ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
Τμήμα Ψηφιακών Συστημάτων
Π.Μ.Σ. Ψηφιακές Επικοινωνίες και Δίκτυα

Σύγκριση Λειτουργιών Ασφαλείας Windows - Linux

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Δημήτριος Φωτόπουλος

2010

Πανεπιστήμιο Πειραιώς

Τμήμα Ψηφιακών Συστημάτων
Π.Μ.Σ. Ψηφιακές Επικοινωνίες και Δίκτυα

Σύγκριση Λειτουργιών Ασφαλείας Windows - Linux

Πτυχιακή Εργασία

Επιμέλεια: Φωτόπουλος Δημήτριος (Α.Μ.: ΜΕ / 0659)
Επιβλέπων Καθηγητής: Κάτσικας Σωκράτης

Εισαγωγή

Η πτυχιακή αυτή εργασία έχει ως θέμα τη σύγκριση των λειτουργιών ασφαλείας των λειτουργικών συστημάτων Windows και Linux. Φυσικά επειδή στην αγορά υπάρχει πληθώρα εκδόσεων τόσο σε ότι αφορά τα Windows όσο και στο Linux, έπρεπε να προαποφασιστεί μία δομή σχετικά με το πώς θα γίνει η ανάλυση αλλά και η σύγκριση μεταξύ των δύο ειδών λειτουργικών συστημάτων.

Σε συνεργασία με τον καθηγητή κ. Σωκράτη Κάτσικα, αποφασίστηκε η εργασία να χωριστεί σε τρείς κύριες ενότητες:

- Windows
- Linux
- Σύγκριση

Στην πρώτη θα αναλυθούν οι λειτουργίες ασφαλείας που αφορούν τα Windows. Επειδή όμως κυκλοφορούν διάφορες εκδόσεις από τη Microsoft και για διαφορετικές χρήσεις σε πολλά σημεία του κειμένου θα υπάρχει διαφοροποίηση τόσο ως προς την έκδοση (π.χ. XP SP1, XP SP2, Vista, Server2003, Server 2008) όσο και προς τη χρήση για την οποία η έκδοση προορίζεται (Εξυπηρετητής, Εξυπηρετούμενος ή μεμονωμένος Η/Υ).

Στη δεύτερη, που αφορά στο Linux, θα αναλυθούν οι λειτουργίες ασφαλείας που αφορούν σε διάφορες διανομές Linux. Επειδή οι διανομές Linux που κυκλοφορούν στην αγορά είναι πάρα πολλές, η εργασία θα επικεντρωθεί στις σημαντικότερες από αυτές (με κριτήριο το εύρος χρήσης τους). Επιγραμματικά αναφέρονται οι Debian, Suse, Red hat, Fedora, Ubuntu, Solaris. Παρόλα αυτά επειδή οι προαναφερθείσες εκδόσεις έχουν πολλά κοινά σημεία θα υπάρχει διαφοροποίηση στο κείμενο όπου υπάρχουν διαφορές και γενικό κείμενο όπου υπάρχουν ομοιότητες.

Σε ότι αφορά την τελευταία κύρια ενότητα η οποία έχει τίτλο «Σύγκριση», θα πραγματοποιηθεί αντιπαράθεση των διαφόρων λειτουργιών ασφαλείας που παρέχονται από τα Windows και από το Linux και που θα έχουν αναλυθεί στις παραπάνω ενότητες. Σκοπός αυτής της ενότητας δεν είναι να χαρακτηριστεί κάποιο είδος λειτουργικού συστήματος ως ανώτερο του άλλου ούτε γενικά αλλά ούτε ως προς κάποια συγκεκριμένη λειτουργία, αλλά η δημιουργία ενός κειμένου που θα μπορούσε να βοηθήσει κάποιον με συγκεκριμένες απαιτήσεις ασφαλείας να αποφασίσει ποιο λειτουργικό θα ήταν καταλληλότερο γι' αυτόν.

WINDOWS

Συστήματα Αρχείων των Windows

Το Σύστημα Αρχείων FAT

Το σύστημα αρχείων FAT είχε αρχικά εισαχθεί με το λειτουργικό σύστημα MS-DOS, όταν οι σκληροί δίσκοι ήταν πολύ μικρότεροι, και η δομή των φακέλων δεν ήταν τόσο περίπλοκη όσο σήμερα. Το σύστημα αρχείων FAT συνεχίζει να υποστηρίζεται από τα λειτουργικά συστήματα της Microsoft ακόμα και σήμερα. Το σύστημα αρχείων FAT μπορούσε αρχικά να υποστηρίξει μέγιστο μέγεθος σκληρού δίσκου των 2GB. Αυτό σημαίνει ότι στην περίπτωση που ένας σκληρός δίσκος ήταν μεγαλύτερος από 2GB, για να λειτουργήσει έπρεπε να χωριστεί σε διαμερίσματα μικρότερα ή ίσα των 2GB. Το σύστημα αρχείων FAT προστατεύει την αποθήκευση αρχείων δημιουργώντας δύο αντίγραφα του πίνακα εκχώρησης αρχείων. Σε περίπτωση που ένα αντίγραφο του πίνακα εκχώρησης αρχείων καταστραφεί, το άλλο αντίγραφο χρησιμοποιείται, προκειμένου να μη χαθούν τα αρχεία. Το αρχείο του πίνακα εκχώρησης της θέσης καθορίζεται στο BIOS (Παράμετρος Block / BPB). Αυτό εξασφαλίζει ότι όλα τα έγγραφα που είναι αναγκαία για την εκκίνηση του συστήματος μπορεί να βρεθεί.

Το σύστημα αρχείων Fat έχει βελτιωθεί με την πάροδο των χρόνων κι έτσι έχει 3 διαφορετικές εκδόσεις. Η βασική διαφορά των εκδόσεων είναι το πλήθος των bit που χρησιμοποιούνται για τον πίνακα εκχώρησης. Έτσι, το FAT12 χρησιμοποιεί 12 bit στον πίνακα εκχώρησης αρχείων, το FAT16 χρησιμοποιεί 16 bit, και το FAT32 χρησιμοποιεί 32 bit.

Λειτουργίες Ασφάλειας στο FAT16

Το σύστημα αρχείων Fat16 θεωρείται ξεπερασμένο, και χρησιμοποιείται μόνο από ένα μικρό ποσοστό υπολογιστών, οι οποίοι δεν έχουν αναβαθμίσει το λειτουργικό τους από την έκδοση Windows 98 και μετά. Οι λειτουργίες ασφάλειας που παρέχει είναι ελάχιστες:

- Εντοπισμός και σήμανση χαλασμένων cluster στο δίσκο.

  Ο εντοπισμός και η σήμανση αυτών των cluster, αποσκοπεί στην μη χρησιμοποίησή τους από το σύστημα, ώστε να μην υπάρξει αλλοίωση ή απώλεια των αρχείων που θα αποθηκευτούν σε αυτά τα σημεία του αποθηκευτικού μέσου.

- Διατήρηση αντιγράφου του πίνακα εκχώρησης αρχείων.

  Στην περίπτωση που ο πίνακας εκχώρησης αρχείων αλλοιωθεί, αυτό γίνεται αντιληπτό από το σύστημα και χρησιμοποιείται ο εφεδρικός.

- Διατήρηση για κάθε αρχείο των εξής παραμέτρων:
    - Όνομα
    - Παράμετροι (Μόνο για ανάγνωση, αρχείο συστήματος, κρυφό αρχείο κ.α.)
    - Ημερομηνία δημιουργίας
    - Ώρα δημιουργίας
    - Ημερομηνία τελευταίας φοράς που προσπελάστηκε
    - Ημερομηνία τελευταίας τροποποίησης
    - Ώρα τελευταίας τροποποίησης
    - Μέγεθος αρχείου
    - Θέση αρχείου στο δίσκο

  Η αποθήκευση αυτών των δεδομένων στο σύστημα αρχείων βοηθά, είτε με παρακολούθηση από το χρήστη, είτε με τη χρήση λογισμικού να παρακολουθείται η χρήση των αρχείων και ο εντοπισμός κακόβουλων ενεργειών.

Φυσικά, λόγω της παλαιότητάς του, στο FAT16 εντοπίζονται και αρκετά μειονεκτήματα:

- Δεν παρέχεται κανενός είδους τοπική ασφάλεια για τα αρχεία συστήματος, κάτι το οποίο σημαίνει ότι αυτά μπορούν να τροποποιηθούν ή και να διαγραφούν πολύ εύκολα, ακόμα και κατά λάθος και να δημιουργηθεί σοβαρό πρόβλημα στο σύστημα.
- Δεν διατηρείται αντίγραφο του τομέα εκκίνησης (boot sector), κι έτσι στην περίπτωση που το συγκεκριμένο σημείο του δίσκου αλλοιωθεί, το σύστημα δε θα εκκινεί.
- Το FAT 16 δε λειτουργεί σωστά με αποθηκευτικά μέσα άνω των 2GB, κάτι που μπορεί να οδηγήσει σε απώλεια δεδομένων.

Λειτουργίες Ασφάλειας στο FAT32

Οι αλλαγές που πραγματοποιήθηκαν κατά την αναβάθμιση του συστήματος αρχείων Fat ήταν ελάχιστες. Ειδικά στον τομέα της ασφάλειας, το σύστημα αρχείων βελτιώθηκε μόνο στην υποστήριξη μεγάλων αποθηκευτικών μέσων, κάτι που θα επέτρεπε σε χρήστες με δίσκους μεγαλύτερους από 2 GB να αισθάνονται ασφαλείς.

Το Σύστημα Αρχείων NTFS

Τα διαμερίσματα FAT που χρησιμοποιούνται από τα λειτουργικά συστήματα της Microsoft, όπως το DOS, τα Windows 95, Windows 98 και Windows Me δεν επιτρέπουν τον καθορισμό ασφάλειας για το σύστημα αρχείων εφόσον ένας χρήστης συνδεθεί. Αυτό σημαίνει ότι όλα τα δεδομένα που είναι αποθηκευμένα σε ένα διαμέρισμα FAT είναι διαθέσιμα σε κάθε χρήστη που μοιράζεται τον ίδιο υπολογιστή. Το σύστημα αρχείων FAT επίσης, δεν περιλαμβάνει υποστήριξη για τη συμπίεση αρχείων ή για την κρυπτογράφησή τους.

Τα διαμερίσματα NTFS από την άλλη, επιτρέπουν τον καθορισμό επιπέδου ασφάλειας για κάθε χρήστη ξεχωριστά. Τα δικαιώματα που μπορούν να δοθούν ελέγχουν την πρόσβαση των χρηστών και των ομάδων στα αρχεία και τους φακέλους ενός αποθηκευτικού μέσου. Είναι δυνατός ο ορισμός επιπέδων πρόσβασης και η παραχώρηση αυτών σε κάθε χρήστη ή ομάδα ώστε να καταστεί δυνατή η πρόσβαση σε κάποια αρχεία ή φακέλους NTFS, και να αρνηθεί την πρόσβαση σε κάποια άλλα. Με τον τρόπο αυτό, το NTFS υποστηρίζει τοπική ασφάλεια. Το σύστημα αρχείων NTFS περιλαμβάνει επίσης και άλλες λειτουργίες όπως η κρυπτογράφηση αρχείων, η συμπίεση αρχείων και πολλαπλές ροές δεδομένων.

Οι παρούσα έκδοση του NTFS είναι η 5.0, η οποία χρησιμοποιείται από τα Windows Server 2000 και μετά, αλλά υπάρχουν ακόμα αρκετοί εν ενεργεία υπολογιστές που χρησιμοποιούν προγενέστερη έκδοση των Windows (NT), συνεπώς και προγενέστερη έκδοση του NTFS (4.0).

Το σύστημα αρχείων NTFS περιλαμβάνει όλες εκείνες τις λειτουργίες ασφάλειας που περιγράφηκαν στην ενότητα του FAT, αλλά η βασική του διαφοροποίηση, όπως προαναφέρθηκε, είναι η υποστήριξη τοπικής ασφάλειας:

Τοπική ασφάλεια στο Σύστημα Αρχείων NTFS

Όπως αναφέρθηκε και παραπάνω, το NTFS προσφέρει τη δυνατότητα καθορισμού δικαιωμάτων πρόσβασης σε επίπεδο αρχείων και φακέλων για τον κάθε χρήστη ή κάθε ομάδα χρηστών ξεχωριστά. Τα δικαιώματα αυτά αναλύονται αναλυτικά παρακάτω, στην ενότητα «Έλεγχος Πρόσβασης».

Έλεγχος Πρόσβασης

Η απεριόριστη πρόσβαση των χρηστών σε πόρους του συστήματος και του δικτύου μπορεί να θέσει σε κίνδυνο την ασφάλεια και τη σταθερότητα ενός οργανισμού. Ακόμη και αν οι χρήστες και οι υπολογιστές πρέπει να έχουν πρόσβαση σε ένα δίκτυο και στους πόρους του για την εκτέλεση ορισμένων καθηκόντων τους, η πρόσβαση που χρειάζονται πρέπει να περιορίζονται σε αυτές που είναι αναγκαίες για να εκτελούν τα καθήκοντα αυτά.

Ο έλεγχος πρόσβασης στα Windows είναι η διαδικασία εκείνη που ελέγχει εάν ένας χρήστης στον οποίο έχει γίνει έλεγχος ταυτότητας, μπορεί να εκτελέσει συγκεκριμένες δραστηριότητες. Έτσι, όταν γίνεται προσπάθεια από κάποιο χρήστη να αποκτήσει πρόσβαση σε κάποιο αντικείμενο, ο έλεγχος πρόσβασης καθορίζει αν το αντικείμενο είναι διαθέσιμο σε αυτόν. Τα αντικείμενα αυτά μπορεί να είναι αντικείμενα Active Directory, αρχεία και φάκελοι, κοινόχρηστοι φάκελοι, υπηρεσίες δικτύου, εκτυπωτές, κλειδιά μητρώου, καθώς και οι υπηρεσιών απομακρυσμένης διαχείρισης.

Λίστες ελέγχου πρόσβασης (ACL) και καταχωρήσεις ελέγχου πρόσβασης (ACE)

Μια λίστα ελέγχου πρόσβασης (ACL) ελέγχει την πρόσβαση στους πόρους ενός συστήματος. Υπάρχουν δύο είδη ACLs:

- Λίστες διακριτικού ελέγχου πρόσβασης (DACL): Οι λίστες αυτές χρησιμοποιούνται για τον εντοπισμό των χρηστών και των ομάδων που έχουν τη δυνατότητα πρόσβασης (ή την άρνηση αυτής) σε ένα συγκεκριμένο πόρο.
- Σύστημα Access Control Lists (SACLs): Οι λίστες αυτές ελέγχουν πως η πρόσβαση είναι ελεγχόμενη και προσδιορίζει τα γεγονότα, τα οποία θα ελέγχονται για ένα χρήστη ή μια ομάδα

Οι πόροι στους οποίους μπορεί να απαγορευτεί ή να επιτραπεί πρόσβαση μέσω των λιστών ελέγχου πρόσβασης είναι οι εξής:

- Αρχεία
- Φάκελοι
- Κλειδιά Μητρώου (Registry Keys)
- Υπηρεσίες
- Αρχεία Λειτουργιών (System logs)
- Διεργασίες

- Η σειρά με την οποία εκτελούνται κάποιες διεργασίες (Named pipe)
- Περιοχές μνήμης δεσμευμένες από τον πυρήνα του συστήματος (Kernel objects)
- Πόρτες Δικτύου

Κάθε λίστα ACL περιλαμβάνει ορισμένες καταχωρήσεις ελέγχου πρόσβασης (ACE). Οι καταχωρήσεις αυτές περιέχουν τις ακόλουθες πληροφορίες:

- Το αναγνωριστικό ασφαλείας (SID) για ένα χρήστη ή ομάδα.
- Την ενέργεια στην οποία αναφέρεται η καταχώρηση.
- Αν το δικαίωμα κληρονομείται από υποφακέλους.
- Πληροφορίες σχετικά με το εάν η συγκεκριμένη καταχώρηση αφορά σε μία επιτρεπόμενη ή μια απαγορευμένη ενέργεια.

Τα δικαιώματα που μπορούν να δοθούν μέσω μίας λίστας πρόσβασης, όπως αναφέρθηκε και παραπάνω, μπορεί να αφορούν σε αρχεία και φακέλους, αντικείμενα active directory, εκτυπωτές, κλειδιά μητρώου, καθώς και σε υπηρεσίες απομακρυσμένης διαχείρισης:

Δικαιώματα Πρόσβασης σε Αρχεία και Φακέλους

Τα δικαιώματα πρόσβασης που μπορούν να καθοριστούν σε επίπεδο φακέλου, αναφέρονται παρακάτω:

- **Πλήρης έλεγχος:** Επιτρέπεται στο χρήστη να δει ή να αλλάξει τα χαρακτηριστικά ενός φακέλου, τα δικαιώματα ιδιοκτησίας. Ο χρήστης έχει επίσης τη δυνατότητα να δημιουργήσει, να τροποποιήσει και να διαγράψει φακέλους. Ο χρήστης μπορεί επίσης να εκτελέσει αρχεία που περιέχει ο φάκελος. Τέλος, επιτρέπεται η συμπίεση αρχείων.
- **Ανάγνωση και Εκτέλεση:** Τα δικαιώματα αυτά, αφορούν στην ανάγνωση των αρχείων που περιλαμβάνονται σε ένα φάκελο και στην εκτέλεσή τους.
- **Σύνταξη:** Οι χρήστες με αυτό το δικαίωμα έχουν τη δυνατότητα να δημιουργήσουν νέους φακέλους, υποφακέλους νέα αρχεία. Ο χρήστης έχει επίσης τη δυνατότητα να αλλάξει τις ιδιότητες ενός φακέλου.
- **Προβολή Περιεχομένου (List Folder Contents):** Οι χρήστες έχουν τη δυνατότητα να δουν σε λίστα τα περιεχόμενα του φακέλου, και να προβάλετε τις ιδιότητές του.
- **Τροποποίηση:** Ένας χρήστης μπορεί να αλλάξει τις ιδιότητες ενός φακέλου, να δημιουργήσει έναν νέο φάκελο, καθώς επίσης και να διαγράψει φακέλους.

- **Ανάγνωση:** Η παρούσα άδεια επιτρέπει στο χρήστη να δει το φάκελο, καθώς και στους υποφακέλους του και τα αρχεία που αποθηκεύονται μέσα σε αυτούς.

Τα δικαιώματα πρόσβασης που μπορούν να καθοριστούν σε επίπεδο αρχείου, είναι τα εξής:

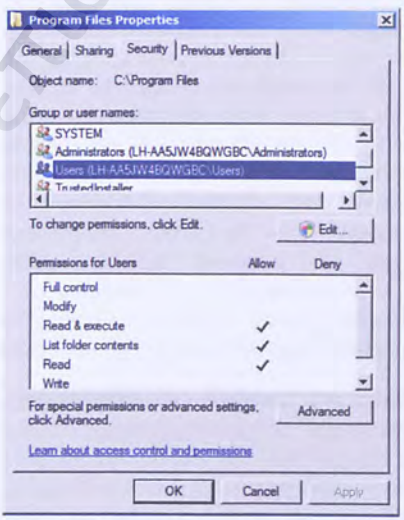
- **Πλήρης έλεγχος:** Ο χρήστης με αυτά τα δικαιώματα μπορεί να δει ή να αλλάξει τα χαρακτηριστικά ενός αρχείου και τα δικαιώματα ιδιοκτησίας. Ο χρήστης έχει επίσης τη δυνατότητα να δημιουργήσει, να τροποποιήσει και να διαγράψει αρχεία. Τέλος μπορεί να εκτελέσει και να συμπιέσει αρχεία.

- **Ανάγνωση και Εκτέλεση:** Τα δικαιώματα που ενεργοποιούνται από αυτή την άδεια εκτέλεσης, αφορούν στην ανάγνωση ενός αρχείου, καθώς και την προβολή των ιδιοτήτων του.

- **Σύνταξη:** Ο χρήστης έχει τη δυνατότητα να δημιουργήσει νέα αρχεία, να αλλάξει τις ιδιότητες ενός αρχείου, να εγγράψει δεδομένα σε αρχεία, και να δει τα δικαιώματα ιδιοκτησίας τους.

- **Τροποποίηση:** Ο χρήστης με αυτό το δικαίωμα μπορεί να αλλάξει τις ιδιότητες ενός αρχείου, να δημιουργήσει νέα αρχεία, να διαγράψει αρχεία, να εγγράψει δεδομένα σε αρχεία, καθώς και να προβάλει τις ιδιότητές τους.

- **Ανάγνωση:** Η παρούσα άδεια επιτρέπει στο χρήστη να δει τα χαρακτηριστικά του αρχείου και του φακέλου που το περιέχει.



Παραμετροποίηση της Λίστας ελέγχου πρόσβασης για τον φάκελο "Program Files" στα Windows 2003 Server

Κρυπτογράφηση αρχείων / EFS

Το σύστημα κρυπτογράφησης αρχείων (EFS) επιτρέπει στους χρήστες να κρυπτογραφήσουν αρχεία και φακέλους ή ακόμα και ολόκληρα μέσα αποθήκευσης διαμορφωμένα με το σύστημα αρχείων NTFS. Έτσι, ακόμα και όταν ένα πρόσωπο χωρίς άδεια διαχειρίζεται αρχεία και φακέλους (είτε γιατί απέκτησε αυτό το δικαίωμα λόγω εσφαλμένης ρύθμισης των δικαιωμάτων του NTFS, είτε γιατί μπόρεσε με δόλια μέσα να αποκτήσει πρόσβαση) τα αρχεία και οι φάκελοι θα είναι κρυπτογραφημένα κι έτσι δεν θα μπορεί να δει το περιεχόμενό τους. Μόνο ο ιδιοκτήτης των αρχείων και οποιοδήποτε άλλο εξουσιοδοτημένο από το χρήστη πρόσωπο μπορεί να αποκρυπτογραφήσει τα αρχεία και να τα διαβάσει.

