גירסה 2.00 – 14.3.2002

בעיות אבטחה בWindows

מסמך זה הורד מהאתר http://underwar.livedns.co.il.
אין להפיץ מסמך זה במדיה כלשהי, ללא אישור מפורש מאת המחבר.
מחבר המסמך איננו אחראי לכל נזק, ישיר או עקיף, שיגרם עקב השימוש במידע המופיע במסמך, וכן לנכונות התוכן של הנושאים המופיעים במסמך. עם זאת, המחבר עשה את מירב המאמצים כדי לספק את המידע המדויק והמלא ביותר.

כל הזכויות שמורות ל**ניר אדר**

Nir Adar
Email: underwar@hotmail.com
Home Page: http://underwar.livedns.co.il

במסמך זה נציג בעיות אבטחה בWindows, המאפשרים למשתמשים לבצע פעולות שונות במערכת למרות הגבלות שהוטלו עליהם.
אחת הבעיות הגדולות ביותר של Windows היא אבטחה כנגד אנשים בעלי גישה כלשהי למערכת, המנסים להשיג גישה גבוהה יותר. אף אחת מגירסאות הWindows בשוק אינה מאפשרת אבטחה מלאה למערכת.

במהלך כתיבת מסמך זה נעזרתי במסמך שנכתב במקור על ידי Bio ב1995, בשם "How To Hack To Resist Windows 95 Systems".
מסמך זה מכיל נקודות רבות משם, שחודשו על מנת להתאים לימים אלו, וכן נושאים חדשים נוספים.
ידע קודם הנדרש עבור המסמך : שליטה בסיסית בWindows ובDos.

מחשבים ציבוריים הם מחשבים אליהם כל אדם יכול להיכנס, או לחילופין מחשבים המשרתים מספר גדול של אנשים, כדוגמת מחשבים בספריות, בחדרי מחשבים, ב"אינטרנט קפה" למיניהם והדוגמאות עוד רבות.
רבים ממחשבים אלו מוגבלים על ידי תוכנות עזר שונות, ועל ידי Windows עצמה, על מנת שהמשתמשים בהם לא יזיקו למערכת, או לא יפעילו תוכנות שמנהל המחשבים לא רוצה שהמשתמשים יפעילו.
אם זאת, להגנות אלו בעיות רבות, וקיימות דרכים רבות לעקוף אותן.
דוגמאות לתוכנות מגבילות הן למשל התוכנה KIOSK, שמונעת מהמשתמש גישה לחלק מהאפשרויות בתפריטים, לדוגמא General Preferences בתפריט האפשרויות ב-Netscape, או השורה Connect to בתוך Telnet ב-Windows 95.
תוכנה פופלרית נוספת היא Fortress 101, המאפשרת חסימת תפריט ה"התחל", מניעת צפייה בקבצים, ועוד.
דרכים נוספות להגביל את המשתמש הן, למשל, מניעת האפשרות להעלות את המערכת דרך דיסקט או דיסק, ומניעת הכניסה לSetup של המחשב על ידי ססמא.
לכאורה נראה שניתן ליצור מערכת מוגנת, אך לא כך.

#1

בWindows 95, ישנה תוכנה בשם TaskMan. זוהי תוכנה קטנה המופעלת על ידי לחיצה על Ctrl+Esc במסך הססמאות בכניסה ל-Windows 95. תוכנה זו מאפשרת לך להריץ תוכניות במחשב. ניתן למשל להריץ את Command.Com על מנת לקבל Dos Shell, או להריץ את Explorer.exe, ולהיכנס לWindows בלי סיסמא. והאפשרויות עוד רבות.
TaskMan יוצר פירצת אבטחה המאפשרת למשתמש לעקוף את ההגנות שהוטלו על המחשב.
הדרך היעילה ביותר, כמנהל, לחסום פירצה זו, היא מחיקת TaskMan.exe מספריית Windows.

#2

בעיה חמורה נוספת בWindows 95 וגם במערכות Windows 98 : ניתן להיכנס למערכת גם ללא כל ססמא! כל מה שצריך לעשות, הוא במסך הפתיחה של Windows, כאשר המחשב דורש סיסמא, ללחוץ על Windows .ESC יעלה עם הגבלות מסוימות (למשל סיסמאות אינטרנט ואחרות לא יהיו נגישות), אולם אין חסימה של ממש על מנת להיכנס למערכת.
אין פתרון לבעיה זו שאותו מספקת מערכת ההפעלה. אם על מחשב מותקן Windows 95 או Windows 98, המשמעות היא שבעל המחשב מוכן לאפשר גישה למערכת לכל אדם שידרוש בכך.
האפשרות היחידה לעקוף מגבלה זו היא על ידי התקנת תוכנת צד שלישי כלשהי, שתספק מערכת ססמאות מאובטחת לWindows.

