**WiFi Treasure Hunt**

**עקרונות:**

* כל AP הוא משימה.
* אחרי שמצליחים במשימה אפשר למצא ב-AP את הרמז למשימה הבאה
* בסופו של דבר צריך להגיע בשלב האחרון למדפסת שתדפיס את שמות המשתתפים או קוד מסוים ששייך לקבוצה באופן חד ערכי
* התחרות תהיה הזדמנות להקנות לסטודנטים ידע ב-wifi כמו גם לחשוף אותם בפני כלים כמו:
  + kismet
  + wireshark
  + snort
  + linux - wifi headers don't show under windows
* ה-SSID יכול להיות מוסתר ובעל פורמט של: next clue: info
* חלק מהפריצות יוכלו להתבצע ב-brute force פשוט. חלקם יצריך שיטות יותר מתוחכמות
* על מנת למצא אתגרים מעניינים צריך לחקור פירצות wifi עדכניות \ מעניינות
* שימוש ברשתות מלכודת פתוחות דוגמת Aroma או egged.co.il שמשתתפים יתחברו אליה אוטומטית.

**רעיונות נוספים:**

* בהנחה שאפשר לגלות את מספר הקפיצות שלי מ-AP מסוים. לתת משימה שדורשת למצא את מספר הקפיצות ולבצע איזשהו חישוב (אולי מודולו) עם המספר כדי להגיע לתוצאה
* שימוש בסקריפט פשוט ל-SHELL
* על מנת להגיע לשלב הבא צריך לקבל 2 מפתחות:
  1. ניתן ע"י משימה במקום
  2. ניתן ע"י רמז שצריך לפתור \ להבין ב-SSID
* בשרת web השאלה לאן מתחברים היא עניין של directory listing
* mac spoofing - לשלב רשת מאובטחת mac. דורש spoofing בשביל להתחבר
* ftp ללא הצפנה הוא פריץ לגמרי. מחברים מחשב ל-ap ,שבאמצעות סקריפט מתחבר כל פעם מחדש לשרת ftp ומעלה איזשהו קובץ. באמצעות סניפינג אפשר למצא פאקטים של פרוטוקול ftp. או שהססמה והפתרון נמצאים בטקסט רגיל בפאקט עצמו או שהססמה תאפשר להיכנס לשרת ftp והרמז יהיה בתוך הקובץ שהועלה
* "ארגז כלים" - שכולל סניפר, כלי לפריצת ססמאות, סטגנוגרפיה, אמצעי שמירת רמזים קודמים ...
* לארגן AP עם DD-WRT ולחבר לכל אחד PI או סרבר אחר או לחבר ל-VM על שרת מרכזי
* לשחק "רוצח" במקום סתם להגיע לנקודה האחרונה
  1. המטרה יכולה להיות (או חלק ממנה) לזהות מאיפה המדליף מדליף ( לדוגמה github או מקור אחר)
  2. צריך למצא תשדורת רנדומלית של טקסט

**רעיונות מתוך 1Interrupt:**

* קישור <http://blog.zer0w1re.net/1nterrupt-wifi-treasure-hunt-write-up/>
* לאפשר יותר מדרך פיתרון אחת לכל בעיה
  + לדוגמה מידע בקובץ רגיל להורדה
  + לעומת מידע steganographic
* highlight לטקסט מציג מידע חדש (שהיה בלתי נראה קודם)
* *index.html* הוא הדף הדיפולטיבי אבל לאו דווקא זה שצריך לחפש
* להחביא רמז בתוך ה-javascript
* שימוש ב-SSH
* port scans

**ניקוד:**

* אפשר לתת ניקוד לפי כמה פרמטרים. כמו לדוגמה:
  + מהירות (הראשון שסיים הכל)
  + דיוק פיזי (מי שהצליח להגיע הכי קרוב פיזית ל-AP)

**משימות**:

1. מציאת AP בעל שם שמתחיל עם המילה WTH והמשך השם בצורה של WTH\_56.0.49
2. מציאת AP בעל שם שמתחיל עם המילה WTH והמשך השם בצורה של WTH\_surf\_throw\_me לצורך התחברות ל-AP ואז דף הבית יכיל את הרמז עם find this MAC using kismet
3. תרגיל הכרות ב-kismet, תמצא Mac של AP, הרמז הבא לינק ל-pcap עם רמז
4. תרגיל הכרות ב-wireshark, תמצא SSID של AP, שיקרא WTH????
5. מציאת AP שנמצא במצב של hidden SSID
6. אתגר מחשבתי
   1. בצורה של מספר QRs שהסידור שלהם יתן את הסיסמא ל-AP ומשם הרמז הבא
   2. פריצה ל-AP בעל סיסמא של wep בעזרת aircrack
7. למצא מיקום פיזי של AP מוסתר שעליו יהיה QR
8. לזהות מסלול של drone לפי ה-AP שהוא עבר

* תוספת לרעיון של ה-drone: המזלט עף באיזשהו מסלול שצריך לזהות לפי הסדר הכרונולוגי של ה-AP שהוא עבר. מכניסים את המסלול לתוך google maps / earth ורואים רמז חדש
* **נבנה שרת IRC שכולם יתחברו אליו על מנת להכניס את הרמזים ולקבל ניקוד וכך כולם יוכלו לראות את הניקוד של כל הקבוצות.(רועי לבדוק)**

**משימות עתידיות:**

1. עבודה מול שרת FTP שקוד ב-java מנסה לפרוץ ולתת להם חלק מהסימנים על מנת שייעל את מציאת הקוד
2. VPN - ליצור חסימה על IP מסויים ולתת להם להשתמש במעקפים (חיבור ל hulu)
3. הסנפה של הרשת לצורך זיהוי כניסה לשרת FTP לא מאובטח
4. "תגיעו ל-X. זהו מי מהחברים שלכם הגיע \ נמצא" באמצעות סניפר על הפלאפון וכתובת MAC
5. משימה שדורשת שיפור טווח שידור \ קליטה באמצעות כלים פשוטים כמו חבילת פרינגלס
6. להריץ אלגוריתם בצורה יעילה. רק זמן ריצה שקטן שווה לסף מסוים יתקבל. למשל בדיקה אם מחרוזת אחת מכילה מחרוזת שניה בזמן לינארי במקום פולינומהבאה
7. שאלות היגיון מראיונות עבודה / משחקי חידות כמו "לחשוב מחוץ לקופסא"
8. להחביא מידע ב-meta data - כמו למשל ב-htm
9. פריצת סיסמאות - brute force איטית אל מול פתירת סדרה חשבונית או כללים מסויימים שיאפשרו לפרוץ את הססמה יותר מהר
10. משחק של שני צדדים - צריך לגלות את ה-key של השני שנמצא במקום ציבורי. הצדדים יכולים לחבל במאמצים של השני באמצעות כלום כמו DoS או מלכודות במקום הציבורי