Το EFS χρησιμοποιεί αλγόριθμους κρυπτογράφησης δημόσιου κλειδιού για την κρυπτογράφηση των αρχείων και των φακέλων. Τα αρχεία που είναι κρυπτογραφημένα, επομένως, είναι πάντα εμπιστευτικά. Ακόμη και αν τα δικαιώματα που έχουν δοθεί μέσω του NTFS δικαιώματα είναι προσανατολισμένα στην προστασία των εμπιστευτικών δεδομένων, το EFS χρησιμοποιείται για την προσθήκη ενός πρόσθετου στρώματος ασφάλειας. Αυτό διασφαλίζει ότι ακόμα και αν κάποιος, με δόλιο τρόπο, αποκτήσει πλήρη πρόσβαση στο χώρο αποθήκευσης δεδομένων του υπολογιστή, τα δεδομένα που βρίσκονται σε αρχεία είναι εξασφαλισμένα λόγω της κρυπτογράφησης EFS.

Η λειτουργία του EFS

Το σύστημα κρυπτογράφησης EFS είναι ενσωματωμένο στο NTFS, και γι' αυτό το λόγο επιτυγχάνεται πλήρης διαφάνεια κατά τη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης. Αυτό σημαίνει ότι όταν κάποιος χρήστης αποθηκεύει ένα αρχείο, το σύστημα EFS κρυπτογραφεί τα δεδομένα όπως τα δεδομένα που είναι γραμμένο στο δίσκο και όταν, αντίστοιχα, ανοίξει ένα αρχείο, αυτό αποκρυπτογραφείται από το EFS. Ο χρήστης ουσιαστικά αγνοεί αυτή τη διαδικασία και δεν χρειάζεται να προβεί σε οποιαδήποτε ενέργεια για την κρυπτογράφησης και αποκρυπτογράφησης. Εκτός από το EFS, υπάρχουν και τεχνολογίες τρίτων που μπορούν να παρέχουν δυνατότητες κρυπτογράφησης φακέλων και αρχείων, αλλά αυτά τα προγράμματα δεν είναι πλήρως διαφανή για τους χρήστες. Με τα προγράμματα αυτά, η ευθύνη να θυμηθούν να χρησιμοποιήσουν το πρόγραμμα κρυπτογράφησης ανατίθεται στους χρήστες, κάτι που μπορεί πολύ εύκολα να ξεχαστεί ή ακόμα και να παραμεληθεί σκόπιμα.

Τα κλειδιά που χρησιμοποιεί το EFS για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων, είναι ένα ζεύγος ενός δημόσιου και ενός ιδιωτικού κλειδιού, καθώς και ένα κλειδί για κάθε αρχείο που κρυπτογραφείται. Το EFS δημιουργεί ένα κλειδί για την κρυπτογράφηση του κάθε αρχείου (FEK / File Encryption Key), το οποίο, μέσω συμμετρικής κρυπτογράφησης

χρησιμοποιείται για την κρυπτογράφηση των δεδομένων. Στη συνέχεια, το κλειδί κρυπτογράφησης αρχείου (FEK) κρυπτογραφείται μέσω ασύμμετρης κρυπτογράφησης με το δημόσιο κλειδί του χρήστη και αποθηκεύεται μαζί με το κρυπτογραφημένο αρχείο. Όταν το αρχείο πρέπει να αποκρυπτογραφηθεί, αποκρυπτογραφείται πρώτα το FEK την αποκρυπτογράφηση των δεδομένων του αρχείου.

Παρακάτω αναφέρονται οι διαδικασίες που εκτελούνται όταν ένα αρχείο κρυπτογραφείται:

- Το αρχείο διαβάζεται από την υπηρεσία EFS.
- Οι ροές δεδομένων του αρχείου αντιγράφονται σε ένα απλό αρχείο κειμένου το οποίο βρίσκεται στον προσωρινό κατάλογο του συστήματος .
- Η υπηρεσία EFS δημιουργεί το μοναδικό FEK.
- Πραγματοποιείται η κρυπτογράφηση των αρχείων είτε μέσω του αλγόριθμου κρυπτογράφησης και με τη χρήση του FEK. Ο αλγόριθμος κρυπτογράφησης που μπορεί να χρησιμοποιηθεί, διαφέρει ανάλογα με την έκδοση του NTFS που χρησιμοποιείται. Οι διαθέσιμοι αλγόριθμοι κρυπτογράφησης σε κάθε έκδοση του NTFS φαίνονται στο παρακάτω σχήμα:

Έκδοση NTFS	Έκδοση MS-Windows	Διαθέσιμοι Αλγόριθμοι Κρυπτογράφησης
5.0	W2K	DESX
5.1	XP Pro	DESX, 3DES
5.1	XP Pro SP1	DESX, 3DES, AES
5.2	W2K3	DESX, 3DES, AES
6.0	Vista	DESX, 3DES, AES

- Δημιουργείται, μέσα στο κρυπτογραφημένο αρχείο, ο χώρος αποκρυπτογράφησης αρχείου το (DDF / Data Decryption Field). Στο DDF αποθηκεύεται το κρυπτογραφημένο FEK, καθώς και κάποιες απαραίτητες πληροφορίες για να είναι δυνατή η ανάκτηση του αρχείου από το διαχειριστή του συστήματος, σε περίπτωση που ο χρήστης ξεχάσει το ιδιωτικό κλειδί .

- Το αρχείο που βρίσκεται στον προσωρινό κατάλογο του συστήματος διαγράφεται.

Αντίστοιχα, η διαδικασία αποκρυπτογράφησης ενός αρχείου έχει ως εξής:

- Το NTFS αναγνωρίζει αν το αρχείο στο οποίο ζητείται πρόσβαση είναι κρυπτογραφημένο και εφ' όσον είναι, υποβάλει αίτηση για την αποκρυπτογράφηση στην υπηρεσία EFS.
- Η υπηρεσία EFS αποσπά από το αρχείο το χώρο αποκρυπτογράφησης αρχείου (DDF / Data Decryption Field)..
- Το EFS ζητά το ιδιωτικό κλειδί του χρήστη και το χρησιμοποιεί για την αποκρυπτογράφηση του DDF.
- *Το FEK που αποκρυπτογραφήθηκε αποστέλλεται στην υπηρεσία EFS.*
- Η υπηρεσία EFS χρησιμοποιεί το FEK για την αποκρυπτογράφηση των δεδομένων στο αρχείο.
- Τέλος, η υπηρεσία EFS περνάει το αποκρυπτογραφημένο αρχείο στο NTFS.

Σύγκριση ασφάλειας συστημάτων αρχείων FAT – NTFS

Κατά την εγκατάσταση μίας εκ των εκδόσεων του λειτουργικού συστήματος Windows, πολλές φορές εγείρεται το ερώτημα αν το σύστημα αρχείων που θα χρησιμοποιηθεί θα πρέπει να είναι το FAT ή το NTFS. Στον παρακάτω πίνακα παρατίθενται οι διαφορές των δύο συστημάτων αρχείων σε ότι αφορά θέματα ασφάλειας.

Χαρακτηριστικό	NTFS 5	NTFS 4	FAT 32	FAT 16
Λειτουργικά Συστήματα	Windows 2000, Windows XP, Windows 2003 Server	Windows NT, Windows 2000, Windows XP, Windows 2003 Server	DOS v7 και μεταγενέστερο, Windows 98, Windows ME, Windows 2000, Windows XP	DOS, Όλες οι εκδόσεις των Microsoft Windows
Μέγιστος όγκος αποθηκευτικού μέσου	2 TB	2 TB	2 GB σε εκδόσεις προγενέστερες των XP και 200 GB σε XP και μεταγενέστερες	16MB
Μέγιστος αριθμός αρχείων ανά αποθ. μέσο	Απεριόριστος	Απεριόριστος	4.177.918	65.520
Μέγιστο μέγεθος αρχείου	Ίσο με το μέγεθος του αποθ. μέσου	Ίσο με το μέγεθος του αποθ. μέσου	4 GB	2 GB
Αντίγραφο του συστήματος αρχείων	Ναι (Αντίγραφο του MFT)	Ναι (Αντίγραφο του MFT)	Ναι (Αντίγραφο του FAT)	Ναι (Αντίγραφο του FAT)
Δυνατότητα Κρυπτογράφησης	Ναι	Όχι	Όχι	Όχι
Δυνατότητα ανάκτησης κρυπτογρ. αρχείων	Ναι	Ναι	Όχι	Όχι
Δυνατότητα για απόδοση δικαιωμάτων	Ναι	Ναι	Όχι	Όχι

Παρακολούθηση και Ανίχνευση Εισβολών

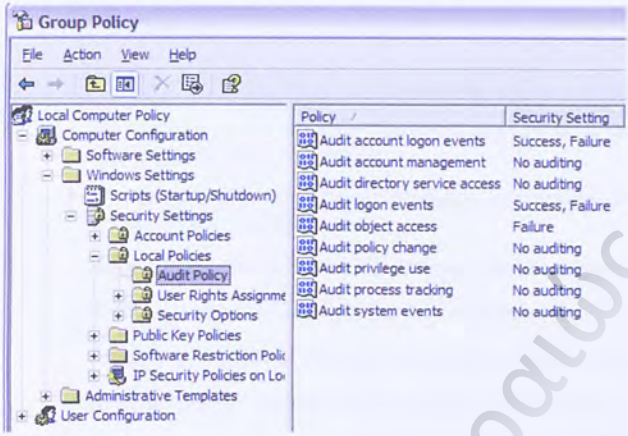
Στα λειτουργικά συστήματα της Microsoft δεν προσφέρεται αυτοματοποιημένο λογισμικό για την ενεργή ανίχνευση εισβολών (active intrusion detection). Παρόλα αυτά όμως η ίδια η Microsoft στην ιστοσελίδα της τονίζει τη σημασία της παρακολούθησης και της ανίχνευσης εισβολών (Auditing and Intrusion Detection) και προσφέρει μαζί με τα λειτουργικά της συστήματα όλα τα απαραίτητα εργαλεία για την παθητική ανίχνευση εισβολών (passive intrusion detection). Οι λόγοι για τους οποίους είναι τόσο σημαντική αυτή η διαδικασία είναι οι εξής:

- Ανεξαρτήτως του επιπέδου της ασφάλειας ενός συστήματος και ανεξαρτήτως των προληπτικών μέτρων που έχουν παρθεί, κάθε σύστημα είναι υποψήφιος στόχος επίθεσης.
- Οι επιτυχημένες επιθέσεις πολλές φορές είναι απόρροια στοιχείων που συλλέγονται βάσει προηγούμενων ανεπιτυχών προσπαθειών. Συνεπώς όταν πραγματοποιούνται επιθέσεις, ακόμα και ανεπιτυχείς, πρέπει να ανιχνεύονται και να λαμβάνονται αντίμετρα.
- Όσο νωρίτερα αντιληφθεί κανείς μία επίθεση στο σύστημα για το οποίο είναι υπεύθυνος, τόσο μεγαλύτερες πιθανότητες έχει να περιορίσει τη ζημιά που θα προκληθεί από την επίθεση.
- Πολλές φορές, μέσω της παρακολούθησης, είναι εφικτό να εντοπιστεί ο υπαίτιος της επίθεσης.
- Η παρακολούθηση και η ανίχνευση εισβολών βοηθά να εντοπιστούν κενά ασφαλείας και να ληφθούν τα κατάλληλα μέτρα ώστε να μην δημιουργηθούν παρόμοια προβλήματα και μελλοντικά.
- Τέλος, ακόμα και αν η επίθεση επιτύχει απόλυτα, η παρακολούθηση και η ανίχνευση εισβολών βοηθά στον εντοπισμό της ζημιάς ώστε να πραγματοποιηθούν όλες οι απαραίτητες ενέργειες από τον διαχειριστή ώστε το σύστημα να επανέλθει.

Παθητική Ανίχνευση Εισβολών (Auditing)

Ένα σημαντικό κομμάτι της ασφάλειας ενός πληροφοριακού συστήματος είναι η διαδικασία της παρακολούθησης των προσπαθειών για εισβολή. Στα Microsoft Windows (εκδόσεις Server 2000 και όλες οι επόμενες και XP καθώς και αυτές που ακολούθησαν) μπορεί κανείς να ενεργοποιήσει

την παρακολούθηση εισβολών από το εξής σημείο: Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy



Η ενεργοποίηση της παρακολούθησης εισβολών (Auditing) στα Windows XP

Απ' ότι φαίνεται και στην παραπάνω εικόνα, τα γεγονότα στα οποία μπορεί να ενεργοποιηθεί η παρακολούθηση είναι τα εξής:

- Account Logon Events (Σύνδεση λογαριασμού στον Τομέα Δικτύου)
- Account Management (Διαχείριση των λογαριασμών)
- Directory Service Access (Έλεγχος πρόσβασης στην υπηρεσία καταλόγου)
- Logon Events (Σύνδεση λογαριασμού στον Η/Υ που πραγματοποιείται η παρακολούθηση)
- Object Access (Πρόσβαση σε Αντικείμενα)
- Policy Change (Αλλαγή Πολιτικής)
- Privilege Use (Έλεγχος χρήσης Δικαιωμάτων)
- Process Tracking (Παρακολούθηση Διεργασιών)
- System Events (Γεγονότα Συστήματος)

Παρακολούθηση Σύνδεσης Λογαριασμού στον Τομέα Δικτύου

Όταν ένας λογαριασμός προσπαθεί να συνδεθεί σε έναν τομέα δικτύου, η ενέργεια αυτή, εφόσον έχει ενεργοποιηθεί η παρακολούθηση συνδέσεων

λογαριασμών στον τομέα δικτύου, καταγράφεται. Οι ενέργειες αυτές καταγράφονται με τη μορφή κωδικών οι οποίοι σύμφωνα με τη Microsoft, ερμηνεύονται ως εξής:

Κωδικός	Ερμηνεία
672	Ένα «εισιτήριο της υπηρεσίας πιστοποίησης» (authentication service ticket) παραδόθηκε με επιτυχία.
673	Ένα «εισιτήριο της υπηρεσίας παράδοσης εισιτηρίων» (ticket granting service ticket) παραδόθηκε.
674	Ανανεώθηκε κάποιο από τα 2 προαναφερθέντα εισιτήρια.
675	Απέτυχε η προ-πιστοποίηση (pre-authentication).
676	Απέτυχε η διαδικασία λήψης εισιτηρίου από κάποιο λογαριασμό.
677	Δεν παραδόθηκε εισιτήριο της υπηρεσίας πιστοποίησης.
678	Ένας λογαριασμός εισήλθε με επιτυχία σε κάποιον τομέα δικτύου.
680	Η εγγραφή αυτή χρησιμεύει στην αναγνώριση του λογαριασμού που εισήλθε στον τομέα.
681	Επιχειρήθηκε η είσοδος στον τομέα δικτύου.
682	Κάποιος χρήστης επανασυνδέθηκε σε μία αποσυνδεδεμένη σύνοδο απομακρυσμένης διαχείρισης.
683	Κάποιος χρήστης αποσυνδέθηκε από μία σύνοδο απομακρυσμένης διαχείρισης με ανορθόδοξο τρόπο.

Για καθένα από τα παραπάνω γεγονότα, τα Windows παρέχουν τη δυνατότητα προβολής λεπτομερειών.

Παρακολούθηση Διαχείρισης των Λογαριασμών

Η παρακολούθηση διαχείρισης των λογαριασμών χρησιμεύει για την ανίχνευση δημιουργίας, αλλαγής ή διαγραφής χρηστών ή ομάδων χρηστών. Μέσω της παρακολούθησης αυτής μπορεί να προσδιοριστεί πότε πραγματοποιήθηκε η αλλαγή και από ποιον. Και σε αυτή την παρακολούθηση, όπως σε όλες άλλωστε, τα συμβάντα καταγράφονται με την μορφή κωδικών που ερμηνεύονται ως εξής:

Κωδικός	Ερμηνεία
624	Δημιουργία λογαριασμού χρήστη.
625	Αλλαγή είδους λογαριασμού χρήστη.
626	Ενεργοποίηση λογαριασμού χρήστη.
627	Απόπειρα αλλαγής κωδικού πρόσβασης.
628	Αλλαγή κωδικού χρήστη.
629	Απενεργοποίηση λογαριασμού χρήστη.
630	Διαγραφή λογαριασμού χρήστη.
631	Δημιουργία ευρείας ομάδα χρηστών (Global Group) με ενεργοποιημένη πολιτική ασφάλειας.
632	Προσθήκη χρήστη σε ευρεία ομάδα χρηστών (Global Group) με ενεργοποιημένη πολιτική ασφάλειας.
633	Διαγραφή χρήστη από ευρεία ομάδα χρηστών (Global Group) με ενεργοποιημένη πολιτική ασφάλειας.
634	Διαγραφή ευρείας ομάδα χρηστών (Global Group) με ενεργοποιημένη πολιτική ασφάλειας.
635	Δημιουργία τοπικής ομάδας χρηστών (Local Group) χωρίς ενεργοποιημένη πολιτική ασφάλειας.
636	Προσθήκη χρήστη σε ομάδα με ενεργοποιημένη πολιτική ασφάλειας.
637	Διαγραφή χρήστη από ευρεία ομάδα χρηστών (Global Group) με ενεργοποιημένη πολιτική ασφάλειας.
638	Διαγραφή τοπικής ομάδας χρηστών (Local Group) χωρίς ενεργοποιημένη πολιτική ασφάλειας.
639	Μεταβολή τοπικής ομάδας χρηστών (Local Group) χωρίς ενεργοποιημένη πολιτική ασφάλειας.
641	Μεταβολή ευρείας ομάδα χρηστών (Global Group) με ενεργοποιημένη πολιτική ασφάλειας.
642	Μεταβολή λογαριασμού χρήστη.
643	Μεταβολή πολιτικής ασφάλειας στον τομέα δικτύου.
644	Κλείδωμα λογαριασμού χρήστη.

Όπως και στην παρακολούθηση σύνδεσης λογαριασμού στον τομέα δικτύου, έτσι κι εδώ δίνεται η δυνατότητα προβολής λεπτομερειών για κάθε συμβάν που καταγράφεται.

Έλεγχος πρόσβασης αντικειμένων

Σε ένα δίκτυο ηλεκτρονικών υπολογιστών με εξυπηρετητή την έκδοση Windows NT ή κάποια νεώτερη, μπορεί να ενεργοποιηθεί η παρακολούθηση της πρόσβασης των διαφόρων χρηστών σε αντικείμενα. Η διαδικασία αυτή επιτυγχάνεται μέσω των λιστών ελέγχου πρόσβασης οι οποίες χρησιμοποιούνται αποκλειστικά και μόνο σε λειτουργικά συστήματα της Microsoft με σύστημα αρχείων NT. Ως αντικείμενο θεωρείται οτιδήποτε μπορεί ένας χρήστης να χειριστεί. Αυτό μπορεί να είναι αρχείο, φάκελος, μέσο αποθήκευσης, εκτυπωτής, κλειδί μητρώου κ.α.

Στη λίστα πρόσβασης για κάθε αντικείμενο, περιέχονται τρεις μεταβλητές μέσω των οποίον πραγματοποιείται η παρακολούθηση σε κάθε αντικείμενο:

- Το αντικείμενο στο οποίο ασκείται έλεγχος.
- Οι διαδικασίες που παρακολουθούνται (π.χ. ανάγνωση, εγγραφή κ.λ.π.).
- Μία σημαία (flag) η οποία υποδεικνύει εάν θα παρακολουθείται η επιτυχής πρόσβαση, η αποτυχία πρόσβασης ή και τα δύο.

Μέσω των παραπάνω εγγραφών και εφ' όσον η σημαία υποδεικνύει ότι κάποιο αντικείμενο παρακολουθείται, καταγράφονται η ενέργεια που πραγματοποιήθηκε ή που επιχειρήθηκε να πραγματοποιηθεί, ο χρήστης που προέβη στην ενέργεια αυτή και το αντικείμενο στο οποίο προσπάθησε να αποκτήσει ή απέκτησε ο χρήστης πρόσβαση.

Η απρόσεκτη χρήση του ελέγχου πρόσβασης σε αντικείμενα, σύμφωνα με τη Microsoft, μπορεί να οδηγήσει σε πολύ μεγάλο αριθμό εγγραφών και να καταστήσει την παρακολούθηση από τον διαχειριστή από πολύ δύσκολη έως αδύνατη.

Ο έλεγχος πρόσβασης σε αντικείμενα προξενεί τη δημιουργία των εξής κωδικών:

Κωδικός	Ερμηνεία
560	Επετράπη η πρόσβαση σε ένα ήδη υπάρχον αντικείμενο.
562	Τερματίστηκε η πρόσβαση ενός αντικειμένου.
563	Επιχειρήθηκε να διαγραφεί ένα αντικείμενο
564	Ένα προστατευμένο αντικείμενο διεγράφη.

565	Επετράπη η πρόσβαση σε έναν υπάρχοντα τύπο αντικειμένου.

Αξίζει να σημειωθεί πως η βασικότερη ενέργεια που καταγράφεται είναι αυτή με τον κωδικό 560, μέσω της οποίας μπορεί ο διαχειριστής του συστήματος να αποσπάσει σημαντικές πληροφορίες σχετικά με τη χρήση διαφόρων αντικειμένων από τους χρήστες του συστήματος.

