Experiment 9: Implementation of IT Audit, malware analysis and Vulnerabilityassessment and generate the report.

Step1:

Collection Information about Malware:

How a malware is collected.

Step2:

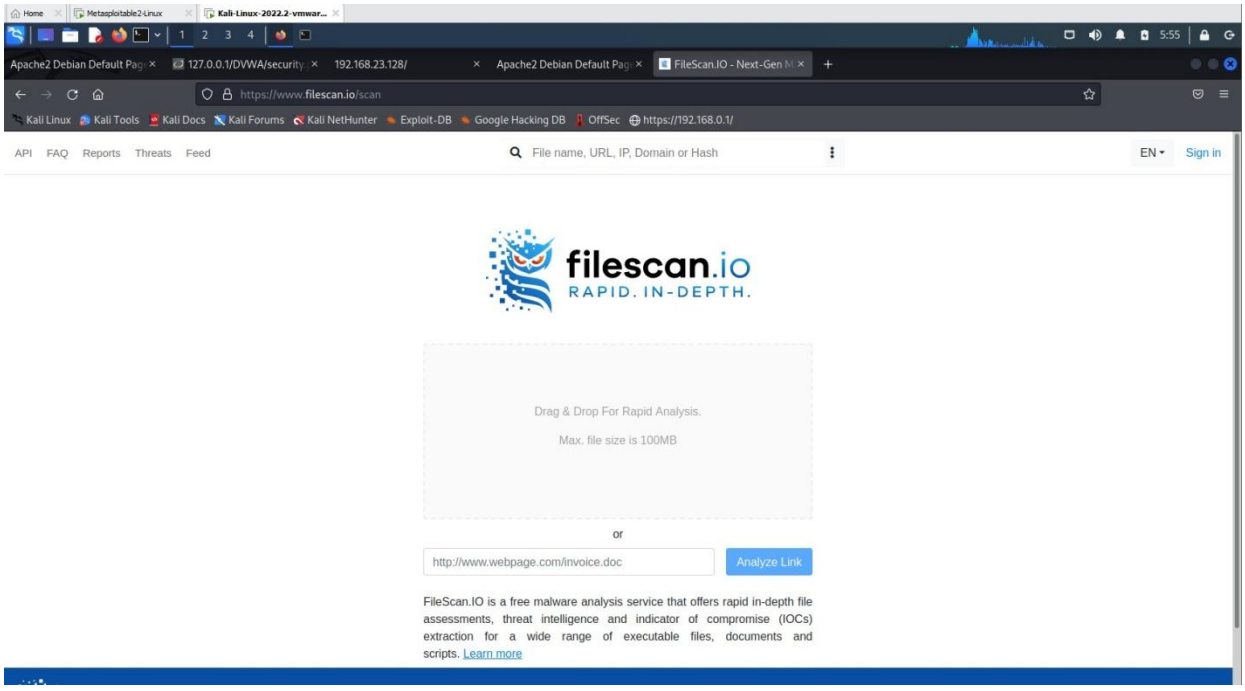
Basic Information about malware:

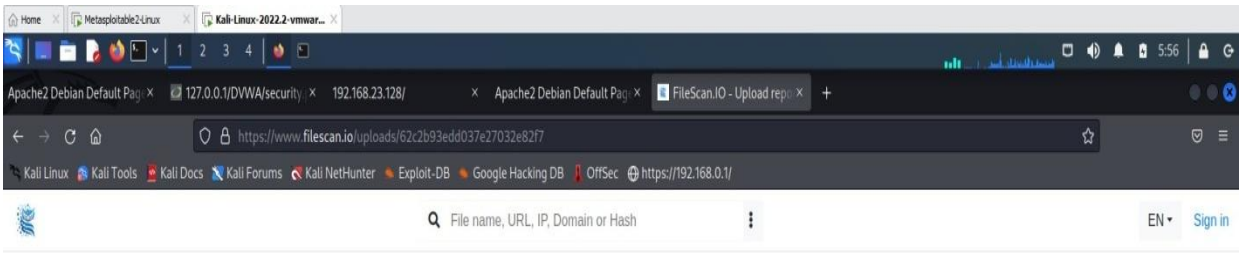
Name: file.exe
Media Type: application/x-msdownload
SHA-256: d01d08621690c1a7a0f41bdd1bb02ec05d418ef68b06cd3cfd54fbb3f58ba80a
Report ID: 37cec6e6-0778-4c35-9cb3-d177c1e6e34a
Submission ID: 62c24f59783441cda10213de
Submission Date: 07/04/2022, 02:24:27

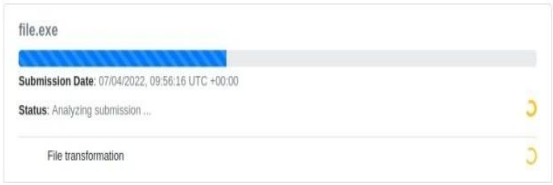
Step3:

