

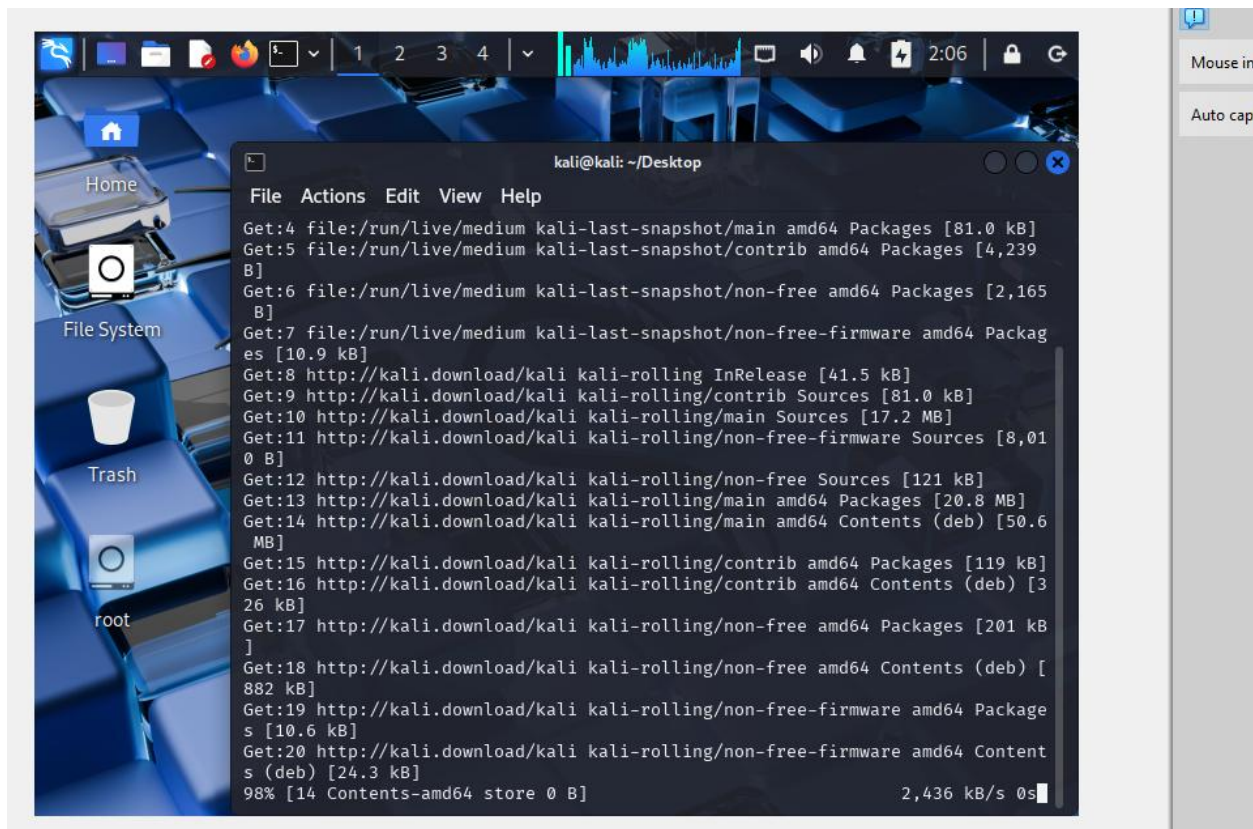
Group – 3

Step 4: Monitoring

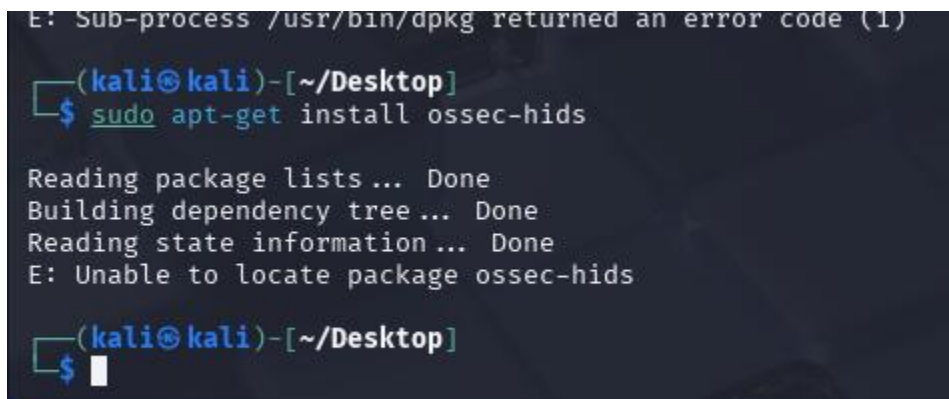
Monitoring stage

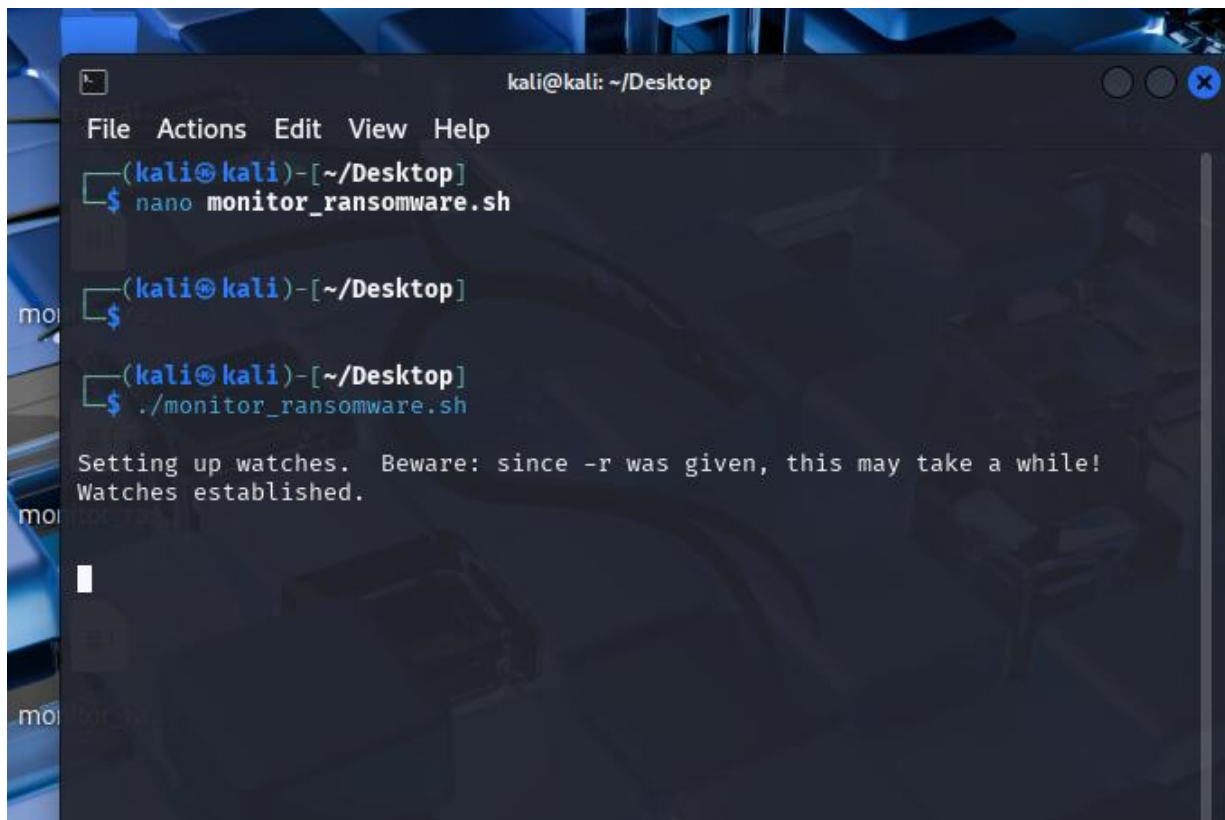
install OSSEC;

Update your system to make sure all packages are up-to-date



Install OSSEC;



A terminal window titled 'kali@kali: ~/Desktop' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(kali@kali)-[~/Desktop]'. The user enters '\$ nano monitor_ransomware.sh'. The prompt changes to '\$'. The user enters '\$./monitor_ransomware.sh'. The output is 'Setting up watches. Beware: since -r was given, this may take a while!' followed by 'Watches established.' and a blank line with a cursor.