Έλεγχος πρόσβασης στην υπηρεσία καταλόγου

Τα αντικείμενα της υπηρεσίας καταλόγου (Active Directory Objects), είναι συσχετισμένα με λίστες πρόσβασης και μέσω αυτών πραγματοποιείται ο έλεγχος. Αντιθέτως, όταν ο έλεγχος αφορά σε χρήστες ή ομάδες χρηστών, ο έλεγχος πραγματοποιείται μέσω του ελέγχου διαχείρισης λογαριασμών. Οι κωδικοί με τους οποίους καταγράφονται τα γεγονότα που αφορούν στην υπηρεσία καταλόγου είναι οι ίδιοι με τις προαναφερθείσες περιπτώσεις με τη διαφορά ότι στις λεπτομέρειες αναγράφεται ότι αφορούν σε χρήστες ή αντικείμενα της υπηρεσίας καταλόγου.

Έλεγχος Σύνδεσης Λογαριασμού σε Η/Υ

Κάθε φορά που ένας χρήστης συνδέεται ή αποσυνδέεται από έναν Η/Υ, η ενέργεια αυτή καταγράφεται τοπικά. Επίσης, κάθε φορά που ένας χρήστης συνδέεται απομακρυσμένα με έναν εξυπηρετητή, το γεγονός αυτό καταγράφεται στον εξυπηρετητή. Τα δύο αυτά είδη γεγονότων είναι πολύ χρήσιμα για τον εντοπισμό επιθέσεων από κάποιον συγκεκριμένο Η/Υ.

Και στον έλεγχο σύνδεσης λογαριασμού, τα διάφορα γεγονότα καταγράφονται με τη μορφή κωδικών:

Κωδικός	Ερμηνεία
528	Ένας χρήστης συνδέθηκε επιτυχώς στον Η/Υ.
529	Επιχειρήθηκε η σύνδεση στον Η/Υ είτε με χρήση σωστού ονόματος χρήστη είτε με χρήση λάθος ονόματος χρήστη.
530	Επιχειρήθηκε η σύνδεση σε χρόνο που δεν επιτρέπεται από την πολιτική ασφάλειας του Η/Υ.
531	Επιχειρήθηκε η σύνδεση μέσω λογαριασμού που έχει απενεργοποιηθεί.
532	Επιχειρήθηκε η σύνδεση με χρήση λογαριασμού που έχει λήξει.
533	Δεν επετράπη η σύνδεση του χρήστη στον συγκεκριμένο Η/Υ.
534	Ο χρήστης επιχείρησε να συνδεθεί με τρόπο που δεν είναι επιτρεπτός

(π.χ. μέσω δικτύου).

535	Ο κωδικός πρόσβασης για κάποιο λογαριασμό έχει λήξει.
536	Η υπηρεσία "Net Logon" δεν είναι ενεργή.
537	Η σύνδεση ενός λογαριασμού απέτυχε για άλλους λόγους (πλην των προαναφερθέντων).
538	Κάποιος χρήστης αποσυνδέθηκε.
539	Ο λογαριασμός κλειδώθηκε τη στιγμή που επιχειρήθηκε η σύνδεση. Αυτό μπορεί να οφείλεται σε αποτυχημένη επίθεση με κωδικούς πρόσβασης (password attack).
540	Πραγματοποιήθηκε επιτυχημένη σύνδεση μέσω δικτύου.
682	Κάποιος χρήστης επανασυνδέθηκε σε μία αποσυνδεδεμένη σύνοδο απομακρυσμένης διαχείρισης.
683	Κάποιος χρήστης αποσυνδέθηκε από μία σύνοδο απομακρυσμένης διαχείρισης με ανορθόδοξο τρόπο.

Έλεγχος Χρήσης Δικαιωμάτων

Όλοι οι χρήστες που αλληλεπιδρούν με ένα σύστημα Η/Υ. αργά ή γρήγορα χρησιμοποιούν τα δικαιώματα που τους έχουν παραχωρηθεί από το διαχειριστή του συστήματος. Εάν πραγματοποιείται ο έλεγχος χρήσης δικαιωμάτων, κάθε φορά που ένας χρήστης προσπαθεί να χρησιμοποιήσει κάποιο δικαίωμα που του έχει αποδοθεί.

Οι σημαντικότερες περιπτώσεις στις οποίες πραγματοποιείται καταγραφή κάποιου γεγονότος όταν ο έλεγχος χρήσης δικαιωμάτων είναι ενεργός, είναι οι εξής:

- Αλλαγή ώρας του συστήματος. Μία τέτοια ενέργεια μπορεί να αποσκοπεί στην απόκρυψη της ορθής καταγραφής της ώρας κατά την οποία ο χρήστης πραγματοποίησε κάποια ενέργεια.
- Απομακρυσμένη απενεργοποίηση συστήματος.
- Προσθήκη ή αφαίρεση προγραμμάτων οδήγησης συσκευών.
- Διαχείριση του ελέγχου εισβολών.
- Τοπική απενεργοποίηση συστήματος.
- Αλλαγή στην ιδιοκτησία (ownership) αρχείων ή άλλων αντικειμένων.
- Συμπεριφορά που προσομοιώνει λειτουργίες του συστήματος (κάποιος χρήστης εκτέλεσε με τρόπο όμοιο με αυτόν που θα την εκτελούσε το σύστημα) .

Οι κωδικοί με τους οποίους τα γεγονότα χρήσης δικαιωμάτων εμφανίζονται στην οθόνη ελέγχου χρήσης δικαιωμάτων είναι οι εξής:

Κωδικός	Ερμηνεία
576	Δόθηκαν δικαιώματα χρήσης σε έναν συγκεκριμένο χρήστη.
577	Κάποιος χρήστης αποπειράθηκε να εκτελέσει μία λειτουργία του συστήματος που απαιτεί συγκεκριμένα δικαιώματα.
578	Κάποιος χρήστης χρησιμοποίησε τα δικαιώματά του σε ένα προστατεμένο αντικείμενο.

Έλεγχος Διεργασιών

Εάν είναι ενεργοποιημένος ο έλεγχος των διεργασιών, κάθε φορά που μία διεργασία θα ξεκινά ή κάθε φορά που μία διεργασία θα τερματίζεται, αυτό θα καταγράφεται. Επίσης θα καταγράφονται η έμμεση πρόσβαση σε ένα αντικείμενο (μέσω μίας διεργασίας) και ο διπλασιασμός της πρόσβασης σε ένα αντικείμενο (duplicated handle to an object).

Οι κωδικοί μέσω των οποίων πραγματοποιείται ο έλεγχος των διεργασιών είναι οι εξής:

Κωδικός	Ερμηνεία
592	Δημιουργήθηκε μία καινούρια διεργασία.
593	Μία διεργασία τερματίστηκε.
594	Διπλασιάστηκε η πρόσβαση σε ένα αντικείμενο μέσω μίας διεργασίας.
595	Πραγματοποιήθηκε έμμεση πρόσβαση σε ένα αντικείμενο.

Ο έλεγχος των διεργασιών παράγει υπερβολικά μεγάλο αριθμό εγγραφών στο αρχείο καταγραφής (log file) και η συνηθισμένη πρακτική που ακολουθείται είναι να αποφεύγεται εκτός και αν υπάρχει συγκεκριμένος λόγος να είναι ενεργή.

Γεγονότα συστήματος

Ο έλεγχος που πραγματοποιείται όταν επιλεχθεί η ενεργοποίηση ελέγχου στα γεγονότα συστήματος αφορά τις αλλαγές στο περιβάλλον του συστήματος που μπορεί να πραγματοποιηθούν από κάποιο χρήστη ή κάποια διεργασία. Επίσης ελέγχεται η κατάσταση του αρχείου καταγραφής. Αν αυτό σβηστεί, τότε στο νέο αρχείο καταγραφής θα αναφέρεται πότε και από ποιόν σβήστηκε.

Αντίστοιχα με τα υπόλοιπα είδη παρακολούθησης κι εδώ παράγονται καταγραφές με κωδικούς:

Κωδικός	Ερμηνεία
512	Πραγματοποιήθηκε εκκίνηση των Windows.
513	Τα Windows τερματίστηκαν.
514	Ένα πακέτο πιστοποίησης, εντοπίστηκε από την από την διεργασία που αφορά στην τοπική ασφάλεια (Local Security Authority).
515	Μία διεργασία που αφορά σε είσοδο χρήστη στο σύστημα, πιστοποιήθηκε από την διεργασία που αφορά στην τοπική ασφάλεια (Local Security Authority).
516	Οι πόροι του Η/Υ που απαιτούνται για την καταγραφή των διαφόρων συμβάντων εξαντλήθηκαν, με αποτέλεσμα να μην πραγματοποιείται πλέον παρακολούθηση και καταγραφή των διαφόρων συμβάντων.
517	Το αρχείο καταγραφής (security log) καθαρίστηκε από εγγραφές.

Αλλαγή Πολιτικής Ελέγχου

Η πολιτική ελέγχου που ακολουθείται σε ένα σύστημα, καθορίζει ποιες αλλαγές στο περιβάλλον του συστήματος παρακολουθούνται, ώστε ο διαχειριστής του συστήματος να είναι σε θέση να αποφανθεί αν η οποιαδήποτε αλλαγή που πραγματοποιήθηκε είναι αποτέλεσμα εισβολής ή φυσιολογικής χρήσης του συστήματος.

Παρόλα αυτά, ένας επίδοξος εισβολέας, είναι πολύ πιθανό να προσπαθήσει να αλλάξει την πολιτική ελέγχου, ώστε να μην καταγραφούν οι κινήσεις του. Η Microsoft έχει προβλέψει για μια τέτοια περίπτωση να καταγράφονται οι αλλαγές στην πολιτική παρακολούθησης. Οι εγγραφές που μπορούν να προκληθούν από μία τέτοια περίπτωση είναι οι εξής:

Κωδικός	Ερμηνεία
608	Δόθηκε ένα δικαίωμα σε κάποιο χρήστη.
609	Αφαιρέθηκε ένα δικαίωμα από κάποιο χρήστη.
610	Δημιουργήθηκε σχέση εμπιστοσύνης με έναν άλλο τομέα δικτύου.
611	Αφαιρέθηκε η σχέση εμπιστοσύνης με έναν άλλο τομέα δικτύου.
612	Πραγματοποιήθηκε μεταβολή στην πολιτική ελέγχου.
768	Υπήρξε σύγκρουση (collision) μεταξύ δύο στοιχείων του δικτύου.

Άλλοι Τρόποι Ελέγχου Εισβολών

Εκτός από τη συχνή παρακολούθηση των διαφόρων γεγονότων που καταγράφονται μέσω του εργαλείου ελέγχου εισβολών των Microsoft Windows, υπάρχουν ακόμα κάποιες τεχνικές τις οποίες μπορεί ο εκάστοτε ενδιαφερόμενος να αξιοποιήσει για να ανιχνεύσει εισβολές.

Παρακολούθηση αρχείων καταγραφής άλλων προγραμμάτων

Εκτός από τα αρχεία καταγραφής που παράγονται από το λειτουργικό σύστημα, υπάρχει περίπτωση να χρησιμοποιούνται σε έναν Η/Υ και άλλα προγράμματα τα οποία παράγουν τέτοια αρχεία. Τα προγράμματα αυτά μπορεί να είναι είτε της ίδιας της Microsoft (π.χ. IIS, ISA Server, IAS κ.λ.π.) είτε κάποιου τρίτου (π.χ. Apache). Σε πολλές περιπτώσεις τα αρχεία καταγραφής αυτών των προγραμμάτων, μπορεί να προσφέρουν περαιτέρω πληροφορίες για κάποια επίθεση και να καταστήσουν τη δουλειά του διαχειριστή του δικτύου πολύ ευκολότερη.

Παρακολούθηση Εγκατεστημένων Υπηρεσιών και Προγραμμάτων Οδήγησης Συσκευών

Πολλές φορές, επιθέσεις εναντίον ενός συστήματος, στοχεύουν είτε τις εγκατεστημένες σε αυτές υπηρεσίες, είτε τα προγράμματα οδήγησης διαφόρων συσκευών, αντικαθιστώντας τα με παρόμοια, τα οποία περιέχουν όμως και επιβλαβή κώδικα.

Τα παρακάτω εργαλεία μπορούν να χρησιμοποιηθούν ώστε να ανιχνευθούν και να αντιμετωπιστούν τέτοιου είδους επιθέσεις:

- Κονσόλα Υπηρεσιών (Services Console)

  Η κονσόλα MMC μπορεί να χρησιμοποιηθεί για την παρακολούθηση των εγκατεστημένων υπηρεσιών είτε στον τοπικό υπολογιστή είτε σε κάποιον απομακρυσμένο. Μέσω αυτής της διεπαφής, ο διαχειριστής ενός συστήματος μπορεί να εκκινήσει, να σταματήσει, να επανεκκινήσει, ακόμα και να παραμετροποιήσει όλες τις υπηρεσίες που είναι εγκατεστημένες στο σύστημα.

- Netsvc.exe

  Αυτό το εργαλείο εκκινείται μέσω της γραμμής εντολών και χρησιμεύει στην απομακρυσμένη διαχείριση των υπηρεσιών. Ο διαχειριστής μπορεί να εκκινήσει, να σταματήσει, να επανεκκινήσει ή απλώς να ελέγξει την κατάσταση των υπηρεσιών σε έναν απομακρυσμένο υπολογιστή.

- SvcMon.exe

  Το εργαλείο αυτό ελέγχει την κατάσταση των διεργασιών και επικοινωνεί μέσω e-mail με το διαχειριστή του συστήματος σε περίπτωση που κάποια διεργασία ξεκινήσει, σταματήσει ή επανεκκινήσει.

- Drivers.exe

  Το εργαλείο αυτό εμφανίζει όλα τα προγράμματα οδήγησης συσκευών στον Η/Υ που εκτελείται. Οι πληροφορίες που παρέχονται περιλαμβάνουν το όνομα του αρχείου του κάθε προγράμματος οδήγησης, το μέγεθος που καταλαμβάνει στο σκληρό δίσκο και την ημερομηνία που εγκαταστάθηκε.

Παρακολούθηση Θυρών (Port Monitoring)

Είναι συχνό φαινόμενο, πριν από μία επίθεση να πραγματοποιείται μία σάρωση των θυρών (port scanning) από τον επιτιθέμενο ώστε να εντοπιστεί η θύρα μέσω της οποίας θα γίνει η επίθεση. Από αυτό το γεγονός προκύπτει ότι είναι πολύ σημαντικό να μπορεί γνωρίζει ο διαχειριστής ενός συστήματος ποιες θύρες στο σύστημά του είναι ανοιχτές ανά πάσα στιγμή.

Τα Windows για τη χρήση αυτή, παρέχουν το εργαλείο Netstat.exe. Μέσω της γραμμής εντολών, ο διαχειριστής μπορεί να δει όλες τις ανοιχτές θύρες για τα πρωτόκολλα TCP και UDP.

Ενεργητική Ανίχνευση Εισβολών

Το λογισμικό ενεργητικής ανίχνευσης εισβολών αναλύει τα πακέτα που διακινούνται μέσα σε ένα τοπικό δίκτυο στο επίπεδο εφαρμογής και με ανάλυση αυτών των πακέτων εντοπίζονται είτε ύποπτα πακέτα είτε γνωστοί τύποι επιθέσεων (π.χ.Exploit attacks, reconnaissance attacks, DoS attacks κ.α.)

Τέτοιο λογισμικό δεν συμπεριλαμβάνεται σε καμία έκδοση του λειτουργικού συστήματος Windows. Υπάρχουν στην αγορά διάφορα πακέτα με λογισμικό ενεργητικής ανίχνευσης εισβολών συμβατό με λειτουργικά συστήματα της Microsoft (π.χ. Cisco Secure IDS, eTrust Intrusion Detection, Snort, Tripwire κ.α.) , αλλά κανένα από αυτά δεν αποτελεί χαρακτηριστικό ασφαλείας του λειτουργικού συστήματος κι έτσι δεν κρίνονται στην συγκεκριμένη εργασία.

Πύρινο Τείχος Προστασίας

Όταν τα Windows XP κυκλοφόρησαν για πρώτη φορά, τον Οκτώβριο του 2001, περιείχαν ένα περιορισμένων δυνατοτήτων τείχος προστασίας, το "Internet Connection Security". Το ίδιο ακριβώς τείχος προστασίας συμπεριλαμβανόταν και με τα Windows Server 2003. Μετά την εγκατάσταση του λειτουργικού, το τείχος προστασίας αυτό, ήταν απενεργοποιημένο και έπρεπε ο χρήστης να το ενεργοποιήσει από μόνος του, εφ' όσον βέβαια γνώριζε για την ύπαρξή του. Επίσης, όταν ήταν ενεργό, προκαλούσε πολλά προβλήματα, κυρίως όταν ο υπολογιστής στον οποίον χρησιμοποιούνταν δεν συνδεόταν απ' ευθείας στο διαδίκτυο, αλλά μέσω ενός άλλου υπολογιστή ή ενός δρομολογητή.

Το 2003, μετά την επίθεση των σκουληκιών Blaster και Sasser, και αφού προκλήθηκε σάλος με την προστασία που προσέφερε η Microsoft στα δεδομένα των πελατών της, αποφασίστηκε να πραγματοποιηθούν βελτιώσεις τόσο στη λειτουργικότητα του τείχους προστασίας, όσο και στις διεπαφές, ώστε να γίνει αποτελεσματικότερο και πιο εύχρηστο.

Τείχος Προστασίας των Windows XP SP2 και Windows Server 2008

Όπως αναφέρθηκε και παραπάνω, με την αναβάθμιση του λειτουργικού συστήματος Windows XP με το Service Pack 2, η Microsoft βελτίωσε κατά πολύ το τείχος προστασίας. Οι βελτιώσεις που πραγματοποίησε το κατέστησαν ένα καθ' όλα λειτουργικό τείχος προστασίας που λίγα είχε να ζηλέψει από άλλα τείχη προστασίας του εμπορίου.

Οι βελτιώσεις που πραγματοποιήθηκαν είναι οι εξής:

Η αρχική του κατάσταση είναι «σε λειτουργία» (on by default).

Στις προηγούμενες εκδόσεις των Microsoft Windows XP, το "Internet Connection Firewall" ήταν απενεργοποιημένο. Αυτό σημαίνει ότι οι χρήστες έπρεπε να γνωρίζουν την ύπαρξή του για να το ενεργοποιήσουν και να ψάξουν βαθιά στις ρυθμίσεις του συστήματος για να το παραμετροποιήσουν.

Στην έκδοση που συμπεριλαμβάνεται στο Service Pack 2, το τείχος προστασίας είναι ενεργοποιημένο αυτόματα για όλες τις συνδέσεις είτε αυτές είναι ενσύρματες (LAN, Dial-up) είτε ασύρματες (Wi-fi).

Μολονότι η πρακτική αυτή απέφερε αποτελέσματα στον τομέα της ασφάλειας στο λειτουργικό σύστημα, δημιούργησε και πολλά εμπόδια, καθώς πολλοί οργανισμοί αντιμετωπίζουν σημαντικά προβλήματα σχετικά με τη συμβατότητα του λογισμικού που χρησιμοποιούν με την έκδοση αυτή του τείχους προστασίας.

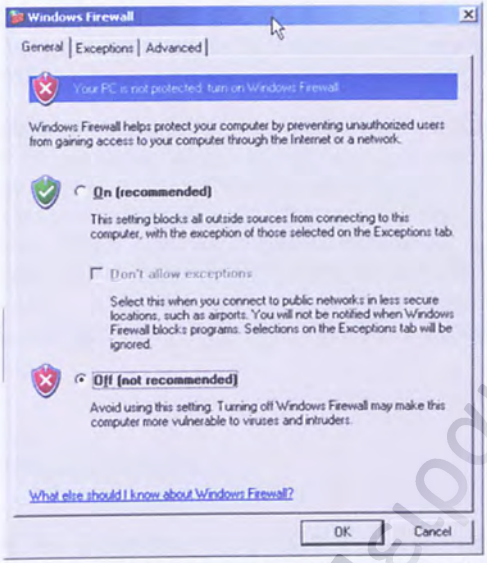
Μπορούν να πραγματοποιηθούν γενικές ρυθμίσεις οι οποίες αφορούν σε όλες τις συνδέσεις.

Σε αντίθεση με το τείχος προστασίας που «συνόδευε» το SP1, το τείχος προστασίας στα Windows XP SP2, διαθέτει τη δυνατότητα να πραγματοποιηθούν ρυθμίσεις που θα αφορούν σε όλες τις συνδέσεις του Η/Υ που χρησιμοποιείται. Εκτός από την προφανή ευκολία, αυτό το χαρακτηριστικό προσφέρει και ασφάλεια καθώς με αυτό τον τρόπο είναι πλέον δύσκολο να πραγματοποιηθεί λάθος ρύθμιση (σε περίπτωση βιασύνης ή σε περίπτωση που ξεχαστεί κάτι), καθώς η αρχική παραμετροποίηση του τείχους προστασίας αρκεί και για συνδέσεις που θα δημιουργηθούν μελλοντικά.

Διαχείριση

Οι ρυθμίσεις για το τείχος προστασίας των Windows XP SP2 πραγματοποιούνται μέσα από τον πίνακα ελέγχου, κάτι το οποίο καθιστά το Firewall πολύ πιο εύχρηστο. Επίσης, πολύ σημαντικό είναι ότι μόνο οι διαχειριστές του συστήματος έχουν πρόσβαση στις ρυθμίσεις αυτές και όχι όλοι οι χρήστες, όπως συνέβαινε με την παλαιότερη έκδοση.

