

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

### Step1:

#### Collection Information about Malware:

How a malware is collected.

### Step2:

#### Basic Information about malware:

Name: file.exe

Media Type: application/x-msdownload

SHA-256: d01d08621690c1a7a0f41bdd1bb02ec05d418ef68b06cd3cfd54fbb3f58ba80a

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

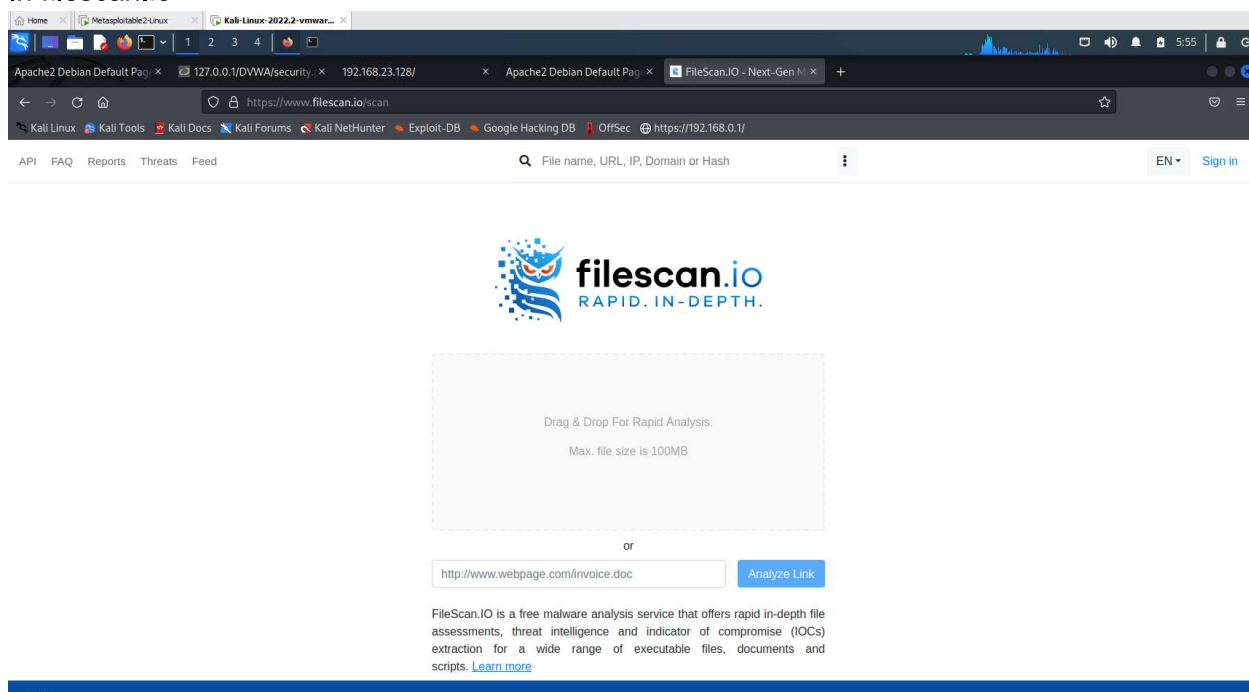
Submission ID: 62c24f59783441cda10213de

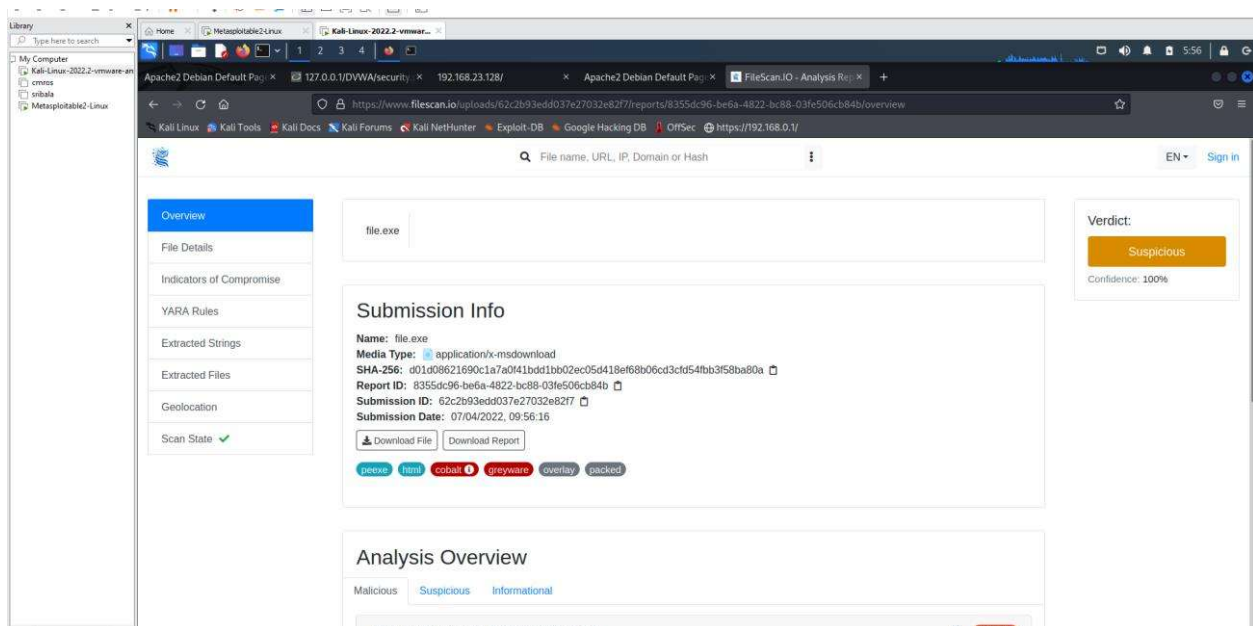
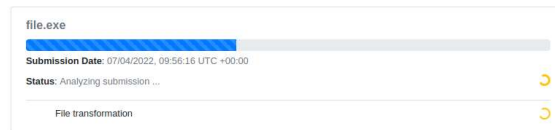
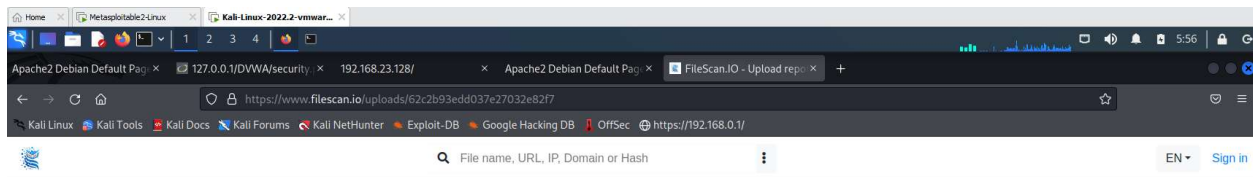
Submission Date: 07/04/2022, 02:24:27

### Step3:

#### Report from filescan.io

In filescan.io





## Report in virustotal

50 / 68 security vendors and 1 sandbox flagged this file as malicious

d01d08621690c1a7a0f41bdd1bb02ec05d418ef68b06cd3cfd54fbb3f58ba80a

72.07 KB Size | 2021-11-28 15:50:22 UTC 7 months ago

ab.exe

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Security Vendors' Analysis

Acronis (Static ML)	Suspicious	Ad-Aware	Trojan.CryptZ.Gen
AhnLab-V3	Trojan.Win32.Shell.R1283	ALYac	Trojan.CryptZ.Gen
Arcabit	Trojan.CryptZ.Gen	Avast	Win32:Meterpreter-C [Trj]
AVG	Win32:Meterpreter-C [Trj]	Avira (no cloud)	TR/Patched.Gen2
BitDefender	Trojan.CryptZ.Gen	BitDefenderTheta	Gen:NN.ZenxF.34294.eq1@a8wLcagi
Bkav Pro	W32.FamVT.RorenNHc.Trojan	ClamAV	Win.Trojan.Swroot-5710536-0
Comodo	Trojan.Win32.Rozena.A@4jwdqr	CrowdStrike Falcon	Win/malicious_confidence_100% (D)
Cybereason	Malicious/m086	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W32/Swroot.A.sen/Fidbrado

Final deduction

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`]**