הטכניון - מכון טכנולוגי לישראל
הפקולטה למדעי המחשב סמסטר אביב תשפ"ב

הגנה ברשתות 236350

תרגיל בית מס' 5

הגשה: עד יום ד', 15/06/2022, 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 לתום (tomazoulay@cs)
בנוגע לשאלה 2 נא לפנות לטל (talneoran@cs)

שאלה 1 – אבטחת סיסמאות ב-Unix

1. בתרגול תיארנו שלוש דרכים למימוש בקרת כניסה: "משהו שאני יודע", "תכונה שלי", "משהו שיש לי". תארו דוגמה לכל אחת מהדרכים האלו.
2. נתונה מערכת המאפשרת רק סיסמאות באורך 5 תווים בדיוק, המורכבות מספרות בלבד. הזמן הדרוש לאימות סיסמא הוא 6 שניות. כמה השהייה מכוונת (בשניות) בזמן אימות הסיסמא על בעלי המערכת להוסיף על מנת שמקדם הבטיחות יהיה 1000 שעות? עגלו את התשובה לערך השלם הכי קרוב.
3. מדוע עדיף לשמור סיסמאות באופן מתומצת, במקום להצפין אותן עם מפתח סודי שבוחר אחראי האבטחה? הסבירו.
4. במערכת Facelivre הסיסמאות נשמרות באופן מתומצת ללא salt. עומר הינו בעל גישה לקובץ הסיסמאות, והוא רוצה להוסיף לעצמו לייקים ב-Facelivre. לצורך כך הוא משתמש ב-Phishing כדי שהמשתמשים יגלו לו את הסיסמא של החשבון שלהם. אילו משתמשים כדאי לעומר לתקוף ראשון? האם שימוש ב-salt היה מקשה עליו? נמקו.
5. תמר, המנהלת שרת Unix, הציעה לבצע את השינוי הבא באלגוריתם DES' לתמצות שראינו בתרגול. להזכירכם, באלגוריתם המקורי מצפינים את הקבוע 0 באופן שתלוי בסיסמת המשתמש ובערך ה-salt. תמר תבחר קבוע סודי בן 64 ביט (נקרא לו admin_secret) ובמקום להצפין את הקבוע 0 יוצפן admin_secret.

נדון בתוקף המעוניין לתקוף את השרת. **הניחו כי לתוקף יש חשבון בשרת וכן שקובץ הסיסמאות של השרת נמצא ברשותו.** עם זאת, אין ביכולתו לשנות את דרך הפעולה של השרת, לשנות את קובץ הסיסמאות, או לבצע מתקפות אקטיביות ברשת.

השוו את השינוי המוצע מול הפתרון המקורי, בהתייחסות לנקודות הבאות:
a. האם התוקף יכול לזהות משתמשים בעלי סיסמא זהה על השרת?
b. כיצד השינוי משפיע על יכולת התוקף לפרוץ לחשבון ספציפי (משתמש נתון)?
c. כיצד השינוי משפיע על יכולת התוקף לפרוץ לחשבון כלשהו (משתמש כלשהו)?

6. בתרגול הצגנו את צורת אחסון הסיסמאות במערכות Unix, אך לא דיברנו על איך בפועל מעורב ה-salt בחישוב הסיסמא המתומצתת (שתסומן ב-EP). בסעיף זה נבחן מספר אפשרויות כיצד לשלב את ה-salt בחישוב הסיסמא, ואת יעילותן כנגד תוקף offline.

לגרסה הראשונית שהצגנו (ללא שימוש ב-salt) היו מספר בעיות, כאשר שתיים מתוכן היו:
(1) אם שני משתמשים בחרו את אותה הסיסמא קל לזהות זאת בקובץ הסיסמאות.
(2) תוחלת מספר הסיסמאות שיש לבדוק לצורך פריצת חשבון כלשהו קטנה משמעותית (לעומת תוחלת מספר הסיסמאות שיש לבדוק לצורך פריצה לחשבון מסוים).

האם האפשרויות הבאות פותרות את שתי הבעיות שהצגנו. **התייחסו לכל בעיה בנפרד** והסבירו את תשובתכם.

a. נשמור בקובץ הסיסמאות את הערך:

$$\mathrm{EP} = \mathrm{DES}^{25}_{\mathrm{user\_password}}(0) \oplus \mathrm{salt}$$

כאשר DES^{25} מסמן שמבצעים את ההצפנה 25 פעמים באופן שראינו בתרגול.

b. נשמור בקובץ הסיסמאות את הערך:

$$EP = DES_{user\_password \oplus salt \oplus 25}\left(DES_{user\_password \oplus salt \oplus 24}\left(\dots\left(DES_{user\_password \oplus salt \oplus 1}(0)\right)\dots\right)\right)$$

<u>הערה</u>: היכן שנדרש, הניחו של-salt משורשרים אפסים לכדי מחרוזת באורך הדרוש ושגודל הסיסמא תואם לגודל המפתח של DES.

