

## 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

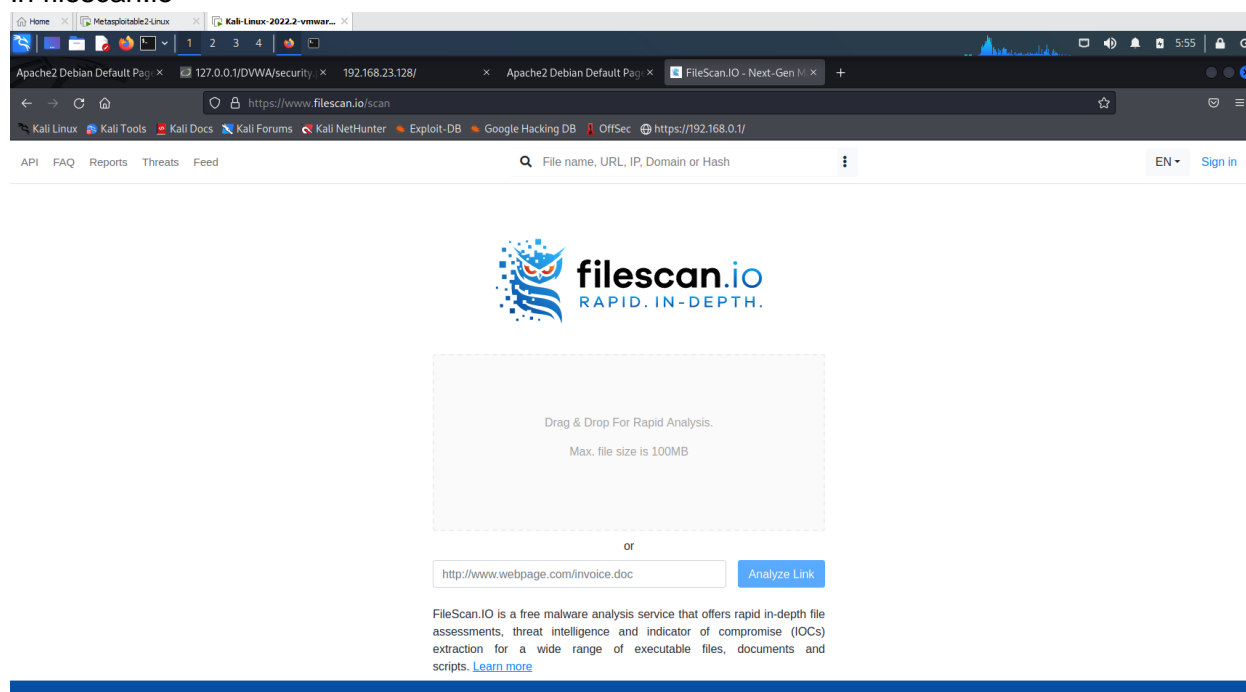
Submission ID: 62c24f59783441cda10213de

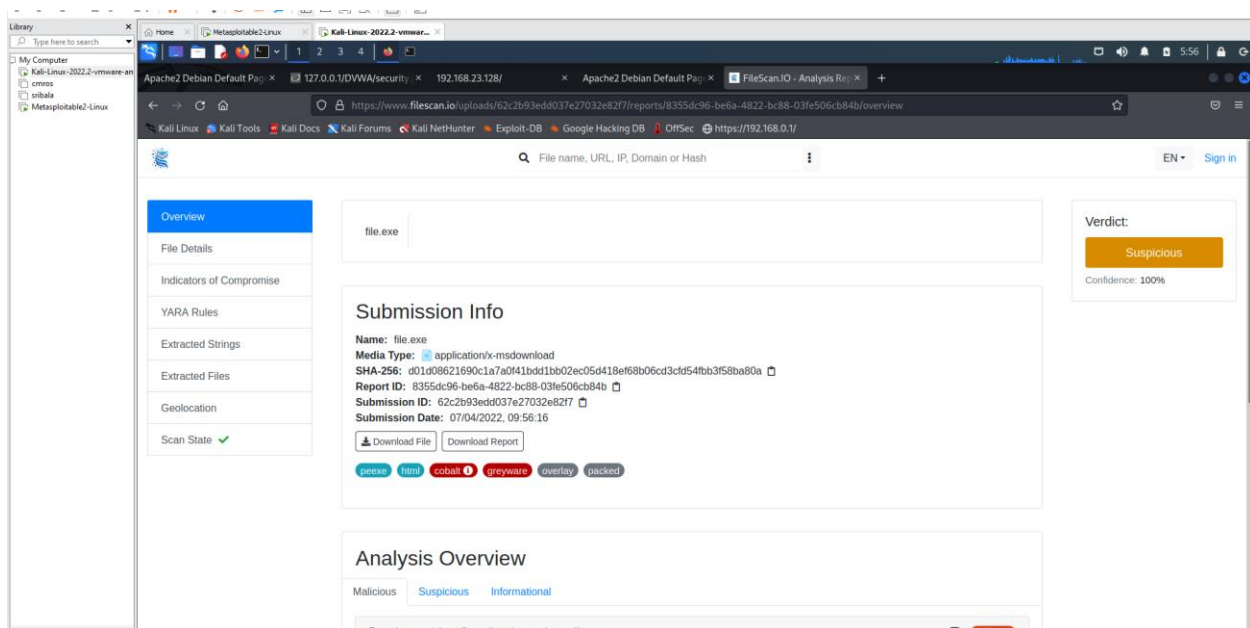
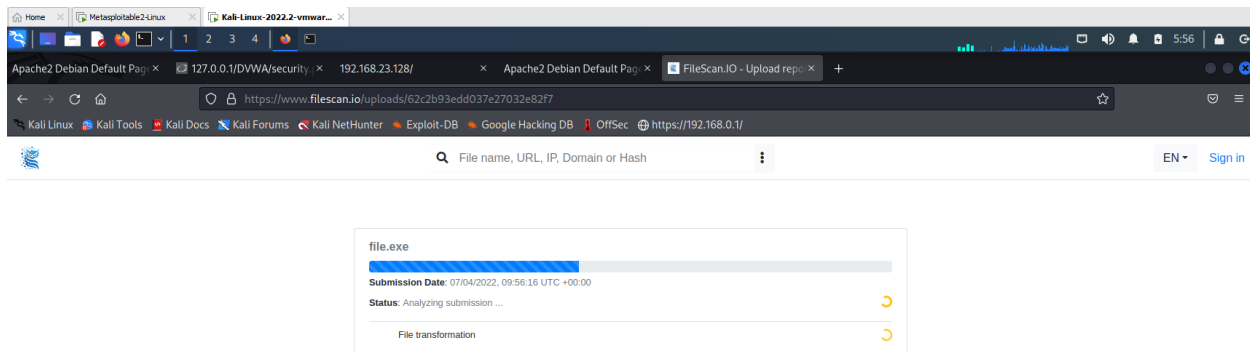
Submission Date: 07/04/2022, 02:24:27

### Step3:

#### Report from filescan.io

In filescan.io





## Report in virustotal

50 / 68

50 security vendors and 1 sandbox flagged this file as malicious

d01d08621690c1a7a0f41bdd1bb02ec05d418ef68b06cd3cfd54fb3f58ba80a

72.07 KB  
Size

2021-11-28 15:50:22 UTC  
7 months ago

EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Security Vendors' Analysis

Acronis (Static ML)	Suspicious	Ad-Aware	Trojan.Crypt2.Gen
AhnLab-V3	Trojan.Win32.Shell.R1283	ALYac	Trojan.Crypt2.Gen
Arcabit	Trojan.Crypt2.Gen	Avast	Win32-Meterpreter-C [Trj]
AVG	Win32-Meterpreter-C [Trj]	Avira (no cloud)	TR/Patched.Gen2
BitDefender	Trojan.Crypt2.Gen	BitDefenderTheta	Gen:NN.ZenxF.34294.eq1@abwl.Cagj
Bkav Pro	W32.FamVT.RorenNHc.Trojan	ClamAV	Win.Trojan.Swerot-5710536-0
Comodo	TrojWare.Win32.Rozena.A@4jwdgr	CrowdStrike Falcon	Win/malicious_confidence_100% (D)
Cybereason	Malicious.f1086	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W32/Swerot.A.gen/Fidorado

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`]**

**VIVA Questions**

1. What is malware?

.....

.....

.....

2. What is port scanning?

.....

.....

.....

3. List out any two websites used to get the malware analysis report?

.....

.....

.....

