1.ขั้นตอนการดำเนินงาน

Task 1: User Management & Password Policy

Groups	Users	password
developers	fifa	162545
testers	Boss	passw0rd
dbadmin	first	passw0rd

1.1 สร้าง Users และ Groups:

```
Jirapat@UbuntuDesktop:~$ sudo groupadd developers
```

สร้างกลุ่มผู้ใช้ใหม่ชื่อ **developers**

```
Jirapat@UbuntuDesktop:~$ sudo groupadd testers
Jirapat@UbuntuDesktop:~$ sudo groupadd dbadmin
```

สร้างกลุ่ม testers dbadmin

```
Jirapat@UbuntuDesktop:~$ sudo passwd Fifa1
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word
Retype new password:
passwd: password updated successfully
Jirapat@UbuntuDesktop:~$ sudo passwd Fifa2
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word
Retype new password:
passwd: password updated successfully
Jirapat@UbuntuDesktop:~$ sudo passwd Boss
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word
Retype new password:
passwd: password updated successfully
Jirapat@UbuntuDesktop:~$ sudo passwd First
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word
Retype new password:
passwd: password updated successfully
```

ปลี่ยนรหัสผ่านให้ผู้ใช้ **Fifa1, Fifa2, Boss และ First** สำเร็จ

1.2 ตั้งค่า Password Policy:

```
Jirapat@UbuntuDesktop:~$ sudo nano /etc/login.defs
```

เปิดไฟล์ตั้งค่า `/etc/login.defs` ด้วย nano เพื่อแก้ไขกฎเกี่ยวกับ **รหัสผ่านและการล็อกอิน** ของผู้ใช้ในระบบ

```
PASS_MAX_DAYS   90
PASS_MIN_DAYS   7
PASS_WARN_AGE   14
PASS_MIN_LEN    12
```

ระบบนี้บังคับให้รหัสผ่าน **ยาว ≥ 12 ตัวอักษร**, เปลี่ยนได้ไม่ถี่เกินไป (อย่างน้อย 7 วัน), มีอายุใช้งาน 90 วัน, และจะแจ้งเตือนก่อนหมดอายุ 14 วัน

```
Jirapat@UbuntuDesktop:~$ sudo apt install libpam-pwquality
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
libpam-pwquality is already the newest version (1.4.5-3build1).
libpam-pwquality set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 21 not upgraded.
```

ตรวจสอบความแข็งแรงของรหัสผ่าน

```
Jirapat@UbuntuDesktop:~$ sudo nano /etc/pam.d/common-password
```

เปิดไฟล์ **/etc/pam.d/common-password** เพื่อแก้ไข **กฎการตั้งรหัสผ่าน** ของระบบ เช่น บังคับความยาวขั้นต่ำ และรูปแบบรหัสผ่านให้ปลอดภัยขึ้นครับ

```
password requisite pam_pwquality.so retry=3 minlen=12 difok=3 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1
```

บังคับให้ผู้ใช้ตั้งรหัสผ่านที่ **ยาว ≥ 12 ตัวอักษร** และต้องมีครบทั้ง **พิมพ์เล็ก, พิมพ์ใหญ่, ตัวเลข, อักขระพิเศษ** และต้องต่างจากรหัสเก่าอย่างน้อย 3 ตัวอักษร

```
Jirapat@UbuntuDesktop:~$ cat /etc/passwd | tail -4
Fifa1:x:1001:1004::/home/Fifa1:/bin/bash
Fifa2:x:1002:1005::/home/Fifa2:/bin/bash
Boss:x:1003:1006::/home/Boss:/bin/bash
First:x:1004:1007::/home/First:/bin/bash
```

แสดงผู้ใช้ 4 คนล่าสุดที่ถูกสร้างในระบบ คือ **Fifa1, Fifa2, Boss, First** พร้อมข้อมูล UID, GID, โฟลเดอร์ home และ shell ที่ใช้ (/bin/bash)

```
Jirapat@UbuntuDesktop:~$ groups Fifa1 Fifa2 Boss First
Fifa1 : Fifa1 developers
Fifa2 : Fifa2 developers
Boss : Boss testers
First : First dbadmin
```

ตอนนี้ผู้ใช้แต่ละคนถูกเพิ่มเข้าไปในกลุ่มที่สร้างไว้แล้ว:

- Developers → Fifa1, Fifa2
- Testers → Boss
- Dbadmin → First

```
Jirapat@UbuntuDesktop:~$ sudo nano /etc/pam.d/common-password
```