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ nano monitor_ransomware.sh
(kali@kali)-[~/Desktop]
$
(kali@kali)-[~/Desktop]
$ ./monitor_ransomware.sh

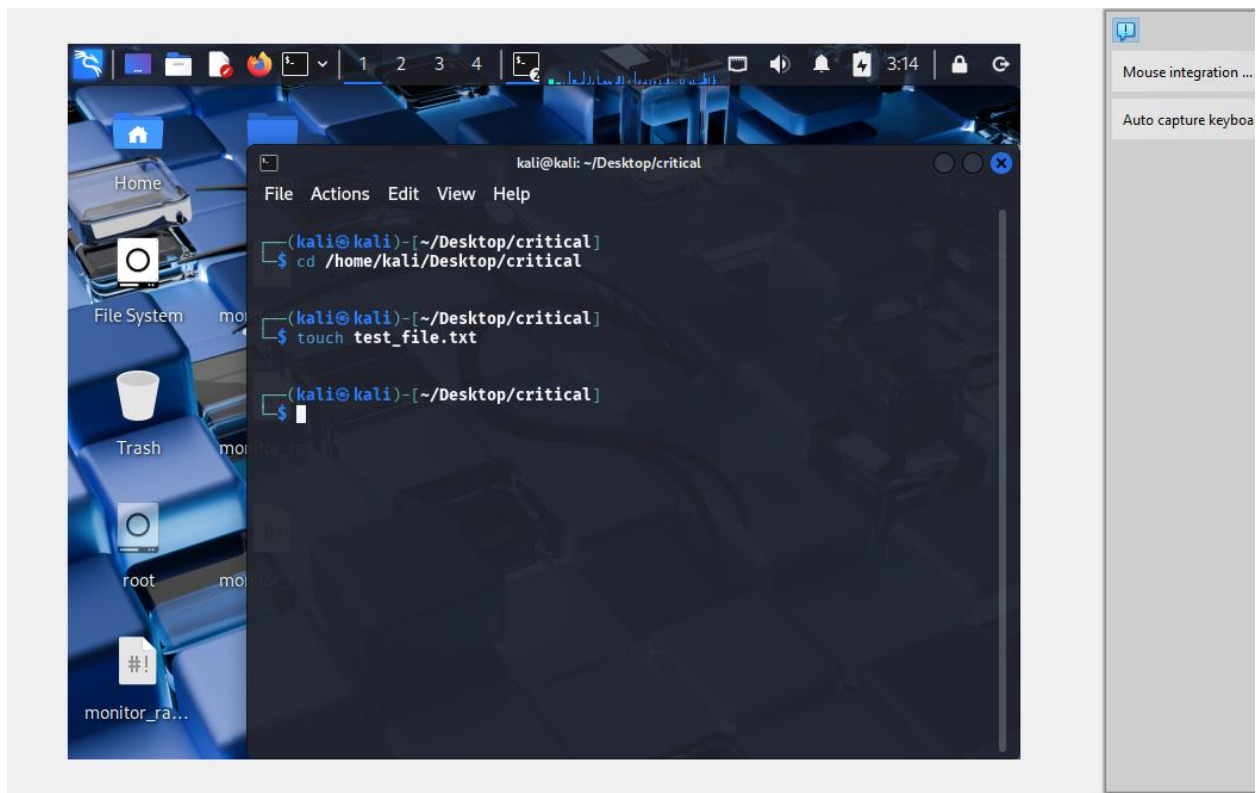
Setting up watches. Beware: since -r was given, this may take a while!
Watches established.

█
```

The script is running successfully now, and the **watches have been established** for the directory! This means the script is actively monitoring the **critical** directory for any file changes, like modifications, creations, or deletions.

Testing:

Try to change anything in the malicious pdf;



See the results in the main terminal;

elp

