פריצת המייל – CTF

כבר הספקתם לפצח את הסיסמה?
טוב אנחנו מבינים עם מי יש לנו עסק, עולים רמה.

בחלק הזה נתמקד בעיקר בלתת לכם כלים לעשות דברים בצורה אוטומטית ומהירה כדי שלא תעשו את זה בצורה איטית וידנית.

בנוסף ניתן לכם כלים לפריצה **ממשית**, כאלה ששימושיים בעולם

האמיתי! לפני שנתחיל שימו לב שיש חלקים בקוד שהם תחומים

בכותרת של "**Don't Touch!**" ובהם אסור לגעת.

לדוגמה:

```
1   import ...
8
9   Drivers - Don't Touch!
14
15
```

ועכשיו באמת בואו נתחיל, עברו לעמוד הבא!

<u>שלב 1: זיהוי הקבצים שחילצנו</u>

אוקיי, רגליים על הקרקע, בואו נעשה סדר. שימו לב שחילצתם לתיקייה "level 2 – extract here!" את כל קובץ ה-zip שפתחתם.

אחרי שעשיתם זאת, אתם תראו 3 קבצים:

ascii-table.jpg	21/06/2022 11:07	קובץ JPG
Bruteforce_script.py	18/09/2022 14:16	Python File
emails.txt	21/06/2022 10:19	מסמך טקסט

1. תמונת תווי ASCII שתבינו בהמשך מה זה ומה הצורך של התמונה בקוד שלנו.

2. הקוד פייתון "Bruteforce_script.py" שעליו נעבוד ונפרוץ למשתמש גוגל של מנהיג החמאס.

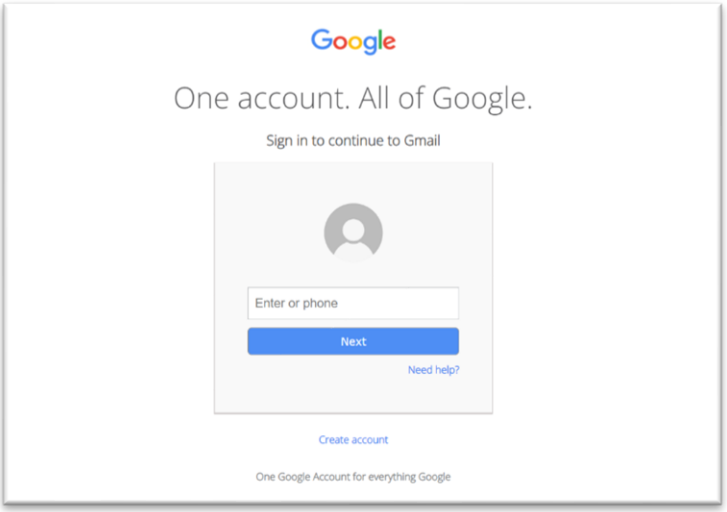
3. קובץ טקסט "emails.txt" שמכיל רשימת מיילים שזיהינו שהם פוטנציאלים להיות המייל של מנהיג ארגון הטרור.

הבנו מה הקבצים שלנו, ועכשיו נמשיך הלאה!

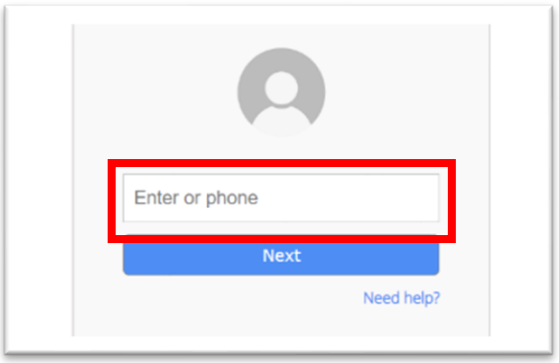
שלב 2: למה צריך את הקוד, ואיך נפתח אותו?

המטרה של הקוד שנבנה עכשיו היא לפרוץ לחשבון הגוגל של אותו מנהיג ארגון טרור.
בשביל לעשות זאת נפרק את המשימה ל-4 שלבים:

א. קודם נבין איך פותחים את גוגל **דרך הקוד שלנו** כך שנגיע לאתר הזנת המייל בגוגל:



ב. לאחר מכן נבין איך אנחנו ניגשים בעזרת קוד לתיבת הטקסט שאליה מכניסים מיילים.



ג. אחרי שעשינו זאת המשימה הבאה שלנו תהיה לפתוח את קובץ המיילים דרך הקוד, לקרוא אותו ולשים את כל המיילים שקראנו ממנו לרשימה של מיילים בפייתון.

ד. לאחר מכן ננסה לשלוח את כל המיילים שברשימה שלנו לתיבת הטקסט וכאשר נמצא שאחד המיילים נכונים והוא באמת של מנהיג ארגון הטרור, נגיע **לשלב מספר 3** אותו תראו ממש בקרוב.

שלב 2א: פתיחת גוגל דרך הקוד שלנו

הקוד שלנו יתחיל מפונקציית ה-()main שכתבנו לכם בתחתית הקוד ותיקרא לפונקציה ()openwebsite ששם נכתוב את הקוד שלנו:

```
if __name__ == "__main__":
    openwebsite()
```

יצרנו לכם אובייקט(לא חשוב לדעת מה זה בדיוק) אבל השם שלו הוא "driver" וכל מה שהוא צריך להגיד לכם זה שהוא מדבר עם הדפדפן "גוגל כרום".