การเข้าไปแก้ไขไฟล์ **/etc/pam.d/common-password** เพื่อกำหนดกฎรหัสผ่านให้เข้มงวดขึ้น เช่น ความยาว, ความซับซ้อน และการห้ามซ้ำกับรหัสเก่า

```
password        requisite                       pam_pwquality.so retry=3 minlen=12 difok=3 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1
password        [success=2 default=ignore]      pam_unix.so obscure use_authtok try_first_pass yescrypt
password        sufficient                      pam_sss.so use_authtok
```

การทดสอบ password policy

```
Jirapat@UbuntuDesktop:~$ sudo passwd Fifa1
New password:
BAD PASSWORD: The password contains less than 1 uppercase letters
Retype new password:
passwd: password updated successfully
```

เปลี่ยนรหัสผ่านของผู้ใช้ **Fifa1** แล้ว ระบบเตือนว่ารหัสผ่านไม่ตรงตามกฎ (ไม่มีตัวพิมพ์ใหญ่) แต่ก็ยังบันทึกสำเร็จ

Task 2: Sudo Permissions

2.1 สร้าง Sudo Groups:

```
Jirapat@UbuntuDesktop:~$ sudo groupadd sudo-developers
```

สร้างกลุ่มใหม่ชื่อ **sudo-developers** เอาไว้สำหรับจัดการสิทธิ์หรือรวมผู้ใช้กลุ่มนักพัฒนาที่ต้องการสิทธิ์ sudo

```
Jirapat@UbuntuDesktop:~$ sudo groupadd sudo-limited
```

คำสั่งนี้สร้างกลุ่มใหม่ชื่อ **sudo-limited** เอาไว้สำหรับจัดการสิทธิ์ sudo แบบควบคุม/จำกัด

```
Jirapat@UbuntuDesktop:~$ sudo usermod -aG sudo-developers Fifa1
Jirapat@UbuntuDesktop:~$ sudo usermod -aG sudo-developers Fifa2
Jirapat@UbuntuDesktop:~$ sudo usermod -aG sudo-limited Boss
```

Fifa1 → อยู่ในกลุ่ม sudo-developers ทำ ทุกคำสั่ง ได้เหมือน root
Fifa2 → อยู่ในกลุ่ม sudo-developers ทำ ทุกคำสั่ง ได้เหมือน root
Boss → อยู่ในกลุ่ม sudo-limited ได้เฉพาะคำสั่งที่กำหนดเท่านั้น เช่น (ดูสถานะ service),(ดู log),(ดู process)

First

ใช้ sudo ได้เฉพาะคำสั่งเกี่ยวกับ MySQL เช่น

- mysql
- mysqldump
- systemctl restart mysql

2.2 Configure Sudoers:

sudo visudo ใช้เพื่อ **แก้ไฟล์สิทธิ์การใช้งาน sudo ของผู้ใช้และกลุ่ม** อย่างปลอดภัย โดยป้องกันไม่ให้พลาดจนระบบใช้ sudo ไม่ได้

```
Jirapat@UbuntuDesktop:~$ sudo visudo
```

```
# Developers - full sudo access
%sudo-developers ALL=(ALL:ALL) ALL

# Limited sudo - specific commands only
%sudo-limited ALL=(ALL) /usr/bin/systemctl status *, /usr/bin/tail /var/log/*, /bin/ps

# Database admin - database commands only
First ALL=(ALL) /usr/bin/mysql, /usr/bin/mysqldump, /bin/systemctl restart mysql

# Sudo session timeout (15 minutes)
Defaults timestamp_timeout=15

# Log sudo commands
Defaults logfile="/var/log/sudo.log"
Defaults log_input, log_output
```

Fifa1 → อยู่ในกลุ่ม sudo-developers ทำ ทุกคำสั่ง ได้เหมือน root

Fifa2 → อยู่ในกลุ่ม sudo-developers ทำ ทุกคำสั่ง ได้เหมือน root

Boss → อยู่ในกลุ่ม sudo-limited ได้เฉพาะคำสั่งที่กำหนดเท่านั้น เช่น

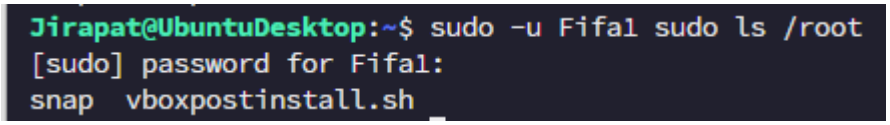
- systemctl status * (ดูสถานะ service)
- tail /var/log/* (ดู log)
- ps (ดู process)

