**Week 9: Implementation of IT Audit, malware analysis and Vulnerability assessment and generate the report.**

**Step1:**

**Collection Information about Malware:**

Collected malware file from

[www.github.com/rampriyakilari/ICS-Needs](http://www.github.com/rampriyakilari/ICS-Needs)

**Step2:**

**Basic Information about malware:**

Name: file.exe

Media Type: application/x-msdownload

SHA-256: d01d08621690c1a7a0f41bdd1bb02ec05d418ef68b06cd3cfd54fbb3f58ba80a

Report ID: 37cec6e6-0778-4c35-9cb3-d177c1e6e34a

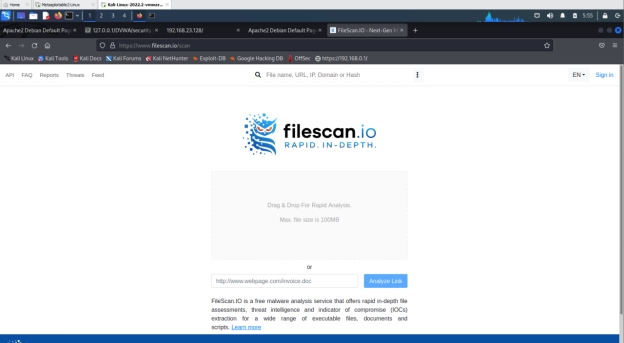
Submission ID: 62c24f59783441cda10213de

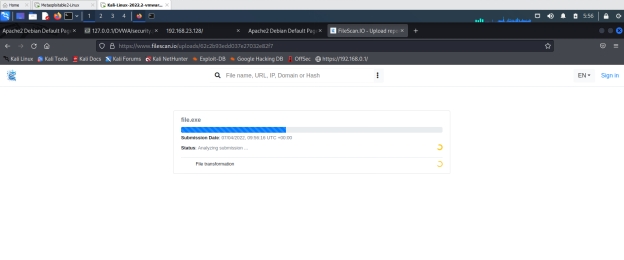
Submission Date: 07/04/2022, 02:24:27

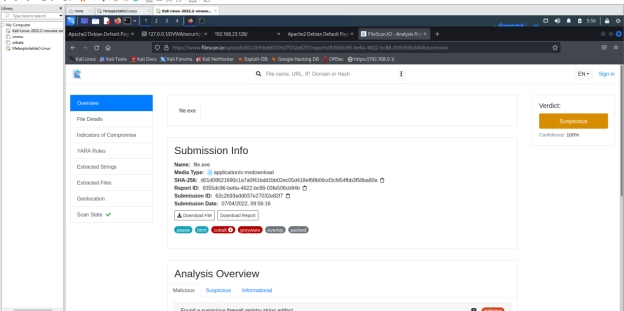
**Step3**:

**Report from filescan.io**

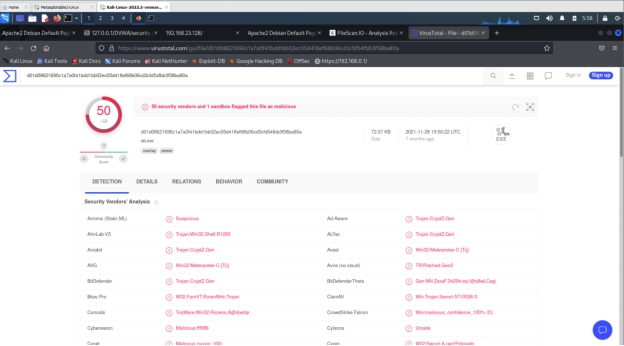
In filescan.io







**Report in virustotal**



Final deduction

**Observation**

There is 50% of malware in the file.exe.

Final report.

**IT Audit: Do the port scanning of the computer using nmap/zenmap to identify the open ports and see if services running on those ports are vulnerable or not. Write a report on it. [Note: Clear any firewall rules that you have added by using the command sudo iptables –F]**