אוריאל אברהם 315479808

תרגיל בית 1:

שאלה 1:

a)פרוטוקול ה-ARP שולח הודעה בתפוצה לכל הרשת המקומית ושואל מי בעל כתובת IP מסוימת ובARP spoofing כשהמחשב התוקף יישאל אם הוא בעל IP זה הוא יענה בחיוב ויעביר את כתובת הMAC שלו.

b)התוקף יכול לקבל הודעות או כל מידע שהיה מיועד למחשב אחר בעל כתובת הIP שהתוקף מתחזה אליה. למשל, ניתן לקרוא מידע סודי זה, למכור אותו, או אף פשוט למנוע קבלת הודעה מהמחשב שהיה אמור לקבל אותה.

c) אם התוקף יודע איזה מחשב הולך לבצע שאילתת ARP התוקף יוכל להגדיל את סיכויי ההצלחה שלו לענות ראשון בכך שהוא יישלח הודעת מענה חיובית כל זמן קצר מסוים למחשב שהולך לבצע את השאילתא, עוד לפני שמחשב זה באמת העלה את השאילתא. כך כל עוד המחשב לא ביצע את השאילתא הוא יתעלם מההודעות אך כאשר הוא יבצע את השאילתא הוא מיד יקבל תשובה חיובית מהמחשב התוקף ויחשוב שהוא מצא את המחשב בעל כתובת הIP שהוא מחפש.

d)יש הרבה שיטות יעילות פחות ויותר, אציע אחת:

מנהל הרשת יכול לשמור טבלת ARP שממפה בצורה סטטית בין כל כתובות הMAC ברשת אל הIP התואם להם.

ובמקום לשלוח הודעות בתפוצה כדי לברר מי צריך לקבל את ההודעה, נוכל להשתמש במיפוי כדי להבין איזה כתובת MAC מתאימה לIP שאליו רוצים לשלוח את ההודעה.

שיטה זו יעילה ביותר אך הבעיה בה היא שכל שינוי ברשת הנוגע לכתובות IP/MAC דורש שינוי ידני במיפוי בכל ה-hosts, ולכן בארגונים גדולים פתרון זה עלול להיות קשה למימוש.

2)ברגע שמפורסם security update יש גורמים שמבינים שיש חולשה שאפשר לנצל והם עלולים לנסות לנצל אותה וכדי שחולשה זו תישאר רלוונטית הם ינסו לתקוף את האתר שממנו ניתן להוריד את העדכון, כדי שמשתמשים אחרים לא יוכלו לקבל את העדכון ולהיות מוגנים מפני החולשה.

דוגמה שראינו לכך היא שתולעת Blaster בתאריכים מסוימים ביצעה התקפת Syn flood כנגד פורט 80 של windowsupdate.com (לא האתר הנכון בטעות)כדי למנוע ממשתמשים להוריד את העדכון שמגן עליהם מפני התולעת.

3)

a)המחשב קרס באותו היום מפני שבאותו היום רוברט טאפין מוריס שחרר את תולעת המחשב ועד מהרה היא פגעה במספר רב של מחשבים ברחבי הרשת. המחשב היה נגוע ובמהרה עוד ועוד עותקים של התולעת נוצרו במחשב עד שטבלאות התהליכים התמלאו לגמרי והמחשב קרס כי לא נשאר לו יותר זיכרון פנוי.

b) קבצי התולעת נמחקו מהדיסק כדי להסוות אותה והם היו רק על הזכרון(שהוא נדיף). לכן בעת כיבוי המחשב התולעת כבר לא הייתה בו אך לאחר הדלקת המחשב הוא נדבק בשנית והתולעת התחילה להשתכפל שוב ושוב עד שלא נשאר מקום בזכרון המחשב.

c)לכבות את המחשב, לנתק אותו מרשת האינטרנט, ובגלל שהתולעת לא שמרה את רבציה על הדיסק אז לאחר כיבוי המחשב אין לה זכר בו וכשהמחשב לא מחובר לרשת היא לא יכולה לחזור ולהדביק את המחשב.