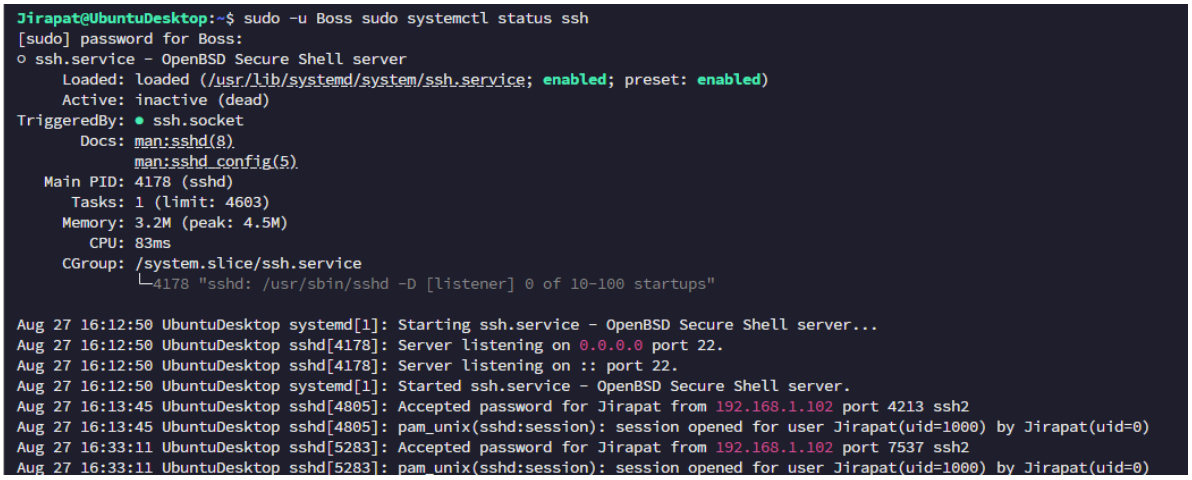
First ใช้ sudo ได้เฉพาะคำสั่งเกี่ยวกับ MySQL เช่น

- mysql
- mysqldump
- systemctl restart mysql

2.3 ทดสอบ Sudo Permissions:

User **Fifal** มีอยู่จริง อยู่ในกลุ่ม **sudo** (ใช้สิทธิ์ root ได้)





สั่งให้ตรวจสอบ **SSH service** โดยใช้ user **Boss**

Service `ssh` ถูกติดตั้งและ enable ไว้ แต่ สถานะปัจจุบันคือ inactive (dead) → หมายความว่า service หยุดอยู่ในตอนนี้

จาก log: เคยมีการเชื่อมต่อ SSH สำเร็จ (login accepted) จาก IP `1XX.168.1.XXX` โดย user `Jirapat`

```
Jirapat@UbuntuDesktop:~$ sudo -u Boss sudo apt update
[sudo] password for Boss:
Sorry, user Boss is not allowed to execute '/usr/bin/apt update' as root on UbuntuDesktop.
```

ผู้ใช้ **Boss** *ไม่มีสิทธิ์ใช้คำสั่ง `apt update` ผ่าน sudo* (ถูกปฏิเสธโดยการตั้งค่าใน **/etc/sudoers**)

Task 3: SSH Security

3.1 Backup และแก้ไข SSH Config

```
Jirapat@UbuntuDesktop:~$ sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.backup
```

คัดลอกไฟล์คอนฟิก SSH (`sshd_config`) ไปเก็บเป็นไฟล์สำรองชื่อ `sshd_config.backup` ในไดเรกทอรีเดียวกัน (`/etc/ssh/`)

```
Fifa1@UbuntuDesktop:~$ sudo nano /etc/ssh/sshd_config
[sudo] password for Fifa1:
```

เปิดไฟล์ **`/etc/ssh/sshd_config`** เพื่อตั้งค่า SSH Server โดยต้องใช้สิทธิ์ผู้ดูแลระบบ และหลังแก้ไขต้อง restart service เพื่อให้การเปลี่ยนแปลงมีผล

เป็นการกำหนด port

```
Port 2222
```

ห้าม root login โดยตรงทาง SSH

```
PermitRootLogin no
```

ปิดให้ใช้ password login ได้

```
PasswordAuthentication yes
```

เปิดใช้งาน **SSH Key-based login**

```
PubkeyAuthentication yes
```

จำกัดการพยายามใส่รหัสสูงสุด 3 ครั้งต่อการเชื่อมต่อ

```
MaxAuthTries 3
```

ถ้า idle 300 วินาที (5 นาที) sshd จะส่ง keep-alive packet ไปถาม client
ถ้า client ไม่ตอบ 2 ครั้งติดต่อกัน → ตัดการเชื่อมต่อ (รวมเวลา ~10 นาที)

```
ClientAliveInterval 300
ClientAliveCountMax 2
```

