Laboratorul 7

1. A) Nu s-a intamplat nimic deosebit cand am deschis imaginea

b) Faptul ca imaginea contine un executabil, ceea ce se poate recunoaste dupa caracterele MZ

c) Exista un trojan in imagine

d) Obtinem rezultatul ca imaginea contine un executabil ce sterge fisierul pdf, recunoscut de 20 de antivirusi din VirusTotal

e) Fisierele din DLL.zip ajuta malware-ul sa functioneze

f) Contine imaginea un malware deoarece, in mod subit, sterge fisiere fara acordul nostru

2.

a) Daca introducem o parola prea lunga, peste 7 caractere, obtinem eroarea \*\*\*stack smashing detected\*\*\* si terminarea programului

b) Orice string de exact 14 caractere

c) atac de tip Buffer Overflow

3.

import hashlib  
filename = "malwar.exe"  
api\_key="e63aec06020b6dfe77fb35fd6bd77c83aa6bdab720b43476639e70d04516b312"  
with open(filename, "rb") as f:  
 bytes = f.read()  
 readable\_hash = hashlib.sha256(bytes).hexdigest()  
import requests  
url='https://www.virustotal.com/vtapi/v2/file/report'  
params={'apikey':api\_key,'resource':readable\_hash}  
response=requests.get(url, params=params)  
for key in response.json():  
 if key=="positives":  
 if response.json()[key]==0:  
 print("Fisierul este sigur")  
 else:  
 print("Fisierul nu este sigur")

4.



