Presentation Outline

Task 1: สร้าง User Accounts สำหรับ Team

```
# สร้าง user
sudo adduser alice
sudo adduser bob
sudo adduser Charlie
sudo adduser david
# เพิ่ม alice เข้า group sudo
sudo usermod -aG sudo alice
# สร้าง group ชื่อ developers
sudo groupadd developers
# เพิ่ม bob และ charlie เข้า group developers
sudo usermod -aG developers bob
sudo usermod -aG developers charlie
```

cat /etc/passwd | tail -4

```
jr@linuxeieiza:~$ cat /etc/passwd | tail -4
alice:x:1001:1004::/home/alice:/bin/bash
bob:x:1002:1005::/home/bob:/bin/bash
charlie:x:1003:1006::/home/charlie:/bin/bash
david:x:1004:1007::/home/david:/bin/bash
```

groups alice bob charlie david

```
jr@linuxeieiza:~$ groups alice bob charlie david
alice : alice developers
bob : bob developers
charlie : charlie testers
david : david dbadmin
```

การทดสอบ Password Policy

```
jr@linuxeieiza:~$ sudo passwd alice
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password fails the dictionary check - it is too simplistic/systematic
Retype new password:
BAD PASSWORD: The password contains less than 1 digits
passwd: password updated successfully
```

Task 2: ตั้งค่า Sudo Permissions

ติดตั้ง pwquality (ตรวจความซับซ้อนรหัสผ่าน)

sudo apt update

sudo apt install libpam-pwquality -y

PASS_MAX_DAYS 90 # อายุสูงสุด 90 วัน

PASS_MIN_DAYS 1 # เวลาขั้นต่ำก่อนเปลี่ยนใหม่ได้

PASS_WARN_AGE 14 # เตือนก่อนหมดอายุ 14 วัน

add groups/users || /etc/sudoers

```
jr@linuxeieiza:~$ sudo groupadd sudo-developers
jr@linuxeieiza:~$ sudo groupadd sudo-limited
jr@linuxeieiza:~$ sudo usermod -aG sudo-developers alice
jr@linuxeieiza:~$ sudo usermod -aG sudo-developers bob
jr@linuxeieiza:~$ sudo usermod -aG sudo-limited charlie
```

ผลการทดสอบ sudo permissions

```
jr@linuxeieiza:~$ sudo -u alice sudo ls /root
[sudo] password for alice:
vboxpostinstall.sh
```

Log file /var/log/sudo.log

```
jr@linuxeieiza:~$ sudo tail -n 20 /var/log/sudo.log
Aug 27 17:43:53 : jr : TTY=pts/0 ; PWD=/home/jr ; USER=alice ; TSID=000001 ;
    COMMAND=/usr/bin/sudo ls /root
Aug 27 17:43:53 : alice : TTY=pts/1 ; PWD=/home/jr ; USER=root ; TSID=000002 ;
    COMMAND=/usr/bin/ls /root
Aug 27 17:44:08 : jr : TTY=pts/0 ; PWD=/home/jr ; USER=charlie ; TSID=000003 ;
    COMMAND=/usr/bin/sudo systemctl status ssh
Aug 27 17:44:08 : charlie : TTY=pts/1 ; PWD=/home/jr ; USER=root ; TSID=000004 ;
    COMMAND=/usr/bin/systemctl status ssh
Aug 27 17:44:19 : jr : TTY=pts/0 ; PWD=/home/jr ; USER=charlie ; TSID=000005 ;
    COMMAND=/usr/bin/sudo apt update
Aug 27 17:44:19 : charlie : command not allowed ; TTY=pts/1 ; PWD=/home/jr ;
    USER=root ; COMMAND=/usr/bin/apt update
Aug 27 17:44:37 : jr : TTY=pts/0 ; PWD=/home/jr ; USER=root ; TSID=000006 ;
    COMMAND=/usr/bin/tail -n 20 /var/log/sudo.log
Aug 27 17:48:23 : jr : TTY=pts/0 ; PWD=/home/jr ; USER=alice ; TSID=000007 ;
    COMMAND=/usr/bin/sudo ls /root
Aug 27 17:48:24 : alice : TTY=pts/1 ; PWD=/home/jr ; USER=root ; TSID=000008 ;
    COMMAND=/usr/bin/ls /root
Aug 27 17:49:04 : jr : TTY=pts/0 ; PWD=/home/jr ; USER=root ; TSID=000009 ;
    COMMAND=/usr/bin/tail -n 20 /var/log/sudo.log
```

