****

**דו"ח סיכום פרוייקט סייבר**

**הוגש בתאריך:** 27.8.21

**מסלול הלימודים:** תואר במדעי המחשב במכללה למינהל, קמפוס בני ברק

**שם הקורס:** מבוא לאבטחת סייבר

**כותרת הפרויקט:** מימוש backdoor מתוחכם בפייתון

**שם מרצה הקורס:** יורם סגל

**חברי הקבוצה:**

* מיכאל רחשה | 323663872
* חיים חוגי | 207686650
* דני קובנר | 208627133

**קוד מזהה הקבוצה:** HMN001

**קוד מזהה של הקבוצה היריבה:** 5Y6ER0

הפרויקט נעשה בהשראת המאמר Backdoor attack in Python  
 נכתב ע"י Tommaso De Ponti , ופורסם בתאריך 15/04/2020

**תוכן עניינים**

[קישור למסמך סיכום](#_tceg5866v4hu) **4**

[קישור לקובץ "מכונת סביבת עבודה"](#_i48zntjbxcwa) **4**

[קוד HASH לקובץ "מכונת סביבת עבודה"](#_esvet7chfaz9) **4**

[קישור לקובץ "מכונה מוגנת"](#_qqs7xn1ugvwa) **4**

[קוד HASH לקובץ "מכונה מוגנת"](#_cn64pa4yjusb) **4**

[סיכום המאמר](#_67pzsqednict) 5

[מטרת התקפה](#_xx41t087bq7c) 5

[מטרת ההגנה](#_531grgiat12x) 5

[תיאור אופן מימוש ההתקפה שלנו והקשרה למאמר](#_7flzxkbs0oku) 6

[תיאור מימוש ההתקפה שלהם למיטב הבנתנו](#_9css2gmz96ir) 8

[תיאור אופן מימוש ההגנה מפני התקפת הקבוצה היריבה](#_ehbfn5fvptoq) 10

[מסקנות וסיכום](#_opjwibh18aev) 13

[**נספחים**](#_px9hbfbno9jh) **14**

[נספח א': מאמר הדגל המלא](#_i5lvel5w5ezy) 14

[נספח ב': תקנון](#_b4ifpoxf65kj) 21

[נספח ג': קטעי קוד חשובים ועיקריים](#_a9cm2gxaklec) 21

# **קישור למסמך סיכום**

<https://docs.google.com/document/d/1bUvMJAXlWu-RQ-7N8F4X0Ym7CjznNC0BisxS4cMhgEU>

# **קישור לקובץ "מכונת סביבת עבודה"**

<https://drive.google.com/file/d/1rrFtrVRsz1gY1uUDrPqi4ZvhMm4DJ3Bb/view?usp=sharing>

# **קוד HASH לקובץ "מכונת סביבת עבודה"**

2ca7a0c9b4d699215c1b3d6c0eecff0b

# **קישור לקובץ "מכונה מוגנת"**

<https://drive.google.com/file/d/1FjMC4P7piiN1uxIHYVctWpHau05Sj44B/view?usp=sharing>

# **קוד HASH לקובץ "מכונה מוגנת"**

e5cdbfbbd1d5b0c85176e089c5a4a0c7

# 

## 

## **מטרת התקפה**

אנו נמצאים בעיצומה של מלחמת העולם הראשונה , ובכדי לנצח את המלחמה עלינו לפרוץ למחשב האויב ולגנוב את הסיסמה שתעזור להשמיד את מערך הסייבר של האויב כליל.

הצלחנו להגניב מרגל לשורות האויב , אשר הכניס בהצלחה למחשב האויב קובץ backdoor שתפקידו לפתוח ערוץ תקשורת עם המחשב שלנו ולנסות לגשת לקובץ המוגן במחשב האויב ולגנוב את הסיסמה שתסיים את המלחמה.

