

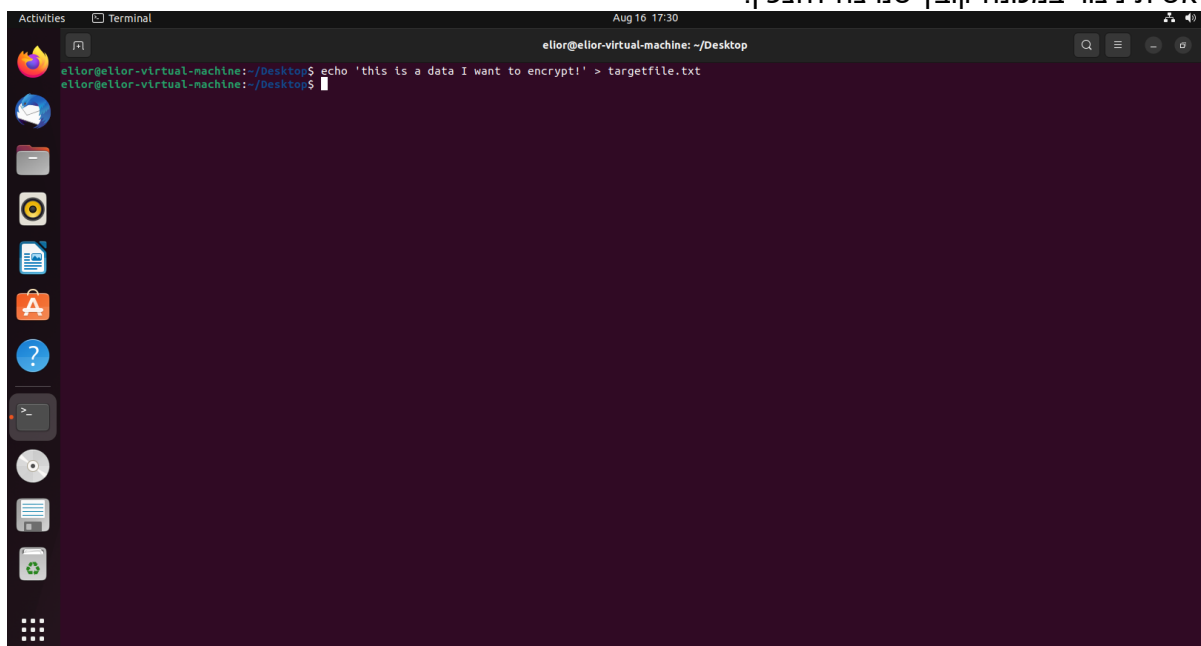
Encrypt and Decrypt Script

מטרת הסקריפט

ביצוע הצפנת קבצים (256-AES) ופענוח שלהם ע"י סקריפט BASH.

