

|  |
| --- |
| אוגדן שאלות אתגר לתלמידי התמחות סייבר |
| הכין ואנונו שלום Send Email Icon of Line style - Available in SVG, PNG, EPS, AI & Icon fontsshalomvanunu@mekifh.edum.org.il |
| גירסא 1.0 – לשימוש חופשי |
|  |
|     |

|  |  |  |
| --- | --- | --- |
| שם התרגיל ומטרה | חומר לימוד כתנאי לביצוע  | קבצים נדרשים |
| אור בחשיכה - מוסד | PythonOS module | אין |
| הספנות - מוסד | WireShark | קובץ דגימת VOIP |
| שלום בלהות - שב״כ | PythonNetworkingSockets | אין |
| גשם ברכה - מוסד | PythonNetworkingSockets | אין |
| אוויר דחוס - מוסד | PythonHASHBruteforce | קובץ דחוס עם סיסמא וקבצי תמונה בפנים |

# המוסד למודיעין ולתפקידים מיוחדים

שלום לסוכן מ׳

1. נציג חמאס בלבנון [אסאמה חמדאן](https://he.wikipedia.org/wiki/%D7%90%D7%95%D7%A1%D7%90%D7%9E%D7%94_%D7%97%D7%9E%D7%93%D7%90%D7%9F) עתיד להגיע לדובאי בשבוע הבא ולשהות במלון Rove Dubai Marina, בחדר 754 בקומה השביעית.
2. על מנת שנוכל לבצע את פעולת *״אור בחשיכה״* במשרדי חמאס בחודש הבא, עלינו להשיג את הסיסמאות של רשתות ה wifi הנמצאות שם.
3. **משימתך הינה הרצת קוד פייתון אשר יאתר את הסיסמאות במחשב הנייד של אסאמה**, ייצור קובץ ויעתיק אותו ל Disk On Key שתחבר למחשבו.
4. לטובת כך עליך לפתח ביממה הקרובה אפליקציה בשפת פייתון. את השיטה להוצאת הסיסמאות מהמחשב תוכל ללמוד בסירטון הבא : 
5. **התוכנה תשמור בקובץ txt את שמות הרשתות והסיסמאות שלהם**. רשתות שהינן Public אין לשמור. (על סמך תוכן קבצי xml ).
6. עליך להגיע לדובאי עם קבוצת אנשי עסקים בנושא שימור אנרגיה סולרית ולשהות באותו מלון של אסאמה בקומה ה-10 בחדר 1034 שהוזמן עבורך.
7. **צוות דלתא**, ידאג להוציא את אסאמה מהחדר ובאותו הזמן אתה תבצע את הרצת התוכנה במחשב הנייד אשר יישאר בחדרו.
8. הנך מתבקש לשלוח בהקדם את התוצרים הבאים לבדיקה לפני אישור האופרציה המבצעית :
	1. קובץ py עם הקוד מקור
	2. קובץ exe שיורץ במחשבו ([ראה המרת py to exe](https://dev.to/eshleron/how-to-convert-py-to-exe-step-by-step-guide-3cfi))
	3. תצלום התוצר מבדיקות QA שביצעת על המחשב שלך.
9. בהצלחה!

ש.ו.

ראש מחלקת סוכני המוסד

# המוסד למודיעין ולתפקידים מיוחדים

שלום לסוכן מ׳

1. בשנה האחרונה הארגון עושה מאמצים רבים להתחקות אחרי איש עסקים בריטי אשר מפר את [הסנקציות מול איראן](https://he.wikipedia.org/wiki/%D7%A2%D7%99%D7%A6%D7%95%D7%9E%D7%99%D7%9D_%D7%A0%D7%92%D7%93_%D7%90%D7%99%D7%A8%D7%90%D7%9F).
2. החברה [Royaye Asre Iranian Shipping](https://www.raishipping.com/)  העסיקה את שירותיו של איש העסקים.
3. בשבוע האחרון בוצעה פריצת דרך, והצלחנו לקבל דגימה מתעבורת הרשת הפנימית.
4. עפי מודיעין מוקדם השיחה התקיימה במכשירי Cisco VoIP ברשת הפנימית של החברה.
5. מצורף הקובץ **VOIP.pcapng** למשימה אשר מכיל את השיחה.
6. **המשימה היא זיהוי שם איש העסקים כפי שמופיעה בשיח**ה.
7. קיימת דחיפות לאיתור איש העסקים על מנת לקטוע את ההפרה.
8. בהצלחה!

ש.ו.

ראש מחלקת סוכני המוסד

#  שירות הביטחון הכללי

שלום הסוכן ד׳,

1. בעקבות תהליך לפייס בין חמאס לפת"ח, הגיע לידינו הקלטה שביצע סגן מנהיג חמאס [סלאח עארורי](https://www.mako.co.il/news-world/2020_q4/Article-30c527490be0571026.htm) עם פעיל בגדה.
2. כדי למנוע הוצאת פיגוע משטח הגדה אנו מוציאים לפועל את תוכנית ״שלום בלהות״ במיידי.
3. מטרת המבצע הינה סריקת הרשת האינטרנטית הביתית של הפעיל הנמצא בגדה , על מנת להתחקות אחר כוונותיו.
4. מגורמי שטח בגדה, איתרנו את מיקום ביתו של הפעיל ואת הפרטים לכניסה לרשת הביתית שלו WiFi. אנו נספק לך את שם הרשת והסיסמא לכניסה.
5. **המשימה שלך היא כתיבת תוכנית בפייתון, אשר תבצע סריקה מהירה ברשת האינטרנט הביתית של הפעיל לאיתור נגישות אפשרית** אשר תבצע את התנאים הבאים :
	1. מציאת סגמנט (Network Address) הרשת המקומית
	2. גילוי כלל הכתובות IP הפעילות ברשת
	3. מיפוי הפורטים ([List of Well-Known Ports](https://www.webopedia.com/quick_ref/portnumbers.asp)) הפעילים עבור כל כתובת IP פעילה
	4. ייצוא הנתונים לקובץ Text מקומי.
	5. הריצה צריכה להיות מהירה ככל האפשר על מנת לא לחשוף את זהות הסוכן בשטח.
6. יש לשלוח את הקוד עם תצלומי תוצר QA לאישור המבצע.
7. בהצלחה!

