סקירה על "סוסים טרויינים".
מהם ואיך מתגוננים מפניהם.

קודם כל, מדוע נקראים כך?
במלחמת טרויה נגד יוון, שלח מלך יוון סוס עץ ענק, כמנחת שלום למלך טרויה.
שומרי הארמון של המלך, שחשבו שזוהי מנחת שלום פתחו את השערים ונתנו לסוס הענק לעבור. מה שהשומרים לא ידעו זה שבתוך הסוס הענק מסתתרים בערך 10,000 חיליים, אשר מחכים לרדת הלילה. כדי לצאת מהסוס החלול ולתקוף את העיר.
וירוסים מסוג "סוס טרוייני" נקראים כך כי הם קבצים, אשר המחשב מזהה כקבצים לכל דבר, ונותן להם להיכנס למחשב.
ברגע שהקורבן נכנס לאינרטנט, ההאקר ששלח לו את הוירוס יכול להיכנס למחשבו דרך תוכנת הסוס הטרייני ששלח לקורבן התמים ולמחוק, להעתיק, לשנות ובעצם לעשות כל פעול שבעל המחשב עצמו יכול לעשות (כל תנועה בין מחשב באינרנט לבין תוכנה מותנית ברשות מן התוכנה אשר מקבלת את המידע, הסוס הטרוייני כמובן ירשה להאקר להיכנס למחשבכם ולעשות מה שיחפוץ).

מילון מונחים קצר שאולי יבהיר כמה דברים:

NetBus	תוכנת הפריצה אולי הכי מפורסמת (בגירסאות האחרונות היא מופצת ככלי לניהול רשתות).
SubSeven	תוכנה לא ממש מפורסמת אשר פועלת בסגנון נטבאס.
DeepThroat	תוכנה לא ממש מפורסמת אשר פועלת בסגנון נטבאס.
NetBuster	תוכנה המזהה פריצה ע"י נטבאס ומשמידה את תוכנת הנטבאס של התוקף.
Port	ערוץ תקשורת (פרטים בהמשך)
IP	כתובת המחשב שלך, המידע הכי חשוב שהאקר צריך כדי לפרוץ למחשבך.
FireWall	"קיר אש", תוכנה החוסמת כניסה לא מורשית למערכת (פרטים בהמשך)
LAN	**L**ocal **A**rea **N**etowrk הרבה מחשבים אשר מחוברי דרך מחשב מרכזי, במחשבים המחוברים לא חייב להיות מודם.

Ports:
פורט, הוא ערוץ תיקשורת. ערוץ תקשורת משמש לשליחת מידע למקומות שמחשבך מתקשר אליהם, לדוגמה:

כשאתם מפעילים את הדפדפן וגולשים לאתר החביב עליכם, מחשבחם מפעיל את פורט 80 כדי לתקשר עם האתר, דרך ערוץ זה מחשבכם גם שולח וגם מקבל מידע.
כשאתה מוריד שירים דרך "נאפסטר" (למי שלא מכיר זוהי תוכנה מפורסמת להורדת שירים) המחשב מתקשר עם המחשב שממנו הוא מוריד את השיר דרך פורט 6699 (נקבע כברירת מחדל), או כשאתם מדפיסים מסמך, המחשב מתקשר עם המדפסת דרך פורט מסוים.
בתוכנת "ווינדוס" (Windows), יש באג (תקלה) קטן אשר משאיר את פורט מספר 139 פתוח. דרך פורט זה אפשר לפרוץ למחשבים דרך תוכנות מיוחדות.
רק כדי להיכנס לקנה-מידה, ישנם יותר מ65,000- פורטים.

מה עושים ?

פיתרונות:

FireWalls:
תפקידה של תוכנות קיר האש הוא להשגיח על העברת המידע בין מחשב מרוחק למחשבך, היא משגיחה על הפורטים הפתוחים וחוסמת כניסה לא מורשית של האקרים.
טיבה של תוכנות קיר האש נמדד ביכולתה לסגור את הפורטים אשר לא נמצאים בשימוש.

תוכנות אנטי וירוס:
(רשימת אתרי ההורדה בסוף)

ESafe Protect
שילוב בין תוכנת "קיר אש" לבין אנטי ווירוס, אחת הטובות בתחום ! מומלץ ! מגיעה גם בעברית

McAfee:
האנטי ווירוס של **מקאפי**, מפורסם מאוד וחזק מאוד.

תוכנות קיר אש:

BlackIce Defender:
הכי מומלץ !!! אני משתמש.
התוכנה ישבת ברקע בצורת עין קטנה ומהבהבת כשמזהה חדירה.
התוכנה גם מזהה את כתובת האייפי של הפורץ וגם את ספק האינטרנט שלו (עוזר אם רוצים להגיש תלונה).

PFW:
תשאל אותכם אל כל חיבור או הורדת קובץ (יכול להיות די מעצבן)

LockDown 2000:
תוכנה דומה לBlackIce Defender-, אשר גם תגלה לכם מאיפה הפורץ מחובר.

Symantec:
האנטי וירוס המפורסם של נורטון.

Internet FireWall 98:
תוכנת קיר אש סטנדרתית (לא תעבוד על מחשב המחובר בLAN-).

רשימת קישורים:	
תוכנות אנטי-וירוס:	
שם התוכנה	האתר
ESafe Protect	www.esafe.com
McAfee:	www.mcafee.com
תוכנות קיר אש	
BlackIce Defender	www.netowrkice.com
PFW	www.symantec.com
LockDown 2000	www.lockdown2000.com
Symantec	www.symantec.com
Internet FireWall 98	www.digitalrobotics.com

הכותב הוא עומר המאירי
hameiri@newmail.co.il
http://www.2call4free.net - שיחות חינם לחו"ל
UIN: 37654482