גירסה 1.01 – 11.9.2004

אבטחת סיסמאות

ניר אדר

גירסה 1.01 – 11.9.2004

- עדכוני ניסוח ועיצוב, עדכון מספר נושאים שהשתנו עם השנים.

גירסה 1.00 – 6.9.2001

- פרסום ראשון

תוכן עניינים

הקדמה

חשיבות נושא בטיחות הסיסמאות עולה בימים אלו גם בעבור כל המשתמשים במחשבים. המשתמש הפרטי הממוצע, המשתמש המתקדם, המשתמש העסקי, בעלי שרתים, על כולם לשקול את הססמאות בהן הם משתמשים.

עליית מהירות המעבדים ועליית מהירויות החיבור של אנשים לאינטרנט מגדילים בצורה משמעותית את הסיכון של פריצה למערכות. עבור המשתמש הפרטי הממוצע באינטרנט, הסיכון העיקר הוא חדירה לתיבת ה-EMAIL שלו, או שימוש בחשבון האינטרנט שלו. כאשר מדובר במשתמש מתקדם יותר, מדובר גם על ססמאות באתרי אינטרנט שונים, ססמאות על חשבונות שרתי UNIX והדוגמאות עוד רבות.

במסמך זה נציג עצות והסברים לגבי דרכים לבחירת ססמאות שיקשו על פורצים להיכנס לחשבונות השונים שלכם, ונביא דוגמאות שונות בנושא. במסמך זה נתייחס לנושא הססמאות בלבד. לפורץ הפוטנציאלי ישנן דרכים נוספות להיכנס למערכות מחשבים, מלבד לשבת מול המסך ולנחש/לפצח ססמאות, אולם במסמך זה לא נתייחס לנושאים אלו.

נציין גם כי אם הנך מנהל של שרת, ישנה חשיבות רבה לאבטחת הססמאות המשתמשים. במידה ופורץ יחדור ולו לחשבון משתמש אחד, הוא יכול להשתמש בשיטות רבות, שחלק גדול מהן מופץ באופן חופשי ברשת, על מנת להשיג זכויות מנהל ולעשות כאוות נפשו במערכת כולה.
לפיכך, הגישה הקיימת אצל אנשים שונים האומרת "לא אכפת לי מי קורא את הקבצים שלי, אז אני לא צריך ססמא טובה שתגן עליהם" פסולה, מכיוון שיתכן שהפורץ ישתמש בחשבון של משתמש במערכת על מנת להשיג אליה גישה, ולא על מנת לעיין בתוכן הקבצים של אותו משתמש. על מנהל המערכת להכיר את נושא הססמאות ולהגדיר מדיניות לגבי בחירת הססמאות במערכת.

כיצד פועל הפורץ?

כיצד פועל הפורץ? כיצד הוא משיג סמאות של משתמשים?
בחלק זה של המסמך נציג מספר שיטות בהן הפורץ יכול להשתמש.

בשתי השיטות הראשונות שנציג, לפורץ יש מידה מסוימת של גישה למערכת.
הוא הצליח להשיג את קובץ הסמאות של המערכת. בUNIX קובץ זה הוא בד"כ

```
/etc/passwd
```

קובץ זה מכיל את סמאות כל המשתמשים במערכת בצורה מוצפנת. (בגרסאות חדשות של UNIX מדובר בקובץ אחר, אך עדיין נניח שברשות התוקף קובץ הסמאות).
בנוסף לכך לפורץ יש את אלגוריתם ההצפנה בעזרתו הצפינו את הקובץ. האלגוריתמים בהם משתמשים להצפנת סמאות ב-UNIX אינם סודיים וניתן להשיגם בקלות. יתרונם הוא שההצפנה היא חד כיוונית, כלומר, אם לפורץ יש את הסמא המוצפנת, הוא אינו יכול בעזרת אלגוריתם פשוט להשיג את הסמא המקורית.
על מנת לגלות מה היא הסמא שלך, על הפורץ לנסות להצפין מילים שונות לפי בחירתו בעזרת האלגוריתם של המערכת, ולהשוות את התוצאה אל הסמא המוצפנת שמצא. אם קיימת התאמה, הרי שהמילה שהוא הצפין היא המילה המקורית.

אילו מילים יבחר הפורץ להשוות לסמא?
קיימות שתי גישות עיקריות:

1. Brute Force- הפורץ משתמש באלגוריתם ההצפנה כדי לבדוק את כל האותיות והסימנים הקיימים, אחד אחרי השני, בכל צירוף אפשרי, ומחפש האם אחת מהסמאות התגלתה. באופן תיאורטי שיטה זו אמורה להצליח תמיד, אולם באופן מעשי, זו שיטה איטית יחסית לשיטות הבאות שנתאר, ואם המשתמש בחר סמא בהתאם לקווים המנחים שיתוארו במסמך, סביר להניח שמבחינת זמן, פריצה בדרך זו לא תהיה מעשית עבור הפורץ.