לאחר גניבת המידע על הbackdoor לשלוח אלינו את הסיסמה , וברגע שנציג את הסיסמא במחשב שלנו ההתקפה הסתיימה בהצלחה , במידה ולא נצליח, גורל העולם יהיה מר…

## **מטרת ההגנה**

אנו נמצאים בעיצומה של מלחמת העולם הראשונה , בזכות מידע מודיעיני מהימן - קיבלנו אזהרה שהאויב רוצה לפרוץ למחשב שלנו ולגנוב את הסיסמה לקוד הטילים הגרעינים שלנו , עלינו לשמור על הקובץ מכל משמר ולהגן עליו בחרף נפשנו. במידה והאויב יצליח לגנוב את הסיסמה ולהציגה במחשב שלהם הפסדנו במלחמה וגורלנו נחרץ.

## **תיאור אופן מימוש ההתקפה שלנו והקשרה למאמר**

במחשב ההתקפה שלנו פתחנו שרת שממתין לחיבורים נכנסים מכל העולם , על מנת שלא נקבל הודעות ספאם ונסיונות להטעות אותנו ,פילטרנו את השרת לקבל הודעות ולהציגם אצלנו רק במידה והן מכילות את המילה השמורה: "result" (זאת מילת הקוד הסודית שסוכמה עם המרגל שלנו מבעוד מועד).

באמצעות קובץ הbackdoor ששם המרגל שלנו במחשב האויב פתחנו חיבור ישיר עם המחשב שלנו , לאחר החיבור קובץ הbackdoor ממתין להוראות , כדי שהאויב לא יצליח לנטר את ההודעה שלנו סיכמנו עם המרגל שבמידה ונשלח את הספרה "1" המתקפה תחל.

לאחר קבלת הספרה 1 , קובץ הbackdoor ינתב לתיקייה שבה נמצאת הסיסמה, הקובץ יכנס לקובץ וישלח אלינו את הסיסמה בצירוף המילה result.

לאחר קבלת המילה במחשבינו ואימות שהיא אכן הגיעה מהמרגל שלנו ולא מנסיון להטעות אותנו נציגה במחשבינו ונסיים את המחלמה בניצחון.

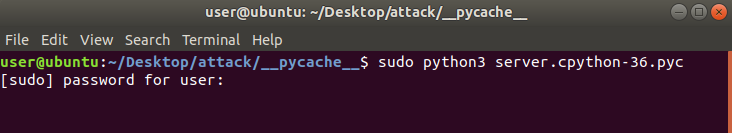
כדי שההתקפה תהיה חזקה יותר , את הפעולה שפרטנו לעיל ביצענו כ 150 (!) פעמים , כאשר בכל פעם ההתקפה תתבצע עם פורט אחר , כמחצית מהפעמים התקיפה תתבצע עם ip נוסף שהגדרנו למחשב ההתקפה שלנו מבעוד מועד כדי לבלבל את האויב.

ההתקפה כולה על בסיס המאמר שלימד אותנו להשתמש ב backdoor ולהפעיל פקודות טרמינל במחשב היריב.

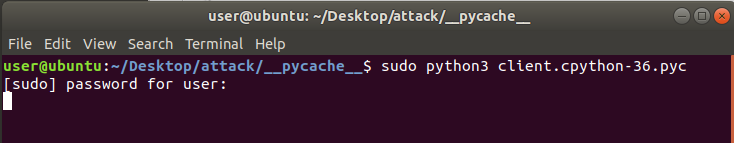
בנוסף המאמר לימד אותנו שצריך לפתוח שרת כדי לקבל את המידע ממחשב היריב.

לקחנו את ההתקפה מהמאמר ושדרגנו אותה בלפחות ארבעה היבטים שונים בזכות חומר שלמדנו בהרצאות .

