Name of the Student:

Branch: CSE-C Subject: ICS

Experiment-9

Implementation of IT Audit, Malware Analysis and Vulnerability Assessment and Generate the Report

Date: 28/8/25

AIM

Implementation of IT Audit, malware analysis and Vulnerability assessment and generate the report.

PROCEDURE

Step-1: Collect information about malware

Step-2: Get the basic information about malware

Step-3: Get the report from filescan.io and virustotal.com

Step-4: Perform IT Audit to get the port information

SOURCECODE

Step1 : Collect Information about malware
How a malware is collected.

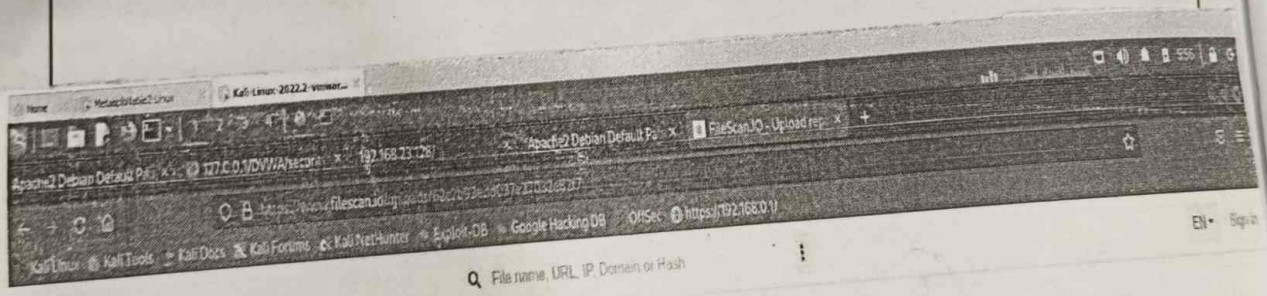
Step2: Basic Information and malware:
Name: file.exe
MediaType: application/x-medownload.
SHA-256: fo1d086216901a6ff16602ex054f5
3f3f586a80a.

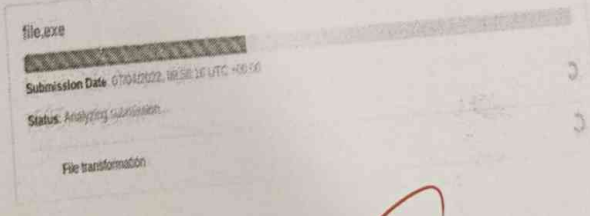
Report Id : 37ceb6b-0778-4c35-9c63-d177c1e7e34a

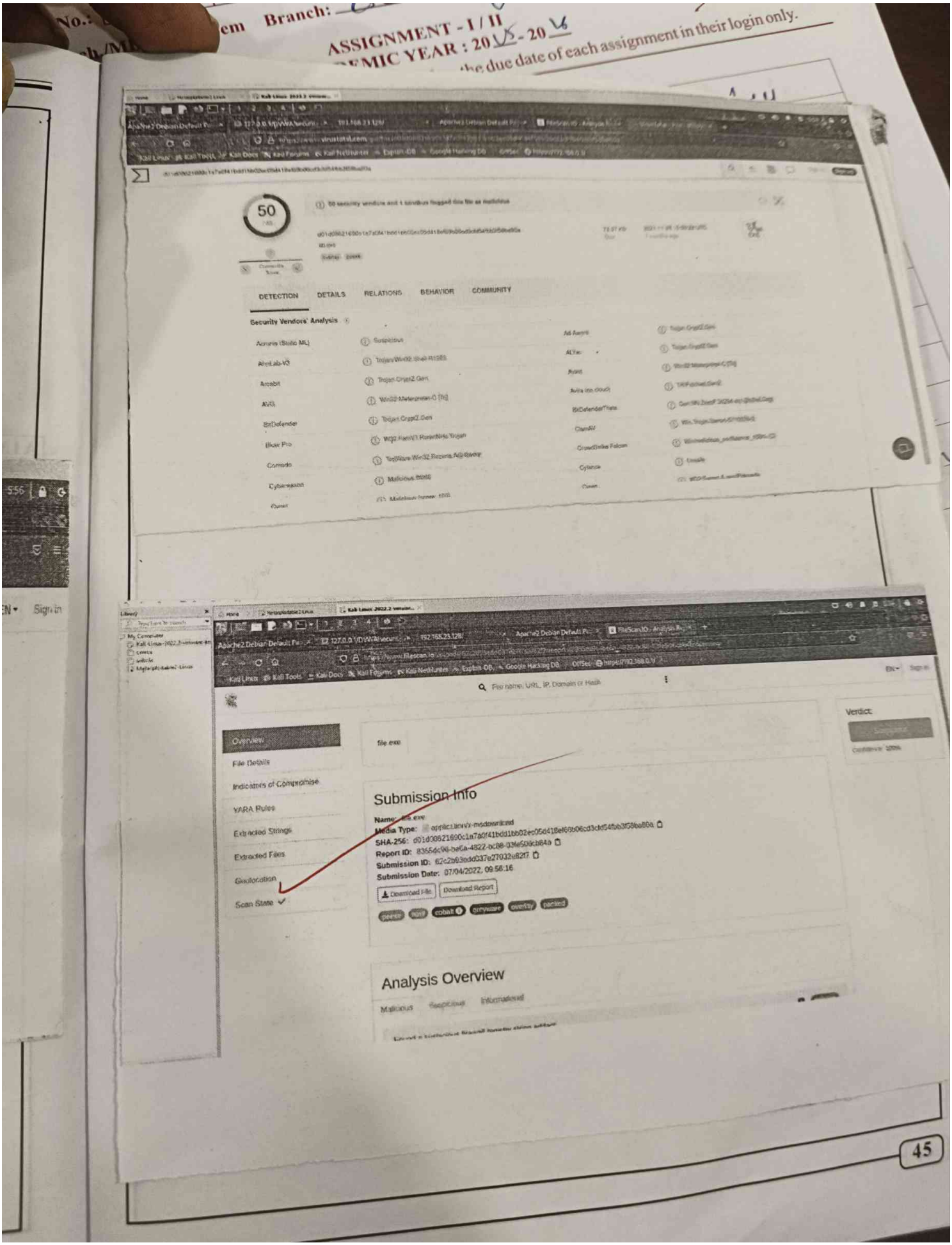
Submission Id : 62c24f0978441a0f01023be

Submission Date : 07/04/2022, 2:24:27

steps. Report from filescan.io.






Branch:
ASSIGNMENT - I / II
the due date of each assignment in their login only.
50
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY
Security Vendors' Analysis
Submission Info
Analysis Overview
Overview
File Details
Indicators of Compromise
YARA Rules
Extracted Strings
Extracted Files
Geolocation
Scan State
Verdict
45

OUTPUT


filescan.io
RAPID. IN-DEPTH.
Drag & Drop For Rapid Analysis
or
http://www.webpage.com/invoice.doc
FileScan.IO is a free malware analysis service that offers rapid in-depth file assessments, threat intelligence and indicator of compromise (IOCs) extraction for a wide range of executable files, documents and scripts. Learn more