עקיפת סיסמאות BIOS ו-WINDOWS

מאת Fareid

מסמך זה הורד מהאתר http://underwar.livedns.co.il.

מה במסמך

מסמך זה מדגים כיצד לעקוף סמאות של מערכות שונות.

נושאים:
1. סמאות BIOS
2. סמאות במערכות Windows 9x
3. סמאות במערכות Windows XP/2000

סמאות BIOS

ההגנות של ה-BIOS מתחלקות לשני סוגים

1. סמא המונעת גישה אל ה-BIOS
2. סמא המונעת גישה אל ה-BIOS וגם מונעת את הפעלת המערכת.

סמא המונעת גישה אל ה-BIOS

עבור סמא סוג זה, יש דרכים רבות לעקוף אותה.

הדרך הראשונה היא כך לנסות לעבור את הסימה באמצעות סימאות המאסטר. סמאות אלו הן סמאות המוגדרות כחלק מהמעבדים ופועלות תמיד, ללא תלות בסמא שבחר האדם שהגן על המערכת. הסמא המתאימה לכל מעבד תלויה בסוג המעבד.

להלן רשימה של סימאות ל-BIOS נפוצים שונים של AWARD+AMI:

AWARD

AWARD_SW, ?award, 013222221EAAh, 256256589589, 589721, admin, alfarome, aLLy, aPAf, award, AWARD SW,award.sw, AWARD?SW, award_?, award_ps, AWARD_PW, awkwardBIOS, bios*, biosstar, biostar, CONCAT,condo,CONDO,djonet, efmukl, g6PJ, h6BB, HELGA-S, HEWITT RAND, HLT, j09F, j256j262, j322, j64 lkw peter, lkwpeter, PASSWORD, SER, setup, SKY_FOX, SWITCHES_SW, Sxyz, SZYX, t0ch20x, t0ch88, TTPTHA, ttptha, TzqF, wodj, ZAAADA, zbaaaca, zjaaadc, zjaaade

AMI

589589, A.M.I., aammii, AMI, ami, AMI!SW, AMI.KEY,ami.kez, AMI?SW, AMI_SW, AMI~, ami°, amiami, amidecod, AMIPSWD, amipswd, AMISETUP, bios310, BIOSPASS, HEWITT RAND, KILLCMOS

דרך שניה לעקיפת הסמא עם בעזרת תוכנות המיועדות לכך, כגון KILLCMOS. תוכנות אלו מנקות את ה-CMOS שנמצא בחריץ ה EEPROM של ה-BIOS, וכך הם מנקות גם את הסיסמה.
הפעלת התוכנה היא פשוטה – לאחר הורדת התוכנה והפעלה, היא מבצעת את פעולתה באופן אוטומטי ושקוף למשתמש.

הדרך השלישית לפרוץ ידנית ולנקות את ה- CMOS ידני באמצעות פקודות ASSEMBLY.

נפעיל את Windows, נפתח חלון DOS ונרשום את הפקודות הבאות:

```
Debug
O 70 2e
O 71 ff
Q
```

פקודות אלו מנקות את ה-CMOS ועל ידי כך מסירות את הסיסמה.

סמא המונעת גישה אל ה-BIOS וגם מונעת את הפעלת המערכת

האפשרות הראשונה היא לנסות שוב את סמאות המאסטר, בהתאם לסוג המעבד. רשימת הסמאות שניתן לנסות זהה לזו שהצגנו לעיל.

אם אחד הסיסמות עברה בהצלחה נוכל לשנות את הסיסמה לסיסמה חדשה מתוך ה-BIOS. אם הסמאות לא עבדו, האפשרות היחידה שנשארה היא לפתוח את המחשב ולנקות את ה CMOS.

יש שתי דרכים לעשות את זה :
דרך ראשונה להוציא את הבטריה לכמה שניות ולאחר מכן להחזיר אותה. לעתים שיטה זו מנקה את הסמא.
במידה ולא, הדרך השניה היא זו: לרוב ליד הבטריה ישנו מגשר. נוציא אותו מפינים 2-1, נכניס אותו לפינים 3-2. נחכה כמה שניות ונחזיר אותו למקומו. שיטה זו תנקה את ה-CMOS.

שיטות אלו מיועדות למחשבי PC רגילים ולא למחשבים ניידים. במחשבים ניידים הדרך מסובכת יותר, והיא לא תכלל במסמך זה.

סמאות במערכות Windows 9x

מערכות Windows 9x אינן מספקות הגנה ממשית. על מנת לעבור מערכת כזו מוגנת סמא, נפעיל מחדש את המחשב ועם עלייתו נזיק במקש (CTRL) לחוץ, עד שנראה את התפריט של Window, בו נבחר באפשרות (Command Prompt Only). נכנס את ספריית השורש של Windows (לרוב זוהי הספרייה C:\Windows) ונכתוב את הפקודה הבאה:

```
Del *.pwl
```

פקודה זו מוחקת את קבצי הסיסמאות. בפעם הבאה ש-Windows יעלה הוא יבקש מאיתנו סמא חדשה עבור המשתמש :-)

סמאות במערכות Windows XP/2000

כאשר באים לפרוץ את הסמא של מערכות אלו, צריך לשים לב שעבור מערכות כאלו הפועלות מעל מערכת קבצים מסוג NTFS, יש צורך בגירסת DOS שתומכת במערכת קבצים זו. אם מערכת הקבצים היא FAT, העבודה קלה יותר. בעלי NTFS יכולים להשתמש בתוכנה NTFSPRO. לאחר ההורדה של תוכנה זו והפעלתה, התוכנה תיצור דיסקט אתחול כולל את התמיכה בכונני NTFS.

בעלי מערכת FAT פועלים בצורה הבאה. ניצור תקליטון אתחול כך:
לוח הבקרה => הוספה הסרה של תוכניות => תקליטון אתחול. נלחץ על "יצירת תקליטון אתחול" ונעקוב אחרי ההוראות. לחילופין, ניתן להוריד קובץ שמיצר באופן אוטומטי את התקליטון מהאתר http://www.bootdisk.com.

לאחר יצירת התקליטון, נאתחל את המחשב מהתקליטון.
עבור מערכות המבוססות על FAT, בזמן העליה נבחר באפשרות COMPUTER START WITHOUT CDROM SUPPORT.

כאשר נקבל Dos Prompt נרשום את הפקודה:

```
Del x:\windows\system32\config\sam
```

X: מסמן את המחיצה שבה מותקנת מערכת ההפעלה שלכם.

מה בעצם עשינו?
מחקנו את הקובץ שמכיל את הסיסמות המוצפנות ע"י ה SYSKEY. בפעם הבא שנכנס ל-Windows נוכל להכנס בלי סמא אל חשבון ה-Admin.