ש.ו.

ראש מחלקת סייבר

# המוסד למודיעין ולתפקידים מיוחדים

שלום לסוכן מ׳

1. *תחילה, אנו מבקשים לברך אתכם על התוצרים וההישגים שאתם מספקים לנו במהלך הפעילות המבצעית בתקופה האחרונה*
2. הארגון עמל על הוצאת מבצע סייבר מורכב ***- ״גשם ברכה״*** לטובת יצירת נגישות למחשבו של [זיאד נח'אלה](https://www.hamichlol.org.il/%D7%96%D7%99%D7%90%D7%93_%D7%A0%D7%97%27%D7%90%D7%9C%D7%94)  - הוא המזכיר הכללי של ארגון הג'יהאד האסלאמי הפלסטיני היושב בסוריה.
3. זיאד נח'אלה נשוי ואב לשישה ילדים (שני בנים וארבע בנות). ממודיעין מקדים שקיבלנו אחד מילדיו משתמש במחשב הנייד שלו מידי פעם לצרכיו האישיים.
4. מטרת המבצע היא לשתול קוד תוכנה במחשבו הנייד של זיאד אשר יבצע **KeySniffer** וישלח אלינו את כל המידע שהינו מקליד. במקביל אתה תידרש גם לכתוב תוכנה לקליטת המידע שייאגר במחשבו . הכנסת הקוד הזדוני יתבצע ע״י הטלפון הנייד של בנו.
5. הנך נדרש לייצר 2 תוכנות קוד בשפת פייתון עפ״י היעדים הבאים :
	1. תוכנת הרצה במחשב הנייד ואוגרת את כל מה שהוקש במקלדת. המידע ישלח על גבי האינטרנט . יש לחשוב על אפשרות הסתרה ככל הניתן לאור העובדה כי על מחשבו קיים AntiVirus & Firewall.
	2. כתיבת תוכנה אשר תרוץ בטלפון הנייד של הסוכן שימצא באזור, אותו יריץ בעזרת [Pydroid 3](https://play.google.com/store/apps/details?id=ru.iiec.pydroid3). המידע אשר מכיל את כל KeySniffer הנשלח מהמחשב הנייד, ישמר טלפון הנייד בקובץ/ים.
	3. הנח כי כתובות IP עדכניים יינתנו בסמוך לביצוע המבצע.
6. הנך מתבקש לשלוח בהקדם את התוצרים הבאים לבדיקה לפני אישור האופרציה המבצעית :
	1. קובצי py עם הקו מקור
	2. תצלום התוצר מבדיקות QA שביצעת על המחשב שלך.
7. בהצלחה!

ש.ו.

ראש מחלקת סוכני המוסד

# המוסד למודיעין ולתפקידים מיוחדים

שלום לסוכן ד׳

1. לאחרונה עלה במקורותינו כי [חמאס מפעיל מטורקיה יחידת סייבר](https://www.mako.co.il/news-world/2020_q4/Article-eb3a88149745571027.htm?sCh=31750a2610f26110&pId=173113802) סודית הכפופה למנהיגי הארגון בעזה.
2. מנהל יחידת הסייבר הינו [סמאח סראג'](https://www.hamal.co.il/post/-LvOogVSIod99eIYNI-D), הוא בכיר בארגון חמאס אשר עתיד להגיע לטורקיה בשבוע הבא.
3. ממידע מודיעיני שהתקבל לאחרונה, ממכשירו של סמאח סראג' נשלח קובץ דחוס Zip עם סיסמא ובתוכו מספר קבצי QR של שם הרשת WiFi והסיסמא בו הוא משתמש.
4. על מנת שנוכל לבצע את פעולת *״אוויר דחוס״* להפלת תשתית יחידת הסייבר, עלינו להשיג את הסיסמא של רשת ה wifi הנמצאת בקובץ.
5. **משימתך הינה פיצוח סיסמת הקובץ Zipומציאת התמונה של QR Wifi הנכונה שבעזרתו תוכל למצוא את הסיסמא.**
6. לטובת כך עליך לפתח ביממה הקרובה אפליקציה **בשפת פייתון**. את השיטה להוצאת הסיסמא מקוד QR תוכל ללמוד בסירטון הבא : 
7. בימים הקרובים יישלח אליך הקובץ הדחוס עם הסיסמא. יש לעבוד עפ״י השלבים הבאים :
	1. מציאת הסיסמא של הקובץ הדחוס. [היעזר בסיסמאות השכיחות](https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/Common-Credentials/10-million-password-list-top-10000.txt)
	2. חילוץ הקבצים ומציאת הקובץ בעל **MD5 Hash**
	3. Hash Code : 5e2a0c62c40b2cb4879b0081ec6db149
	4. מציאת סיסמת רשת Wifi
8. הנך מתבקש לשלוח בהקדם את קובץ py עם הקוד מקור ואת שם וסיסמת ה wifi.
9. בהצלחה!

ש.ו.

ראש מחלקת סוכני המוסד