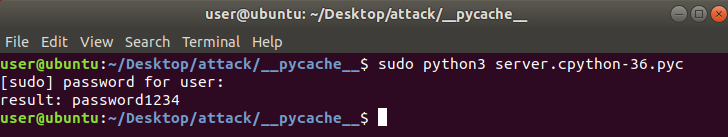
הרצת השרת במכונת ההתקפה והמתנה לחיבור:



הפעלת הקליינט (backdoor) במכונת היריב והתחברות לשרת:



לאחר חיבור השרת והקליינט ,השרת ישלח "1" לקליינט והוא יגנוב את הסיסמה וישלח לשרת עם המילה result.



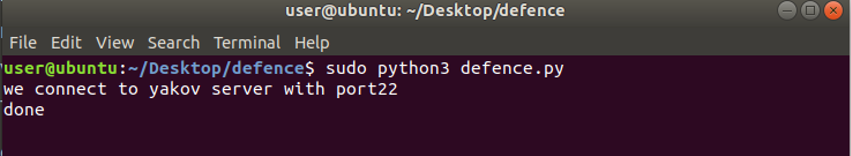
## 

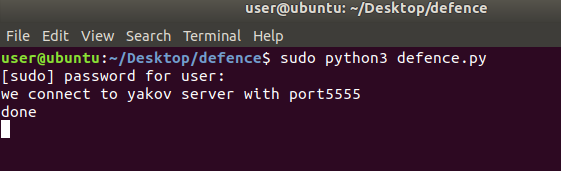
## **תיאור מימוש ההתקפה שלהם למיטב הבנתנו**

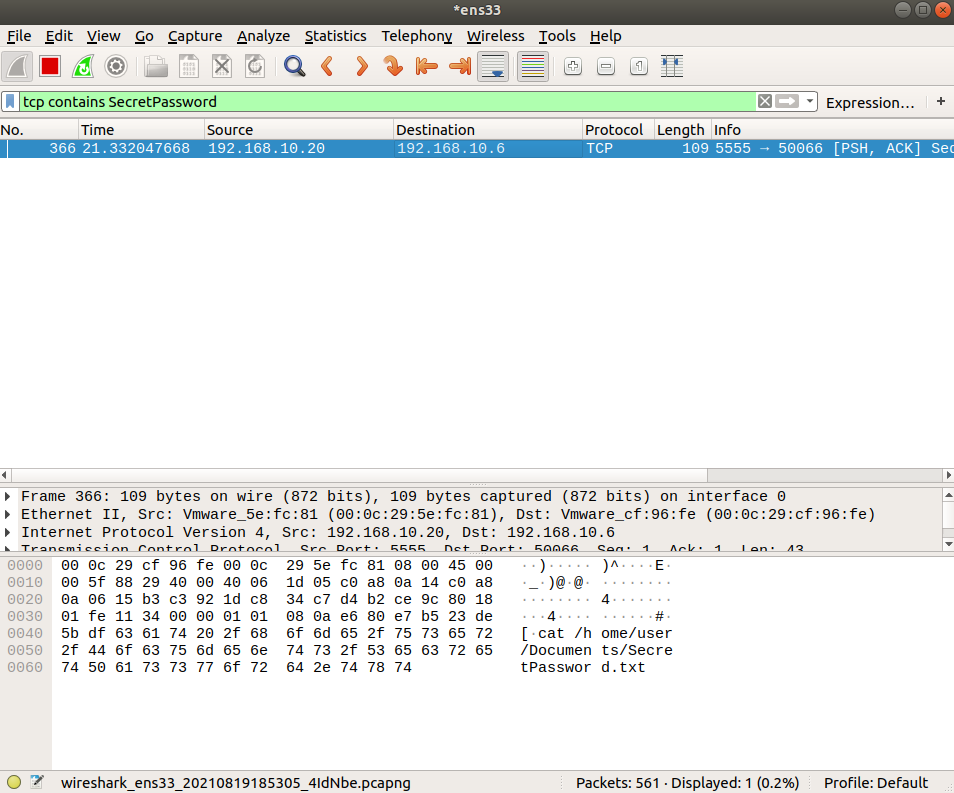
לאחר בדיקה מעמיקה גילינו את ההתקפה של היריב באמצעות ניסוי וטעייה ואימתנו את הדברים באמצעות קליטת הפקטה שלהם שנשלחה מה backdoor חזרה לשרת שלהם.