จำกัดสิทธิ์ login ผ่าน SSH เฉพาะ user ที่ระบุไว้เท่านั้นที่จะเข้าได้

```
AllowUsers Fifa1 Fifa2 Boss First
```

บังคับใช้เฉพาะ **SSH Protocol 2**

```
Protocol 2
```

3.2 สร้าง SSH Keys:

การสร้าง **SSH Key Pair** สำหรับ user `Fifa`

```
Jirapat@UbuntuDesktop:~$ sudo -u Fifa1 ssh-keygen -t rsa -b 4096 -C "Fifa1@company.com"
Generating public/private rsa key pair.
Enter file in which to save the key (/home/Fifa1/.ssh/id_rsa):
Created directory '/home/Fifa1/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/Fifa1/.ssh/id_rsa
Your public key has been saved in /home/Fifa1/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:xCk8Gt3bYuTPfZn8hUOsF1kedIsAKzq/zb0sDjdyJ8Y Fifa1@company.com
The key's randomart image is:
+---[RSA 4096]----+
|         ...   ..|
|     o o .. . o o|
|    . =.*.   . o.|
|     o.*.o   . +.|
|    .o  S .   = .|
|      o..+ . + = |
|       + Eo.o O .|
|        X.*  o o.|
|       ..+.+.   .|
+----[SHA256]-----+
```

คัดลอก Public Key ไปที่ `authorized_keys`
ตอนนี้ user **Fifal** สามารถ login เข้าเครื่องผ่าน SSH โดยใช้ private key (`id_rsa`) ที่สร้างไว้ ไม่จำเป็นต้องใส่ password อีกต่อไป

```
Jirapat@UbuntuDesktop:~$ sudo -u Fifa1 cp /home/Fifa1/.ssh/id_rsa.pub /home/Fifa1/.ssh/authorized_keys
Jirapat@UbuntuDesktop:~$
Jirapat@UbuntuDesktop:~$ sudo -u Fifa1 chmod 600 /home/Fifa1/.ssh/authorized_keys
```

3.3 Configure SSH Banner:

เข้าไปแก้ไขที่ ssh_banner.txt

```
Jirapat@UbuntuDesktop:~$ sudo nano /etc/ssh/ssh_banner.txt
```

ข้อความแจ้งเตือน (SSH Login Banner) ที่จะแสดงทุกครั้งเมื่อผู้ใช้เชื่อมต่อเข้าเซิร์ฟเวอร์ผ่าน SSH ครับ

```
**********************************************
WARNING: Authorized access only!
All connections are monitored and recorded.
Disconnect immediately if you are not an
authorized user.
**********************************************
```

เพิ่มใน `sshd_config`

```
Banner /etc/ssh/ssh_banner.txt
```

3.4 Restart SSH และทดสอบ:

ทดสอบ config ssh โดยกำหนด port เป็น 2222 และใช้ user login เป็น fifa1 บนเครื่องตนเอง

```
Jirapat@UbuntuDesktop:~$ ssh -p 2222 Fifa1@localhost
The authenticity of host '[localhost]:2222 ([::1]:2222)' can't be established.
ED25519 key fingerprint is SHA256:Z76TuS+1hTgx2/8v/VeanZlO43zSGmoyTRyriyQUawU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[localhost]:2222' (ED25519) to the list of known hosts.
****************************************
WARNING: Authorized access only!
All connections are monitored and recorded.
Disconnect immediately if you are not an
authorized user.
****************************************


Fifa1@localhost's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-29-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.
```

Task 4: Firewall Rules (UFW)

4.1 Configure UFW:

```
Fifa1@UbuntuDesktop:~$ sudo ufw --force reset
[sudo] password for Fifa1:
Sorry, try again.
[sudo] password for Fifa1:
Backing up 'user.rules' to '/etc/ufw/user.rules.20250827_173101'
Backing up 'before.rules' to '/etc/ufw/before.rules.20250827_173101'
Backing up 'after.rules' to '/etc/ufw/after.rules.20250827_173101'
Backing up 'user6.rules' to '/etc/ufw/user6.rules.20250827_173101'
Backing up 'before6.rules' to '/etc/ufw/before6.rules.20250827_173101'
Backing up 'after6.rules' to '/etc/ufw/after6.rules.20250827_173101'
```