4)

a)חולשת buffer overflow היא חולשה שבה יש buffer מגודל מסוים שנשמר על המחסנית אך כותבים לbuffer יותר בתים מאשר גודלו ואז יתר הבתים שלא נכנסו לbufferידרסו ערכים כלשהם במחסנית. תולעת יכולה לנצל חולשה זו על ידי כך שהיא תכניס לbuffer הודעה ארוכה ממה שהbuffer יכול להכיל, כך שהחלק הראשון שלה בדר"כ מיועד כדי למלא את הbuffer והחלק השני זדוני ומיועד לדרוס את תוכן המחסנית ולהכניס אליה ערכים אחרים כרצונו(למשל להחליף את כתובת החזרה מפונקצייה בכתובת אחרת כלשהי).

b)

1)תולעת האינטרנט שלמדנו עליה בתרגול 2(שניצלה את פונקציית gets)

2)תולעת Blaster שפנתה לפורט 445 במחשבים בסביבתה ושלחה לפורט זה הודעה מתוכננת היטב שחרגה מחוצץ על המחסנית.

c)תולעת האינטרנט:

ניצלה חור בfingerd שאמורה לקבל שם משתמש ולהחזיר מידע אודותיו. את שם המשתמש היא מנסה לכתוב לbuffer

בגודל 512 שהוא משתנה מקומי ולכן נשמר במחסנית, והיא עושה זאת בעזרת פונקציית gets שאינה יודעת מה כודל החוצץ וכל המידע שהיא מקבלת מוכנס לחוצץ ללא בדיקת חריגה. התולעת אכן שלחה מחרוזת ארוכה יותר בצורה כזאת שכתובת החזרה מfingerd ששמור על המחסנית יידרס ויוחלף בכתובת שבה יושב הקוד של התולעת(שגם הוא יושב על המחסנית ודרס מידע אחר כלשהו). בקוד התולעת מבצעים execve /bins/sh, כלומר מחליפים את התהליך הנוכחי בתהליך shell וכעת במחשב במותקף פתוח shell אשר מחובר לפורט עליו יושבת תולעת האם וניתן להתחיל בהדבקה של המחשב על ידי העברת תכנית ביניים דרך הport למחשב במותקף, ומתכנית זו נפעיל את התולעת.

5)לבטל את התכונה שבממוצע אחד מתוך שבעה עותקים של התולעת אף פעם לא מתאבד. כך מידי פעם ייבדק אם יש עוד עותק של התולעת על אותו מחשב ואם כן אז עותק כלשהו יתאבד ולא נישר עם עותקים שלא מסוגלים להתאבד שילכו ויתרבו.

6)זו התקפה על TCP למניעת זמינות ומטרתה היא האטת הפעילות של השרת או אף הפלתו לגמרי. היא מבוצעת על ידי כך שהתוקף שולח אל המותקף כמות גדולה מאוד של חבילות ראשונות של TCP session בבת אחת שלכל אחת מהן המותקף צריך להגיב ובגלל הכמות הגדולה, למותקף קשה להגיב. המשאב שהתקפה זו מכלה הוא התורים הקטנים של מערכת ההפעלה שמיועדים לשמירת נתונים של חיבורים שנמצאים במהלך ביצוע לחיצת יד משולשת עם המחשב הנוכחי.

<u>שאלה 2:</u>

1)מודל השכבות מתאר את האופן שבו מתנהלת תקשורת ברשתות מחשבים. כל שכבה מספקת שירותים לשכבה שמעליה ומשתמשת בשירותים שמספקת השכבה מתחתיה, וכל שכבה "מנהלת דיאלוג" עם השכבה המקבילה לה במערכת שאיתה היא מתקשרת.

<u>שכבת האפליקציה:</u> פרוטוקול התקשורת שמופעל על ידי תוכנת הקצה, עיבוד נתונים, ניהול תהליכים. התקשורת ברמת האפליקציה מתבצעת בעזרת שמות דומיין ופורטים. ברמת האפליקציה מתנהל הקשר(session) בין 2 שותפים שכל אחד מהם מיוצג על ידי כתובות IP של מקור ויעד ופרטי מקור ויעד. דוגמא: פרוטוקול http.

<u>שכבת התובלה\תעבורה:</u>

-מוודא העברה תקינה של המידע ובקצב המתאים.

-העברת תקשורת בין אפליקציות במחשבים שונים.

-סיפוק שירותים לכל האפליקציות במכונה על ידי חלוקת התעבורה בין כל האפליקציות על פי מספרי פורטים.

דוגמא:UDP/TCP.

<u>שכבת הרשת:</u> תפקידה הוא העברת חבילות בין מחשבים מרוחקים. כל הודעה שנשלחת כוללת כתובת(IP) של השולח ושל הנמען.