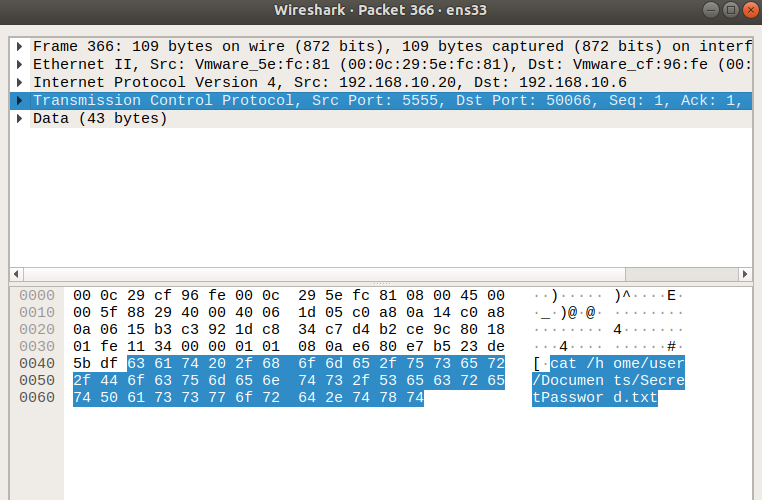
עשינו לולאה שתתחבר לשרת שלהם בכל הפורטים האפשריים וברגע שהיא מצליחה היא כותבת שהיא הצליחה ומדפיסה את מספר הפורט על המסך.

בנוסף גילינו שהפורטים שהם משתמשים בהם הם: 22 ו 5555 , ואכן הצלחנו לאמת זאת באמצעות קליטת הפקטה שאותה הצלחנו לתפוס בזכות זה שידענו שהם ישלחו ל backdoor שלהם את הפקודה שמכילה את המחרוזת "SecretPassword".

מציאת הפורט 22 על ידי ניסוי וטעייה של בדיקת כל הפורטים:

מציאת הפורט 5555 על ידי ניסוי וטעייה של בדיקת כל הפורטים:

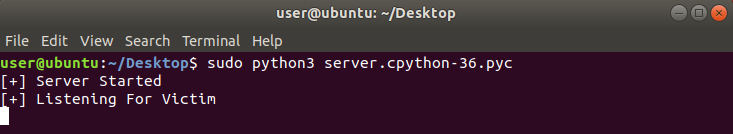
מציאת הפקטה באמצעות המחרוזת SecretPassword:

מידע על הפקטה ותוכנה ודרך ההעברה שלה:

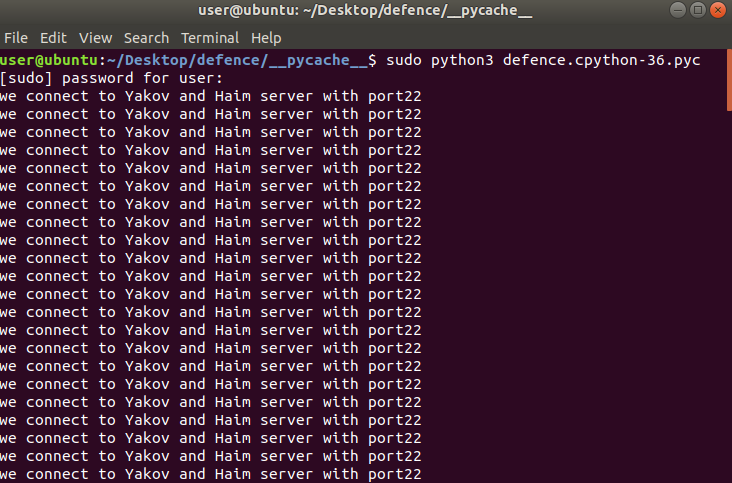
## **תיאור אופן מימוש ההגנה מפני התקפת הקבוצה היריבה**