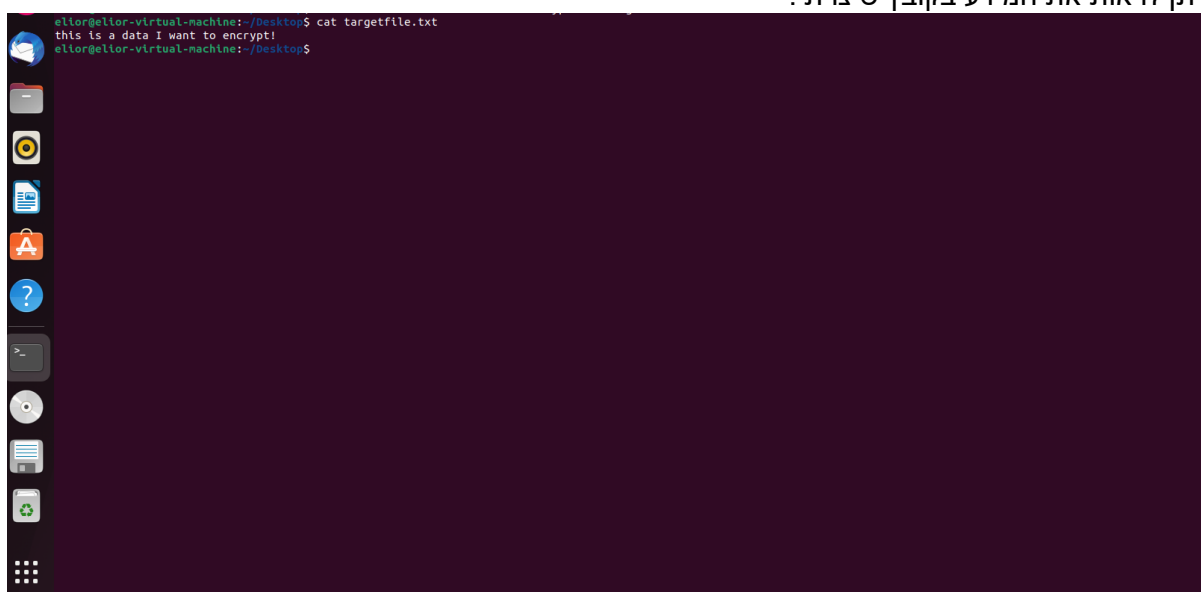
הכנת הסקריפט ו POC

1. ראשית ניצור במכונה קובץ שנרצה להצפין:

A terminal window titled 'Terminal' with a dark background. The prompt is 'elior@elior-virtual-machine: ~/Desktop'. The user enters the command 'echo 'this is a data I want to encrypt!' > targetfile.txt'. The prompt returns to 'elior@elior-virtual-machine: ~/Desktop\$'. On the left side of the terminal, there is a vertical dock with various application icons including a file manager, a terminal, a web browser, and a music player.

```
elior@elior-virtual-machine:~/Desktop$ echo 'this is a data I want to encrypt!' > targetfile.txt
elior@elior-virtual-machine:~/Desktop$
```

2. ניתן לראות את המידע בקובץ שיצרתי:

A terminal window titled 'Terminal' with a dark background. The prompt is 'elior@elior-virtual-machine: ~/Desktop'. The user enters the command 'cat targetfile.txt'. The output of the command is displayed on the next line: 'this is a data I want to encrypt!'. The prompt returns to 'elior@elior-virtual-machine: ~/Desktop\$'. On the left side of the terminal, there is a vertical dock with various application icons including a file manager, a terminal, a web browser, and a music player.

```
elior@elior-virtual-machine:~/Desktop$ cat targetfile.txt
this is a data I want to encrypt!
elior@elior-virtual-machine:~/Desktop$
```

כעת נתחיל בכתיבת הסקריפט

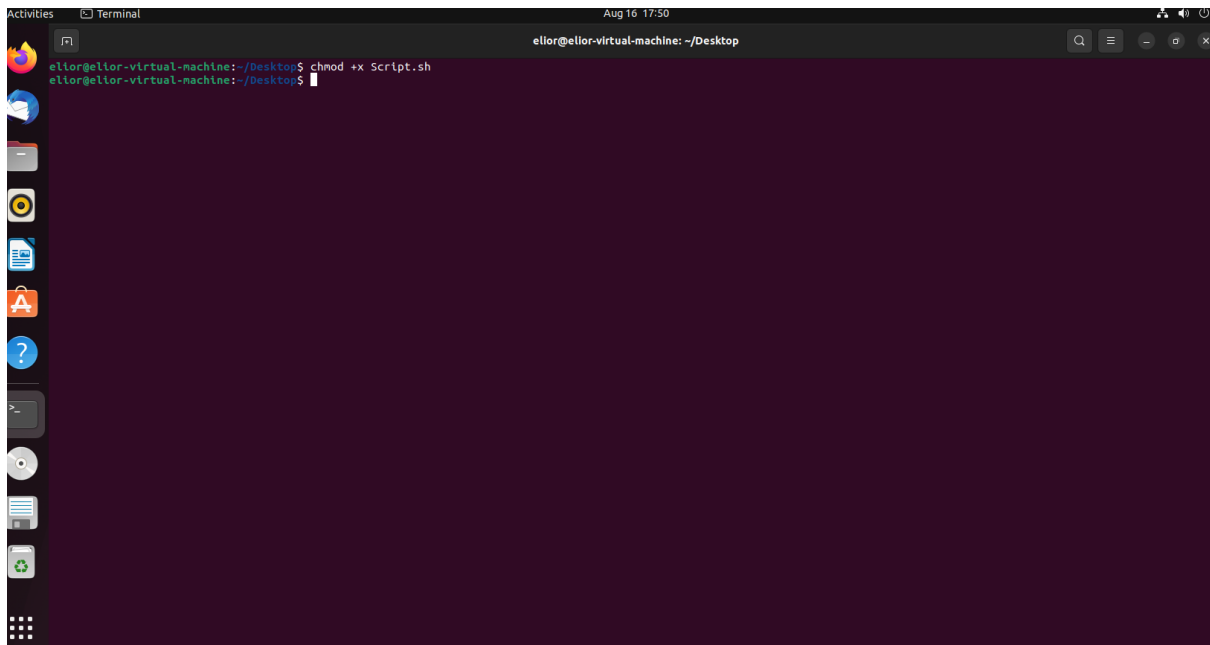
3. ניצור את קובץ הסקריפט:

```
elior@elior-virtual-machine: ~/Desktop$ gedit Script.sh
```