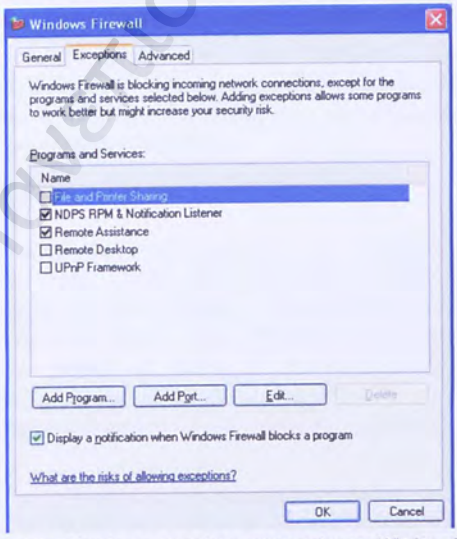
Καρτέλα «Γενικά»



Η καρτέλα "General" του τείχους προστασίας στα Windows XP SP2

Μέσα από την καρτέλα αυτή, ο χρήστης μπορεί να επιλέξει τριών ειδών καταστάσεις του τείχους προστασίας: Ενεργοποιημένο, Ενεργοποιημένο αγνοώντας τις εξαιρέσεις που έχουν οριστεί από το χρήστη, Απενεργοποιημένο.

Καρτέλα «Εξαιρέσεις»



Η καρτέλα «Εξαιρέσεις» του τείχους προστασίας στα Windows XP SP2

Μέσα από αυτό το παράθυρο ο χρήστης μπορεί να προσθέσει ή να αφαιρέσει ένα πρόγραμμα από τις εξαιρέσεις του τείχους προστασίας. Η προσθήκη ενός προγράμματος σε αυτή τη λίστα σημαίνει ότι το τείχος προστασίας δε θα μεσολαβεί κατά την επικοινωνία του προγράμματος αυτού με κάποιο άλλο Η/Υ.

Όταν ο χρήστης προσθέτει ένα πρόγραμμα, ερωτάται για την TCP ή UDP πόρτα που θα χρησιμοποιήσει το πρόγραμμα κατά την επικοινωνία του. Επίσης είναι στην ευχέρεια του χρήστη να επιλέξει εάν το πρόγραμμα αυτό θα επιτρέπεται να επικοινωνήσει με οποιαδήποτε διεύθυνση IP, με διευθύνσεις IP που βρίσκονται μόνο στο ίδιο τοπικό δίκτυο με τον Η/Υ στον οποίο λειτουργεί το τείχος προστασίας ή εάν η επικοινωνία θα επιτρέπεται μόνο με συγκεκριμένους Η/Υ, οι οποίοι ορίζονται σε μία λίστα από το χρήστη. Η τελευταία λειτουργία δεν είναι διαθέσιμη για διευθύνσεις του πρωτοκόλλου IPv6.

Καρτέλα «Για Προχωρημένους»

Από αυτό το παράθυρο, ο χρήστης μπορεί να εκτελέσει τις εξής λειτουργίες:

- Ρυθμίσεις σύνδεσης δικτύου

  Ο χρήστης μπορεί να επιλέξει για ποιες συνδέσεις του τοπικού Η/Υ θα λειτουργεί το τείχος προστασίας.

- Καταγραφή ασφάλειας

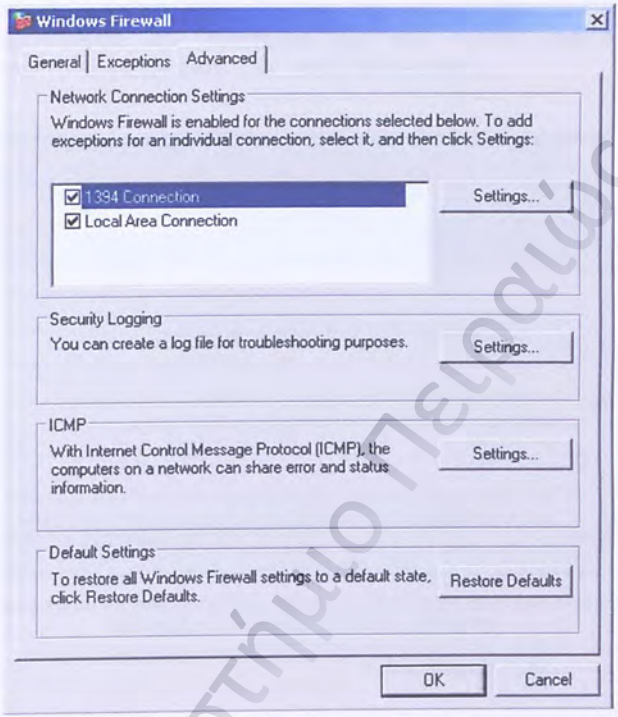
  Ο χρήστης μπορεί να επιλέξει τον τρόπο με τον οποίο θα γίνεται η καταγραφή των διαφόρων γεγονότων. Μπορεί να επιλέξει αν θα καταγράφονται τα πακέτα που απορρίφθηκαν, οι επιτυχημένες συνδέσεις και μπορεί επίσης να καθορίσει το όνομα, τη θέση καθώς και το μέγιστο μέγεθος του αρχείου καταγραφής (log file).

- ICMP

  Η ρύθμιση αυτή αφόρα στο κατά πόσο θα επιτρέπονται μηνύματα του πρωτοκόλλου ICMP. Οι προεπιλεγμένες ρυθμίσεις του τείχους προστασίας δεν επιτρέπουν αυτά τα μηνύματα. Έτσι είναι αδύνατον να απαντήσει ένας υπολογιστής στον οποίο το τείχος προστασίας είναι ενεργό, σε μία εντολή ping που θα σταλεί από κάποιο άλλο Η/Υ, εκτός και αν αυτό ρυθμιστεί από τη συγκεκριμένη καρτέλα.

- Προεπιλεγμένες ρυθμίσεις

  Από εδώ, ο χρήστης μπορεί να επαναφέρει το τείχος προστασίας στην αρχική του κατάσταση, όπως αυτό ήταν δηλαδή κατά την εγκατάσταση του λειτουργικού συστήματος.



Η καρτέλα «Για προχωρημένους» του τείχους προστασίας στα Windows XP SP2

Παρακολούθηση Εισερχόμενων Πακέτων

Αντίθετα με ότι συνέβαινε στις προηγούμενες εκδόσεις του τείχους προστασίας, στα Windows XP SP2 δίνεται η δυνατότητα να καθοριστούν μία ή περισσότερες διευθύνσεις από τις οποίες θα επιτρέπεται να λαμβάνονται τα εισερχόμενα πακέτα. Επίσης δίνεται η δυνατότητα να καθοριστεί αν τα εισερχόμενα πακέτα θα προέρχονται από μία πηγή η οποία είναι άμεσα προσβάσιμη (directly reachable source) ή απ' οπουδήποτε.

Επίσης στο τείχος προστασίας αυτό δίνεται η δυνατότητα να φιλτράρονται πακέτα IPv6.

Ειδοποιήσεις

Το τείχος προστασίας παρέχει τη δυνατότητα στο χρήστη να αλλάξει τον τρόπο με τον οποίο αντιμετωπίζεται ένα πρόγραμμα τη στιγμή που ο χρήστης επιχειρεί να το χρησιμοποιήσει. Όταν οι λειτουργίες του προγράμματος επιβάλουν τη χρήση κάποιας σύνδεσης και εφόσον δεν έχει πραγματοποιηθεί κάποια ρύθμιση που να αφορά στο λογισμικό αυτό, ο χρήστης ειδοποιείται και ερωτάται για τον τρόπο που επιθυμεί να αντιμετωπιστεί το λογισμικό από το τείχος προστασίας.

Το παράθυρο μέσω του οποίου ο χρήστης ερωτάται αν θέλει να εντάξει το χρησιμοποιούμενο πρόγραμμα στις εξαιρέσεις του τείχους προστασίας.

Πύρινο Τείχος Προστασίας στα Windows Vista και Windows Server 2008

Παρά τις σημαντικές βελτιώσεις που πραγματοποίησε η Microsoft στο πύρινο τείχος προστασίας με την προσθήκη στα Windows XP του Service Pack 2, υπήρχαν αρκετές ελλείψεις, τόσο στις λειτουργίες του τείχους προστασίας όσο και στον τρόπο χειρισμού του. Η Microsoft εντόπισε και πραγματοποίησε τις εξής βελτιώσεις στο καινούριο τείχος προστασίας:

- Ρύθμιση του IPsec μέσα από τις διεπαφές του τείχους προστασίας ώστε να υπάρχει συνεργασία μεταξύ των δύο ειδών προστασίας.

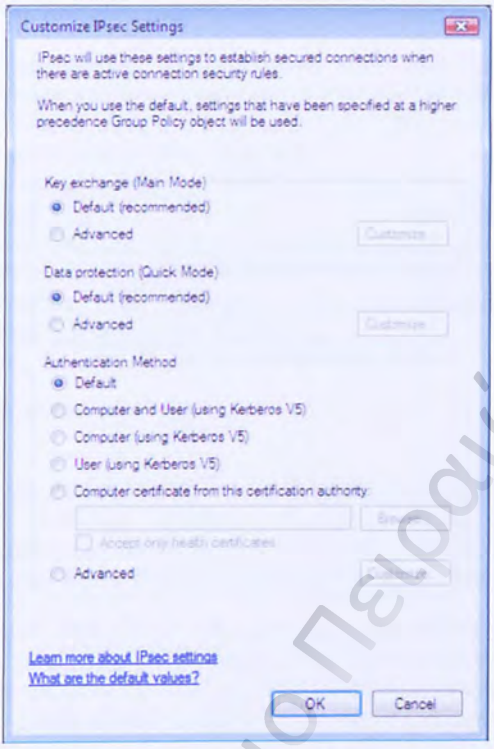
- Αυστηρή καταγραφή της αφετηρίας κάθε πακέτου (Strict Source Mapping)
- Προσθήκη λιστών ελέγχου πρόσβασης στα πρωτόκολλα TCP και UDP.
- Έλεγχος εξερχόμενων πακέτων.
- Υποστήριξη για 3 ή περισσότερα προφίλ δικτύου.
- Διεπαφές για προγραμματισμό του τείχους προστασίας με τη χρήση κώδικα (VBScript).

Συνεργασία με το IPsec

Το IPsec χαρακτηρίζεται από τους ειδικούς ως η πιο αποτελεσματική τεχνολογία που αφορά σε ασφάλεια δικτύων. Μέσα από το IPsec μπορεί να επιβεβαιώνεται η αυθεντικότητα ενός πακέτου αλλά και να κρυπτογραφούνται πακέτα, ώστε να καθίσταται ασφαλής η επικοινωνία μεταξύ Η/Υ, μέσω του πρωτοκόλλου IP.

Η διαφορά ενός τείχους προστασίας με το IPsec είναι ότι το μεν πρώτο καθορίζει ποιες θύρες επιτρέπεται να χρησιμοποιηθούν για τη μεταφορά πακέτων από και προς έναν Η/Υ, ενώ το δεύτερο καθορίζει κάτω από ποιες προϋποθέσεις επιτρέπεται να πραγματοποιηθεί η μεταφορά αυτή. Το IPsec δεν μπορεί να λειτουργήσει από μόνο του, αλλά μπορεί να προσφέρει πολλά όταν χρησιμοποιείται σε συνδυασμό με ένα τείχος προστασίας, όπως συμβαίνει στα Windows Vista και στα Windows 2008 server.

Έτσι λοιπόν, όταν ο χρήστης του τείχους προστασίας προσθέτει ένα νέο κανόνα σε αυτό, μπορεί να επιλέξει εάν τα πακέτα θα πρέπει να ελέγχονται ως προς την αυθεντικότητά τους ή και να κρυπτογραφούνται ταυτόχρονα. Η λειτουργία αυτή φαίνεται στην παρακάτω εικόνα:



Το παράθυρο μέσω του οποίου ο χρήστης παραμετροποιεί το IPsec.

Αυστηρή Καταγραφή της Αφετηρίας κάθε Πακέτου (Strict Source Mapping)

Στο πρωτόκολλο UDP δεν πραγματοποιείται σύνδεση μεταξύ των 2 Η/Υ που ανταλλάσσουν πακέτα. Αυτό καθιστά δύσκολο να αποφευχθεί η ανάμιξη κάποιου άλλου Η/Υ στη διαδικασία. Για παράδειγμα, εάν ο υπολογιστής Α στείλει ένα "request" στον υπολογιστή Β, ο Α θα αποδεχθεί απάντηση από οποιοδήποτε υπολογιστή απαντήσει στην ίδια πόρτα.

Αυτό μπορεί να αποφευχθεί με τη λειτουργία της αυστηρής καταγραφής της αφετηρίας κάθε πακέτου (strict source mapping). Έτσι, όταν σταλεί ένα "request", η απάντηση δε θα πρέπει να γίνει δεκτή παρά μόνο αν προέρχεται από την ίδια IP διεύθυνση που δηλώθηκε κατά την αποστολή του "request".

Προσθήκη λιστών ελέγχου πρόσβασης στα πρωτόκολλα TCP και UDP

Το τείχος προστασίας των Windows Vista (και των Windows Server 2008) παρέχει τη δυνατότητα προσθήκης λιστών ελέγχου πρόσβασης στα πρωτόκολλα UDP και TCP. Αυτό σημαίνει ότι μία πόρτα μπορεί να είναι ανοιχτή μόνο για μία συγκεκριμένη διεργασία.

Μία τέτοια λίστα ελέγχου πρόσβασης περιέχει τον αριθμό της πόρτας και το μοναδικό χαρακτηριστικό (service SID) της διεργασίας που επιτρέπεται να χρησιμοποιήσει αυτή την πόρτα. Έτσι πλέον, μία πόρτα μπορεί να ανοίξει μόνο για τη διεργασία που είναι επιθυμητό να τη χρησιμοποιεί και όχι για όλες, κάτι που αποτελούσε κενό ασφάλειας στις προηγούμενες εκδόσεις του τείχους προστασίας των Microsoft Windows.

Έλεγχος εξερχόμενων πακέτων

Η έλλειψη της δυνατότητας φιλτραρίσματος των εξερχόμενων πακέτων, θεωρείται από πολλούς ειδικούς το μεγαλύτερο μειονέκτημα των προηγούμενων εκδόσεων του Windows Firewall. Η έλλειψη αυτή διορθώθηκε από τη Microsoft στο τείχος προστασίας των Windows Vista.

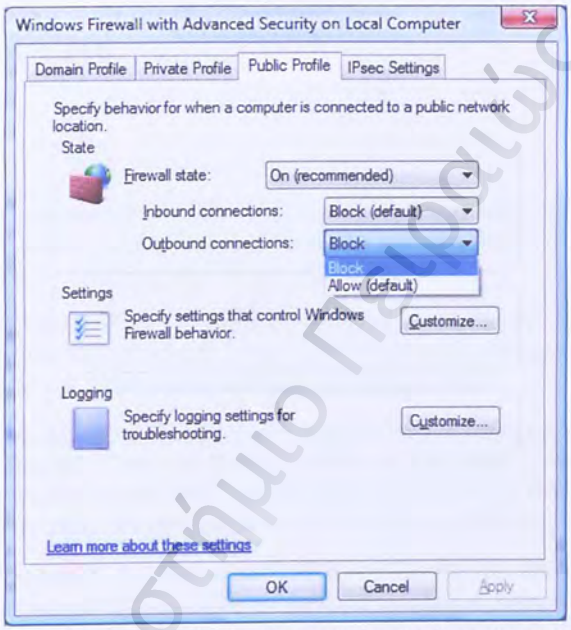
Από την εγκατάσταση των Windows σε έναν Η/Υ το τείχος προστασίας απαγορεύει σε κάποιες διεργασίες να επικοινωνήσουν με το δίκτυο του Η/Υ. Η ρύθμιση των παραμέτρων του ελέγχου εξερχόμενων πακέτων, δε μπορεί να πραγματοποιηθεί μέσω κάποιου παραθύρου των Windows, καθώς κάτι τέτοιο δεν υπάρχει. Για να δει ο διαχειριστής του συστήματος τις ρυθμίσεις του ελέγχου εξερχόμενων πακέτων πρέπει να εντοπίσει στη «registry» του συστήματος το εξής κλειδί: HKLM \ System \ CurrentControlSet \ Services \ SharedAccess \ Parameters \ FirewallPolicy \ RestrictedServices \ Static \ System. Επίσης, για να πραγματοποιηθούν αλλαγές στο φίλτρο των εξερχόμενων πακέτων, ο διαχειριστής πρέπει είτε να τροποποιήσει απ' ευθείας τη «registry» του συστήματος είτε να χρησιμοποιήσει τις διεπαφές προγραμματισμού του τείχους προστασίας, που περιγράφονται παρακάτω. Αυτό καθιστά τη ρύθμιση εξαιρετικά δύσκολη και χρονοβόρα, κάτι που για έναν χρήστη με περιορισμένες γνώσεις αποτελεί τροχοπέδη.

Υποστήριξη για 3 προφίλ δικτύου

Στα Windows XP, ο χρήστης είχε τη δυνατότητα να επιλέξει τον τρόπο συμπεριφοράς του τείχους προστασίας μέσα από δύο προφίλ. Το ένα αφορούσε στην περίπτωση που ο υπολογιστής ήταν συνδεδεμένος σε έναν τομέα δικτύου (domain) και το άλλο ήταν ένα προφίλ «γενικής χρήσης» που χρησιμοποιούνταν σε οποιαδήποτε άλλη περίπτωση. Αυτό επέφερε προβλήματα στην περίπτωση που ο χρήστης επιθυμούσε να χρησιμοποιήσει τρία ή περισσότερα δίκτυα με διαφορετικές απαιτήσεις στον τομέα της ασφάλειας (π.χ εταιρικό δίκτυο, οικιακό δίκτυο, δημόσιο δίκτυο κ.α.).

Στα Windows Vista, υπάρχουν πλέον τρία διαφορετικών προφίλ δικτύου με διαφορετικές ρυθμίσεις ασφαλείας. Τα προφίλ αυτά αφορούν σε οικιακό δίκτυο, εταιρικό δίκτυο και δημόσιο δίκτυο.

Σημαντικό είναι επίσης να αναφερθεί ότι τα Windows Vista είναι σε θέση να ανιχνεύουν από μόνα τους τυχόν αλλαγές στο δίκτυο που είναι συνδεδεμένος ο Η/Υ και να πραγματοποιούν αλλαγή στο προφίλ μέσα σε διάστημα 200msec. Εάν το δίκτυο που συνδέονται είναι άγνωστο (ο χρήστης συνδέεται για πρώτη φορά σε αυτό), επιλέγεται το ασφαλέστερο προφίλ, αυτό του δημοσίου δικτύου).



Η διεπαφή μέσω της οποίας ο χρήστης παραμετροποιεί τα προφίλ του τείχους προστασίας

Διεπαφές για προγραμματισμό του τείχους προστασίας με τη χρήση κώδικα (VBScript)

Το τείχος προστασίας των Vista, προσφέρει τη δυνατότητα να παραμετροποιηθεί το τείχος προστασίας μέσω κώδικα VBScript. Αυτό προσφέρει ευελιξία στην περίπτωση που ο διαχειριστής θέλει να δημιουργήσει κάποιον εξειδικευμένο κανόνα για την πρόσβαση μέσω του δικτύου. Ένα παράδειγμα είναι η ενεργοποίηση του τείχους προστασίας (αν αυτό είναι απενεργοποιημένο) όταν ο χρήστης συνδεθεί μέσω VPN σε κάποιο δίκτυο.

```
Set objFirewall =
CreateObject("HNetCfg.FwMgr")
Set objPolicy =
objFirewall.LocalPolicy.CurrentProfile
Set colPorts = objPolicy.GloballyOpenPorts
Set objPort = colPorts.Item(9999,6)
objPort.Enabled = TRUE
```

Παράδειγμα κώδικα VBScript μέσω του οποίου ο διαχειριστής ανοίγει την πόρτα 9999.

Κακόβουλο λογισμικό

Ιοί

Ένας ιός υπολογιστών είναι ένα πρόγραμμα υπολογιστή, το οποίο μπορεί να αντιγραφεί χωρίς παρέμβαση του χρήστη και να μολύνει τον υπολογιστή χωρίς τη γνώση ή την άδεια του χρήστη του.

Ο αριθμός των ιών που είναι πιθανό να μολύνουν έναν υπολογιστή με λειτουργικό σύστημα της Microsoft, είναι αδύνατο να προσδιοριστεί. Οι ειδικοί μιλούν για μέγεθος της τάξης των δεκάδων εκατομμυρίων.

Από τη Microsoft δεν παρέχεται λογισμικό αντιμετώπισης ιών με καμία έκδοση των Windows. Παρόλα αυτά, η ίδια η Microsoft επισημαίνει την ανάγκη χρήσης τέτοιου λογισμικού, καθώς τόσο η ποσότητα των ιών όσο και ο ρυθμός διάδοσής τους δεν επιτρέπουν να αγνοηθεί ο κίνδυνος αυτός.

Από την έκδοση Windows XP SP2 και μετά σε ότι αφορά τους προσωπικούς υπολογιστές και από την έκδοση Windows Server 2003 σε ότι αφορά τους εξυπηρετητές (Servers), η Microsoft έχει εφοδιάσει τα λειτουργικά της με τη δυνατότητα ειδοποίησης του χρήστη, σε περίπτωση που δεν υπάρχει λογισμικό αντιμετώπισης ιών εγκατεστημένο ή σε περίπτωση που υπάρχει αλλά δεν λειτουργεί σωστά ή δεν είναι ενημερωμένο.

Σκουλήκια (Worms)

Τα σκουλήκια είναι κακόβουλο λογισμικό, που σε αντίθεση με τους ιούς, δεν μολύνουν αρχεία, αλλά καταναλώνουν πόρους του δικτύου, με σκοπό να το καταστήσουν μη λειτουργικό. Επίσης χρησιμοποιούν τα δίκτυα ηλεκτρονικών υπολογιστών για να διαδοθούν.