דוגמא: פרוטוקול IP.

שכבת הMAC: תפקידה הוא העברת חבילות בין מחשבים שכנים בעלי חיבור חוטי ביניהם. החבילה משודרת על החוט.

דוגמא: פרוטוקול Ethernet.

(2

```
PS C:\Users\user\Desktop\CS\Network Security\HW\HW1\Client-Server-Python> python client.py www.google.com 80
b'HTTP/1.1 200 OK\r\nDate: Sun, 03 Apr 2022 18:08:09 GMT\r\nExpires: -1\r\nCache-Control: private, max-age=0\r\nContent-Type: text/html
; charset=ISO-8859-1\r\nP3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."\r\nServer: gws\r\nX-XSS-Protection: 0\r\nX-
Frame-Options: SAMEORIGIN\r\nSet-Cookie: 1P_JAR=2022-04-03-18; expires=Tue, 03-May-2022 18:08:09 GMT; path=/; domain=.google.com; Secur
e\r\nSet-Cookie: AEC=AVQQ_LDLwN5TEyx2w1HPiz5PfDXPk8d-L4j_WIVE4ECGbtg4nPQlrLW0WA; expires=Fri, 30-Sep-2022 18:08:09 GMT; path=/; domain=
.google.com; Secure; HttpOnly; SameSite=lax\r\nSet-Cookie: NID=511=mWEs7lwf5sSD-bGdNiNA9g25fzuNTeY28r-KtMmptDD2JytgZ6e9smpdfNSp2BjXzgv1
mFDXhhmgQU_3Rea3p345DB-xeyHIrpHz9iSReROdQXXOzDHG6aaSCCRjIPaRqVX5ozhXfVkHm83eGVWS6AvW0XYYebdsngyb4rcrAYY; expires=Mon, 03-Oct-2022 18:08
:09 GMT; path=/; domain=.google.com; HttpOnly\r\nAccept-Ranges: none\r\nVary: Accept-Encoding\r\nTransfer-Encoding: chunked\r\n\r\n4d59
\r\n<!doctype html><html dir="rtl" itemscope="" itemtype="http://schema.org/WebPage" lang="iw"><head><meta content='
```

(3

הרצת השרת עם example.html בתור content תניב בדפדפן את:

Network Security

This is an example web page.

(4

הפקודה בשרת: python server.py 50007

הפקודה בצד הלקוח: python client.py localhost 50007

פלט הלקוח:

```
PS C:\Users\user\Desktop\CS\Network Security\HW\HW1\Client-Server-Python> python client.py localhost 50007
b'HTTP/1.1 200 OK\r\nContent-Type: text/html\r\n\r\n<!DOCTYPE html>\n<!-- saved from url=(0121)https://grades.cs.technion.ac.il/grades.
cgi?dbfehjiai2d513d0f2a0d16a2e6a29+2+236350+Spring2022+hw/WCFiles/example.html+56 -->\n<html><head><meta http-equiv="Content-Type" cont
ent="text/html; charset=windows-1252">\n    <title>Network Security</title>\n</head>\n\n<body class="vsc-initialized">\n    <h1>Network
 Security</h1>\n\n\n    <p>This is an example web page.</p>\n\n\n</body></html>'
PS C:\Users\user\Desktop\CS\Network Security\HW\HW1\Client-Server-Python>
```

5)

bind: מקשרת בין ה-socket לבין הכתובת של השרת, שהיא בעצם זוג של host ו-port(כלומר פונקציה זו מקבלת כפרמטר את (host,port)). השתמשנו בפונקציה זו בצד השרת.

listen: השתמשנו בה בצד השרת והיא מאפשרת לשרת לאשר בקשות חיבורים מלקוחות אשר מנסים להתחבר לhost ודרך ה-port שהשרת מייצג.

connect: השתמשנו בה בצד הלקוח והיא מאפשרת לו לנסות להתחבר לשרת המיוצג על ידי הצמד (host, port)

send: השתמשנו בה גם בצד השרת וגם בצד הלקוח. היא מאפשרת להעביר מידע למאזינים דרך הsocket אליו מחוברים.

recv: השתמשנו בה גם בצד השרת וגם בצד הלקוח. היא מאפשרת לקרוא מידע שנכתב ל-socket אליו אנו מחוברים.