4. נכתוב את הקוד הבא (הסבר מפורט מה המשמעות של כל שורה בקוד מפורט בקוד עצמו)

```
1#!/bin/bash
2#Need to write line 1 in every bash script!!
3
4echo '-----'
5Please Choose the relevent number by the following:
61 - To Encrypt a file
72- To Decrypt a file
8-----'
9
10#This command is equivalent to 'Print' in Python
11
12read x
13#This command is equivalent to 'Input' in Python
14if [ $x -eq 1 ]
15#If the user input (1 or 2) = 1 then echo (print ....)
16then
17
18echo '-----'
19What is the name of the file you want to Encrypt?
20-----'
21
22read y
23sudo openssl aes-256-cbc -in $y -out EncryptedFile.txt
24#This command is encrypting using AES 256 bit (Symmetric algorithm) and exporting the encrypted file to EncryptedFile.txt
25$|
26echo '-----'
27Your Encrypted File is under the name EncryptedFile.txt
28-----'
29echo "
30The hash (SHA256) of the Original file is:
31-----"
32echo `sha256sum $y` | cut -c -64
33#This command is showing the Hash of the Original File we're Encrypting
34
35else
36
37echo '-----'
38What is the name of the file you want to Decrypt?
39-----'
40read y
41sudo openssl aes-256-cbc -in $y -out DecryptedFile.txt -d
42#This command is Decrypting using AES 256 bit (Symmetric algorithm) and exporting the decrypted file to DecryptedFile.txt
43
44echo '-----'
45Your decrypted file is under the name DecryptedFile.txt
46-----'
47echo "
48The hash (SHA256) of the Decrypted file is:
49-----"
50echo `sha256sum $y` | cut -c -64
51#This command is showing the Hash of the Decrypted File we've created
52fi
53#Need to write line 42 in the end of every bash script!!
```

5. לאחר ששמרנו את הסקריפט ניתן לו הרשאות הרצה:



6. נריץ את הסקריפט לאחר מכן ונבחר 1 (על מנת להצפין)

```

elior@elior-virtual-machine:~/Desktop$ ./Script.sh
-----
Please Choose the relevent number by the following:
1 - To Encrypt a file
2- To Decrypt a file
-----
1
-----

```

7. נכתוב את השם של הקובץ שברצוננו להצפין

```

-----
What is the name of the file you want to Encrypt?
-----
targetfile.txt

```

8. נקיש את הסיסמא של ROOT ונלחץ אנטר

```

targetfile.txt
[sudo] password for elior:

```

9. נבחר מפתח שישמש אותנו להצפנה ולפענוח ונלחץ אנטר בסיום (צריך פעמיים)

```

enter AES-256-CBC encryption password:
Verifying - enter AES-256-CBC encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
-----
Your Encrypted file is under the name EncryptedFile.txt

```

10. נוכל לראות כי התוכן של הקובץ החדש מוצפן:

```

Your Encrypted file is under the name EncryptedFile.txt
-----
elior@elior-virtual-machine:~/Desktop$ cat EncryptedFile.txt
Salted__$r000&
+00&0z0眞$0#
      00^00
00000
      000K000:0l+N00elior@elior-virtual-machine:~/Desktop$

```

11. נקעת נפענוח את ההצפנה באופן הבא

נריץ את הסקריפט שיצרנו בשנית:

```

elior@elior-virtual-machine:~/Desktop$ ./Script.sh
-----

```

12. נבחר הפעם 2 (לצורך פענוח ההצפנה)

```

Please Choose the relevent number by the following:
1 - To Encrypt a file
2- To Decrypt a file
-----
2
-----

```

13. נזין את השם של הקובץ שברצוננו לפענוח את ההצפנה (הקובץ המוצפן שיצרנו)

```

-----
What is the name of the file you want to Decrypt?
-----
EncryptedFile.txt

```

14. נזין את המפתח שיצרנו על מנת לפענח את ההצפנה ונלחץ אנטר

```
EncryptedFile.txt
enter AES-256-CBC decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
-----
Your decrypted file is under the name DecryptedFile.txt
```

15. נוכל לראות שכאת הקובץ שנוצר הוא לא מוצפן:

```
elior@elior-virtual-machine:~/Desktop$ cat DecryptedFile.txt
this is a data I want to encrypt!
elior@elior-virtual-machine:~/Desktop$
```