Τα σκουλήκια σχεδιασμένα να μολύνουν ηλεκτρονικούς υπολογιστές με λειτουργικό σύστημα Windows, θεωρείται σύμφωνα με τη διαδικτυακή εγκυκλοπαίδεια "Wikipedia" ότι ανέρχονται σε 13,000 περίπου

Σε καμία έκδοση των Windows δεν παρέχεται λογισμικό αντιμετώπισης αυτής της απειλής, παρόλο που τέτοιο λογισμικό θεωρείται απαραίτητο για την ασφαλή λειτουργία του υπολογιστή.

Στην περίπτωση της απειλής αυτής, και κυρίως επειδή τα πακέτα αντιμετώπισης τρίτων κατασκευαστών αντιμετωπίζουν εκτός από τους ιούς και τα σκουλήκια, σύμφωνα με τη Microsoft, η ειδοποίηση που αναφέρθηκε προηγουμένως σχετικά με τους ιούς καλύπτει και αυτή την κατηγορία κακόβουλου λογισμικού.

Δούρειοι ίπποι (Trojan horses)

Οι δούρειοι ίπποι είναι λογισμικό σχεδιασμένο ώστε να επιτρέπουν την απομακρυσμένη διαχείριση ενός υπολογιστή με σκοπό να πραγματοποιηθούν κάποιες διεργασίες σε αυτόν.

Τα πράγματα στην περίπτωση των δούρειων ίππων δεν διαφέρουν σχεδόν καθόλου απ' ότι στην κατηγορία των σκουληκιών. Λογισμικό αντιμετώπισης δεν παρέχεται μαζί με το λειτουργικό, αλλά θεωρείται απαραίτητη η χρήση του.

Spyware

Ως Spyware ορίζεται το λογισμικό αυτό που εγκαθίσταται σε ηλεκτρονικούς υπολογιστές χωρίς τη συγκατάθεση του χρήστη και έχει ως σκοπό τη συλλογή πληροφοριών για τον ίδιο το χρήστη. Οι πληροφορίες αυτές μπορεί να είναι από λιγότερο σημαντικές (π.χ. προτιμήσεις ιστοσελίδων) έως καταστροφικές (π.χ. αριθμός πιστωτικής κάρτας).

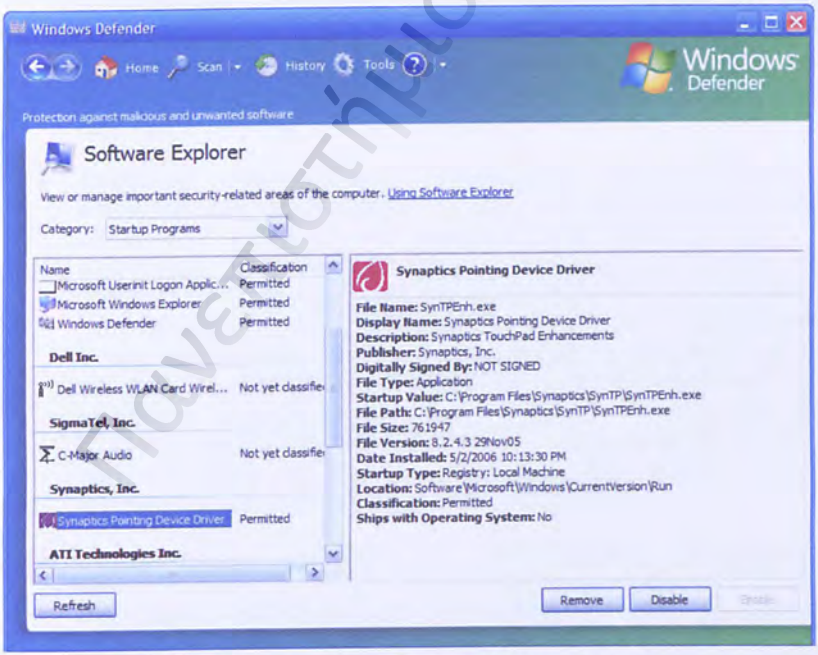
Για το λόγο αυτό και επειδή είναι η μόνη κατηγορία κακόβουλου λογισμικού που μπορεί να επιφέρει άμεσες οικονομικές συνέπειες (και όχι μόνο) η Microsoft, από την έκδοση Vista και μετά, εφοδιάζει τα Windows με το λογισμικό Windows Defender. Φυσικά στις εκδόσεις Windows XP, Windows 2003 Server και Windows 2008 Server δεν παρέχεται προεγκατεστημένο, αλλά ο χρήστης μπορεί να κατεβάσει και να εγκαταστήσει το λογισμικό αυτό μέσω της ιστοσελίδας της Microsoft.

Windows Defender

Το λογισμικό Windows Defender παρέχεται από τη Microsoft δωρεάν (μάλιστα εγκαθίσταται αυτόματα από την έκδοση Vista και μετά) και έχει ως σκοπό την ανίχνευση Spyware σε πραγματικό χρόνο, αλλά και την αφαίρεσή του σε περίπτωση που ο υπολογιστής είναι ήδη μολυσμένος.

Το Windows Defender μπορεί να εκτελέσει τις εξής λειτουργίες:

- Αυτόματη εκκίνηση: Ελέγχει λίστες των προγραμμάτων που επιτρέπονται αυτόματα να εκτελούνται όταν εκκινείται το σύστημα.
- Παράμετροι συστήματος (Ρυθμίσεις): Ελέγχει ρυθμίσεις σχετικές με την ασφάλεια των Windows.
- Πρόσθετα του Internet Explorer: Ελέγχει προγράμματα που εκτελούνται αυτόματα όταν εκκινείται ο Internet Explorer.
- Παράμετροι Internet Explorer (Ρυθμίσεις): Ελέγχει τις ρυθμίσεις ασφαλείας του προγράμματος περιήγησης στο διαδίκτυο.
- Στοιχεία λήψης του Internet Explorer : Ελέγχει αρχεία και προγράμματα που είναι σχεδιασμένα να λειτουργούν με τον Internet Explorer.
- Υπηρεσίες και προγράμματα οδήγησης: Ελέγχει υπηρεσίες και προγράμματα οδήγησης που αλληλεπιδρούν με τα Windows και τα προγράμματά που είναι εγκατεστημένα.
- Εκτέλεση εφαρμογής: Ελέγχει όταν τα προγράμματα εκκινούνται και οποιαδήποτε λειτουργία εκτελούν όταν βρίσκονται σε λειτουργία.
- Δήλωση εφαρμογής: Ελέγχει εργαλεία και αρχεία στο λειτουργικού συστήματος όταν προγράμματα μπορούν να δηλώσουν να εκτελούνται οποιαδήποτε στιγμή.
- Πρόσθετα των Windows: Ελέγχει πρόσθετα προγραμμάτων (γνωστά ως εφαρμογές λογισμικού) για τα Windows.



Το λογισμικό αντιμετώπισης Spyware: Windows Defender

Ασφάλεια λογισμικού

Τα πακέτα που χρησιμοποιούνται από τη Microsoft, από την έκδοση των Windows XP και σε όλες τις μεταγενέστερες, είναι της μορφής .msi. Τα αρχεία msi διαχειρίζονται από τον Windows Installer.

Windows Installer

Ο Windows Installer είναι ένα επεκτάσιμο σύστημα διαχείρισης λογισμικού, διαχειρίζεται την εγκατάσταση λογισμικού, διαχειρίζεται τις προσθήκες και τις διαγραφές στοιχείων λογισμικού, παρακολουθεί την ανοχή των αρχείων και εκτελεί βασικές εργασίες αποκατάστασης μετά από ζημιές, χρησιμοποιώντας τις λειτουργίες επαναφοράς. Επιπλέον, υποστηρίζει την εγκατάσταση και την εκτέλεση λογισμικού από πολλαπλές πηγές και είναι δυνατό να προσαρμοστεί από προγραμματιστές που επιθυμούν να εγκαταστήσουν προσαρμοσμένα προγράμματα.

Σε ότι αφορά θέματα ασφαλείας, σύμφωνα με τη Microsoft, ο Windows Installer είναι σε θέση να:

- Επαναφέρει τον υπολογιστή στην αρχική του κατάσταση, εάν υπάρξει μια αποτυχία κατά την εγκατάσταση. Ο Windows Installer παρακολουθεί όλες τις αλλαγές που γίνονται στο σύστημα κατά τη διαδικασία εγκατάστασης του προγράμματος. Εάν η εγκατάσταση δεν ολοκληρωθεί με επιτυχία, το πρόγραμμα εγκατάστασης μπορεί να επαναφέρει το σύστημα στην αρχική του κατάσταση. Αυτή η διαδικασία είναι γνωστή ως "επαναφορά".

- Συμβάλλει στην αποτροπή ορισμένων τύπων διένεξης στο εσωτερικό των προγραμμάτων. Ένα πρόγραμμα που εγκαθίσταται ή καταργείται ενδέχεται να προκαλέσει ζητήματα σε ένα άλλο πρόγραμμα που υπάρχει ήδη στον υπολογιστή ή ακόμη και να διακόψει τη λειτουργία του υπολογιστή (κάνοντάς τον να "κολλάει"). Το πρόγραμμα εγκατάστασης επιβάλλει κανόνες εγκατάστασης οι οποίοι συμβάλλουν στην αποτροπή διενέξεων που δημιουργούνται είτε όταν μια λειτουργία εγκατάστασης πραγματοποιεί ενημερώσεις σε αρχείο βιβλιοθήκης δυναμικής σύνδεσης (dynamic-link library-DLL) που χρησιμοποιείται από κοινού με άλλο πρόγραμμα, είτε όταν μια λειτουργία κατάργησης διαγράφει ένα αρχείο DLL που χρησιμοποιείται από κοινού με άλλο πρόγραμμα.

- Πραγματοποιεί διάγνωση και επιδιόρθωση κατεστραμμένων προγραμμάτων. Ένα πρόγραμμα είναι δυνατό να ζητήσει από το πρόγραμμα εγκατάστασης να προσδιορίσει εάν ένα εγκατεστημένο πρόγραμμα περιέχει αρχεία που λείπουν ή είναι κατεστραμμένα. Στη συνέχεια μπορεί να ζητήσει από την υπηρεσία να επιδιορθώσει κατάλληλα το πρόγραμμα, αντιγράφοντας ξανά μόνο εκείνα τα αρχεία που λείπουν ή είναι κατεστραμμένα.

- Καταργεί με αξιοπιστία υπάρχοντα προγράμματα. Το πρόγραμμα εγκατάστασης είναι δυνατό να καταργήσει αξιόπιστα οποιοδήποτε πρόγραμμα έχει εγκαταστήσει προηγουμένως και να αφαιρέσει όλες τις συσχετιζόμενες καταχωρήσεις μητρώου και αρχεία προγραμμάτων, εκτός από εκείνα που είναι κοινά με άλλο εγκατεστημένο λογισμικό.

Πακέτα λογισμικού msi

Τα αρχεία με επέκταση msi είναι τα πακέτα λογισμικού που προορίζονται για εγκατάσταση σε υπολογιστές με λειτουργικά συστήματα της Microsoft.

Από τη σκοπιά της ασφάλειας, τα πακέτα msi, όπως φαίνεται και στον παρακάτω πίνακα, πληρούν πολλές προϋποθέσεις ώστε να θεωρούνται αρκετά ασφαλή. Γι' αυτόν ακριβώς το λόγο, κάθε αρχείο με επέκταση msi μπορεί να διατηρεί τις εξής πληροφορίες:

- **Ψηφιακή υπογραφή:** Η πληροφορία αυτή επιτρέπει την πιστοποίηση του δημιουργού του αρχείου.
- **Άθροισμα ελέγχου λάθους (Checksum):** Τα πακέτα msi συνοδεύονται από ένα άθροισμα ελέγχου λάθους, ώστε να διασφαλίζεται ότι δεν έχουν αλλοιωθεί.
- **Έκδοση:** Τα πακέτα τύπου msi περιέχουν πληροφορία σχετική με την έκδοση (version) του λογισμικού που περιέχουν, με σκοπό την επιβεβαίωση του περιεχομένου του.
- **Περιγραφή:** Στα πακέτα αυτά, μπορεί να αποθηκευτεί και η περιγραφή του περιεχομένου, με σκοπό, όπως και με την έκδοση, να επαληθεύεται το περιεχόμενο του πακέτου.
- **Εξαρτήσεις:** Προσφέρεται η δυνατότητα αποθήκευσης του ονόματος των πακέτων που πρέπει να προϋπάρχουν εγκατεστημένα στο σύστημα, ώστε να μην δημιουργηθεί κάποια αστάθεια στο σύστημα κατά την εγκατάσταση.
- **Συγκρούσεις:** Προσφέρεται η δυνατότητα αποθήκευσης του ονόματος των πακέτων που δεν πρέπει να προϋπάρχουν εγκατεστημένα στο σύστημα, ώστε να μην δημιουργηθεί κάποια σύγκρουση (conflict), η οποία θα μπορούσε να δημιουργήσει αστάθεια στο σύστημα.
- **Άδειες, ιδιοκτήτης:** Τα πακέτα msi προσφέρουν τη δυνατότητα να αποθηκεύονται σε αυτά πληροφορίες για τις άδειες χρήσης τους (permissions), τους ιδιοκτήτες τους, και τις ομάδες που τα χρησιμοποιούν.

- **Όνομα:** Παρέχεται η δυνατότητα αποθήκευσης του ονόματος του πακέτου και μέσα στο ίδιο το πακέτο. Αυτό χρησιμεύει για επιβεβαίωση του ονόματος του αρχείου που βλέπει ο χρήστης.

Κατά την εγκατάσταση μίας εφαρμογής, ο Windows Installer διαβάζει τις πληροφορίες που περιέχονται στο msi πακέτο και ενημερώνει το χρήστη

LINUX

Σύστημα Αρχείων και Ασφάλεια.

Υπάρχουν αρκετά συστήματα αρχείων που χρησιμοποιούνται από διάφορες εκδόσεις Linux που κυκλοφορούν. Τα πλέον διαδεδομένα είναι τα εξής τρία:

- ReiserFS
- Ext3
- JFS

Το Σύστημα Αρχείων ReiserFS

Το σύστημα αρχείων ReiserFs ανήκει στην κατηγορία των συστημάτων αρχείων που ονομάζονται "Journaling File Systems". Τα συστήματα αρχείων που ανήκουν σε αυτή την κατηγορία καταγράφουν σε ένα αρχείο λειτουργιών (Journal) οποιαδήποτε αλλαγή πραγματοποιείται σε αυτά, πριν όμως αυτή εφαρμοστεί.

Ενσωματώθηκε για πρώτη φορά στην έκδοση του πυρήνα 2.4.1 και χρησιμοποιείται ως προεπιλεγμένο σύστημα αρχείων από τις διανομές Elive, Xandros, Linspire, GoboLinux και Yoper Linux. Επίσης χρησιμοποιούνταν από τη διανομή Suse Linux της Novell μέχρι και το 2006.

Σήμερα η ομάδα της Nemesys που το κατασκεύασε το θεωρεί ολοκληρωμένο κι έτσι έχει σταματήσει η ανάπτυξή του, και η Nemesys έχει επικεντρωθεί στην ανάπτυξη του διαδόχου του, του Reiser4. Από πολλούς θεωρείται ξεπερασμένο, αν και εξακολουθεί να χρησιμοποιείται ευρέως.

Το Σύστημα Αρχείων ext3

Το ext3, σε αντίθεση με τον προκάτοχό του, ext2, ανήκει στην ίδια κατηγορία συστημάτων αρχείων με το προαναφερθέν Reiserfs, τα "Journaling File Systems" και είναι αυτό που προτείνεται από τις περισσότερες από τις πιο δημοφιλείς διανομές Linux.

Παρόλο που σε ότι αφορά την ταχύτητα προσπέλασης αρχείων είναι λιγότερο γρήγορο σε σχέση με άλλα συστήματα αρχείων που χρησιμοποιούνται από διάφορες διανομές Linux, θεωρείται ασφαλέστερο, λόγω των εκτεταμένων δοκιμών και βελτιώσεων που έχουν γίνει και απαιτεί λιγότερους πόρους από το σύστημα στο οποίο λειτουργεί.

Το Σύστημα Αρχείων JFS

Αρχικά, το JFS σχεδιάστηκε από την IBM για να λειτουργεί με το λειτουργικό σύστημα της εν λόγω εταιρείας AIX. Το 1999, 8 χρόνια μετά την αρχική του εμφάνιση, δόθηκε στην κοινότητα ανοιχτού κώδικα για χρήση. Έτσι, εισχώρησε στο βασικό λειτουργικό σύστημα που υποστηρίζεται από την κοινότητα αυτή, το Linux, από την έκδοση πυρήνα 2.4.1 και μετά.

Όπως και τα δύο προαναφερθέντα συστήματα αρχείων, το JFS ανήκει και αυτό στην κατηγορία των "Journaling File Systems". Έχει εξίσου ικανοποιητική απόδοση και σε συστήματα με ελαφρύ φόρτο αλλά και σε συστήματα με βαρύ φόρτο, σε αντίθεση με άλλα συστήματα αρχείων που συμπεριφέρονται διαφορετικά κάτω από βαρύ ή ελαφρύ φόρτο. Επίσης δεν απαιτεί μεγάλες επεξεργαστικές δυνατότητες από το εκάστοτε σύστημα στο οποίο είναι εγκατεστημένο.

Τρόπος ανάλυσης της ασφάλειας των συστημάτων αρχείων

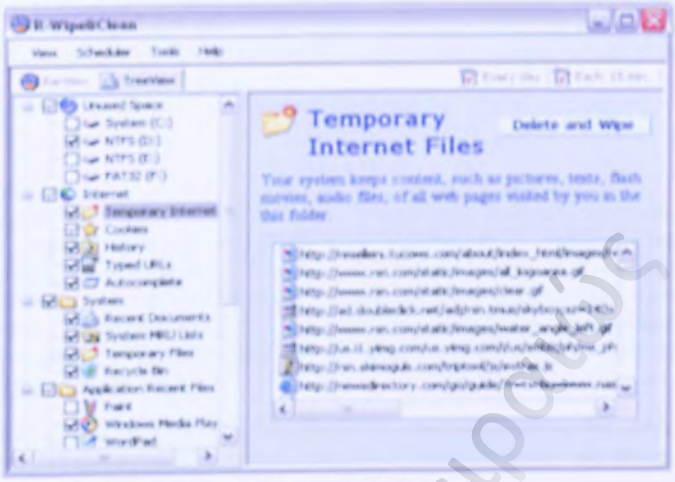
Τα τρία προαναφερθέντα συστήματα αρχείων παρουσιάζουν πολλές ομοιότητες στον τρόπο λειτουργίας τους κι έτσι, στην ανάλυση των διαφόρων τομέων της ασφάλειας που ακολουθεί, θα υπάρχει αναφορά σε αυτά μόνο όπου υπάρχει διαφοροποίηση, αλλιώς ότι γράφεται θα ισχύει και για τα τρία συστήματα αρχείων.

Διαγραφή αρχείων με ασφάλεια

Ένα από τα πράγματα που συνήθως οι χρήστες δεν γνωρίζουν ή ξεχνούν είναι ότι όταν διαγράφουν ένα αρχείο, στην πραγματικότητα αυτό δεν εξαφανίζεται αλλά υπάρχουν τρόποι να το ανακτήσει κάποιος, αν το επιθυμεί, ακόμα και αν έχει πραγματοποιηθεί διαμόρφωση του δίσκου, ή απόπειρα να καταστραφεί ο δίσκος.

Η λύση του προβλήματος αυτού που περιέχεται στις διάφορες εκδόσεις Linux, είτε κατά την εγκατάστασή, είτε μέσω των "repositories" ώστε τα αρχεία να μην είναι ανακτήσιμα, είναι η χρήση προγραμμάτων που «σκουπίζουν» (wipe) τα δεδομένα που έχουν παραμείνει στους δίσκους μετά τη διαγραφή κάποιου αρχείου. Αυτό επιτυγχάνεται με τη συνεχή εναλλαγή των μαγνητικών bits που υπάρχουν στους σκληρούς δίσκους, ώστε μετά το τέλος της διαδικασίας να μην υπάρχει σε αυτά καμία ένδειξη για την προ-της διαγραφής κατάστασή τους. Κάποια από τα προγράμματα τα οποία πραγματοποιούν το "wiping" είναι τα wipe, το R-Wipe και fwip.

Μία δεύτερη λύση είναι η κρυπτογράφηση των σημαντικών αρχείων, ώστε ακόμα και αν υπάρξει ανάκτηση, μετά τη διαγραφή, από κάποιον τρίτο, να μην είναι δυνατή η ανάγνωση τους.



Το πρόγραμμα R-Wipe

Λίστες ελέγχου πρόσβασης (Access Control Lists)

Ένα βασικό μειονέκτημα των περισσότερων εκδόσεων Linux, είναι η έλλειψη λιστών ελέγχου πρόσβασης. Μπορούν να αποδοθούν δικαιώματα σε προκαθορισμένες κατηγορίες χρηστών (π.χ. user, superuser, administrator κλπ) αλλά δεν μπορούν να αποδοθούν δικαιώματα σε μεμονωμένους χρήστες. Αξίζει να σημειωθεί ότι οι διανομές "Red Hat Fedora Core" και "Red Hat Enterprise Linux" έχουν τροποποιημένο πυρήνα ο οποίος επιτρέπει αυτή τη λειτουργία, την ύπαρξη δηλαδή λιστών ελέγχου πρόσβασης.

Κρίσιμα αρχεία συστήματος

Όπως κάθε λειτουργικό σύστημα, έτσι και το Linux, περιέχει κάποια αρχεία στα οποία αποθηκεύονται βασικές πληροφορίες για το σύστημα. Κάποια από αυτά τα αρχεία, όπως για παράδειγμα το αρχείο στο οποίο αποθηκεύονται οι κωδικοί (passwords) των χρηστών, είναι εξαιρετικά σημαντικά. Παρακάτω παρουσιάζονται οι κατάλογοι που περιέχουν αρχεία σημαντικά για το σύστημα, καθώς και ο τρόπος που πρέπει να είναι παραμετροποιημένοι ώστε το σύστημα να λειτουργεί ορθά αλλά και με ασφάλεια.