Task 3: Configure SSH Security

sudo apt update

sudo apt install openssh-server -y

sudo systemctl status ssh --no-pager

ss -tuln | grep ssh

sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.backup

sudo systemctl status ssh --no-pager

ss -tuln | grep ssh

sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.backup

ไฟล์ /etc/ssh/sshd_config

```
Port 2222
PermitRootLogin no
PasswordAuthentication yes
PubkeyAuthentication yes
MaxAuthTries 3
ClientAliveInterval 300
ClientAliveCountMax 2
AllowUsers alice bob charlie david
Protocol 2
Banner /etc/ssh/ssh_banner.txt
```

Gen private key

```
jr@linuxeieiza:~$ sudo -u alice ssh-keygen -t rsa -b 4096 -C "alice@linux.com"
Generating public/private rsa key pair.
Enter file in which to save the key (/home/alice/.ssh/id_rsa):
Created directory '/home/alice/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Passphrases do not match.  Try again.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/alice/.ssh/id_rsa
Your public key has been saved in /home/alice/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:fiN3cILhRumSOpa1PW6xVhDi7J1NZn6GRd8tFuVehF4 alice@linux.com
The key's randomart image is:
+---[RSA 4096]----+
|               oo|
|      . ..  . ooE|
|     o .+. . o ++|
|      o=.o+ . =.+|
|     .+.SOoo.. ..|
|     +.** =+o    |
|    = . =++o.    |
|   . . .+= o     |
|       o.        |
+----[SHA256]-----+
```

การทดสอบ SSH connection

```
jr@linuxeieiza:~$ sudo ss -tulnp | grep ssh
tcp   LISTEN 0      128                0.0.0.0:2222       0.0.0.0:*    users:(("sshd",pid=3864,fd=3))
tcp   LISTEN 0      128                   [::]:2222          [::]:*    users:(("sshd",pid=3864,fd=4))
```

SSH banner message

sudo nano /etc/issue.net

sudo nano /etc/ssh/sshd_config

Banner /etc/issue.net

sudo systemctl restart ssh

ssh alice@192.168.1.123-p 22

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

Task 4: Set up Firewall Rules

sudo ufw default deny incoming

sudo ufw default allow outgoing

อนุญาต SSH (พอร์ตใหม่ เช่น 2222)

sudo ufw allow 2222/tcp

อนุญาต HTTP, HTTPS

sudo ufw allow 80/tcp

sudo ufw allow 443/tcp

sudo ufw status verbose

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

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

sudo ufw status numbered

```
alice@linuxeieiza:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 2222/tcp                   LIMIT IN    Anywhere
[ 2] 80/tcp                     ALLOW IN    Anywhere
[ 3] 443/tcp                    ALLOW IN    Anywhere
[ 4] 3306                       ALLOW IN    192.168.1.0/24
[ 5] 2222/tcp (v6)              LIMIT IN    Anywhere (v6)
[ 6] 80/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 7] 443/tcp (v6)               ALLOW IN    Anywhere (v6)
```

ไฟล์ log ใน /var/log/ufw.log

```
alice@linuxeieiza:~$ sudo journalctl -u ufw --no-pager | tail -n 20
Aug 27 17:17:43 localhost.localdomain systemd[1]: Starting ufw.service - Uncomplicated firewall...
Aug 27 17:17:43 localhost.localdomain systemd[1]: Finished ufw.service - Uncomplicated firewall.
```