รีเซ็ต UFW Firewall กลับค่าเริ่มต้น โดย **สำรองกฎเก่าเก็บไว้ก่อน** เผื่อจะกู้คืนในอนาคต

```
Fifa1@UbuntuDesktop:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
Fifa1@UbuntuDesktop:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
Fifa1@UbuntuDesktop:~$ sudo ufw allow 2222/tcp
Rules updated
Rules updated (v6)
```

บล็อกทุกการเชื่อมต่อขาเข้า ยกเว้นพอร์ต 2222 และยัง เชื่อมต่อออกอินเทอร์เน็ตได้ปกติ

```
Fifa1@UbuntuDesktop:~$ sudo ufw allow 80/tcp
Rules updated
Rules updated (v6)
Fifa1@UbuntuDesktop:~$ sudo ufw allow 443/tcp
Rules updated
Rules updated (v6)
```

firewall **อนุญาตการเข้าเว็บปกติ (HTTP) และเว็บเข้ารหัส (HTTPS)** เรียบร้อยแล้ว → เครื่องพร้อมทำงานเป็นเว็บเซิร์ฟเวอร์ได้

```
Fifa1@UbuntuDesktop:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)?y
Traceback (most recent call last):
  File "/usr/sbin/ufw", line 138, in <module>
    not ui.continue_under_ssh():
        ^^^^^^^^^^^^^^^^^^^^^^^
  File "/usr/lib/python3/dist-packages/ufw/frontend.py", line 916, in continue_under_ssh
    ans = sys.stdin.readline().lower().strip()
          ^^^^^^^^^^^^^^^^^^^^
  File "<frozen codecs>", line 322, in decode
UnicodeDecodeError: 'utf-8' codec can't decode bytes in position 0-1: invalid continuation byte
```

firewall ยังไม่เปิดเพราะติด error encoding แก้คือใช้ `--force` หรือแก้ locale ให้รองรับ UTF-8 แล้วลองใหม่ครับ

```
Fifa1@UbuntuDesktop:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
2222/tcp                   LIMIT IN    Anywhere
80/tcp                     ALLOW IN    Anywhere
443/tcp                    ALLOW IN    Anywhere
3306                       ALLOW IN    192.168.1.0/24
2222/tcp (v6)              LIMIT IN    Anywhere (v6)
80/tcp (v6)                ALLOW IN    Anywhere (v6)
443/tcp (v6)               ALLOW IN    Anywhere (v6)
```

ต้องเปิด เปิดใช้งาน firewalld ก่อนถึงจะเช็ด status ได้

sudo ufw enable

4.2 Advanced UFW Rules:

```
Fifa1@UbuntuDesktop:~$ sudo ufw limit 2222/tcp
Rules updated
Rules updated (v6)
```

ตอนนี้ SSH ที่รันบนพอร์ต **2222/tcp** จะถูก **rate-limited**

ถ้า IP ไหนพยายาม login ผิดรัว ๆ → จะถูกบล็อกอัตโนมัติ

```
Fifa1@UbuntuDesktop:~$ sudo ufw allow from 192.168.1.0/24 to any port 3306
Rules updated
```

เครื่องที่อยู่ใน LAN เดียวกัน (192.168.1.x) จะสามารถเชื่อมต่อ MySQL บนเครื่องนี้ได้

เครื่องที่อยู่นอก LAN (เช่น อินเทอร์เน็ตภายนอก) → จะถูกบล็อก, ไม่สามารถเข้าถึงพอร์ต 3306 ได้

```
Fifa1@UbuntuDesktop:~$ sudo ufw logging on
Logging enabled
```

ตอนนี้ UFW เปิดโหมด **logging สามารถตรวจสอบการเชื่อมต่อที่ถูกอนุญาตหรือบล็อกได้จาก `/var/log/ufw.log`**

```
Fifa1@UbuntuDesktop:~$ sudo ufw status numbered
Status: inactive
```

Task 5: Monitoring & Fail2Ban

5.1 Install Monitoring Tools:

```
Fifa1@UbuntuDesktop:~$ sudo apt update
Hit:1 http://th.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://th.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://th.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:5 http://th.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [175 kB]
Get:6 http://th.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Get:7 http://th.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [377 kB]
Get:8 http://th.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]
Get:9 http://th.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [7,076 B]
Get:10 http://th.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [212 B]
Get:11 http://th.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [19.2 kB]
Get:12 http://th.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Get:13 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [21.6 kB]
Get:14 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Get:15 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [52.3 kB]
Get:16 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [212 B]
Fetched 1,032 kB in 2s (576 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
21 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

