הטכניון - מכון טכנולוגי לישראל

הפקולטה למדעי המחשב | סמסטר חורף תשפ״ד

הגנה ברשתות 02360350

תרגיל בית מס׳ 1

הגשה: עד יום ה׳, 08/02/2024, 23:59

הגשה ביחידים בלבד

חל איסור חמור על החזקת פתרונות של סטודנטים אחרים.
עליך לרשום את התשובות **עצמאית** ובמילים שלך.
נא להקליד את התשובות ולהגישן אלקטרונית בלבד.

בנוגע לשאלה 1 נא לפנות ל- דיאנה (diana.cohen@cs.technion.ac.il)
בנוגע לשאלה 2 נא לפנות ל- תום (tomazoulay@cs.technion.ac.il)

שאלה 1 – סריקת פורטים, Wireshark packet sniffing

בשאלה זו תשתמשו בכלים הבאים כדי לבחון שרתים מרוחקים ותעבורה מקומית. תגלו איך ע״י סריקת פורטים פשוטה בעזרת nmap (https://nmap.org) ניתן לגלות מידע רב אודות שרת מרוחק ותלמדו כיצד להשתמש ב-Wireshark (https://www.wireshark.org) כדי לנטר ולהבין תעבורת רשת אליה יש גישה מהמחשב האישי. ניתן להתקין את הכלים הנדרשים ישירות על המחשב האישי או על מכונה וירטואלית.

חלק 1

סריקת פורטים מאפשרת לבחון אילו פורטים פתוחים על שרת כלשהו ולגלות אילו תוכנות השרת מריץ, שאליהן יש גישה מכתובת חיצונית לשרת. כך ניתן להשיג הבנה טובה יותר של ״איפה״ ו-״איך״ לתקוף את השרת הקורבן. שיטה זו של סריקת פורטים מנצלת מוסכמות מקובלות בפרוטוקולים TCP ו-ICMP, המבקשות לספק לצד השולח מידע מדוע התקשורת נכשלה (ויתכן שיותר מדי מידע).

בחלק זה יש להשתמש בכלי (Wikipedia) nmap ולסרוק את השרת scanme.nmap.org. השימוש בכלי באופן זה יאפשר לך להתרשם מכמות מידע מועיל שניתן להשיג באמצעות סריקת פורטים פשוטה.
על הסריקה שלך לקיים את **כל** הדרישות הבאות יחד:

- יש לסרוק את **scanme.nmap.org** בלבד ולא אף שרת אחר! באופן כללי, יש לסרוק אך ורק שרתים שקיבלת אישור מפורש ממפעיל השרת לסרוק אותם.
  במקרה זה, השרת scanme שייך לפרויקט nmap ונועד לצורכי לימוד הכלי (http://scanme.nmap.org), אולם יש לוודא שאין חריגה ממספר סריקות קטן ביום.
- יש להקליט את כל התעבורה במהלך הסריקה בעזרת Wireshark (ראו חלק 2).
- יש להשתמש בסריקת TCP SYN.
  רמז: מומלץ לקרוא את התיעוד של (man 1 nmap) nmap כדי למצוא את הדגל הנכון.
- יש לאפשר OS detection, version detection, script scanning ו-traceroute.
  רמז: זה דגל יחיד, היעזרו בתיעוד.
- יש לבצע סריקה מהירה: דגל T4-
- יש לסרוק את **כל** הפורטים.

לתשומת ליבך - ייתכן שבזמנים מסוימים הסריקה תחזיר פלט שונה מהמצופה. במקרה שתוצאות הסריקה שקיבלת לא תואמות את הנשאל בסעיפים יש לנסות לבצע סריקה חוזרת במועד אחר. בנוסף, הסריקה עשויה לקחת בין 10-30 דקות, כתלות בתנאי הרשת. יש לוודא שהמחשב אינו נכנס ל-sleep במהלך הסריקה.