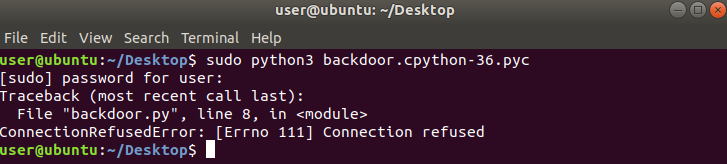
לאחר שאנחנו יודעים איך הקבוצה היריבה מנסה לתקוף אותנו הכנו קובץ הגנה שמנסה בלולאה אינסופית להתחבר אל השרת שלהם עם הפורטים 5555 ו 22 וברגע שהוא מצליח להתחבר הוא מקבל את הבקשה שלהם לפרוץ אלינו ומחזיר אליהם מחרוזת זבל כדי לסיים את ההתקפה שלהם.

הרצת השרת שלהם במחשב התוקף:

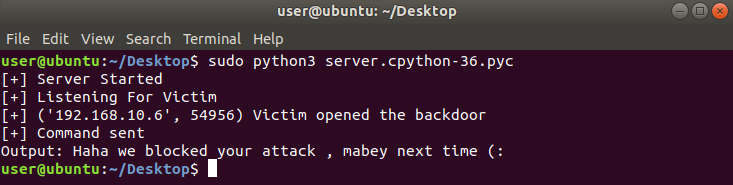


הרצת קובץ ההגנה במחשב הנתקף שלנו שמתחבר לשרת שלהם בלולאה אינסופית:



הרצת הbackdoor שלהם במקביל לקובץ ההגנה שלנו וחסימתו:

התוצאה שהשרת שלהם מקבל ומציג אצלהם כאילו זה הסיסמה שלנו:



**ניתוח סיכונים של היתכנות התקפה במציאות**

במציאות התקפה כזאת יכולה לקרות רק במידה והתוקף יצליח להחדיר מראש למכונת הנתקף קובץ הרצה שבאמצעותו יהיה אפשר להריץ פקודות ולתקשר עם המכונה השנייה (התוקפת), לאתר את הפירצה יכול להיות מאוד קל , פשוט צריך לעקוב אחרי הפורטים במחשב ולעקוב אחרי שליחת מידע לכתובות ip לא רצויות ולחסום אותן. בצבא למשל התקפה כזאת לא יכולה להתקיים כי יש להם רשת אינטרנטית משלהם ולא יהיה ניתן להשתמש במתקפה כמו backdoor כי לא יהיה ניתן לתקשר בין המחשבים.

## **מסקנות וסיכום**

לסיכום ראינו דרך מעניינת איך אפשר לפרוץ לאדם למחשב ולגנוב מידע לגמרי ללא ידיעת הבן אדם, אם הוא לא מבין בסייבר ולא למד אצל יורם הוא לא יידע שקובץ "תמים" יכול לעשות לו נזק בלתי הפיך במחשב, הקובץ ממש פותח דלת אחורית ויכול להכניס משם את כל מי שהוא רוצה למחשב האישי שלך ומאותו הרגע שום דבר לא בטוח במחשב.

בדיעבד היום אחרי הקורס הזה והפרויקט הזה אנחנו יוצאים יותר חכמים ויותר מחושבים בתחום הסייבר וההגנה, גם דברים שלא נראו לנו חשובים כמו לבדוק פורטים ושליחות מידע מהמחשב לבחוץ זה משהו שבטוח נעשה בעתיד כדי לשמור על הקבצים החשובים לנו.