#3

גם לאחר שTaskMan הוסר מהמערכת, ישנן דרכים נוספות לעקוף את ההגבלות שתוכנות שונות מטילות על המחשב.
מלבד TaskMan, ישנה עוד תוכנה, הקשורה קשר הדוק לWindows, המיועדת לטיפול בקבצים. תוכנה זו ה-Explorer.
כמעט בכל תוכנית של Windows, ישנו הדיאלוג "פתח קובץ" או "שמור קובץ" הסטנדרטי של Windows. אם נפתח דיאלוג זה, ונלחץ עם המקש הימני של העכבר על

אחת הספריות, נוכל לבחור Explore (סייר), וחלון של Explorer יפתח. טריק זה יעקוף את רוב תוכנות ההגנה, שמטרתן העיקרית היא למנוע מהמשתמש גישה ישירה לקבצים.
הדרך לחסום את פירצה זו : למצוא תוכנה המסוגלת למחוק את פקודת הExplore מהמקש הימני במצבים אלו.

4#

גם אם כל צעדי ההגנה שפורטו לעיל ננקטו, עדיין סביר להניח שיש פרצות למערכת. ישנן תוכנות רבות לטיפול בקבצים, למשל ProgramManager מWindows 3.11. המשתמש גם יכול להביא איתו (על דיסקט למשל), תוכנה אחרת המטפלת בקבצים, ולהריץ אותה.
הפתרון : על תוכנת ההגנה שמותקנת במחשב, להיות מסוגלות למנוע או להגביל הרצת קבצי EXE.

5#

גם אם נמנעת באופן מוחלט הרצת קבצים דרך המקש הימני, עדיין ישנה פירצה נוספת בדיאלוג זה.
אם המשתמש יכול ליצור קובץ כלשהו עם סיומת של תוכנה מבוקשת, ניתן יהיה לפתוח קובץ זה. Windows יקרא אוטומטית לתוכנה שתריץ קובץ זה, וכך ניתן להריץ תוכנות גם בדרך עקיפה.
הדרך היחידה לחסום פירצה זו, היא על ידי מערכת מבוססת משתמשים כגן Windows NT, בה ניתן להגדיר שלמשתמש מסוים אין הרשאות גישה לספריית התוכנה.

6#

אם במחשב מותקנות תוכנות Dos ישנות שרצות תחת Windows, יתכן שיש בהן את האפשרות לקבל Dos Shell.
אם כן, אבטחה המיועדת לסביבת Windows לא תועיל במקרים כאלו.
פיתרון אפשרי לבעיה : הימנעות משימוש בתוכנות כאלו. בימים אלו, לכל התוכנות כמעט יש גירסאות או מקבילות המיועדות לרוץ תחת Windows.

7#

מקרואים – במחשבים הכוללים VBScript, כגון Microsoft Office, ישנה אפשרות לכתיבת Macros, שאלו למעשה קטעי תכנות קצרים, הבאים להפוך פעולות שונות לאוטומטיות.
נריץ למשל את Word. נלחץ על "כלים", "מאקרו", נבחר שם למקרו ונלחץ "צור". נוכל, למשל, לכתוב את השורה הבאה :

```
Shell("<Any File>")
```

<Any File> יכול להיות Explorer, Command.com, וכדומה. אם הגישה לקבצים אלו חסומה, ניתן למשל לקרוא לwinfile.exe, מנהל הקבצים של Windows 3.11.
פקודה זו תריץ את התוכנה המבוקשת.

#8

תיכנות.
מול המתכנת לרוב ההגנות אין הרבה מה לעשות.
אם מתכנת עובד מול מערכת, הוא מסוגל לשחזר את כל השירותים שהוגבלו, על ידי יצירה מחדש שלהם.
למשל, הגבלת גישה ל Registry לא תועיל בהרבה, כאשר המתכנת יבוא עם Registry Editor שכתב בעצמו.
הגבלת גישה לקבצים לא תעזור בהרבה כאשר המתכנת יגיע עם מנהל קבצים שכתב.
אפילו הגבלת הרצת קבצי EXE לא תוכל לעזור, כי למשל, שפת המקרו VBScript כוללת כמעט את כל המרכיבים של השפה, ומאפשרת קריאה, מחיקה, ושינוי של קבצים, ובעצם מאפשרת גישה אליהם.

מול המתכנת הדרך היחידה להתמודד היא הגבלות במערכת ההפעלה.
חסימה של משתמש מסויים לגשת לקבצים, שתיתמך על ידי מערכת ההפעלה ולא תהיה קשורה לשום תוכנת עזר.
יש לשים לב שיש להגביל את כל הקבצים עליהם צריך להגן, וכל פעם שמותקנת תוכנה חדשה, יש לדאוג להגבלת הגישה אליה, וכן יש לבדוק שתוכנה זו לא משנה את ההגנות הקיימות.

סיכום

הנקודות שרציתי להציג במסמך זה, הן הבעייתיות הקיימות בהגנה על מערכות מבוססות Windows מפני משתמש שיש לו גישה מסוימת למחשב, וכן דרכי מחשבה לפריצה ולהתגוננות. הצגתי רעיונות כיצד לעקוף הגנות שונות, לצד הדרכים להתגונן מפני רעיונות אלו.
לא ניתן ליצור מערכת מוגנת לחלוטין. תמיד יש לזכור שככל שהמערכת מוגנת יותר היא שמישה פחות ורצה לאט יותר. על מנהל המערכת להחליט באילו אמצעים הוא רוצה להגן את המערכת, על אלו הוא מוותר, ומי האנשים המורשים להשתמש במחשבים.

EOF