בסיום הסריקה, ולאחר קבלת התוצאות, יש לענות על הסעיפים הבאים על פי תוצאות הריצה.
יש לענות בקצרה - תשובה עבור סעיף מסוים אמורה להיות לכל היותר שלושה משפטים.

1) מהי הפקודה המלאה בה השתמשת כדי להריץ את סריקת הפורטים שתוארה לעיל?

2) מה כתובת ה-IP של השרת scanme.nmap.org שסרקת?

3) אילו פורטים פתוחים על השרת?
   אילו אפליקציות מאזינות על הפורטים הללו?
   בסעיף זה יש לכתוב את שם השירות (service) כפי שמדווח nmap
   יש לציין את כל הפורטים פתוחים, אמורים להתקבל 4 כאלה לפחות.

4) השרת scanme.nmap.org מריץ שרת רשת. מהי התוכנה וגרסת התוכנה שבה משתמש שרת הרשת?
<u>רמז</u>: מעל איזה פורט בדרך כלל רץ שרת רשת (Web server)?

5) מהו הדגל היחיד שהשתמשת בו על מנת לקיים את הדרישה 4 מהסריקה?
מהו חסרון אפשרי בשימוש בדגל זה לצורך סריקה לקראת התקפה? היעזרו בתיעוד.

6) יש לבחור 3 מתוך 4 האפשרויות שהופעלו על ידי הדרישה 4 מהסריקה.
עבור כל אחת מאלה, יש לתת דוגמה לחלק מהפלט של הסריקה שהתקבל בעקבות הפעלת האפשרות, ולהסביר את משמעותו.

<u>חלק 2</u>

Wireshark הוא כלי לניטור תעבורת רשת מקומית. ל-Wireshark יש גישה לכל ה-headers של פקטות מידע העוברות בממשק הרשת המנוטר, והוא מציג ממשק ויזואלי שימושי המאפשר להבין את המבנה של פרוטוקולי רשת שונים. ולכן, Wireshark יכול לשמש ככלי debug לפרויקטי תקשורת.

יש להשתמש ב-(<u>Wikipedia</u>) <u>Wireshark</u> על מנת לבחון את התעבורה הנוצרת ע"י nmap במהלך הסריקה בחלק 1. עליך להתחיל את ההקלטה ב-Wireshark לפני הרצת הסריקה ולעצור אותה לאחר סיום הסריקה.
יש לוודא כי ההקלטה מכוונת לממשק הרשת מעליו רץ nmap.

לאחר קבלת התוצאות יש להשתמש בפונקציונליות הפילטרים שמספק Wireshark בשביל להבין כיצד nmap סורק פורט מסוים.
יש לענות על הסעיפים הבאים לגבי scanme.nmap.org בהתבסס על תוצאות הסריקה, מומלץ להיעזר בתיעוד:

7) הסבירו את המשמעות של פורט "סגור" בשרת scanme.nmap.org.
באופן יותר ספציפי – ציינו את סוג חבילת TCP, אם קיימת כזו, שהשרת שולח כתגובה לחבילת SYN הנשלחת לפורט שהוא "סגור".

8) הסבירו את המשמעות של פורט "filtered" בשרת scanme.nmap.org.
באופן יותר ספציפי – ציינו את סוג חבילת TCP, אם קיימת כזו, שהשרת שולח כתגובה לחבילת SYN הנשלחת לפורט שהוא "filtered".

שאלה 2 – 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) הסבירו בקצרה את צורת ההדבקה של וירוס ILOVEYOU.
מדוע היא הייתה יעילה כל כך, בהשוואה לווירוסים אחרים דומים?
ציינו מה נאלצו לעשות הממשלות על מנת להגן על עצמן מהווירוס 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) תארו מה הן התקפות Phishing ומה ההבדל בינן לבין Spear Phishing.

8) מה היא הסיבה העיקרית שהתקפות של הנדסה חברתית יכולות להיות יעילות במקרים שהתקפות דיגיטליות אחרות יכשלו?

9) מהן הדרכים המוצעות לטפל בהתקפות הנדסה חברתית?