שאלה 2 – IPsec

1. כפי שלמדנו, כאשר שרתי Gateway מפעילים IPsec ב-Tunnel mode, הם מוסיפים כותרת IP חדשה בה מופיעות כתובות ה-IP של ה-Gateways במקום כתובות ה-IP המקוריות.
   a. מדוע נחוצה כותרת חדשה זו?
   b. האם גרסה של IPsec שבה בכותרת החדשה ישתמשו בכתובות ה-IP המקוריות (ולא באלו של ה-Gateways) תעבוד? אם לא, מדוע? אם כן, מהם יתרונותיה וחסרונותיה של גרסה זו ביחס ל-IPsec המקורי?
2. ידוע שחבילות לא תמיד מגיעות ליעדן, ולכן TCP דואג לשלוח נתונים שנית במידת הצורך. הניחו שחבילה כלשהי מהשולח המקורי הגיעה לשכבת IPsec אצל המקבל המיועד. החבילה נשלחה ב-Transport Mode, באמצעות תת-הפרוטוקול AH, ואומתה בהצלחה ע"י המקבל. לאחר מכן, שכבת IPsec אצל המקבל קיבלה חבילה נוספת, שידוע שתוכנה הוא שידור חוזר לגיטימי של אותה חבילה ע"י שכבת TCP, או זיוף של אותה חבילה. שימו לב ש-IPsec מחויבת לזרוק חבילה נוספת זו אם היא נשלחה ע"י תוקף, אך להעבירה הלאה אם היא חבילה חוקית מ-TCP.
   הסבירו כיצד שכבת IPsec של המקבל יכולה להבחין בין שידור חוזר של החבילה שנעשה ע"י שכבת ה-TCP של השולח המקורי לבין כזה שנעשה ע"י תוקף. התייחסו למקרים הבאים:
   a. שידור חוזר ע"י שכבת ה- TCP של השולח המקורי.
   b. שידור חוזר ע"י תוקף, ללא שינוי החבילה.
   c. שידור חוזר ע"י תוקף ששינה את החבילה.
3. תארו מקרה שבו נדרש שה-SPD של שכבת ה- IPsec יכיל את הכלל הבא:

Rule	Direction	Src Addr	Dst Addr	Next Protocol	Src Port	Dst Port	ACK	Action	Additional Parameters
Generic_in	in	any	any	AH or ESP	Any	Any	Any	**forward**	

בסעיפים 4-6 מתוארים שלושה שינויים לפרוטוקול IPsec. לכל אחד מהשינויים חוו דעתכם על השיטה המוצעת מבחינת:

- אבטחה – אם לדעתכם השיטה המוצעת עדיין בטוחה, נמקו מדוע. אם לא, תארו התקפה חדשה שלא הייתה אפשרית קודם לכן.
- יעילות.

שימו לב, השינויים הינם בלתי תלויים זה בזה ויש להתייחס אליהם **בנפרד**.

4. נשנה את תהליך קבלת החבילה כך שבעת קבלת חבילה מאובטחת, נפענח אותה עפ"י ה-SPI המופיע בה, נצפין אותה מחדש עפ"י הכללים ב-SPD, ונוודא זהות לחבילה המקורית טרם שנסכים להעבירה לשכבות הגבוהות.

   התהליך המפורט נראה כך:
   - שליפת SA על סמך ה-SPI שמופיע בחבילה (נסמנו SA_1).
   - בדיקה שה-sequence number בחבילה תואם את SA_1.
   - בדיקה שה-MAC בחבילה תואם את נתוני החבילה.
   - אם אחת הבדיקות נכשלת, זרוק את החבילה.
   - פענוח החבילה באמצעות SA_1, לפי ה-IV שבחבילה.
   - שליפת SPI בודד מה-SPD, בהתאם להתאמה בין הכללים ב-SPD והחבילה המפוענחת. הניחו כי ה-SPD מחזיר SPI בודד במקום להחזיר רשימה של SPI-ים (נסמנו SPI_2).
   - שליפת SA על סמך SPI_2 (נסמנו SA_2).
   - הצפנה ואימות מחודשים של החבילה המפוענחת, באמצעות SA_2.
     נעשה שימוש ב-IV שבחבילה וב-sequence number שמופיע ב-SA_2.
   - השוואת התוצאה האחרונה לחבילה המקורית שהתקבלה. במקרה של זהות, יש לקבל את החבילה ולהעבירה לעיבוד על ידי השכבות הגבוהות. אחרת, יש לדחותה.

5. במוד ESP עם אימות והצפנה, אך ורק נתוני השכבות הגבוהות יאומתו (כרגיל, לאחר שהוצפנו). כלומר, הצפנה מבוצעת כמו ב-ESP המקורי, אך ה-MAC עבור Authentication Data יחושב אך ורק על תוצאת ההצפנה ולא על נתונים נוספים הקיימים ב-ESP Header שנכללו בחישוב ה-MAC בשיטה המקורית.

6. במוד ESP עם אימות והצפנה, שדה ה-sequence number של IPsec יוצפן אף הוא. כלומר, הצפנה מבוצעת על אותם חלקים כמו ב-ESP המקורי ובנוסף מצפינים את שדה ה-sequence number של שכבת IPsec. לאחר מכן, ה-MAC עבור Authentication Data מחושב על אותם חלקים כמו ב-ESP המקורי.