# Incident Response Report
## Project: Ransomware Simulation using EICAR

## 1. Incident Description

In this project, I created a fake ransomware test using the EICAR file. The EICAR file is not a real virus, but antivirus s

To create the test file, I used this command:

```
echo "X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*" > eicar.txt
```

This created the test virus file in my system.

## 2. Detection

I used ClamAV antivirus to scan the system.

First, I updated the virus database:

```
sudo freshclam
```

Then I scanned the system:

```
clamscan -r /
```

ClamAV detected the EICAR file as a malicious file. This showed that the antivirus was working correctly.

## 3. Containment

After detection, I disconnected the system from the network to stop any possible spread.

I checked running processes using:

```
ps aux
```

If needed, I stopped a suspicious process using:

```
kill -9 process_id
```

This helped control the situation.

## 4. Eradication

After that, I removed the infected file using:

```
rm eicar.txt
```

This deleted the test virus from the system.

## 5. Recovery

Finally, I scanned the system again:

```
clamscan -r /
```

The system was clean and there was no data loss.

## Conclusion

This project helped me understand how to detect, control, and remove a ransomware attack in a safe lab environmen

Now I have better understanding of how incident response works in real life.