

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: d01d08621690c1a7a0f41bdd1bb02ec05d418ef68b06cd3cf54fbb3f58ba80a

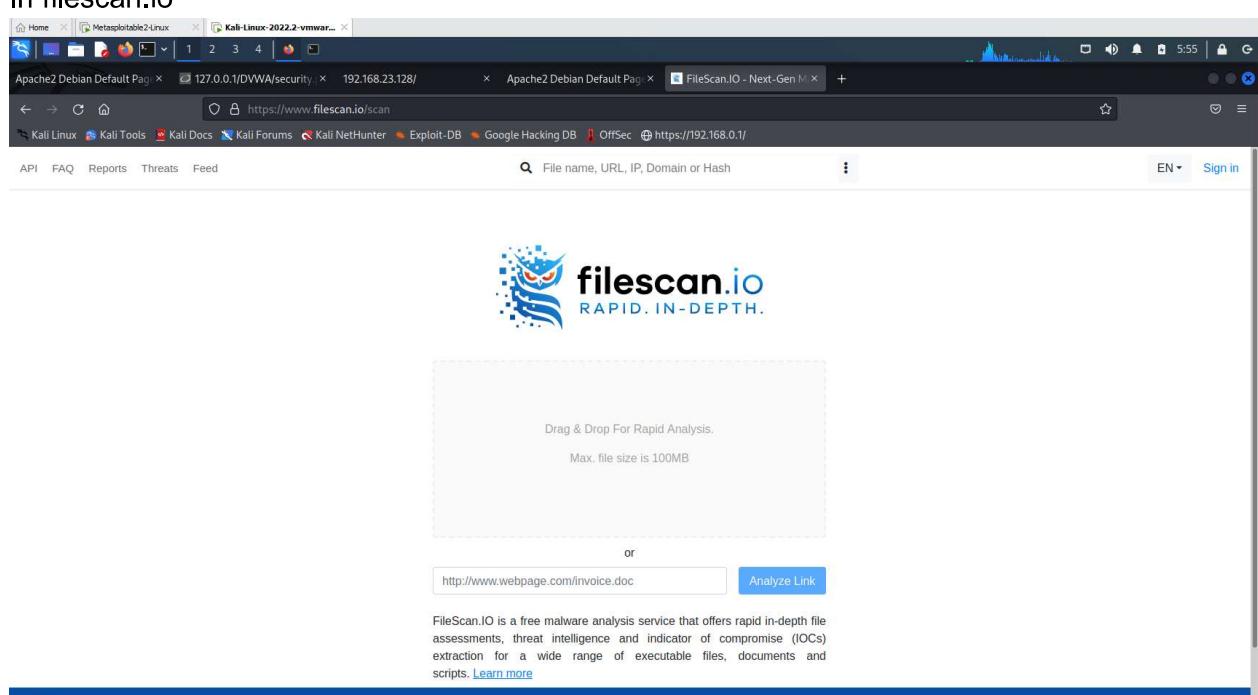
Report ID: 37cec6e6-0778-4c35-9cb3-d177c1e6e34a

Submission ID: 62c24f59783441cda10213de

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

Step3:**Report from filescan.io**

In filescan.io



Report in virustotal

50 / 68

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

d01d08621690c1a7a0f41bdd1bb02ec05d418ef68b06cd3cf54fb3f58ba80a
ab.exe

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

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Security Vendors' Analysis				
Acronis (Static ML)	① Suspicious	Ad-Aware	① Trojan.CryptZ.Gen	
AhnLab-V3	① Trojan.Win32.Shell.R1283	ALYac	① Trojan.CryptZ.Gen	
Arcabit	① Trojan.CryptZ.Gen	Avast	① Win32-Meterpreter-C [Tr]	
AVG	① Win32-Meterpreter-C [Tr]	Avira (no cloud)	① TR/Patched.Gen	
BitDefender	① Trojan.CryptZ.Gen	BitDefenderTheta	① Gen:NN.Zexaf.34294.eq1@a8wLcagi	
Bkav Pro	① W32.FamVT.RorenNHc.Trojan	ClamAV	① Win:Trojan.Swbot-5710536-0	
Comodo	① TrojWare.Win32.Rozena.A@4jwdqr	CrowdStrike Falcon	① Win/malicious_confidence_100% (D)	
Cybereason	① Malicious.ff086	Cylance	① Unsafe	
Cynet	① Malicious (score: 100)	Curen	① W32/Swbot A.nem/Fidnado	

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]