שאלה 3:

1)מיקום מוצרי הבסיס(מוצרי חלב, ירקות, לחם ועוד...) נמצא בדרך כלל בסופרים בפינות מרוחקות של המבנה כך שהלקוח ייאלץ לעבור על פני מוצרים רבים בדרך לשם וכך אולי יעצור לקנות גם מוצרים שהוא לא דווקא חשב לקנות אותם.

2)הנדסה חברתית בהקשר של הנדסת מחשבים היא הדרך שבא תוקף יכול לתמרן, להטעות ולהשפיע על אדם שלו יש גישה למידע מסווג כלשהו כדי שאדם זה ימסור לידי התוקף את המידע המסווג.

3)הן נאלצו להשבית את מערכות הדואר האלקטרוני שלהן כדי למנוע את קריסתן.

4)ניצול באג באתר האינטרנט של חברת tmobile כדי להתחבר לרשת האינטרנט הפנימית של החברה ולקבל גישה לחשבונות הטלפון של כל הלקוחות, אך לשם כך היה צורך בשם משתמש וסיסמא של אחד מעובדי החברה. הנער הפורץ התקשר למרכז המכירות של החברה, התחזה לטכנאי, והשיג מאחד העובדים את שם המשתמש והסיסמא שלו, ובעזרתם הוא קיבל גישה לפלאפון של פאריס הילטון שהיה נעול בסיסמא. הנער ניסה לאפס את הסיסמא, אך איפוס הסיסמא היה כרוך בשאלה אישית "מה שם חיית המחמד שלך?" אך פאריס פרסמה את שם חיית המחמד ברחבי האינטרנט וכך יכל הנער לאפס את סיסמתה ומשם הייתה לו גישה לכל קבצי הפלאפון שלה.

5) היא פרסמה את שם חיית המחמד שלה ברחבי האינטרנט למרות ששם חיית המחמד שלה היה קריטי לאבטחת הפלאפון שלה. כדאי לבחור בשאלות שאת התשובות להן רק אתה יודע ובטח לא לפרסם תשובות לשאלת האבטחה בשום מקום.

6)דרך שיחה טלפונית מאוד קשה להבין אם האדם שמדבר איתך דובר אמת או מייצג את מי שהוא מתיימר להיות, לעומת שיחה פנים מול פנים שבה יותר קל לזהות שקר. התוקף ניצל יכולת זאת בכך שהתחזה לטכנאי דרך הטלפון והיה קשה לחשוד בו מפני שדרך הטלפון לא היה ניתן לדעת שהוא בסך הכל ילד בן 17 ולכן כלל לא סביר שהוא טכנאי.

7)התקפות Phishing הן התקפות מסוג של הנדסה חברתית שבדר"כ משמשות לגניבת מידע משתמש, למשל פרטי התחברות לחשבון בנק או מספר כרטיס אשראי. התוקף בדר"כ מתחזה בהודעה\מייל לישות אמינה שמבקשת ממך בתואנה כלשהי לבצע פעולות מסוימות שכוללות הכנסת פרטים אישיים כלשהם.

התקפות Spear Phishing הן התקפות Phishing שמכוונות לתקוף אדם או קבוצת אנשים ספציפית, למשל מנהלי חברות או אנשי מפתח בארגונים.

8)קניית הרבה מניות מאוד זולות של חברה כלשהי, ואז מהכסף של האדם שחשבון הבנק שלו נפרץ נקנות הרבה מניות של אותו החברה, ובגלל קנייה זו ערך המנייה עולה ומיד לאחר מכן הפורץ ימכור את המניות שהוא החזיק שכעת ערכן גבוה בהרבה.

9)גם אם ארגון מאובטח בעזרת תוכנות האבטחה הטובות ביותר, חומות אש, ואמצעים טכנולוגיים מתקדמים, הוא לא יהיה חסין מפני התקפות הנדסה חברתית שיתרגטו את החוליה החלשה בארגון וינסו לדלות מעובדים בארגון מידע מסווג, או לגרום להם לבצע פעולה תמימה מבחינתם אך כזו שתסכן את הארגון.

10)

-חינוך עובדי כל הארגון ובמיוחד אלו שיש להם קשר יומיומי עם גורמים מחוץ לחברה.

-מן הרשאות וחשיפה למידע לעובד רק כשהוא באמת צריך הרשאות אלו.

-להבהיר לעובדים לדווח לגבי כל פעילות חשודה.