Malware Analysis Report

Aim

To study different types of malware and analyze a malware sample using **VirusTotal** in **Kali Linux**.

Tools Used

- Operating System: **Kali Linux**
- Tool: **VirusTotal**
- Analysis Type: **Static Analysis (Hash based)**

Malware Types Studied

- Virus
- Worm
- Trojan
- Ransomware

Malware is harmful software that damages the system or steals data.

Malware Sample Used

For safe analysis, **EICAR test malware hash** is used.
It is not real malware but used to test antivirus detection.

Hash Value:

```
MD5: 44d88612fea8a8f36de82e1278abb02f
```

Practical Steps Followed

1. Kali Linux terminal was opened
2. Firefox browser was opened using command:

   ```
   $ firefox https://www.virustotal.com
   ```

- .The EICAR MD5 hash was pasted in VirusTotal search
- Detection results were observed

Detection Report

- Detection Ratio: **Detected by many antivirus engines**
- Malware Name: **EICAR Test Malware**
- File Status: **Malicious (Test File)**

VirusTotal successfully detected the malware hash.

Behavior Analysis

From VirusTotal report:

- The file is identified as malware test file
- Antivirus engines flag it as malicious
- No real execution was done

Malware Lifecycle(CDEID)

1. Creation
2. Distribution
3. Execution
4. Infection
5. Damage

Malware Spread Methods

- Email attachments
- Internet downloads
- USB devices

Prevention Methods

- Use antivirus software
- Do not open unknown files
- Keep system updated
- Use firewall

Result

The given hash was successfully detected as malware using VirusTotal.

Conclusion

In this experiment, malware analysis was performed using **VirusTotal** in Kali Linux.
The EICAR test malware hash was detected by multiple antivirus engines.
This shows that VirusTotal is useful for identifying malware safely without executing it.