2. השיטה השניה היא שימוש בקובץ מילון. גם בשיטה זו מנסה הפורץ להשוות סמאות שונות מול קובץ הסמאות המוצפן, אולם בשיטה זו הסמאות אינן כל צירוף אותיות, אלא מילים ממילון, מילים בעלות משמעות. מילון יכול להכין מאות אלפי מילים מתחומים שונים.

גישה שלישית לא מחייבת שבידי הפורץ יהיה קובץ הססמאות. בגישה זו הפורץ מנסה בד"כ מספר קטן יותר של צירופים, ולעיתים הוא יכול להקלידם ישירות למערכת. אם זאת, לפורץ עם קובץ ססמאות יש יתרון להשתמש בו, ולא להקליד את הססמאות מול המערכת מכיוון שיתכן שניסיונות התחברות כושלים למערכת נשמרים בה, וכך מנהל המערכת יוכל לדעת על ניסיון הפריצה, וגם עבודה מול קובץ ססמאות תהיה בד"כ מהירה יותר.

בשיטה זו הפורץ הוא אדם בעל ידע על בעל החשבון. הפורץ מנסה להשתמש במילים, שמות, תאריכים ומספרים המתאימים לאותו אדם. שיטה זו פחות נפוצה מהקודמות עבור הפורץ המזדמן, המחפש למצוא ססמאות במהירות, אולם אם פורץ סימן אדם מסוים כמטרה, שיטה זו עשויה לעזור לו לפרוץ לחשבון המבוקש.

למשל, חשבונות הדוא"ל של באתר של וואלה (http://www.walla.co.il). בזמן האחרון רמת האבטחה של האתר עלתה, עקב החלטת וואלה להפוך את שירות הדואר שלהם לשירות בין לאומי. נציג את המצב שהיה עד לשנה האחרונה (כ-6 שנים, מ-1998 עד 2004). למרות שביכולתך לבחור כמעט כל צירוף בתור ססמא, היתה קיימת "ססמא" נוספת לדוא"ל וואלה. במקרה ששכחת את הססמא שלך, היה עליך להזין מספר בן 4 ספרות אותו בחרת במהלך ההרשמה, וכן את תאריך הלידה שלך. נניח שפורץ המגיע לפרוץ את החשבון שלך יודע מהו תאריך הלידה שלך, עליו לנסות רק 9999 צירופים שונים (ובמונחים של אבטחת ססמאות זה זניח. פורץ עם מודם K56 יכול לפרוץ לכל חשבון בוואלה בתוך פחות מ-10 דקות). בקטגוריה זו נכנס גם שם החשבון שלך. אם שם החשבון שלך הוא mcohen ושמך הוא Moshe Cohen,אזי ססמאות כגון:

Mcohen, moshe, Moshe, cohen, MOSHE, [moshe]

וכדומה, הן ססמאות גרועות.

כעת, לאחר שהצגנו את הבעיה, נסביר כיצד אתה, המשתמש, יכול לשפר את רמת האבטחה של הססמא שלך.

בחירת שם משתמש

לא תמיד הנך יכול לקבוע את שם המשתמש שלך במערכת, אולם במקרים שניתנת לך הבחירה, ישנן מספר שיקולים שעליך לשקול:

1. האם זהו חשבון דואר אלקטרוני או חשבון דומה, שאנשים אחרים מלבדך יצטרכו לזכור? במידה שכן, על שם החשבון לרמז על בעליו. אם שמך Moshe Cohen, אזי שם משתמש כגון moshe, או mcohen הוא בחירה הגיונית. לעומת זאת, אם אנשים אחרים מלבדך, אין להם צורך בשם המשתמש שלך, מומלץ לבחור שם משתמש שלא ירמז על שום פרט לגביך.
2. שם משתמש המכיל תעודת זהות, או פרטיים אישיים כגון כתובת או טלפון, הוא לרוב גרוע, מכיוון שהוא מעניק לפורץ הפוטנציאלי מידע נוסף עלייך.

בחירת הססמא

נושא זה הוא הקריטי ביותר, והבעייתי ביותר.
למרות שהרבה אנשים מודעים לכך שקיימים אנשים המנסים לפרוץ ססמאות, אנשים רבים מאמינים שהנושא לא נוגע אליהם – "לי זה לא יקרה". זו אחת מהטעויות הקשות ביותר. אבטחת ססמאות חשובה לכל אחד. "פורץ" הוא לא רק גאון מחשבים מסתורי שיושב במרתף כל היום ומנסה לפרוץ ססמאות. חבר/ה לשעבר, עובד במקום העבודה שלך, עמית ללימודים, מתחרים עסקיים – כולם פורצים פוטנציאלים. אנשים אלו לרוב מכירים אותך, ויש להם מידע עליך. (וגם סיבות לפרוץ אליך). רק מכיוון שלא שמת לב שפרצו אליך, זה לא אומר שלא פרצו אליך. אם הפורץ הוא מתחרה, למשל, סביר להניח שהוא ינסה למצוא מידע סודי שלך, ולהשאיר כמה שפחות עקבות.