```
Fifa1@UbuntuDesktop:~$ sudo apt install fail2ban logwatch sysstat htop iotop
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
sysstat is already the newest version (12.6.1-2).
sysstat set to manually installed.
The following additional packages will be installed:
  libdate-manip-perl libnsl2 postfix python3-pyasyncore python3-pyinotify python3-setuptools whois
Suggested packages:
  mailx monit sqlite3 lm-sensors libsys-cpu-perl libsys-meminfo-perl mail-reader postfix-cdb postfix-doc postfix-ldap postfix-lmdb
  postfix-mta-sts-resolver postfix-mysql postfix-pcre postfix-pgsql postfix-sqlite procmail sasl2-bin | dovecot-common python-pyinotify-doc
  python-setuptools-doc
The following NEW packages will be installed:
  fail2ban htop iotop libdate-manip-perl libnsl2 logwatch postfix python3-pyasyncore python3-pyinotify python3-setuptools whois
0 upgraded, 11 newly installed, 0 to remove and 21 not upgraded.
Need to get 3,693 kB of archives.
After this operation, 23.9 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://th.archive.ubuntu.com/ubuntu noble/main amd64 libnsl2 amd64 1.3.0-3build3 [41.4 kB]
Get:2 http://th.archive.ubuntu.com/ubuntu noble/main amd64 postfix amd64 3.8.6-1build2 [1,254 kB]
Get:3 http://th.archive.ubuntu.com/ubuntu noble-updates/main amd64 python3-setuptools all 68.1.2-2ubuntu1.2 [397 kB]
Get:4 http://th.archive.ubuntu.com/ubuntu noble/main amd64 python3-pyasyncore all 1.0.2-2 [10.1 kB]
Get:5 http://th.archive.ubuntu.com/ubuntu noble-updates/universe amd64 fail2ban all 1.0.2-3ubuntu0.1 [409 kB]
Get:6 http://th.archive.ubuntu.com/ubuntu noble/main amd64 htop amd64 3.3.0-4build1 [171 kB]
Get:7 http://th.archive.ubuntu.com/ubuntu noble/main amd64 iotop amd64 0.6-42-ga14256a-0.2build1 [24.4 kB]
Get:8 http://th.archive.ubuntu.com/ubuntu noble/main amd64 libdate-manip-perl all 6.95-1 [923 kB]
Get:9 http://th.archive.ubuntu.com/ubuntu noble/main amd64 logwatch all 7.7-1ubuntu1 [388 kB]
Get:10 http://th.archive.ubuntu.com/ubuntu noble/main amd64 python3-pyinotify all 0.9.6-2ubuntu1 [25.0 kB]
Get:11 http://th.archive.ubuntu.com/ubuntu noble/main amd64 whois amd64 5.5.22 [51.7 kB]
Fetched 3,693 kB in 2s (2,204 kB/s)
Preconfiguring packages ...
```

ชุดเครื่องมือสำหรับความปลอดภัยและการมอนิเตอร์ระบบ ได้แก่

- ป้องกันการโจมตี (`fail2ban`)
- วิเคราะห์ log (`logwatch`)
- เก็บ performance metrics (`sysstat`)

- จัดการ process (`htop`)
- ตรวจสอบ domain (`whois`)

```
Fifa1@UbuntuDesktop:~$ sudo apt install elasticsearch logstash kibana -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  elasticsearch kibana logstash
0 upgraded, 3 newly installed, 0 to remove and 21 not upgraded.
Need to get 1,477 MB of archives.
After this operation, 3,124 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 elasticsearch amd64 8.19.2 [655 MB]
Get:2 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 kibana amd64 8.19.2 [383 MB]
Get:3 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 logstash amd64 1:8.19.2-1 [439 MB]
Fetched 1,477 MB in 10min 48s (2,279 kB/s)
Selecting previously unselected package elasticsearch.
(Reading database ... 155204 files and directories currently installed.)
Preparing to unpack .../elasticsearch_8.19.2_amd64.deb ...
Creating elasticsearch group... OK
Creating elasticsearch user... OK
Unpacking elasticsearch (8.19.2) ...
Selecting previously unselected package kibana.
```

ติดตั้ง **ELK Stack (Elasticsearch + Logstash + Kibana)** เรียบร้อยแล้ว

- **Elasticsearch** → เก็บและค้นหาข้อมูล
- **Logstash** → นำเข้าข้อมูลและประมวลผล
- **Kibana** → แสดงผลข้อมูลแบบ dashboard

5.2 Configure Fail2Ban:

```
Fifa1@UbuntuDesktop:~$ sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.conf.backup
```

backup ไฟล์ตั้งค่า Fail2ban (`jail.conf`) เรียบร้อยแล้ว เพื่อเตรียมแก้ไข config โดยไม่เสี่ยงเสียไฟล์ต้นฉบับ