/etc/

Σε αυτόν τον κατάλογο περιέχεται η πλειοψηφία των αρχείων που περιέχουν τις ρυθμίσεις (configuration files) για το σύστημα και τις εφαρμογές που είναι εγκατεστημένες σε αυτό. Εάν κάποιος επιτιθέμενος μπορεί να μεταβάλλει τα αρχεία αυτού του φακέλου, κατά πάσα πιθανότητα σύντομα θα γίνει "root".

/etc/passwd

Το αρχείο αυτό είναι ίσως το πιο σημαντικό αρχείο συστήματος στο Linux. Εκεί περιέχονται τα ονόματα των χρηστών, η ομάδα στην οποία ανήκουν (user, root κ.λ.π.). Επίσης εξαρτάται από τις ρυθμίσεις του administrator εάν σε αυτό το αρχείο θα περιέχονται και οι κωδικοί (passwords) των χρηστών. Το αρχείο αυτό πρέπει να μπορεί να αναγνωστεί από οποιοδήποτε χρήστη, γιατί αλλιώς δεν θα είναι δυνατή η εκτέλεση ακόμα και των απλούστερων εντολών.

Είναι πολύ πιο ασφαλές οι κωδικοί να αποθηκεύονται σε άλλο αρχείο (αυτό είναι το /etc/shadows) καθώς έτσι είναι δυσκολότερο να κλαπούν από τον επιτιθέμενο.

/etc/shadow

Εδώ, κατά πάσα πιθανότητα, βρίσκονται αποθηκευμένα τα ζεύγη username-password των χρηστών, καθώς και πληροφορίες για τους λογαριασμούς όπως η ημερομηνία λήξης τους και άλλα ειδικά πεδία. Αυτό το αρχείο πρέπει να είναι προστατευμένο και μόνο ο root θα πρέπει να έχει πρόσβαση να το διαβάσει.

/etc/groups

Σε αυτό το αρχείο περιέχονται πληροφορίες για τις ομάδες στις οποίες ανήκουν οι χρήστες. Ίσως σε αυτό το αρχείο να περιέχονται και οι κωδικοί των ομάδων αλλά όπως και με τους κωδικούς των μεμονωμένων χρηστών δεν συνηθίζεται καθώς δεν είναι τόσο ασφαλές.

/etc/gshadow

Όπως αναφέρθηκε και παραπάνω, όταν οι κωδικοί των ομάδων δεν βρίσκονται στο αρχείο /etc/groups (κάτι που δεν είναι ασφαλές) βρίσκονται τοποθετημένοι στο /etc/gshadow. Και αυτό το αρχείο, όπως και το /etc/shadows πρέπει να είναι απόλυτα προστατευμένο και μόνο ο root να έχει πρόσβαση σε αυτό.

Κρυπτογράφηση αρχείων

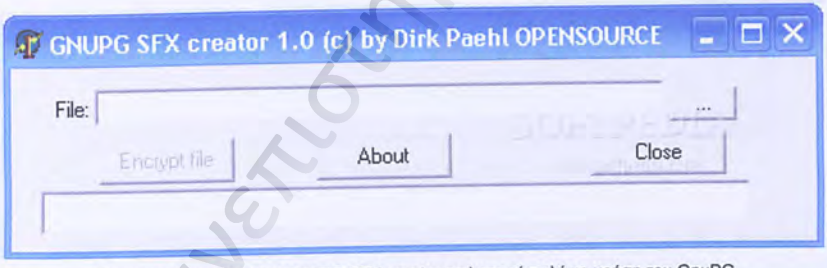
Εάν σε ένα σύστημα υπάρχουν αρχεία τα οποία δεν πρέπει να αναγνωστούν από τρίτους, είναι απαραίτητη η κρυπτογράφησή τους. Πολύ περισσότερο εάν αυτά τα αρχεία πρόκειται να μεταφερθούν μέσα από ένα τοπικό δίκτυο ή το διαδίκτυο. Παρακάτω παρουσιάζονται κάποια εργαλεία που προσφέρονται για το λειτουργικό σύστημα Linux, τα οποία κρυπτογραφούν τα ευαίσθητα δεδομένα.

PGP (Pretty Good Privacy)

Το PGP είναι ένα πρόγραμμα το οποίο περιέχεται στις περισσότερες εκδόσεις Linux. Η χρήση του πραγματοποιείται από τη γραμμή εντολών, αλλά είναι δυνατή η χρήση του με GUI, καθώς έχουν γίνει διάφορες προσπάθειες από εταιρίες και ιδιώτες να ενσωματωθούν γραφικά σε αυτό. Δεν χρησιμοποιείται πολύ καθώς αντικαταστάθηκε από το GnuPG το οποίο αναλύεται παρακάτω.

GnuPg

Το GnuPG είναι ένα γερμανικό πρόγραμμα ανοιχτού κώδικα, το οποίο διατίθεται για όλες τις ευρέως γνωστές διανομές Linux. Η χρήση του είναι παρόμοια με του PGP, καθώς είναι σχεδιασμένο να λειτουργεί από κονσόλα, αλλά υπάρχουν διάφορα εργαλεία που του προσθέτουν γραφικό περιβάλλον.



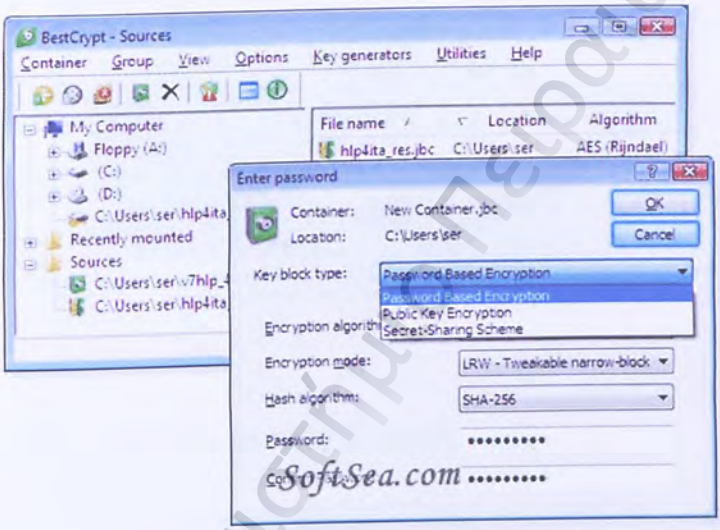
Το γραφικό περιβάλλον GNUPG SFX creator απλοποιεί πολύ τη χρήση του GnuPG

Κρυπτογράφηση συστήματος αρχείων

Δυστυχώς, η διαδικασία της κρυπτογράφησης κάποιων μεμονωμένων αρχείων είναι πολύ πιθανό να έχει διαρροές. Προσωρινά αρχεία (temporary files), μη σωστό «σκούπισμα» (wiping) των αρχείων που κρυπτογραφήθηκαν και άλλοι παράγοντες, μπορεί να βοηθήσουν κάποιον επιτιθέμενο στο σύστημα να αποκτήσει πρόσβαση στις ευαίσθητες πληροφορίες.

Μία λύση που προτείνεται, είναι η κρυπτογράφηση όλου του συστήματος αρχείων. Φυσικά, κάτι τέτοιο κοστίζει πολύ σε πόρους συστήματος, καθώς κάθε φορά που κάποιος (εξουσιοδοτημένος φυσικά) χρήστης επιθυμεί να αποκτήσει πρόσβαση σε κάποιο κρυπτογραφημένο αρχείο, πρέπει αυτό να αποκρυπτογραφηθεί όλο το σύστημα αρχείων και στο τέλος της εργασίας του χρήστη να επανακρυπτογραφηθεί όλο το σύστημα αρχείων.

Ένα από τα προγράμματα που προσφέρει τη δυνατότητα αυτή είναι το πρόγραμμα BestCrypt. Μέσω αυτού του προγράμματος μάλιστα, οι χρήστες έχουν τη δυνατότητα να δημιουργούν ένα "container", ένα κρυπτογραφημένο αρχείο δηλαδή, το οποίο μπορεί μέσω του προγράμματος να γίνει mount και το λειτουργικό σύστημα να το αναγνωρίζει ως ξεχωριστή μονάδα δίσκου.



Το πρόγραμμα BestCrypt

Αξίζει να σημειωθεί ότι η κρυπτογράφηση που πραγματοποιείται από τα συστήματα αρχείων του Linux δεν είναι διαφανής, δηλαδή δεν γίνεται τα αρχεία να βρίσκονται αποθηκευμένα στο δίσκο κρυπτογραφημένα και μόλις ο χρήστης ή το σύστημα επιχειρήσει να προσπελάσει κάποιο από αυτά να αποκρυπτογραφείται αυτόματα.

Πιστοποίηση χρηστών (User authentication).

Η πιστοποίηση των χρηστών είναι, αν όχι η κύρια, μία από τις βασικότερες γραμμές άμυνας στην οποία βασίζονται τα συστήματα ή τα δίκτυα που υλοποιούνται με λειτουργικό σύστημα το linux. Η πλειοψηφία των συστημάτων βασίζεται σε ζεύγη ονόματος χρήστη με κωδικό (username-password). Παρόλο που δεν είναι συνηθισμένο, υποστηρίζονται και άλλοι τύποι πιστοποίησης όπως έξυπνες κάρτες (smartcards), ειδικές συσκευές (tokens) κ.α.

Ένας αναγνώστης έξυπνων καρτών (smartcard reader) που μπορεί να χρησιμοποιηθεί σε περιβάλλον Linux για την πιστοποίηση των χρηστών

P.A.M. (Pluggable Authentication Modules)

Το P.A.M. είναι μία σουίτα από βιβλιοθήκες που επιτρέπουν στον τοπικό διαχειριστή του συστήματος να επιλέξει τον τρόπο με τον οποίο οι εφαρμογές θα πιστοποιούν τους χρήστες.

Στο P.A.M. εισήχθη για πρώτη φορά ένα ενδιάμεσο στρώμα (middleware) μεταξύ της εφαρμογής και του μηχανισμού πιστοποίησης. Τα δύο αυτά κομμάτια συνδέθηκαν έτσι ώστε οποιοσδήποτε τρόπος πιστοποίησης κάποιου χρήστη μπορεί να γίνεται μέσω του P.A.M., να μπορεί να χρησιμοποιηθεί από το πρόγραμμα. Για παράδειγμα μέσω του P.A.M., μπορεί ο διαχειριστής του συστήματος να επιλέξει ότι η ομάδα χρηστών users δεν επιτρέπεται να κάνουν login από τις 6μ.μ. μέχρι και τις 7π.μ. Τις υπόλοιπες ώρες θα μπορούν να εισέρχονται στο σύστημα και η πιστοποίησή τους θα γίνεται μέσω ενός αναγνώστη δαχτυλικών αποτυπωμάτων. Το σενάριο αυτό δε θα μπορούσε να υλοποιηθεί χωρίς το P.A.M..

Οι διανομές Linux των Red Hat και Debian διαθέτουν προεγκατεστημένο το P.A.M. ενώ υπάρχει υλοποιημένο για όλες σχεδόν τις

νέες διανομές Linux, παρόλο που η χειροκίνητη εγκατάστασή του είναι αρκετά χρονοβόρα και δύσκολη.

Διατήρηση αρχείου λειτουργιών (Logging)

Ένα αναπόσπαστο κομμάτι οποιουδήποτε λειτουργικού συστήματος, είναι η διατήρηση αρχείων λειτουργιών (logs). Η πλειοψηφία των αρχείων λειτουργιών δημιουργείται από 2 κυρίως προγράμματα: το syslogd και το klogd. Το πρώτο είναι υπεύθυνο για τη διατήρηση των logs που αφορούν σε υπηρεσίες και προγράμματα ενώ το δεύτερο δημιουργεί τα logs που αφορούν στον πυρήνα (kernel) του Linux. Στα δύο αυτά προγράμματα γίνεται εκτενέστερη αναφορά

Klogd

Το klogd δημιουργεί τα logs που αφορούν στον πυρήνα (kernel) του Linux τα οποία στη συνέχεια αποστέλλει στο syslogd.

Syslogd

Το syslogd είναι υπεύθυνο για τη δημιουργία και αποθήκευση των logs που αφορούν σε υπηρεσίες και προγράμματα, καθώς και για την αποθήκευση των logs του πυρήνα που δημιουργούνται από το klogd.

Φυσικά υπάρχουν προγράμματα, των οποίων τα αρχεία λειτουργιών δεν δημιουργούνται με κάποιο από τα syslogd και klogd, αλλά από εσωτερική λειτουργία δική τους. Το Linux προσφέρει τη δυνατότητα τα αρχεία που δημιουργούνται από τέτοιου είδους προγράμματα να αποθηκεύονται σε συγκεκριμένο φάκελο (συνήθως είναι ο /var/log/{όνομα-προγράμματος}/). Είναι πολύ σημαντικό ο φάκελος αυτός να είναι σε ξεχωριστό διαμέρισμα του δίσκου (partition) από το κυρίως σύστημα, καθώς κάποια είδη επιθέσεων μπορεί να γεμίσουν τα αρχεία αυτά, συνεπώς και το διαμέρισμα του δίσκου, με αποτέλεσμα να υπολειτουργεί ή να καταρρεύσει το σύστημα.

Μία σημαντική παράμετρος του συστήματος διατήρησης αρχείων, η οποία πολλές φορές αγνοείται, είναι η διασφάλιση των αρχείων αυτών, ώστε να μην μπορούν να διαβαστούν ή ακόμα χειρότερα να αλλαχθούν από χρήστες που δεν έχουν δικαιώματα root.

Παρακάτω παρουσιάζονται μερικά προγράμματα που καθιστούν τη διαδικασία τήρησης αρχείων λειτουργιών ασφαλέστερη:

- **modular syslog**

  Ακόμα και αν δικαίωμα εγγραφής στα αρχεία log έχει μόνο ο χρήστης root, αν κάποιος επιτιθέμενος μπορέσει με κάποιο τρόπο να αποκτήσει τον κωδικό αυτό, θα είναι σε θέση και να μεταβάλλει τα αρχεία

αυτά. Μία πιθανή λύση είναι η χρήση του modular syslog, το οποίο επιτρέπει την κρυπτογράφηση των αρχείων λειτουργιών. Φυσικά δεν αποτρέπεται το ενδεχόμενο ο επιτιθέμενος να σβήσει τα αρχεία αυτά.

- **Next generation syslog**

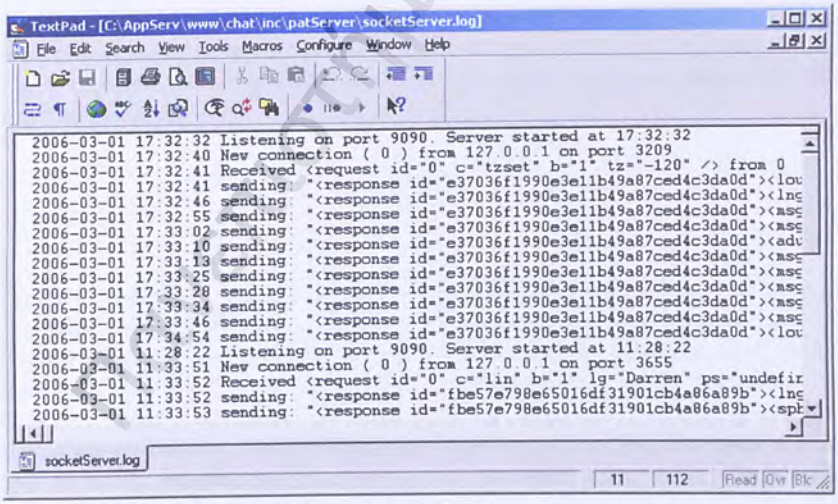
  Το next generation syslog ή syslog-ng δεν είναι τίποτα άλλο παρά η εξέλιξη του syslogd. Αναφέρεται ως ξεχωριστό πρόγραμμα διότι δεν συμπεριλαμβάνεται μέχρι στιγμής στις καινούριες διανομές Linux. Προσφέρει τη δυνατότητα να χρησιμοποιηθεί η ψηφιακή υπογραφή για την αποφυγή αλλοίωσης των αρχείων log από μη εξουσιοδοτημένα άτομα.

- **Psionic Logcheck**

  Η παρακολούθηση των αρχείων log είναι εξαιρετικά χρονοβόρα και ανιαρή διαδικασία. Το πρόγραμμα αυτό αναλαμβάνει να εκτελεί αυτή τη διαδικασία σε τακτά χρονικά διαστήματα και να ενημερώνει τον διαχειριστή του συστήματος μέσω e-mail για οποιαδήποτε καταγραφή ύποπτων ενεργειών.

- **Colorlogs**

  Το πρόγραμμα αυτό αναλαμβάνει το χρωματισμό των αρχείων log, με σκοπό τον ευκολότερο εντοπισμό διαφόρων ενεργειών μέσα σε αυτά.



Το αρχείο log ενός server που αφορά στην δημιουργία μίας νέας tcp σύνδεσης.

Ανίχνευση Εισβολών

Όσο ισχυρή και αν είναι η ασφάλεια κάποιου συστήματος, είναι δυνατόν να σπάσει. Αυτός είναι και ο λόγος για τον οποίο πρέπει κάθε σύστημα να έχει τη δυνατότητα της ανίχνευσης εισβολών.

Η ανίχνευση εισβολών ουσιαστικά επιτυγχάνεται με την παρακολούθηση του συστήματος και την ανίχνευση μη φυσιολογικών συμπεριφορών του. Βασικές παράμετροι του συστήματος όπως η χρήση της μνήμης, η λειτουργία των σκληρών δίσκων, η κίνηση του δικτύου ή οι πόρτες (ports) που είναι ανοιχτές, μπορούν να ανιχνεύσουν με σχετικά καλή πιθανότητα επιτυχίας μία εισβολή. Παρακάτω αναλύονται διάφοροι τρόποι ανίχνευσης και αντιμετώπισης εισβολών, καθώς και λογισμικό για λειτουργικά συστήματα Linux που προσφέρουν αυτές τις δυνατότητες.

Επίβλεψη του συστήματος αρχείων

Ένα από τα συνήθη πράγματα που κάνει κάποιος hacker, μόλις αποκτήσει πρόσβαση στα αρχεία συστήματος ενός υπολογιστή, είναι να τα αλλοιώσει. Ο διαχειριστής του συστήματος λοιπόν, οφείλει μόλις αντιληφθεί ότι η ασφάλεια του συστήματος διαπεράστηκε, να μπορεί να ανιχνεύσει ποια αρχεία έχουν υποστεί αλλοίωση και ποια όχι. Μία πιθανή λύση είναι η επανεγκατάσταση όλου του λογισμικού, ακόμα και του λειτουργικού συστήματος. Μία ευκολότερη είναι η χρήση λογισμικού τέτοιου, που να δημιουργεί ψηφιακές υπογραφές των αρχείων που επιθυμούμε να γνωρίζουμε εάν έχουν υποστεί αλλοίωση, έτσι ώστε να μπορούμε να τα εντοπίσουμε μετά από κάποια επίθεση.

AIDE

Το AIDE είναι λογισμικό ανίχνευσης εισβολών με τη μέθοδο ελέγχου της ακεραιότητας των αρχείων. Ευθύνη του προγράμματος αυτού είναι η δημιουργία μίας βάσης δεδομένων, όπου αποθηκεύονται σημαντικές πληροφορίες για τα αρχεία που θέλει ο διαχειριστής να εξασφαλίσει την ακεραιότητα, όπως τα δικαιώματα, ο χρόνος τελευταίας τροποποίησης, ο χρήστης που τελευταίος τροποποίησε το αρχείο, το μέγεθος του αρχείου κ.α. Επίσης, το AIDE δημιουργεί για καθένα από τα προστατευόμενα αρχεία ένα άθροισμα ελέγχου (checksum), χρησιμοποιώντας έναν ή περισσότερους από τους αλγορίθμους sha1, sha256, sha512, md5, rmd160.

Για να είναι ουσιαστική η χρήση αυτού του εργαλείου, πρέπει ο διαχειριστής να το χρησιμοποιήσει πριν το σύστημα που θέλει να προστατεύσει συνδεθεί για πρώτη φορά στο δίκτυο. Επίσης είναι σημαντικό

να αναφέρουμε ότι στη βάση δεδομένων που δημιουργεί το AIDE αποθηκεύονται πληροφορίες μόνο για τα αρχεία τα οποία δεν διαφοροποιούνται στο σύστημα και όχι αυτά που αλλάζουν σε τακτά χρονικά διαστήματα, όπως είναι τα αρχεία log, τα αρχεία που αφορούν σε e-mails, οι προσωρινοί φάκελοι (temporary folders) και οι αρχικοί φάκελοι των χρηστών (user's home folders).

Pikt

Το Pikt είναι ένα εξαιρετικά χρήσιμο εργαλείο για τους διαχειριστές συστημάτων Linux. Πρόκειται για μία scripting γλώσσα η οποία επιτρέπει στο χρήστη της να τερματίζει διεργασίες που κρίνονται ύποπτες ή που απλώς δεν χρειάζονται, να παρακολουθεί το σύστημα για ασυνήθιστη χρήση (π.χ. χρήση από κάποιον πωλητή ενός μαγαζιού, όταν το μαγαζί είναι κλειστό) και πολλά άλλα. Σημαντικός ανασταλτικός παράγοντας στη χρήση της γλώσσας αυτής, αποτελεί ο χρόνος εκμάθησης που απαιτείται.