החלק האבטחתי הוא החלק הכי חשוב בכל חברה , אם המוצר שחברה עובדת עליו יש בו בעיה אז תמיד אפשר לתקן ,אבל אם האבטחה לא טובה ופרטים דולפים החברה תהיה חשופה לתביעה וזה יכול להגיע למצב של זמן בבית הסוהר על רשלנות! זהו נושא מאוד חשוב שאנחנו שמחים שלמדנו אצלך.

### 

# **נספחים**

## **נספח א': מאמר הדגל המלא**

Hacking is to identify weaknesses in computer systems or networks to exploit its vulnerabilities and gaining access. Hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate-personal data, etc. Cybercrimes cost many companies millions of dollars every year. Businesses need to protect themselves against such attacks.

On the other hand, Python is a high-level powerful programming language, and yes, it is also used in hacking as it is supported on all operating systems.

Furthermore, it is relatively simple and fast to write codes in Python and, above all, thanks to its community Python has many libraries related to cybersecurity.

Among the many hacking techniques and tools, I choose to talk about backdoors: a sort of Bad-ware whose main purpose is to send and receive data, mostly commands, through a port to another system. Basically, the hacker installs a malicious program on the victim’s computer, which executes (on the victim’s computer) all the commands given by the hacker.

There are several ways through which hackers can install this malware on your computer, mainly by incorporating it into a pleasant and useful app, which is the Trojan.

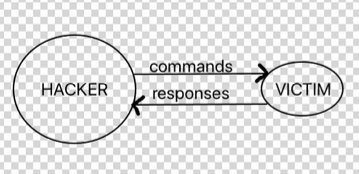
Today we will see how to create a simple and efficient backdoor that will make you understand how a computer can be easily hacked by anyone who knows how to code. Finally, I will suggest how to avoid backdoor attacks.

Getting started with the socket connection

To build our locally-working backdoor, we will use the socket module. Sockets and the socket API are used to send messages over the network.

As we already know to send messages, there’s who sends the message, here the Hacker, and who receives the message and replies, here the Victim.

After the Victim runs the malware we’ll create, it’s going to set up this type of connection between the hacker’s and victim’s machine:



Here, the hacker sends the commands, the victim executes them and returns the outputs to the hacker.

Intuitively, we have to create the tool that sends the commands and receives the outputs and the malware that executes the commands given and returns the outputs.

Creating the hacker’s tool

This tool will allow us to send commands to the victim and to receive the outputs

To build this tool, we will use the socket API by creating a socket server that sends and receives data:



Line 1: socket module imported.

Lines 4–5: defined my IP address (you have to enter yours) and the port, we used port 4444 since you are probably not using it.

Line 7: Created the Server.

Lines 8–10: Started the server.

Lines 11: Waiting for the victim to open the malware that we will create later.

Lines 12–13: when the victim (after opening the backdoor) asks the server to connect and we accept it.

By running this code, the victim will connect to our server (the hacker’s tool). Now we want the server to send commands to the victim and receive the output from the victim.



Line 1: We use the while because we want the action of sending commands and receiving output to be repeated until the program is closed.

Lines 2–5: wait for the hacker to enter the command to run on the victim’s computer, then we code it and send it

Lines 6–8: we receive the output from the victim and decode it.

The hacker’s tool is ready, but obviously, it won’t work without the backdoor.

Creating the backdoor

The backdoor is gonna connect our computer to the victim’s one. After that, it is going to receive the commands from the hacker’s tool, execute them, and send the output back to us. 

Lines 1–2: imported socket and subprocess modules. We will use the subprocess to run the commands on the victim’s computer.

Lines 5–6: define the IP of our server and the port. They must be exactly like the ones we used for the server.

Lines 8–9: created the backdoor and connected it to the server.

This code will link the victim’s computer to the hacker’s computer. Now we need the backdoor to receive the commands and send the outputs to the hacker:

 Line 1: As in the server, we use the while to repeat the action of receiving commands and sending the outputs forever until the hacker closes his tool.