```
Fifa1@UbuntuDesktop:~$ sudo nano /etc/fail2ban/jail.local
```

เปิด `jail.local` คือการเข้าไปแก้ไข **ไฟล์คอนฟิกที่แนะนำสำหรับ Fail2ban** ใช้เพื่อกำหนดกฎการป้องกัน brute-force (เช่น SSH login fail) โดยไม่ไปแตะไฟล์หลัก `jail.conf`

```
  GNU nano 7.2
# เนื้อหาไฟล์:
[DEFAULT]
bantime = 3600
findtime = 600
maxretry = 3
backend = systemd

[sshd]
enabled = true
port = 2222
logpath = /var/log/auth.log
maxretry = 3
bantime = 3600

[apache-auth]
enabled = true
port = http,https
logpath = /var/log/apache2/error.log

[apache-badbots]
enabled = true
port = http,https
logpath = /var/log/apache2/access.log
bantime = 86400
maxretry = 1
```

บล็อก SSH brute force (port 2222)

ป้องกันการเดา password ใน Apache

แบน bad bots ที่ยิงเว็บ

5.3 Configure System Monitoring:

```
Fifa1@UbuntuDesktop:~$ sudo systemctl enable sysstat
Synchronizing state of sysstat.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable sysstat
Fifa1@UbuntuDesktop:~$ sudo systemctl start sysstat
```

เปิดใช้งาน sysstat ให้เริ่มอัตโนมัติเมื่อบูต และ สั่ง start ทันที และระบบสามารถเก็บ performance log และสามารถใช้เครื่องมือใน sysstat เพื่อตรวจสอบการทำงานของเครื่องได้

```
Fifa1@UbuntuDesktop:~$ sudo nano /usr/local/bin/system_monitor.sh
```

เปิดไฟล์สคริปต์ที่ชื่อ `system_monitor.sh` ใน `/usr/local/bin/` เพื่อสร้าง/แก้ไขสคริปต์ที่สามารถเรียกใช้งานได้จากทุกที่ในระบบ

```
  GNU nano 7.2                                                /usr/local/bin/system_
#!/bin/bash
# System monitoring script
DATE=$(date)
echo "=== System Monitor Report - $DATE ===" >> /var/log/system_monitor.log

# CPU Usage
echo "CPU Usage:" >> /var/log/system_monitor.log
top -bn1 | grep "Cpu(s)" >> /var/log/system_monitor.log

# Memory Usage
echo "Memory Usage:" >> /var/log/system_monitor.log
free -h >> /var/log/system_monitor.log

# Disk Usage
echo "Disk Usage:" >> /var/log/system_monitor.log
df -h >> /var/log/system_monitor.log

# Active Users
echo "Active Users:" >> /var/log/system_monitor.log
who >> /var/log/system_monitor.log

# Failed Login Attempts
echo "Recent Failed Logins:" >> /var/log/system_monitor.log
tail -10 /var/log/auth.log | grep "Failed password" >> /var/log/system_monitor.log

echo "==================================" >> /var/log/system_monitor.log
```

สคริปต์นี้จะเก็บข้อมูล system monitoring ลงไฟล์ log เดียว (`/var/log/system_monitor.log`) โดยบันทึก:

- CPU, Memory, Disk usage
- Active users ที่กำลังใช้งาน
- ความพยายาม login ผิดล่าสุด

```
Fifa1@UbuntuDesktop:~$ sudo chmod +x /usr/local/bin/system_monitor.sh
```

ทำให้ `system_monitor.sh` กลายเป็น สคริปต์รันได้ (เหมือนคำสั่ง Linux อื่น ๆ) โดยไม่ต้องใช้ `bash` หรือ `sh` นำหน้าแล้ว

```
Fifa1@UbuntuDesktop:~$ sudo crontab -e
no crontab for root - using an empty one

Select an editor.  To change later, run 'select-editor'.
  1. /bin/nano        <---- easiest
  2. /usr/bin/vim.tiny
  3. /bin/ed

Choose 1-3 [1]: 1
Choose 1-3 [1]: 1
crontab: installing new crontab
```

คือการเปิด **crontab ของ root** เพื่อเพิ่มงานที่ต้องรันอัตโนมัติบน Linux

```
0 * * * * /usr/local/bin/system_monitor.sh
```

5.4 Configure Log Rotation:

```
Fifa1@UbuntuDesktop:~$ sudo nano /etc/logrotate.d/system_monitor
```

เข้าไปสร้าง config ของ **logrotate** สำหรับสคริปต์ `system_monitor.sh` เพื่อไม่ให้ไฟล์ log โตจนเต็มดิสก์

```
 GNU nano 7.2
/var/log/system_monitor.log {
    daily
    missingok
    rotate 30
    compress
    delaycompress
    notifempty
    copytruncate
}
```

ไฟล์นี้ตั้งค่าให้ log ของ `/var/log/system_monitor.log`

- rotate ทุกวัน
- เก็บย้อนหลัง 30 วัน
- บีบอัดไฟล์เก่าเพื่อลดพื้นที่
- ไม่ทำงานถ้าไฟล์ว่าง
- ตัดไฟล์เดิมเป็นศูนย์เพื่อให้ script เขียนต่อได้

2.Security Checklist

รายการ	ก่อนทำ	หลังทำ
User Accounts	มี root user เท่านั้น	สร้าง users แบ่งกลุ่มชัดเจน
Password Policy	ไม่มี enforce	มี enforce minlen, complexity
Sudo Control	ทุก user ใช้ sudo ได้หมด	จำกัดสิทธิ์ตาม role
SSH Config	root login ได้, ใช้ password	เปลี่ยน SSH port → 2222, ปิด root login, จำกัดให้เฉพาะ users: Fifa1, Fifa2, Boss, First เท่านั้น
Firewall	ไม่ได้เปิดใช้	Deny all
Monitoring	ไม่มี	ติดตั้ง fail2ban, logwatch, sysstat

3.สรุปปัญหาที่พบและข้อเสนอแนะเพิ่มเติม

ปัญหา 1: การตั้งค่า Password Policy

สาเหตุ: ในไฟล์ /etc/pam.d/common-password พบว่ามีการเพิ่มบรรทัด

```
password        requisite                       pam_pwquality.so retry=3 minlen=12 difok=3 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1
password        [success=2 default=ignore]      pam_unix.so obscure use_authtok try_first_pass yescrypt
password        sufficient                      pam_sss.so use_authtok
```

ปัญหา 2: เปลี่ยนรหัสผ่านผู้ใช้ไม่ได้

```
Jirapat@UbuntuDesktop:~$ sudo passwd Fifa1
passwd: Authentication token manipulation error
passwd: password unchanged
```

วิธีแก้

ห้ามมีคำสั่งนี้ซ้ำกัน

`password requisite pam_pwquality.so retry=3 minlen=12 difok=3 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1`

ปัญหา 3: เช็ค port ว่า เป็น 2222

sudo systemctl edit ssh.socket (check)

```
Jirapat@UbuntuDesktop:~$ sudo ss -ltnp | grep sshd
LISTEN 0      128          0.0.0.0:2222      0.0.0.0:*    users:(("sshd",pid=651
4,fd=3))
LISTEN 0      4096         0.0.0.0:22        0.0.0.0:*    users:(("sshd",pid=417
8,fd=3))
LISTEN 0      128             [::]:2222         [::]:*    users:(("sshd",pid=651
4,fd=4))
LISTEN 0      4096            [::]:22           [::]:*    users:(("sshd",pid=417
8,fd=4))
```

sudo systemctl daemon-reload
sudo systemctl restart ssh.socket

ถึงจะเข้าได้

```
Jirapat@UbuntuDesktop:~$ ssh -p 2222 Fifa1@localhost
The authenticity of host '[localhost]:2222 ([::1]:2222)' can't be established.
ED25519 key fingerprint is SHA256:Z76TuS+1hTgx2/8v/VeanZlO43zSGmoyTRyriyQUawU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[localhost]:2222' (ED25519) to the list of known hosts.
**************************************
WARNING: Authorized access only!
All connections are monitored and recorded.
Disconnect immediately if you are not an
authorized user.
**************************************


Fifa1@localhost's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-29-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.
```

ปัญหา 4: เมื่อ ใช้คำสั่ง sudo apt install elasticsearch logstash kibana

สาเหตุ: Ubuntu/Debian ยังไม่มี repo ของ Elastic โดยตรง ทำให้ต้องติดตั้ง prerequisites และเพิ่ม repo ก่อน

sudo apt install elasticsearch logstash kibana ต้องติดตั้ง prerequisites

sudo apt update

sudo apt install apt-transport-https curl gnupg -y

เพิ่ม Elasticsearch GPG key

curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg

เพิ่ม Elasticsearch APT repository
echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list

อัปเดต repo
sudo apt update

ถึงจะติดตั้งได้
sudo apt install elasticsearch logstash kibana -y