Επίβλεψη του Δικτύου

Υπάρχουν αρκετά είδη εργαλείων για Linux τα οποία επιβλέπουν ένα ή περισσότερα δίκτυα, με διαφορετική προσέγγιση το καθένα. Παρακάτω αναλύονται τα σημαντικότερα εξ' αυτών.

TCP-Wrappers

Τα TCP-Wrappers είναι σουίτες εργαλείων που επιτρέπουν τον περιορισμό συνδέσεων βάσει της ip της υπηρεσίας που ζητείται. Για παράδειγμα ο διαχειριστής μπορεί να απαγορέψει τις συνδέσεις με την ip 208.65.153.253 (www.youtube.com). Επίσης, με κατάλληλη παραμετροποίηση, μπορεί να εντοπιστεί ο επιτιθέμενος υπολογιστής.

Scanlogd

Το scanlogd είναι ένα πολύ απλό πρόγραμμα, του οποίου αρμοδιότητα είναι να μετρά την κίνηση ενός δικτύου και μόλις αυτή υπερβεί ένα, ορισμένο από το διαχειριστή, κατώφλι, κρατάει αρχεία logs για τα πακέτα της επιπλέον κίνησης. Το πρόγραμμα αυτό μπορεί να βοηθήσει σημαντικά στον εντοπισμό πιθανών τρυπών στην ασφάλεια του συστήματος.

Psionic Trisentry

Το λογισμικό αυτό αποτελείται από 3 διαφορετικά προγράμματα:

- Portsentry: Χρησιμοποιείται για τον εντοπισμό και την καταγραφή σάρωσης των θυρών του συστήματος (port scans). Επίσης μπορεί να ρυθμιστεί ώστε να διακόπτει μία σάρωση.

- Hostsentry: Το πρόγραμμα αυτό χρησιμεύει για τον εντοπισμό κάποιας «παράξενης» συμπεριφοράς από κάποιον χρήστη. Για παράδειγμα ειδοποιεί το διαχειριστή εάν κάποιος υπάλληλος συνδέθηκε στο σύστημα την Κυριακή που κανονικά δεν εργάζεται.

- Logsentry: Τέλος, το logsentry καταγράφει σε αρχεία log οποιαδήποτε παράξενη συμπεριφορά άλλου προγράμματος.

Deception Toolkits

Τα deception toolkits είναι μία κατηγορία προγραμμάτων, τα οποία, όπως λέει και το όνομά τους, αποσκοπούν στο να ξεγελάσουν τον επιτιθέμενο. Τα deception toolkits δημιουργούν ένα εικονικό περιβάλλον, έτσι ώστε ο επιτιθέμενος να νομίζει ότι το σύστημα έχει πολλές γνωστές αδυναμίες και να αναλώνεται προσπαθώντας να επιτεθεί βασιζόμενος σε αυτές. Έτσι δίνεται ένα σημαντικό χρονικό πλεονέκτημα στον διαχειριστή του συστήματος που δέχεται επίθεση να αντιδράσει ή ακόμα και να εντοπίσει τον επιτιθέμενο.

Αντιμετώπιση εισβολών

Ο τρόπος αντιμετώπισης μίας εισβολής εξαρτάται από πολλούς παράγοντες. Οι σημαντικότεροι από αυτούς είναι:

- Είναι σε εξέλιξη η επίθεση; Αν ναι, τότε είναι πολύ πιθανό να χρειαστεί ακόμα και να αποσυνδεθεί ο υπολογιστής από το δίκτυο προκειμένου να περισωθεί κάποιο κομμάτι του συστήματος.

- Ποια είναι η πρώτη προτεραιότητα μετά την επίθεση; Είναι καλό να υπάρχει ένα πολύ συγκεκριμένο σχέδιο για τη σειρά με την οποία πρέπει να αντιμετωπιστούν οι βλάβες που προήλθαν από την επίθεση.

- Πώς πραγματοποιήθηκε η επίθεση; Εάν η επίθεση έχει γίνει μέσω τρίτων υπολογιστών (spoof attack), είναι σχεδόν αδύνατος ο εντοπισμός του επιτιθέμενου.

- Ακόμα και αν είναι δυνατός ο εντοπισμός του επιτιθέμενου, είναι πολύ πιθανό, εφ΄ όσων γίνει καταγγελία στις αρχές, ο εξοπλισμός να δεσμευτεί ως αποδεικτικό στοιχείο, κάτι το οποίο είναι απευκταίο για κάθε εταιρία.

- Είναι δυνατόν να εντοπιστεί ο τρόπος με τον οποίο ο επιτιθέμενος διαπέρασε την ασφάλεια του συστήματος; Αν ναι, τότε το πιθανότερο σενάριο είναι να σφραγιστούν οι «τρύπες» που επέτρεψαν την εισβολή και να μη δοθεί συνέχεια στο ζήτημα.

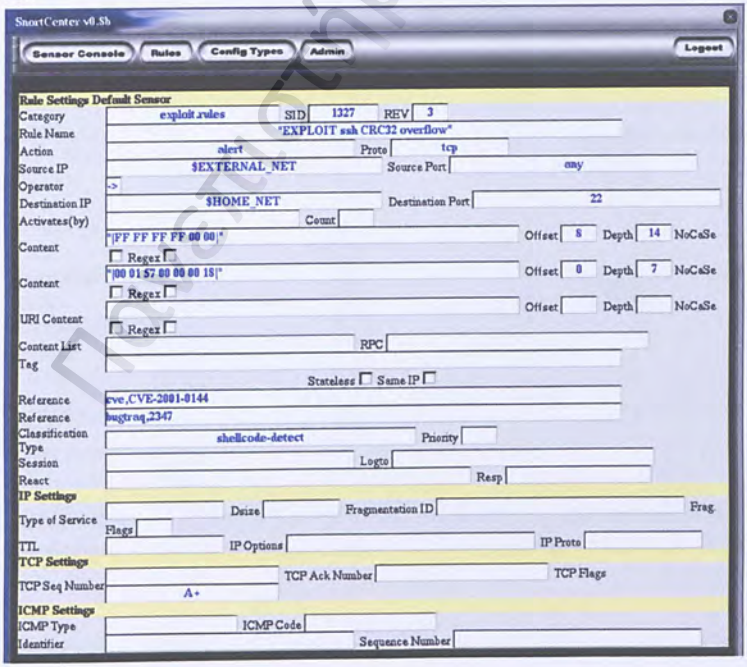
Ανιχνευτές πακέτων (Packet sniffers)

Οι packet sniffers χρησιμοποιούνται για να αποσπώνται πακέτα τα οποία δεν προορίζονται για τον υπολογιστή στον οποίο «τρέχει» ο sniffer. Δυστυχώς, δεν υπάρχει κάποιος 100% αξιόπιστος τρόπος ανίχνευσης ενός sniffer σε ένα δίκτυο. Παρακάτω παρουσιάζονται μερικοί sniffers για λειτουργικό σύστημα linux, καθώς και το εργαλείο Antisniff.

Snort

Το Snort είναι ένα λογισμικό ανοιχτού κώδικα που προσφέρει λειτουργίες πρόληψης εισβολών (Network Intrusion prevention system – NIPS), ανίχνευσης εισβολών (Network intrusion detection system – NIDS) καθώς και λειτουργίες ενός sniffer.

Χρησιμοποιείται ευρέως σε συνδυασμό με λογισμικό όπως τα SnortSnarf, Sigil, OSSIm για τη γραφική αναπαράσταση των δεδομένων που συλλέγει.



Το σύστημα ανίχνευσης εισβολών "Snort" με το γραφικό περιβάλλον SnortCenter

tcpdump

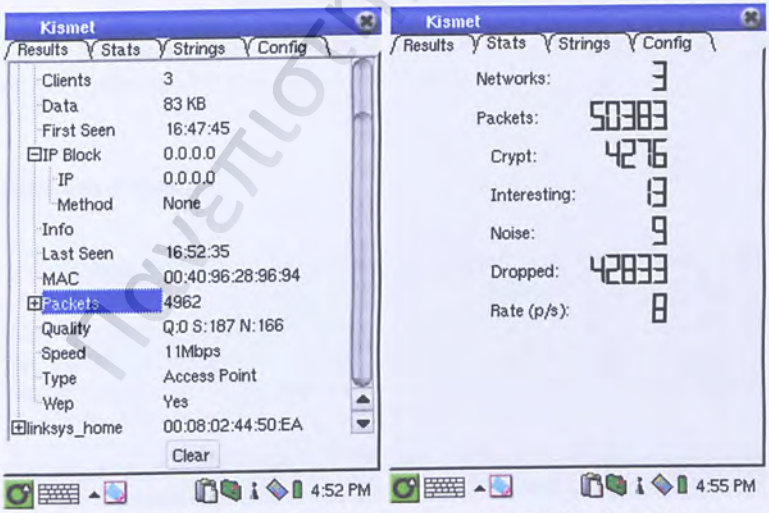
Είναι ο πρόγονος όλων των sniffers για λειτουργικά συστήματα linux. Θεωρείται πλέον ξεπερασμένο, καθώς δεν προσφέρει τις δυνατότητες που προσφέρει ένας σύγχρονος sniffer, όμως χρησιμοποιείται ευρέως για την εύρεση ατελειών (bugs) σε δίκτυα και γι' αυτό συμπεριλαμβάνεται στις περισσότερες εκδόσεις του λειτουργικού linux.

Ethereal

Είναι ίσως ο γνωστότερος sniffer για λειτουργικό σύστημα linux. Επιτρέπει την παρακολούθηση της κίνησης σε ένα δίκτυο με εύκολο τρόπο και υποστηρίζει την συντριπτική πλειοψηφία των πρωτοκόλλων που υλοποιούνται σε ένα δίκτυο (http, tftp, Netbios κ.λ.π.). Δημιουργήθηκε για να συνεργάζεται με τη μηχανή δημιουργίας γραφικού περιβάλλοντος GTK, άρα η χρήση του συνίσταται μόνο με γραφικό περιβάλλον gnome.

Kismet

Το Kismet είναι λογισμικό που εκτελεί χρέη ενός packet sniffer αλλά και ενός συστήματος ανίχνευσης εισβολών σε ασύρματα δίκτυα. Συνεργάζεται με οποιαδήποτε ασύρματη κάρτα δικτύου που μπορεί να λειτουργήσει σε κατάσταση παρακολούθησης (monitoring mode ή rfmon) και δύναται να αποσπάσει πακέτα που προέρχονται από δίκτυα 802.11a, 802.11b και 802.11g.



Το σύστημα ανίχνευσης εισβολών "Kismet" με το γραφικό περιβάλλον SnortCenter

Άλλοι Sniffers

Εκτός από το προαναφερθέν λογισμικό, κυκλοφορεί μία πληθώρα από sniffers για λειτουργικά συστήματα linux. Μερικοί από αυτούς είναι οι: angst, darkstat, echolot, ettercap, Getdata, ggsniff, justniffer, KSnuffle, passlogd, Scapy, tcptrack κ.α.

Πύρινα τείχη προστασίας (Firewalls)

Τα πύρινα τείχη είναι λογισμικό που χρησιμοποιείται για το φιλτράρισμα των πακέτων που διακινούνται μεταξύ του δικτύου που επιθυμούμε να προστατευτεί και άλλων δικτύων. Έτσι, ένα πύρινο τείχος είναι σε θέση, ανάλογα με την παραμετροποίηση που έχει κάνει ο διαχειριστής του δικτύου, να «αποφασίζει» αν ένα πακέτο είναι επιθυμητό να εισέλθει ή να εξέλθει από ένα δίκτυο. Με αυτό τον τρόπο μπορεί να αποφευχθεί η είσοδος πακέτων που μπορούν να βλάψουν το δίκτυο.

Πύρινα τείχη για Linux

Έχουν υπάρξει πολλών ειδών πύρινα τείχη για Linux. Τα παλαιότερα και πλέον ξεπερασμένα πύρινα τείχη είναι τα IPF και Sinus, τα οποία μάλιστα δεν μπορούν να χρησιμοποιηθούν με την έκδοση 2.4 του πυρήνα του Linux. Νεότερο λογισμικό αποτελούν τα πύρινα τείχη ipchains, ipfwadm και φυσικά η τελευταία λέξη της τεχνολογίας λογισμικού που ακούει στο όνομα IPTables.

Η επιλογή ενός πύρινου τείχους πρέπει να γίνεται βάσει της πολιτικής που υπάρχει για το δίκτυο που πρέπει να προστατευτεί. Είναι προτιμότερο η πολιτική που ακολουθείται να απαγορεύει τα πάντα εκτός από αυτά που πρέπει να επιτρέπονται παρά το αντίστροφο.

IPchains και IPfwadm

Τα IPchains και IPfwadm είναι λογισμικά που φιλτράρουν πακέτα. Το είδος αυτό πύρινου τείχους είναι στατικό, δηλαδή οι κανόνες που ορίζονται από τον διαχειριστή ακολουθούνται κατά γράμμα χωρίς καμία απόκλιση. Το γεγονός αυτό τα καθιστά «μη ευέλικτα», καθώς δεν μπορεί να γίνει προσαρμογή ώστε το λογισμικό να ενεργήσει ανάλογα με το περιεχόμενο των πακέτων που φιλτράρονται.

Τα πύρινα τείχη IPchains και IPfwadm προσφέρουν τις εξής δυνατότητες στο διαχειριστή του δικτύου:

- Φραγή πακέτων βασισμένη στις IP διευθύνσεις αφετηρίας ή προορισμού (source / destination IP's)

- Masquerading των συνδέσεων, δηλαδή κατάλληλη επεξεργασία των κεφαλίδων των πακέτων, ώστε αυτά να φαίνονται ως πακέτα που έχουν δημιουργηθεί από το δρομολογητή.

Επιπλέον των προαναφερθέντων, το IPchains υποστηρίζει και:

- Port forwarding.
- Δημιουργία πιο περίπλοκων κανόνων.
- Ευκολότερη διαχείριση.
- Ποιότητα υπηρεσίας στη δρομολόγηση (Quality of Service Routing), κάτι που είναι πολύ χρήσιμο σε συνδέσεις χαμηλής ταχύτητας ή σε κορεσμένα δίκτυα.
- Αντίστροφο ορισμό κανόνων (π.χ. : Επιτρέπεται η είσοδος πακέτων από όλες οι πόρτες εκτός από την 80)

Σημειώνεται ότι το είδος αυτό firewall θεωρείται ξεπερασμένο και ως εκ' τούτου δεν υποστηρίζεται από διανομές Linux που βασίζονται σε έκδοση πυρήνα 2.4 ή νεώτερη.

IPTables ή NETFILTER

Το IPTables ή αλλιώς είναι ένα νέο είδος Firewall, το οποίο αποτελεί την τελευταία λέξη της τεχνολογίας λογισμικού. Υποστηρίζεται μόνο από πυρήνες έκδοσης 2.4 και νεώτερους και σε αντίθεση με τα IPchains και IPfwadm, παρέχει προστασία με μη στατικό τρόπο, αλλά με βάση την κατάσταση της σύνδεσης.

Το πύρινο αυτό τείχος, είναι σε θέση να συγκρατεί στη μνήμη του υπολογιστή σημαντικά χαρακτηριστικά για κάθε σύνδεση, από την ώρα που πραγματοποιείται μέχρι την ώρα που τελειώνει. Αυτά τα χαρακτηριστικά ορίζονται ως κατάσταση της σύνδεσης και μερικά από αυτά είναι η IP διεύθυνση, οι πόρτες μέσω των οποίων γίνεται η επικοινωνία και η σειρά των πακέτων που ανταλλάσσονται. Η λειτουργία αυτή απαιτεί αρκετή επεξεργαστική ισχύ, αλλά μόνο κατά τη διάρκεια δημιουργίας μιας σύνδεσης. Στη συνέχεια, ο έλεγχος των πακέτων πραγματοποιείται γρήγορα και με μικρό κόστος σε πόρους. Τέλος, μόλις μία σύνδεση τερματιστεί, η εγγραφή στη μνήμη που διατηρεί τα στοιχεία της κατάστασης της σύνδεσης, διαγράφεται.

Το IPTables, βασίζεται στη γνωστή τριπλή χειραψία του πρωτοκόλλου TCP. Όταν δημιουργείται μία νέα σύνδεση, ο υπολογιστής που τη ζητά, αποστέλλει ένα πακέτο με τη σημαία (flag) SYN με τιμή 1. Στη συνέχεια, εάν η υπηρεσία που ζητείται είναι διαθέσιμη, ο έτερος υπολογιστής της σύνδεσης, απαντά με ένα πακέτο στο οποίο έχουν πάρει την τιμή 1 οι σημαίες SYN και

ACK. Τέλος, μόλις παραληφθεί το παραπάνω πακέτο, ο υπολογιστής που ζήτησε τη σύνδεση, απαντά με ένα πακέτο που έχει την τιμή 1 μόνο στη σημαία ACK. Από τη στιγμή που θα παραληφθεί αυτό το πακέτο, η σύνδεση θεωρείται ότι έχει εγκατασταθεί η σύνδεση (Established connection). Το IPTables, θα επιτρέψει τη διέλευση μόνο των πακέτων αυτών, τα οποία ανήκουν σε μία ήδη εγκατεστημένη σύνδεση (δηλαδή τα πακέτα στα οποία η σημαία SYN δεν έχει την τιμή 1), εξασφαλίζοντας ότι κάποιος πιθανός εισβολέας δεν μπορεί να εκκινήσει νέες συνδέσεις.

Σε ότι αφορά τις συνδέσεις UDP, προκειμένου να μπορεί το πύρινο τείχος να φιλτράρει τα πακέτα, αντιμετωπίζονται ως συνδέσεις TCP στις οποίες η χειραψία έχει πραγματοποιηθεί.

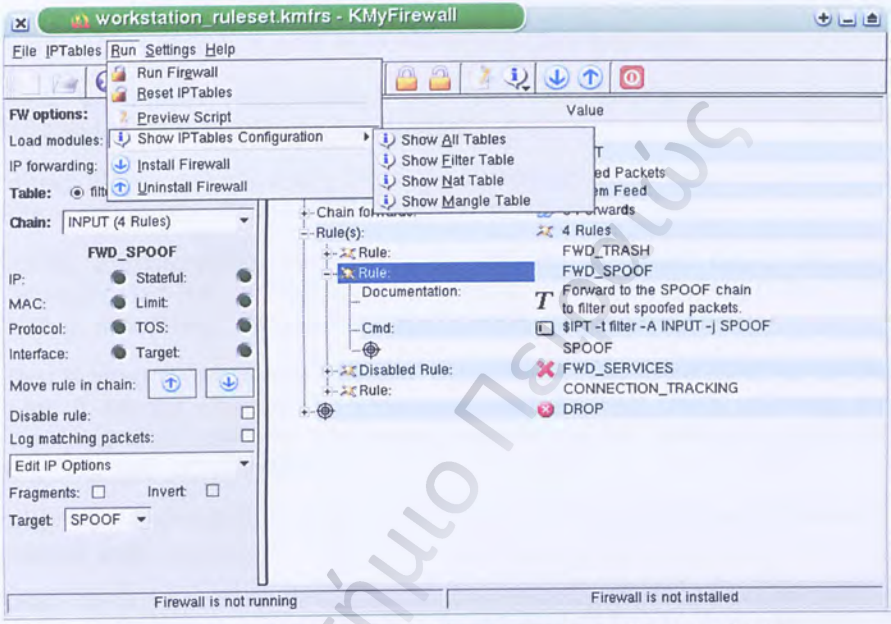
Όπως αναφέρθηκε και προηγουμένως, το IPTables, διατηρεί έναν πίνακα στη μνήμη του ηλεκτρονικού υπολογιστή, στον οποίο αποθηκεύονται σημαντικές πληροφορίες για την κάθε σύνδεση. Προκειμένου αυτός ο πίνακας να μη γίνει πολύ μεγάλος και να προκαλέσει μείωση της απόδοσης του υπολογιστή, λόγω αύξησης των χρησιμοποιούμενων πόρων, χρησιμοποιείται η μέθοδος "time out". Έτσι, αν μία σύνδεση παραμείνει ανενεργή (δηλαδή αν δεν υπάρχει κίνηση δεδομένων) για κάποιο διάστημα, η σύνδεση διαγράφεται από τον πίνακα. Γι' αυτόν το λόγο, πολλές εφαρμογές στέλνουν μηνύματα "keepalive" (μηνύματα που επιβεβαιώνουν ότι η σύνδεση χρειάζεται) για να μη θεωρηθεί κάποια σύνδεση που χρησιμοποιούν ανενεργή.

```
#
# First set some default policies
#

iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD DROP

#
# Then block the reserved network 10.* on the external interface eth0
#

-A INPUT -s 10.0.0.0/255.0.0.0 -d 0.0.0.0/0.0.0.0 -i eth0 -j DROP

#
# Then we allow SSH, SMTP and DNS
#
-A INPUT -s 0.0.0.0/0.0.0.0 -d 0.0.0.0/0.0.0.0 -i eth0 -p tcp -m tcp --dport
22:22 -j ACCEPT
-A INPUT -s 0.0.0.0/0.0.0.0 -d 0.0.0.0/0.0.0.0 -i eth0 -p tcp -m tcp --dport
25:25 -j ACCEPT
-A INPUT -s 0.0.0.0/0.0.0.0 -d 0.0.0.0/0.0.0.0 -i eth0 -p udp -m udp --dport
53:53 -j ACCEPT
-A INPUT -s 0.0.0.0/0.0.0.0 -d 0.0.0.0/0.0.0.0 -i eth0 -p tcp -m tcp --dport
53:53 -j ACCEPT
#
# Now we block all incoming traffic to ports between 1 and 1024. For your
system
#
-A INPUT -s 0.0.0.0/0.0.0.0 -d 0.0.0.0/0.0.0.0 -i eth0 -p tcp -m tcp --dport
1:1024 -j REJECT
-A INPUT -s 0.0.0.0/0.0.0.0 -d 0.0.0.0/0.0.0.0 -i eth0 -p udp -m udp --dport
1:1024 -j REJECT
```

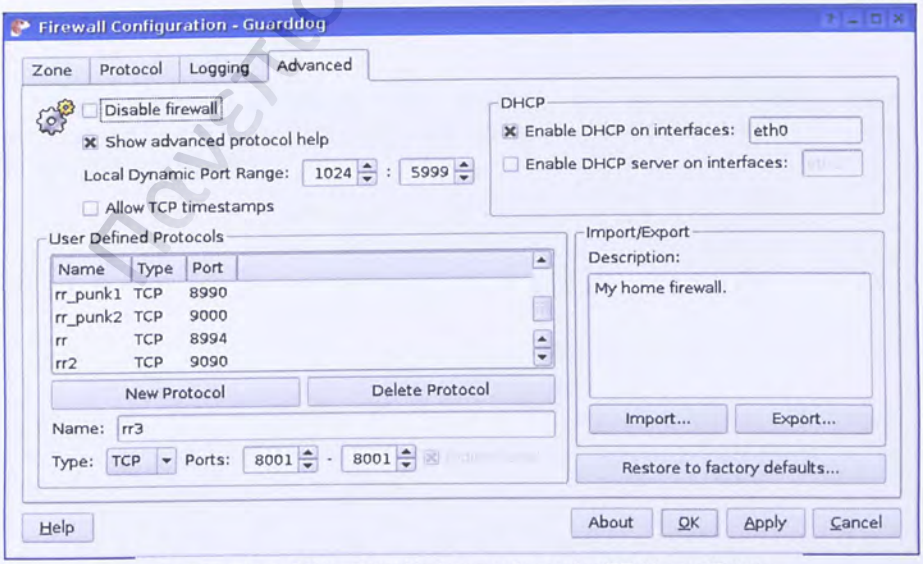
Εντολές για την παραμετροποίηση του IPTables σε υπολογιστή με 1 interface

Τα τρία είδη (IPchains, IPfwadm και IPTables) στα οποία έγινε αναφορά προηγουμένως, αποτελούν το σύνολο των διαθέσιμων πύρινων τειχών για linux. Οι διαφορές των διανομών linux σε αυτόν τον τομέα οφείλονται στο γραφικό περιβάλλον (GUI) που χρησιμοποιείται για την απεικόνιση των ρυθμίσεων.