Lines 2–4: the backdoor is waiting for the hacker to send the commands, so when it receives them it decodes them.

Line 5–7: Run the command and read the output and error.

Line 8: send output and error (if any) to the hacker.

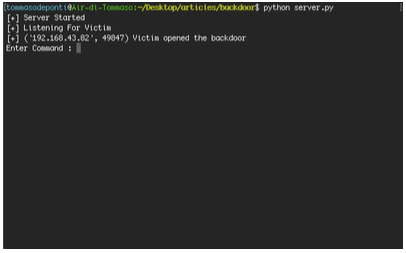
Testing

Done! Now we need to test what we have created:

• Open your terminal (UNIX) or command prompt (Windows) and run the hacker’s tool (server) with: python server.py

• Run the backdoor on the victim’s computer

On the hacker’s computer terminal you should see the following:



Now by entering the bash commands in the Enter Command input field, you will see the outputs displayed on your terminal, from which we can conclude that we have hacked the victim’s computer.

Conclusion

In this tutorial, we saw how powerful could 38 lines of python code be. The backdoor attack is powerful because it can’t always be detected; an antivirus can’t stop you installing an innocent-looking app. To embed the backdoor we’ve created in an innocent-looking app, I suggest you use the Kivy Python framework, I will write about that soon. See you in the next article!

## 

## **נספח ב': תקנון**

<https://docs.google.com/document/d/1m_e-J_sHjV7eEyS8neygSgopaJBEm6zx/edit?usp=sharing&ouid=106328805860596035095&rtpof=true&sd=true>

## **נספח ג': קטעי קוד חשובים ועיקריים**

פתיחת פורטים מ 1000 עד 4000 בקפיצות של 40 לכל פורט, פתחנו 2 ת'רדים שונים אחד לכל ip כאשר הת'רד השני יעבוד עם פורט + 1:





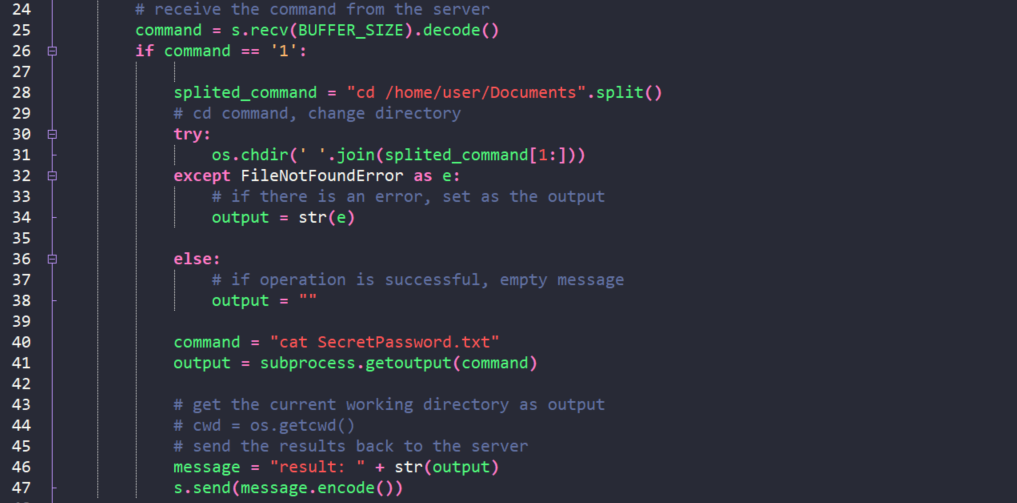
חיבור מהמחשב הנתקף לכל הפורטים שפתחנו



לאחר החיבור נשלח את הפקודה 1 בכל אחד מהפורטים לקליינט ונמתין לתוצאה



קבלת הפקודה 1 מהשרת וביצוע ההתקפה:



בדיקה שאכן התוצאה מכילה את המילה המוסכמת result ואימות ה-integrity של ההודעה