אבל איך פותחים את האתר כניסה של גוגל בעזרת קוד!?!?

נתחיל לכתוב בפונקציה ()openwebsite.

בשביל לפתוח URL(כתובת של אתר) נשתמש בפונקציה עם הפרמטר של כתובת האתר (URL)get ממש ככה:

```
driver.get(os.path.dirname(__file__) + "/website/gmail-page/gmail-mail-form.html")
```

קריאה לדפדפן שלנו(driver)

ואז קריאה לפונקציה (url)get שתנווט אותנו לאתר שנרצה

ה-url שניתן כפרמטר לפונקציה get.

שימו לב שלא צריך להבין את ה-url שנתנו לכם אלא פשוט להעתיק אותו כמו שהוא בדיוק.

כתבתם את השורת קוד הזאת? תריצו ותראו שאתם פותחים את אתר הגוגל.

שימו לב שלא משנה איזה URL ניתן בתור פרמטר, הפונקציה תיפתח את האתר הזה מיד אחרי שנריץ אותה. **נסו בעצמכם לפתוח איזה אתר שתרצו!**

קדימה לשלב הבא!

שלב 2ב: גישה לתיבת טקסט

כדי לגשת לתיבת הטקסט של המיילים או בעצם כל אובייקט באתר, צריך לדעת מה ה- XPATH שלו, המשימה הזאת תהיה עליכם, תחקרו את האתר תמצאו את ה-XPATH והעתיקו אותו.

נמשיך לכתוב בפונקציה ()openwebsite.

ניצור משתנה חדש בשם "input_mail_box" ונשווה אותו לדבר הבא:

```
input_mail_box = driver.find_element(                    )
```

קריאה לדפדפן שלנו(driver) ואז קריאה לפונקציה find_element(x, y) באשר x מסמל את **הסוג** של מה שהעתקנו, ו-y מסמל את מה שהעתקנו.

הפונקציה מקבל 2 פרמטרים: x ו-y. שהפרמטר הראשון יהיה מסוג **מחרוזת** ויקרא "xpath". לשים לב שהפרמטר השני הוא ה-XPATH עצמו שמצאתם והוא במרכאות **לא כפולות!**

ומעכשיו כל פעם שנקרא לinput_mail_box נתייחס לתיבת הטקסט ישירות.

שלב 2ג: רשימה של מיילים

איך תקראו מקובץ המיילים שהיה על שולחן העבודה
של אחד העובדים שלו ?

בקצרה:

אנחנו רוצים לכתוב קוד שבו פותחים את הקובץ emails.txt על מצב קריאה ומכניסים למשתנה בשם **file**.

אחר כך נרצה שאת התוכן של הקובץ תכניסו למשתנה בשם emails.

שימו לב אנחנו חייבים **רשימה** של מיילים!

קדימה!

שלב 2ד: פריצת המיילים!

הצלחתם ליצור רשימה של מיילים ולשים במשתנה? עכשיו נשאר לפרוץ את המייל,

לדבר שנעשה קוראים brute force כלומר פריצה בכוח.

אנחנו הולכים להשתמש ברשימה של המיילים שנמצאים במשתנה **emails,**
ולנסות כל מייל אפשרי נגד משתמש הגוגל של מנהיג ארגון הטרור.
ברגע שנמצא מייל נכון, הסקריפט יעצור ויקרא לפונקציה openwebpass() שייצרנו לכם בהמשך הקוד.

צרו אובייקט(חפץ) בשם "object" שאליו נשלח את המידע הבא:
- רשימת מיילים(emails)
- אובייקט התיבת טקסט (input_mail_box).

hack_email הוא היוצר של האובייקט הזה ואליו נשלח את הפרמטרים.

```
object = hack_email(emails, input_mail_box)
```

ל-object יש המון פונקציות בתוכו.

כל פעם שנתייחס לפונקציה ששייכת לאובייקט "object" הוא ידע להשתמש לבד בפרמטרים ששלחנו לו למעלה, כלומר הם כבר קיימים בתוכו ולא צריך לשלוח כל פעם מחדש פרמטרים לפונקציות שיש בתוכו.

הנה גם דוגמה וגם קוד שאנו צריכים לכתוב:

```
statement = object.bruteforce_emails()
```

כאן קראנו לפונקציה bruteforce_emails() דרך האובייקט שלנו.
הפונקציה יודעת לבד מה הפרמטרים ששלחנו לה כי קראנו לה דרך object.

מה שהפונקציה תעשה זה לבדוק כל מייל אפשרי מהרשימת מיילים ששלחנו, אם נמצא מייל נכון היא תחזיר **True**, אבל אם היא לא תמצא היא תחזיר **False** ובסוף תשים את התשובה בstatement.

- עכשיו כתבו בעצמכם את השורות קוד האחרונות לפונקציה openwebsite():
אם נמצא מייל נכון, פתחו את פונקציית **openwebpass().**

הרצתם את הקוד ופרצתם את המייל? אם כן תמשיכו לפריצת הסיסמה!