4. What is nmap/Zenmap tool?Why is it used?

.....

.....

.....

5. How is malware collected?

.....

.....

.....

**Experiment 10: Test security of UPI applications on Desktop sharing applications.****Step 1:**

Download and install UPI application on your phone

Download and install Teamviewer on your phone and computer

Download and install Anydesk on your phone and computer

**Step 2:**

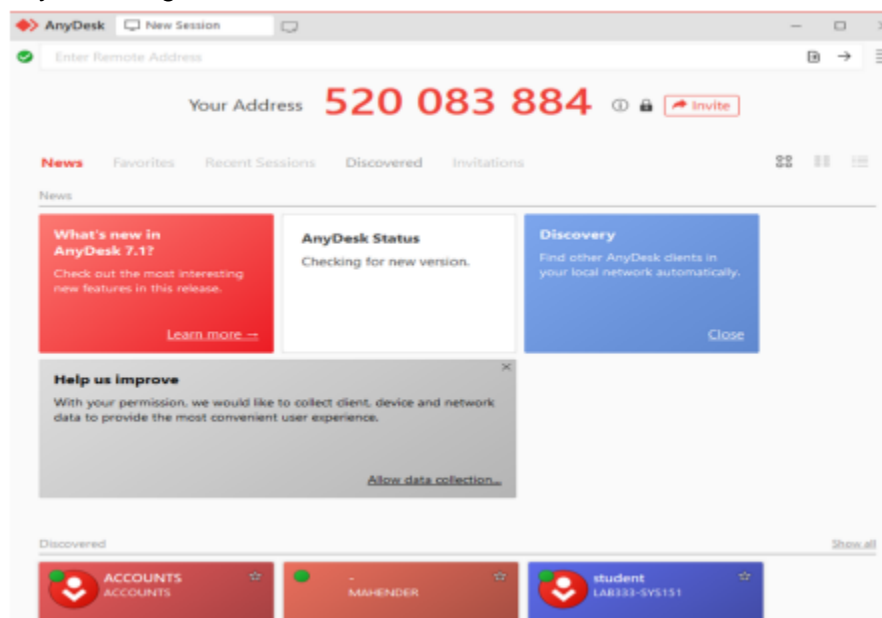
Test the security of the application and fill the table (keep adding more applications as you test)

**List of UPI Apps**

UPI Apps      Team Viewer    Any Desk

BHIM

Google Pay

**AnyDesk Login**

Download anyDesk in mobile

Connect both Mobile with Desktop

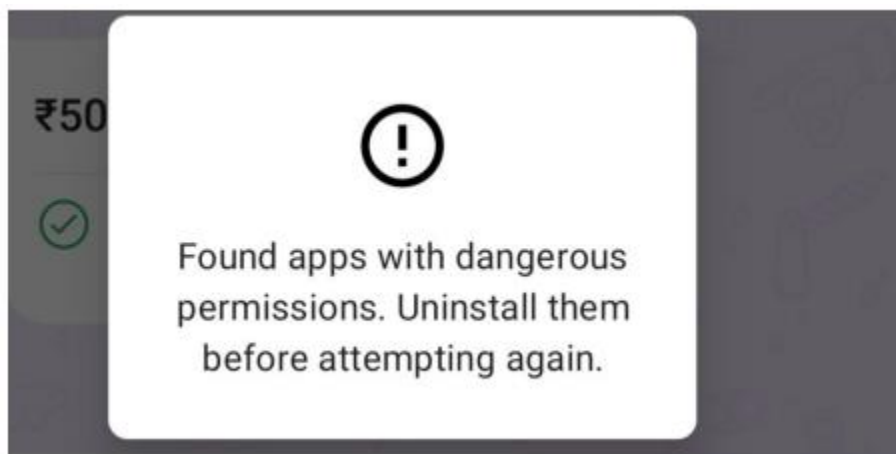
Open any UPI Application



Try to perform any online transaction like sending a negligible amount to any of your contacts.

With the security measures followed by UPI applications it should not allow any transactions

It should display following message in the mobile.



**VIVA Questions**

1. List out a few UPI Apps?

.....

.....

.....

2. What is security policy?

.....

.....

.....

3. What is a software license?

.....

.....

.....

4. Why is security testing required?

.....

.....

.....

5. What is Steganography?

.....

.....

.....