

cd etc/issue | tail → ดูบรรทัดสุดท้าย

หาไฟล์ที่เกี่ยวข้อง เช็กสิทธิ์:

log มีหลายตัว / ดูที่บันทึกเหตุการณ์ ที่บันทึกเวลา จากที่บันทึก

ls -al /var/log → ดูใน folder log

1. ดูใน folder log มีอะไรบ้าง / ดูว่าบันทึกไว้ที่ folder อะไร

2. output ของคำสั่งที่พิมพ์ ดูว่า format output อย่างไร

3. ดูว่าไฟล์ log/text มี format อะไร หากพบความผิดปกติ (ข้อควรระวัง)

ใช้คำสั่งที่คล้ายกัน

(ในกรณี text file) (option)

secure shell diamond

(ดูว่าบันทึกไว้ที่ folder อะไร)

(pipe)

grep -i "sshd" /var/log/authlog ... | tail → ดูว่ามี sshd หรือไม่ secure shell ไม่พบ (file ที่เกี่ยวข้องกับเหตุการณ์)

wc -l /var/log/authlog → มีกี่บรรทัดทั้งหมดใน file /var/log/authlog

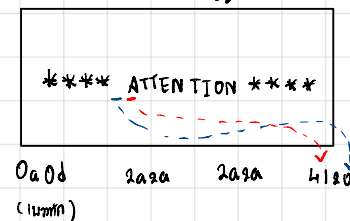
head -5 /etc/issue → ดูบรรทัดแรกๆ ของ /etc/issue

od -x /etc/issue | head -10 → ดูข้อมูลใน hex 00000000
↓
dump ของ binary file จักรหา
ดูว่าบันทึกไว้ที่ folder อะไร

head -5 /var/log/authlog → ดูบรรทัดแรกๆ ของ /var/log/authlog

grep "sshd" /var/log/authlog | head -5 → ดูว่ามี sshd หรือไม่ 5 บรรทัดแรกๆ

little endian = บันทึกด้วย byte



การเขียน ท้าย 1. Unix redirection

2. rwx

ทำไม Unix มี permission? เพราะมันทำงาน multiuser มีคนใช้มัน owner กับคนอื่น permission