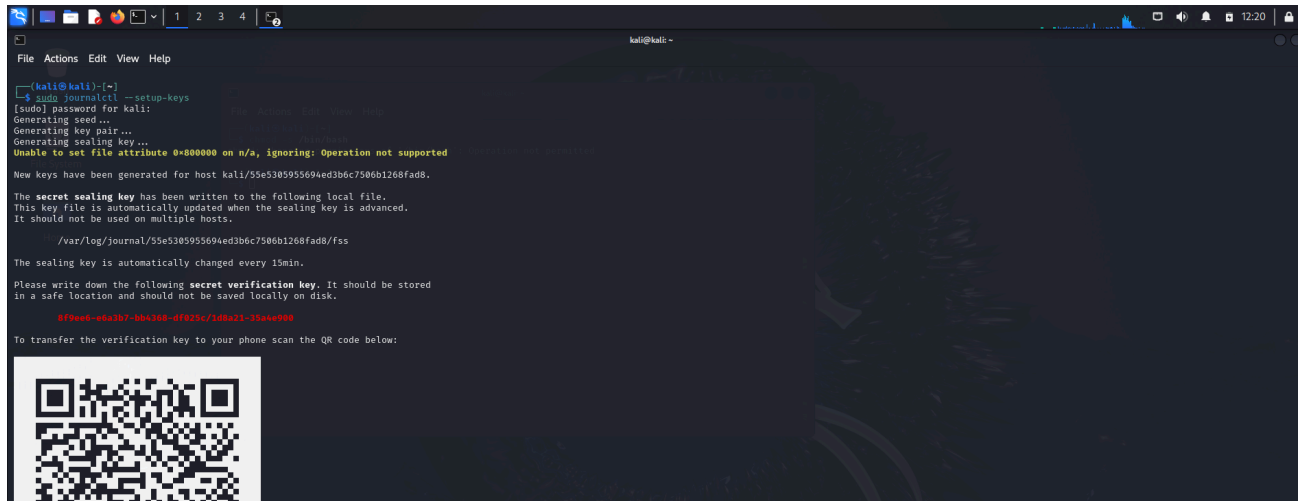


## PoC Task 6: Log Analysis & Intrusion Detection

### 1) Setup

#### 1.1) Enable system logging:

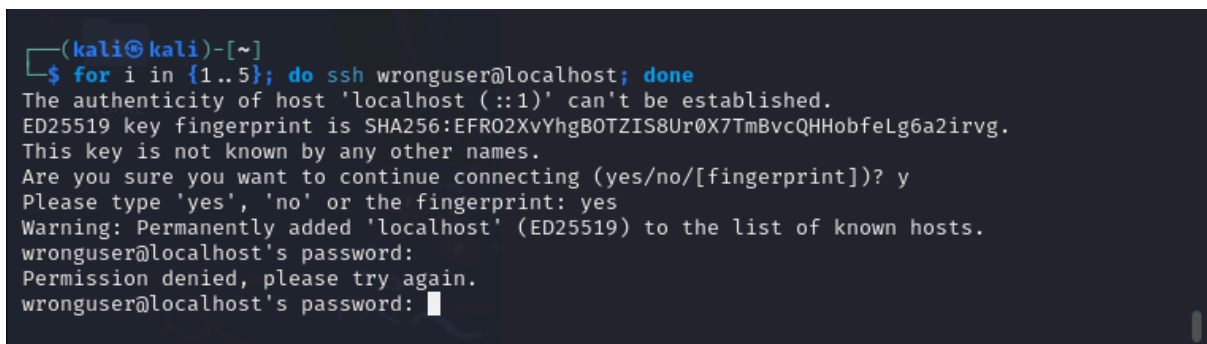
`sudo journalctl --setup-keys`



```
kali@kali:~$ sudo journalctl --setup-keys
[sudo] password for kali:
Generating seed...
Generating key pair...
Generating sealing key...
Unable to set file attribute 0x000000 on n/a, ignoring: Operation not supported
New keys have been generated for host kali/55e5305955694ed3b6c7506b1268fad8.
The secret sealing key has been written to the following local file.
This key file is automatically updated when the sealing key is advanced.
It should not be used on multiple hosts.
/var/log/journal/55e5305955694ed3b6c7506b1268fad8/fss
The sealing key is automatically changed every 15min.
Please write down the following secret verification key. It should be stored
in a safe location and should not be saved locally on disk.
8FPeed-mka3b7-bba308-df025c/1dka21-35aco908
To transfer the verification key to your phone scan the QR code below:
```

#### 1.2) Simulate failed SSH attempts:

`for i in {1..5}; do ssh wronguser@localhost; done`



```
(kali@kali)-[~]
$ for i in {1..5}; do ssh wronguser@localhost; done
The authenticity of host 'localhost (::1)' can't be established.
ED25519 key fingerprint is SHA256:EFRO2XvYhgBOTZIS8Ur0X7TmBvcQHobfeLg6a2irvg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.
wronguser@localhost's password:
Permission denied, please try again.
wronguser@localhost's password: 
```

### 2) Exploit

#### 2.1) Analyze logs:

`grep "Failed password" /var/log/auth.log`

### 3) Mitigation

#### 3.1) Implement fail2ban:

`sudo apt install fail2ban`

`sudo systemctl start fail2ban`

#### 3.2) Automate log monitoring:

`sudo apt install logwatch`

`sudo logwatch --detail High --mailto admin@example.com`