Task 5: Enable System Monitoring

sudo apt update

sudo apt install fail2ban logwatch sysstat htop iotop -y

sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.conf.backup

sudo nano /etc/fail2ban/jail.local

sudo systemctl restart fail2ban

sudo systemctl enable fail2ban

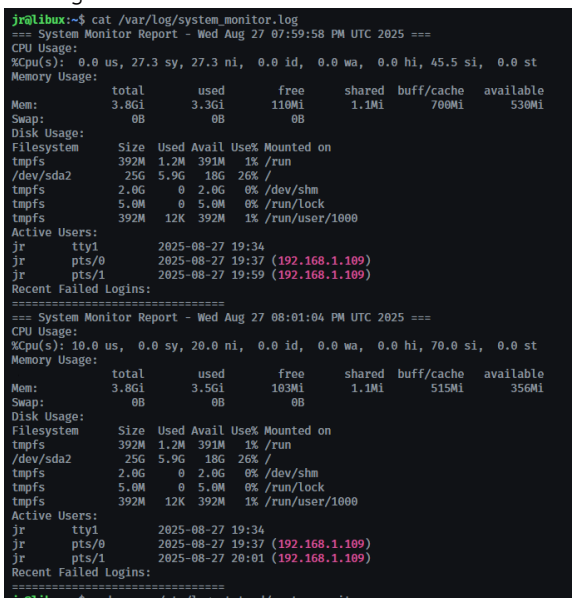
sudo fail2ban-client status

```
jr@libux:~$ sudo fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:   sshd
```

sudo fail2ban-client status sshd

```
jr@libux:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
```

ไฟล์ /var/log/system_monitor.log



```
jr@libux:~$ cat /var/log/system_monitor.log
=== System Monitor Report - Wed Aug 27 07:59:58 PM UTC 2025 ===
CPU Usage:
%Cpu(s):  0.0 us, 27.3 sy, 27.3 ni,  0.0 id,  0.0 wa,  0.0 hi, 45.5 si,  0.0 st
Memory Usage:
               total        used        free      shared  buff/cache   available
Mem:           3.8Gi       3.3Gi       110Mi       1.1Mi       700Mi       530Mi
Swap:             0B          0B          0B
Disk Usage:
Filesystem      Size  Used Avail Use% Mounted on
tmpfs           392M  1.2M  391M   1% /run
/dev/sda2        25G  5.9G   18G  26% /
tmpfs           2.0G     0  2.0G   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           392M   12K  392M   1% /run/user/1000
Active Users:
jr       tty1         2025-08-27 19:34
jr       pts/0        2025-08-27 19:37 (192.168.1.109)
jr       pts/1        2025-08-27 19:59 (192.168.1.109)
Recent Failed Logins:
================================
=== System Monitor Report - Wed Aug 27 08:01:04 PM UTC 2025 ===
CPU Usage:
%Cpu(s): 10.0 us,  0.0 sy, 20.0 ni,  0.0 id,  0.0 wa,  0.0 hi, 70.0 si,  0.0 st
Memory Usage:
               total        used        free      shared  buff/cache   available
Mem:           3.8Gi       3.5Gi       103Mi       1.1Mi       515Mi       356Mi
Swap:             0B          0B          0B
Disk Usage:
Filesystem      Size  Used Avail Use% Mounted on
tmpfs           392M  1.2M  391M   1% /run
/dev/sda2        25G  5.9G   18G  26% /
tmpfs           2.0G     0  2.0G   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           392M   12K  392M   1% /run/user/1000
Active Users:
jr       tty1         2025-08-27 19:34
jr       pts/0        2025-08-27 19:37 (192.168.1.109)
jr       pts/1        2025-08-27 20:01 (192.168.1.109)
Recent Failed Logins:
================================
```

sudo systemctl status fail2ban

```
jr@libux:~$ sudo systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
     Active: active (running) since Wed 2025-08-27 19:38:56 UTC; 23min ago
       Docs: man:fail2ban(1)
   Main PID: 2811 (fail2ban-server)
      Tasks: 5 (limit: 4606)
     Memory: 22.2M (peak: 24.9M)
        CPU: 5.134s
     CGroup: /system.slice/fail2ban.service
             └─2811 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Aug 27 19:38:56 libux systemd[1]: Started fail2ban.service - Fail2Ban Service.
Aug 27 19:38:56 libux fail2ban-server[2811]: 2025-08-27 19:38:56,734 fail2ban.configreader   [2811]: WARNING 'allowipv6' not defined in 'Definition'. Using default one: 'auto'
```