הטכניון - מכון טכנולוגי לישראל

הפקולטה למדעי המחשב | סמסטר אביב תשפ״ב

הגנה ברשתות 236350

תרגיל בית מס׳ 1

הגשה: עד יום ד׳, 13/04/2022, 23:59

הגשה ביחידים

חל איסור חמור על החזקת פתרונות של סטודנטים אחרים. על כל סטודנט לרשום את תשובותיו **עצמאית** ובמילותיו שלו.

נא להגיש את התרגילים אלקטרונית בלבד

בנוגע לשאלה 1 נא לפנות להדר (hadarsivan@cs)

בנוגע לשאלה 2 נא לפנות לטל (talneoran@cs)

בנוגע לשאלה 3 נא לפנות לתום (tomazoulay@cs)

שאלה 1 – התקפות על רשתות ונוזקות

1. סעיף זה עוסק ב-ARP spoofing.
   a. תארו התקפת ARP spoofing.
   b. מה תוקף יכול להשיג מהתקפה זו?
   c. בהרצאה ראיתם שבכדי להצליח בהתקפה, על התוקף ״לענות ראשון״. תארו דרך שבה תוקף יכול לפעול כדי להגדיל את הסיכויים שלו לענות ראשון. הניחו שתוקף יודע איזה מחשב ברשת הולך לבצע שאילתת ARP.
   d. הציעו למנהל רשת דרך להתגונן כנגד התקפת ARP spoofing.
2. מדוע מומלץ למשתמשים להתקין במהירות security updates, אפילו אם לא ידוע על נוזקה המנצלת את החולשה אותה העדכון בא לתקן? תנו דוגמה מהתרגול המחזקת את טענתכם.
3. ב-2 בנובמבר 1988 ישב סטודנט באוניברסיטת MIT בחוות המחשבים והקליד לאחד המחשבים בחווה את תשובותיו לתרגיל בית אותו קיבל, אותן כתב בתחילה על דף. בכל כמה דקות שמר הסטודנט את תוכן המסמך לקובץ מקומי על המחשב. כאשר לסטודנט נותרו כשעתיים של עבודת הקלדה של המסמך, קרס המחשב עליו עבד הסטודנט. בכל פעם שהדליק הסטודנט את המחשב, הוא קרס שוב לאחר מספר דקות של עבודה.
   a. הסבירו מדוע קרס המחשב באותו יום.
   b. הסבירו מדוע לאחר שהדליק הסטודנט את המחשב לקח מספר דקות עד הקריסה הבאה והמחשב לא קרס מיד.
   c. הציעו דרך פשוטה מאוד שבה יכול היה הסטודנט (אילו היה יודע מדוע קורס המחשב) להימנע מקריסות נוספות עד שהיה מסיים לכתוב את מסמך התשובות שלו.
4. סעיף זה עוסק בחולשת buffer overflow.
   a. הסבירו מהי חולשה buffer overflow. כיצד יכולה תולעת לנצל חולשה זו?
   b. תנו שתי דוגמאות לתולעים מפורסמות שניצלו חולשה זו.
   c. בחרו אחת מהתולעים שציינתם בסעיף ב׳ ופרטו כיצד היא ניצלה את החולשה הספציפית הזו.
5. מה היה צריך לתקן בתולעת האינטרנט כדי שבממוצע יהיה רק עותק אחד של התולעת שרץ באותו מחשב?
6. הסבירו מהי התקפת syn attack, כיצד היא מבוצעת ואיזה משאב היא מכלה. מה מטרת התקפה זו?

שאלה 2 – TCP/IP

בשאלה זו תתנסו בהקמת קשר TCP/IP באמצעות מימוש שרת ולקוח HTTP פשוטים ב-Python.
קראו באינטרנט על ספריית הסוקטים של Python https://docs.python.org/3/library/socket.html. עליכם להשתמש בספרייה זו לצורך השאלה, ואין להשתמש בספריות אחרות לצורך מימוש התקשורת הנדרשת.
לאורך השאלה ניתן להיעזר באינטרנט, אך אתם נדרשים לכתוב את הקוד בעצמכם, ולענות על השאלות במילים שלכם. שימו לב שבקישור לעיל יש דוגמה שאתם יכולים להיעזר בה.