לפיכך, ססמאות הקשורות אליך הן גרועות. שמה של אשתך, תאריך הנישואין, תאריך יום ההולדת, מספר הטלפון שלך, מספר כרטיס אשראי, צירופים שונים של שמך ושם המשפחה שלך, מספר לוחית הרישוי של רכבך, כל אלו הן ססמאות מאוד גרועות. לישראלים יש מנהג נוסף שהוא פסול – כתיבת שמם בעברית, אבל כאשר המקלדת של המחשב במצב אנגלית, לדוגמא, מישהי בשם מאיה, עם הססמא nthv.

הדוגמאות הנוספות הן רבות. הקו המנחה הראשון בנוגע לבחירת ססמא טובה הוא שלא יהיה לססמא שום קשר אליך. הקו המנחה השני הוא שאסור שהססמא תהייה בעלת משמעות מילולית כלשהי.

מחשבה כגון "מי יחשוב על המילה הזו" מתבססת על ההנחה השגויה שהפורץ יסתפק בניסיונות ניחוש של הססמא. כל ססמא המבוססת על מילה בעלת משמעות ניתנת לפריצה בקלות בעזרת תוכנה מבוססת מילון. מילה בעלת משמעות היא לאו דווקא מילה הנמצאת במילון רשמי. שמות של אנשים, של מקומות, של מפורסמים, של דמויות מצויירות הן גם ססמאות גרועות. שמות מאגדות, מסיפורי מד"ב, מילים מקצועיות מתחומים שונים – את כולם ועוד ניתן למצוא בתוך קובץ הססמאות של הפורץ.

המנע גם מססמאות קלות להקלדה בהן קיים שימוש שכיח, דוגמת הססמאות הבאות:
abcd, ***, XXX, 12345678, 12345, 1234 וכו'.

הססמא "password" היא הססמא הכי גרועה שאתה יכול לבחור. (רמז דק לספקית AquaNet, המגלה חיבה יתרה לשימוש בססמא זו).

מהן ססמאות טובות?

ססמא המבוססת על תווים אקראיים ומכילה אותיות גדולות וקטנות, אותיות ומספרים, היא הטובה ביותר, אולם לרוב האנשים קשה לזכור ססמא כזו. כיצד ניתן בכל זאת ליצור ססמא סבירה שקל לזכור?

השיטה הקלה ביותר המספקת אבטחה סבירה, אבל לא אידיאלית, היא לחבר שתי מילים שונות למילה אחת. מומלץ שבין מילים אלו לא יהיה קשר. למשל foodworm – שתי מילים שקל לזכור, שאין להן משמעות ביחד למרות שלכל אחד מהן כן יש משמעות.
ברגע שחלק מהאותיות בססמא יהיו גדולות (Uppercase) וחלקן קטנות, רמת הבטיחות של הססמא עולה בצורה דרסטית. אפילו אם רק אות אחת בתוך הססמא היא גדולה, הזמן שייקח לפרוץ את הססמא יכול לעלות במאות אחוזים.

אם ניתן לשלב בתוך הססמא מספרים או סימנים אחרים שאינם אותיות, רמת האבטחה עולה עוד יותר. הססמא FunNy!passwoRd למשל, תהיה קשה ביותר לפיצוח בשיטות שתוארו לעיל.
נקודה נוספת היא שססמא שמספר האותיות שלה רב יותר, תהיה קשה יותר לפיצוח (בייחוד אם הפורץ מנסה לפרוץ אותה בשיטת Brute Force).

יש להזכיר ולהדגיש את מה שנאמר בתחילת חלק זה של המסמך, שססמא אקראית לחלוטין היא הטובה ביותר. אפילו ססמא של 5 תווים יכולה להיות בלתי פריצה בזמן סביר.
ססמא טובה יכולה להיות למשל: sG4xaT .

סיכום

1. קיימת חשיבות לגבי בחירת הססמא עבור כל משתמש, בלי קשר לשימוש של החשבון המסוים.
2. במידה וישנה האפשרות, יש צורך להקדיש מחשבה לבחירת שם המשתמש. בחר שם משתמש המוסר פרטים עלייך (כגון שם או ת.ז.) אך ורק אם אנשים אחרים יצטרכו לדעת את שם החשבון על מנת לשלוח לך דברים. במידה ולא, בחר שם משתמש שאין לו שום קשר אליך.
3. אל תבחר ססמאות שהן מילים בעלות משמעות. המחשבה "אף אחד לא יחשוב על המילה הזו" מבוססת על הנחה מוטעית שהפורץ לא יעשה שימוש בתוכנה אוטומטית על מנת לפרוץ את הססמא.
4. אל תבחר ססמאות הקשורות אליך, למשפחתך או לכל פן אישי אחר שלך.
5. אם ניתן, השתמש בססמאות אקראיות, המשלבות מספרים אותיות גדולות וקטנות.