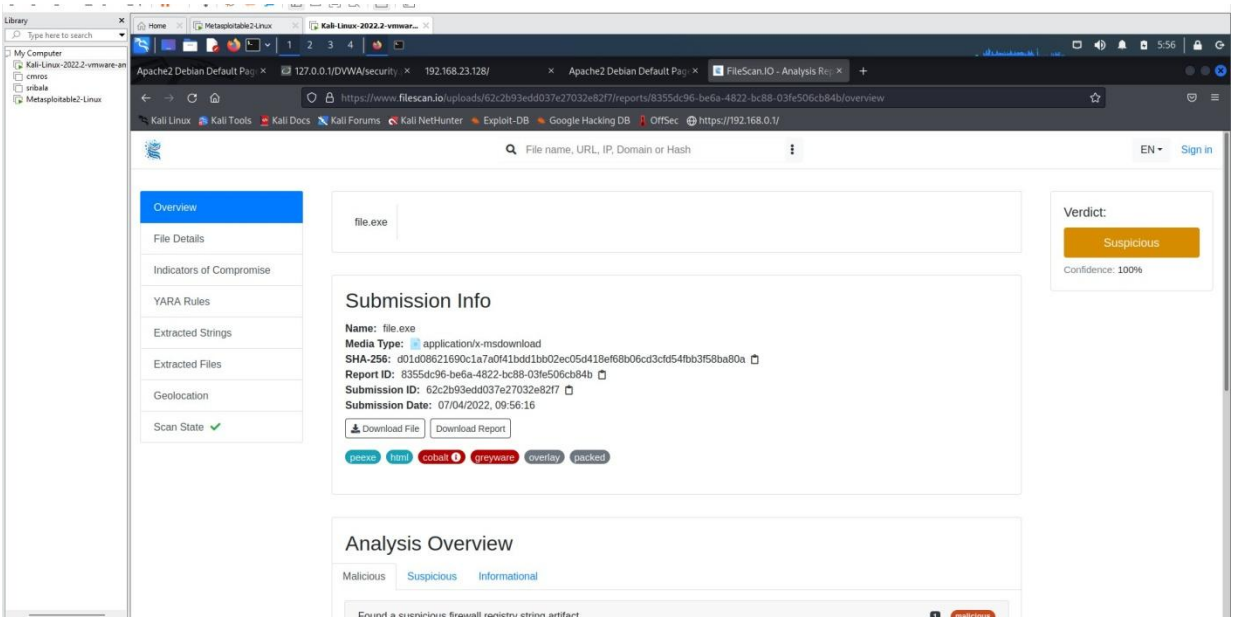
Report from filescan.io

In filescan.io

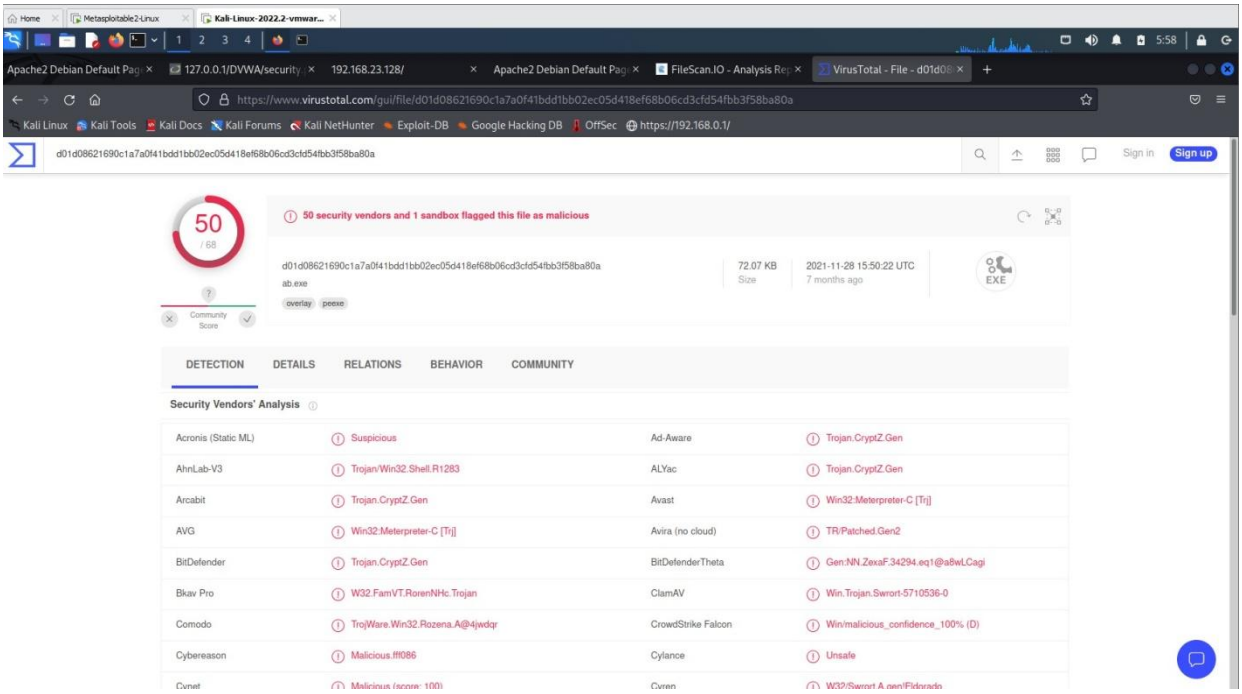








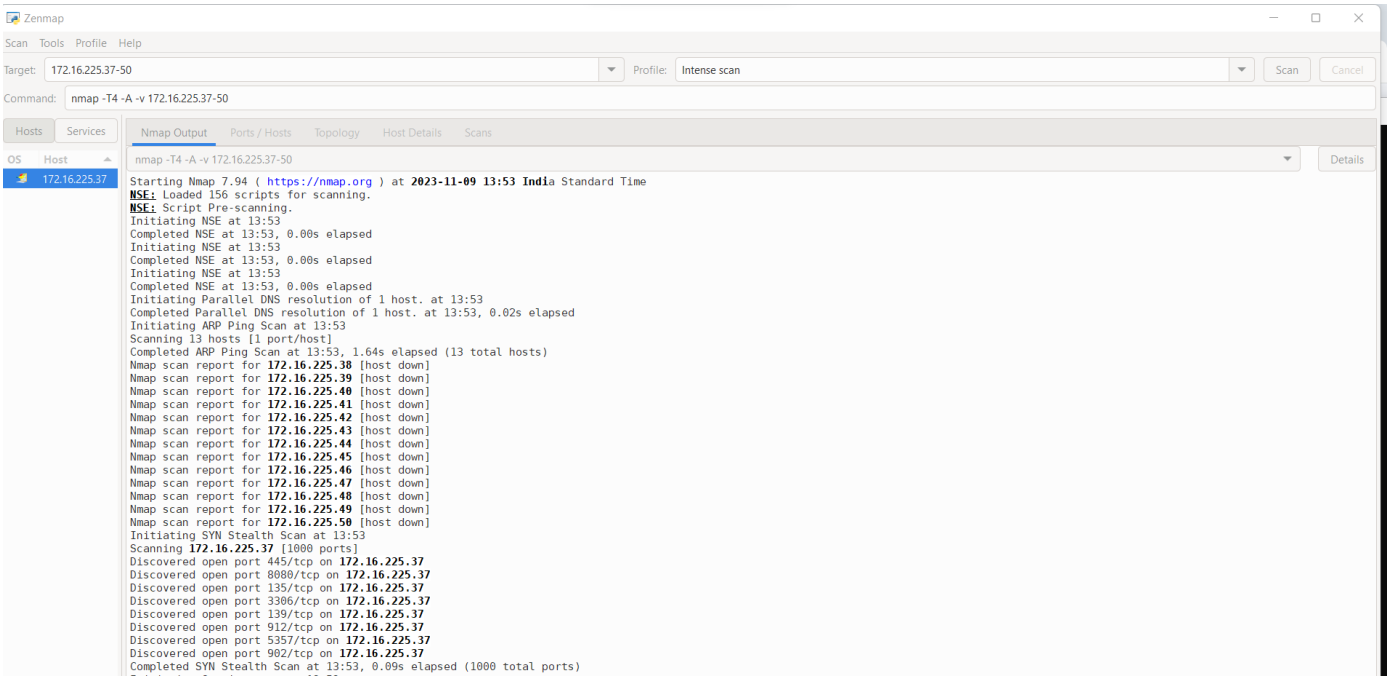
Report in virustotal



Final report.

IT Audit: Do the port scanning of the computer using nmap/zenmap to identify the openports and see if services running on those ports are vulnerable or not. Write a report on it.

NMAP-ZEN MAP Scanning:



Command in nmap scanning:

➔ **nmap -Pn 172.16.192.124**

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn 172.16.225.37
Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-09 03:49 EST
Nmap scan report for 172.16.225.37
Host is up (0.0020s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 30.59 seconds
```

Port Scanning:

➔ **nmap –Pn –p 135-150 172.16.102.124**

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn -p 135-150 172.16.225.37
Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-09 03:51 EST
Nmap scan report for 172.16.225.37
Host is up (0.00088s latency).

PORT    STATE    SERVICE
135/tcp open     msrpc
136/tcp filtered profile
137/tcp closed   netbios-ns
138/tcp filtered netbios-dgm
139/tcp open     netbios-ssn
140/tcp filtered emfis-data
141/tcp filtered emfis-cntl
142/tcp filtered bl-idm
143/tcp filtered imap
144/tcp filtered news
145/tcp filtered uaac
146/tcp filtered iso-tp0
147/tcp filtered iso-ip
148/tcp filtered cronus
149/tcp filtered aed-512
150/tcp filtered sql-net

Nmap done: 1 IP address (1 host up) scanned in 1.25 seconds

┌──(kali㉿kali)-[~]
└─$
```

Result:

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