1. תארו בקצרה את מודל השכבות כפי שנלמד בהרצאה. עבור כל שכבה, הסבירו את מטרתה ותנו דוגמה לפרוטוקול בשכבה זו.
2. כתבו תוכנית המקבלת כארגומנטים בשורת הפקודה hostname ו-port ושימו אותה בקובץ client.py. על התוכנית להתחבר לשרת המתאים ולשלוח אליו בקשת GET בפורמט הבא:
   GET / HTTP/1.1
   Host: <host>
   כאשר <host> מציין את שם השרת שהתקבל בשורת הפקודה, וירידת שורה מצוינת לפי CR LF על ידי \r\n. יש לשרשר שתי ירידות שורה בסיום הבקשה, כך שהבקשה המלאה היא:
   GET / HTTP/1.1\r\nHost: <host>\r\n\r\n
   לאחר שליחת הבקשה, יש להמתין לתשובה מהשרת ולהדפיס את תוכנה. ניתן להניח שאורך התשובה קטן מ-1024 תווים, ואם הוא יהיה יותר מספיק לקרוא את ה-1024 הראשונים.

   הרצה של התוכנית מתבצעת על ידי הפקודה python client.py <host> <port> כאשר <host> ו-<port> מציינים את השרת שאליו יש להתחבר. הריצו את התוכנית עבור host=www.google.com ו-port=80, וצרפו צילום מסך של התוצאה.
3. כתבו תוכנית המקבלת כארגומנט בשורת הפקודה port ושימו אותה בקובץ server.py. על התוכנית לפתוח socket המאזין לחיבורים בכתובת localhost (127.0.0.1) על הפורט שניתן כארגומנט. כאשר לקוח מתחבר על התוכנית להמתין לבקשה ממנו, ובעת קבלת בקשה, ללא התייחסות לתוכנה, לשלוח תשובה בפורמט הבא:
   HTTP/1.1 200 OK\r\nContent-Type: text/html\r\n\r\n<content>
   כאשר <content> מציין תוכן דף HTML לבחירתכם. לצורך נוחות מצורף לתרגיל קובץ example.html המכיל תוכן לדוגמה. ניתן לקרוא את התוכן מהקובץ ולהכניס אותו כחלק מהתשובה.

   הרצה של התוכנית מתבצעת על ידי הפקודה python server.py <port> כאשר <port> מציין את הפורט שעליו מקשיב השרת. הריצו את התוכנית עם פורט לבחירתכם וגלשו בדפדפן לכתובת http://localhost:<port>. צרפו צילום מסך של דף ה-HTML שהתקבל בדפדפן.
4. הריצו את תוכניות השרת והלקוח במקביל כך שיתחברו אחת לשנייה. כתבו את שורות הפקודה שהרצתם וצרפו צילום מסך של פלט ה-client.
5. עבור כל אחת מהפונקציות הבאות ב-socket API, הסבירו את מטרת הפונקציה וציינו מתי השתמשתם בה או בגרסה שלה בתוך הקוד שלכם.
   a. bind
   b. listen
   c. connect
   d. accept
   e. send
   f. recv

אל תשכחו להגיש את הקבצים client.py ו-server.py, ולצרף את צילומי המסך הנדרשים לתשובות שלכם.

שאלה 3 – הנדסה חברתית

האזינו לפרק על הנדסה חברתית מהפודקאסט של רן לוי שנמצא באתר הקורס וענו על הסעיפים הבאים:

1. תארו יישום בחיי היומיום של הנדסה חברתית.
2. מהי הנדסה חברתית בהקשר של אבטחת מחשבים?
3. מה נאלצו לעשות הממשלות על מנת להגן על עצמן מווירוס ILOVEYOU?
4. תארו בקצרה את ההתקפה אשר הובילה בסופו של דבר להפצת מידע מהטלפון של פריס הילטון לרשת האינטרנט.
5. מה הייתה הטעות של פריס הילטון? הציעו דרך שבעזרתה היא יכלה למנוע את ההתקפה.
6. מהו הכוח הנוסף של הנדסה חברתית בתקשורת דיגיטלית לעומת הנדסה חברתית בחיי היומיום? כיצד התוקף ניצל זאת בהתקפה משני הסעיפים הקודמים?
7. מה הן התקפות Phishing? ומה ההבדל בינן לבין Spear Phishing?
8. מהי השיטה שתוארה שבה מי שהשיג גישה לחשבון בנק, יכול להעביר כסף לעצמו מבלי להתגלות?
9. מה היא הסיבה העיקרית שהתקפות של הנדסה חברתית יכולות להיות יעילות במקרים שהתקפות דיגיטליות אחרות יכשלו?
10. מהן הדרכים המוצעות לטפל בהתקפות הנדסה חברתית?