Παρακάτω παρατίθενται μερικά screenshots από γραφικά περιβάλλοντα για πύρινα τείχη προστασίας για Linux.



Το γραφικό περιβάλλον "ΚΜυΦιρεξαλλ" για τα πύρινα τείχη IPTables και IPchains



Το γραφικό περιβάλλον "Guarddog" για τα πύρινα τείχη IPTables και IPchains

Ασφάλεια λογισμικού στο Linux

Η συγκεκριμένη ενότητα αφορά στην ασφάλεια που προσφέρεται όσον αφορά στα πακέτα λογισμικού που διατίθενται από εταιρίες ή ιδιώτες για διανομές του λειτουργικού συστήματος Linux και προβλήματα που μπορεί να προκύψουν κατά την εγκατάσταση αυτών.

Κάθε έκδοση Linux χρησιμοποιεί διαφορετικό σύστημα διαχείρισης πακέτων (Package Management System, PMS) και προκειμένου να μπορεί ένα πακέτο να εγκατασταθεί στον υπολογιστή, πρέπει να είναι συμβατό με το PMS που χρησιμοποιείται από τη συγκεκριμένη διανομή Linux.

Τα συστήματα διαχείρισης πακέτων που χρησιμοποιούν οι πιο διαδεδομένες διανομές Linux, είναι τα εξής:

- **dkpg:** Χρησιμοποιείται στις διανομές Debian και σε παράγωγες διανομές όπως το Ubuntu. Τα συμβατά πακέτα είναι σε μορφή .deb.
- **RPM:** Δημιουργήθηκε από τη Red Hat αλλά σήμερα εκτός από τις διανομές Red Hat και Fedora, χρησιμοποιείται και από πολλές άλλες (π.χ. SUSE, Mandriva). Τα συμβατά πακέτα είναι σε μορφή .rpm.
- **tgz:** Χρησιμοποιείται στις διανομές της εταιρίας Slackware αλλά τα αρχεία (.tgz ή .tar.gz) μπορούν να αναγνωριστούν και από άλλες εκδόσεις και συχνά χρησιμοποιούνται για την εγκατάσταση μικρών πακέτων που έχουν δημιουργηθεί από χρήστες.
- **pkg:** Χρησιμοποιείται στις διανομές Solaris και τα συμβατά αρχεία είναι σε μορφή .pkg
- **ipkg:** Χρησιμοποιείται σε διανομές Linux που προορίζονται για συσκευές με χαμηλή επεξεργαστική ισχύ (π.χ. palmtops).

Παρακάτω παρουσιάζεται ένας πίνακας με τις δυνατότητες που προσφέρει κάθε τύπος αρχείου και στη συνέχεια ακολουθεί επεξήγηση για κάθε γραμμή του πίνακα.

A/A	Δυνατότητα	.deb	.rpm	.tgz	.pkg
1	Ψηφιακή υπογραφή	✔	✔	✗	✗
2	Checksum	✔	✔	✗	✔
3	Άδειες, Ιδιοκτήτης	✔	✔	✔	✔
4	Όνομα	✔	✔	✗	✔
5	Έκδοση	✔	✔	✗	✔
6	Περιγραφή	✔	✔	✔	✔
7	Εξαρτήσεις	✔	✔	✗	✔
8	Συγκρούσεις	✔	✔	✗	✔
9	Προτεραιότητα	✔	✗	✗	✗

Οι δυνατότητες των πακέτων .deb, .rpm, .tgz και .pkg.

1. **Ψηφιακή υπογραφή:** Το πεδίο αυτό του πίνακα αναφέρεται στη δυνατότητα υποστήριξης ψηφιακής υπογραφής (GPG ή PGP) στο αρχείο, ώστε να μπορεί να πιστοποιηθεί ο δημιουργός του αρχείου.

2. **Άθροισμα ελέγχου λάθους (Checksum):** Για την ασφάλεια του συστήματος, όλα τα αρχεία που περιέχονται σε ένα πακέτο, είναι καλό να συνοδεύονται από ένα άθροισμα ελέγχου λάθους, ώστε να διασφαλίζεται ότι δεν έχουν αλλοιωθεί.

3. **Άδειες, ιδιοκτήτης κ.λ.π.:** Κάποια είδη πακέτων προσφέρουν τη δυνατότητα να αποθηκεύονται σε αυτά πληροφορίες για τις άδειες χρήσης τους (permissions), τους ιδιοκτήτες τους, και τις ομάδες που τα χρησιμοποιούν.

4. **Όνομα:** Σε κάποια από τα είδη των πακέτων που αναλύονται, προσφέρεται η δυνατότητα αποθήκευσης του ονόματος του πακέτου και μέσα στο ίδιο το πακέτο. Αυτό χρησιμεύει για επιβεβαίωση του ονόματος του αρχείου που βλέπει ο χρήστης.

5. **Έκδοση:** Όπως και με το όνομα, έτσι σε μερικά είδη πακέτων, είναι δυνατή η αποθήκευση της έκδοσης της εφαρμογής που περιέχεται στο πακέτο και χρησιμεύει στην επιβεβαίωση του περιεχομένου του.

6. **Περιγραφή:** Όπως και με τα δύο προηγούμενα πεδία, έτσι σε μερικά πακέτα μπορεί να αποθηκευτεί η περιγραφή των περιεχομένων του πακέτου. Η χρησιμότητά του, όμοια με των προηγούμενων δύο.

7. **Εξαρτήσεις:** Σε κάποια από τα είδη των πακέτων προσφέρεται η δυνατότητα αποθήκευσης του ονόματος των πακέτων που πρέπει να προϋπάρχουν εγκατεστημένα στο σύστημα, ώστε να μην δημιουργηθεί κάποια αστάθεια στο σύστημα κατά την εγκατάσταση.

8. **Συγκρούσεις:** Αντίθετα με προηγουμένως, σε κάποια από τα είδη των πακέτων προσφέρεται η δυνατότητα αποθήκευσης του ονόματος των πακέτων που δεν πρέπει να προϋπάρχουν εγκατεστημένα στο σύστημα, ώστε να μην δημιουργηθεί κάποια σύγκρουση (conflict), η οποία θα μπορούσε να δημιουργήσει πρόβλημα στο σύστημα.

9. **Προτεραιότητα:** Στα πακέτα τύπου .deb υπάρχει η δυνατότητα αποθήκευσης της προτεραιότητας (priority) του πακέτου. Πακέτο με υψηλή προτεραιότητα είναι εκείνο το πακέτο που πρέπει να εγκατασταθεί οπωσδήποτε από το χρήστη για να λειτουργήσει το σύστημα σωστά, ενώ πακέτο με χαμηλή προτεραιότητα δε χρήζει εγκατάστασης, εκτός και αν ο ίδιος ο χρήστης επιθυμεί να την πραγματοποιήσει.

Παρακολούθηση και περιορισμός των χρηστών

Τα προβλήματα που προκύπτουν απ' το γεγονός ότι πρέπει σε ένα σύστημα, εκτός από το διαχειριστή (που θεωρείται δεδομένο πως κάνει ότι καλύτερο μπορεί για το σύστημα), πρέπει να έχουν πρόσβαση και άλλοι χρήστες, οι οποίοι μπορεί να προκαλέσουν προβλήματα είτε εσκεμμένα είτε εν αγνοία τους. Γι' αυτό το λόγο, είναι πολύ σημαντικό να περιορίζονται οι χρήστες όσον αφορά στις ενέργειες που μπορούν να πραγματοποιήσουν αλλά και να παρακολουθούνται, ακόμα και όταν οι ενέργειες τους είναι απολύτως επιτρεπτές.

Παρακολούθηση των χρηστών

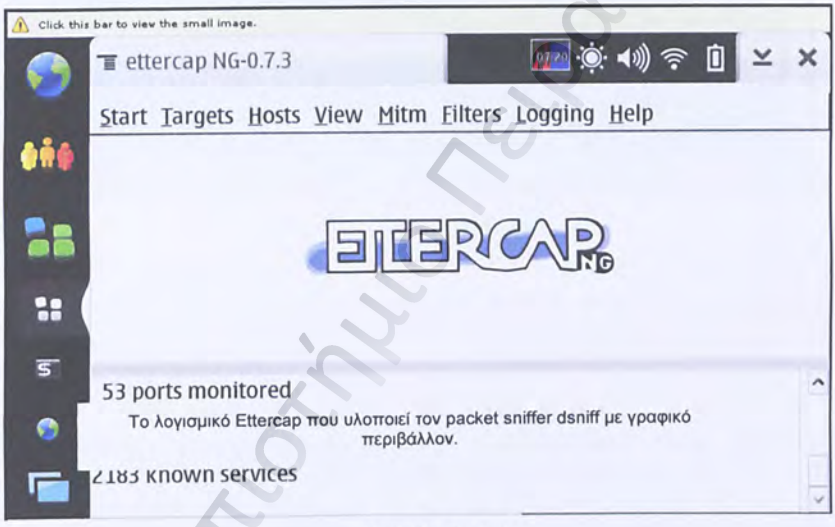
Παλαιότερα, το θέμα της παρακολούθησης των χρηστών αποτελούσε μία απλή διαδικασία. Πλέον, με τη χρήση νέων πρωτοκόλλων κρυπτογράφησης, όπως είναι τα SSH και SSL, η διαδικασία αυτή έχει περιπλεχθεί αρκετά.

Για να είναι αποτελεσματική η παρακολούθηση των χρηστών πρέπει να ακολουθηθεί ένας εκ' των δύο παρακάτω τρόπων. Η χρήση και των δύο ταυτόχρονα προσφέρει εξαιρετικά αποτελέσματα και είναι ότι καλύτερο, σύμφωνα με τη βιβλιογραφία που χρησιμοποιήθηκε.

Παρακολούθηση με τη χρήση sniffer

Η παρακολούθηση των χρηστών με τη χρήση κάποιου sniffer είναι αόρατη σε αυτούς και δεν αποτελεί κάποια σημαντική παρέμβαση στον server του συστήματος. Δεν αρκεί όμως η χρήση ενός sniffer όπως ο Ethereal για την αποτελεσματική καταγραφή των κινήσεων των χρηστών. Γι' αυτόν το σκοπό, έχουν δημιουργηθεί sniffers οι οποίοι μπορούν να πραγματοποιούν επιθέσεις MTM (Man-in-The-Middle attacks) στα πρωτόκολλα SSH και SSL, με αποτέλεσμα να αποκρυπτογραφείται οποιαδήποτε επικοινωνία του επιτιθέμενου με τον προστατευόμενο υπολογιστή.

Ένας τέτοιος packet sniffer, που προσφέρει τις παραπάνω δυνατότητες και ο οποίος προτείνεται κατά κόρον σε μεγάλες διαδικτυακές κοινότητες από πολλούς διαχειριστές συστημάτων είναι ο dsniff.



Το λογισμικό Ettercap που υλοποιεί τον packet sniffer dsniff με γραφικό περιβάλλον.

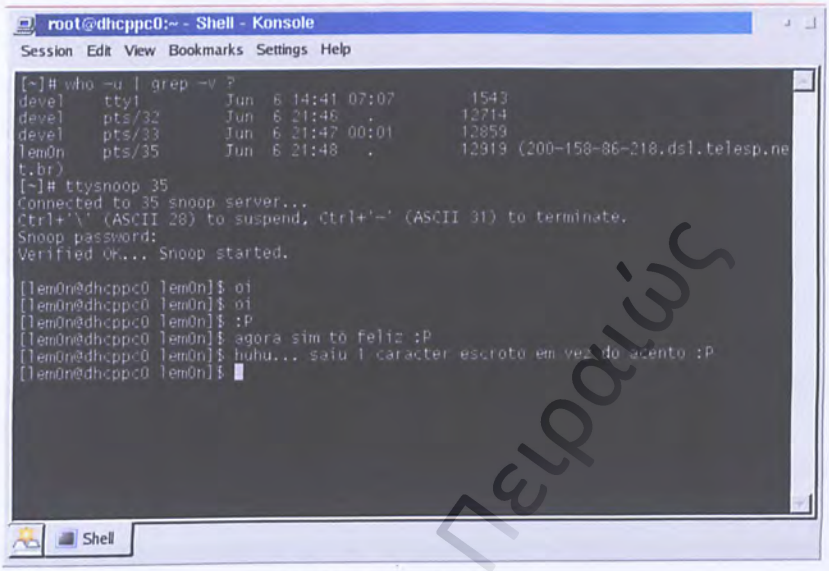
Ο Sniffer Ettercap

Παρακολούθηση από τον server

Η παρακολούθηση από τον διαχειριστή του συστήματος μέσω του server μπορεί να γίνει με ενεργοποίηση του shell logging (παρακολούθηση του κάθε account που κάνει login στο server). Κάτι τέτοιο όμως είναι τελείως άχρηστο στην περίπτωση που ο επιτιθέμενος είναι έμπειρος, καθώς μπορεί πολύ εύκολα να το απενεργοποιήσει.

Ο καλύτερος τρόπος παρακολούθησης των χρηστών μέσω του server είναι με τη χρήση του εργαλείου ttysnoop. Το λογισμικό αυτό επιτρέπει στο διαχειριστή του συστήματος, όχι μόνο να παρακολουθεί τι συμβαίνει σε οποιοδήποτε τερματικό επιθυμεί, αλλά και να επεμβαίνει σε αυτό, ακόμα και να αποκτά τον έλεγχό του. Επίσης προσφέρει τη δυνατότητα στο διαχειριστή

να συν-διαχειρίζεται το σύστημα μαζί με το χρήστη, κάτι το οποίο μπορεί να χρησιμοποιηθεί και για εκπαιδευτικούς σκοπούς.



Η χρήση του εργαλείου ttysnoop.

Περιορισμός των χρηστών

Οι χρήστες, για τη διεκπεραίωση των εργασιών τους, χρειάζονται πόρους, όπως επεξεργαστική ισχύ, μνήμη, χώρο στο σκληρό δίσκο κ.λ.π. Αν δεν έχει προβλεφθεί από το διαχειριστή του συστήματος σωστή κατανομή των πόρων, τότε είναι πολύ πιθανό κάποιος ή κάποιοι χρήστες να κάνουν υπερκατανάλωση των πόρων αυτών εις βάρος των υπολοίπων, ή ακόμα και να κάνουν τον εξυπηρετητή να σταματήσει να ανταποκρίνεται. Για την αντιμετώπιση των παραπάνω προβλημάτων προσφέρεται από όλες τις εκδόσεις Linux, εκτός ίσως ελαχίστων εξαιρέσεων (παλιές εκδόσεις ή εκδόσεις που έχει αφαιρεθεί εσκεμμένα), το εργαλείο P.A.M. .

P.A.M.

Όλες οι καινούριες διανομές Linux, εμπεριέχουν το εργαλείο P.A.M. (Pluggable Authentication Modules), το οποίο επιτρέπει στο διαχειριστή με σχετικά απλό τρόπο, να θέτει όρια είτε σε μεμονωμένους χρήστες είτε σε ομάδες χρηστών.

Τα όρια που μπορούν να τεθούν μέσω του εργαλείου αυτού είναι τα εξής:

- ✓ core: Περιορισμός του μεγέθους της μνήμης που μπορεί να καταληφθεί από τη χρήση ενός αρχείου. Χρησιμοποιείται για την αποφυγή υπερβολικής χρήσης μνήμης από προγράμματα που σταματούν να *ανταποκρίνονται*.
- ✓ data: Μέγιστο μέγεθος δεδομένων που μπορούν να διακινηθούν από το χρήστη.
- ✓ fsize: Μέγιστο μέγεθος αρχείου που μπορεί να αποθηκευτεί από το χρήστη.
- ✓ Nofile: Μέγιστος αριθμός ταυτόχρονα ανοιχτών, από το χρήστη, αρχείων.
- ✓ Cpu: Μέγιστη χρήση του επεξεργαστή. Μετράται σε χρόνο επεξεργαστή (cpu time)
- ✓ nproc: Μέγιστος αριθμός διεργασιών που μπορούν να εκκινηθούν από το χρήστη.
- ✓ maxlogins: Μέγιστος αριθμός από συνδέσεις (log-ins) που μπορεί να κάνει ο χρήστης.
- ✓ priority: η προτεραιότητα με την οποία εκτελούνται οι διεργασίες από τους χρήστες.
- ✓ memlock: Μέγιστη ποσότητα μνήμης που μπορεί να δεσμευθεί από έναν χρήστη.

Κακόβουλο λογισμικό στο λειτουργικό σύστημα Linux.

Ιοί

Το Linux ως λειτουργικό σύστημα δεν είναι το ίδιο επιρρεπές σε ιούς συγκριτικά με άλλα λειτουργικά συστήματα. Το γεγονός αυτό οφείλεται στον τρόπο με τον οποίο είναι δομημένα τα επίπεδα ασφάλειας. Για παράδειγμα στο Linux ο χρήστης δεν μπορεί να γράψει σε οποιοδήποτε σημείο της μνήμης αυτός επιθυμεί, κάτι το οποίο τα Windows επιτρέπουν.

Μέχρι αυτή τη στιγμή, οι γνωστοί ιοί για Linux δεν ξεπερνούν τους 100. Παρόλα αυτά, σε πολλές περιπτώσεις, είναι πιθανό σε αρχεία που μπορούν να αναγνωστούν και από λειτουργικά συστήματα Linux αλλά και από Windows (π.χ. αρχεία office) να κρύβονται ιοί για Windows, οι οποίοι να

μολύνουν μέσω ενός Linux server άλλους υπολογιστές του δικτύου. Γι' αυτό το λόγο, η χρήση λογισμικού αντιμετώπισης ιών κρίνεται απαραίτητη.

Worms

Τα worms είναι πολύ διαδεδομένα στο Linux, καθώς εκμεταλλεύονται τα όποια κενά ασφαλείας ανακαλύπτονται στην εκάστοτε διανομή. Παρόλα αυτά, λόγω της μεγάλης κοινότητας των προγραμματιστών που χρησιμοποιούν Linux, αλλά λόγω και της άμεσης ανταπόκρισης των εταιριών που διανέμουν λειτουργικά συστήματα Linux, αντιμετωπίζονται σχεδόν ακαριαία. Η καλύτερη λύση λοιπόν για την αποφυγή μόλυνσης ενός υπολογιστή με Linux, είναι η διαρκής αναβάθμιση του λογισμικού του, τουλάχιστον σε ότι αφορά την ασφάλεια. Επίσης, τα λογισμικά αντιμετώπισης ιών αποτελούν καλή λύση, καθώς είναι σε θέση να εντοπίσουν και να καθαρίσουν τον υπολογιστή από τέτοιου είδους προγράμματα.

Δούρειοι ίπποι (Trojan horses)

Όπως και τα worms, έτσι και οι δούρειοι ίπποι είναι αρκετά δημοφιλείς στα λειτουργικά συστήματα Linux. Και σε αυτή την απειλή όμως, η ανταπόκριση των εταιριών αλλά και των μεμονωμένων χρηστών είναι άμεση με αποτέλεσμα ο κίνδυνος βλάβης να ελαχιστοποιείται. Ένας καλός τρόπος, προκειμένου να μην κινδυνεύσει ένας υπολογιστής από δούρειους ίππους, είναι πριν από την εγκατάσταση να ελέγχεται η ψηφιακή υπογραφή (PGP) του αρχείου.

Λογισμικό αντιμετώπισης κακόβουλου λογισμικού.

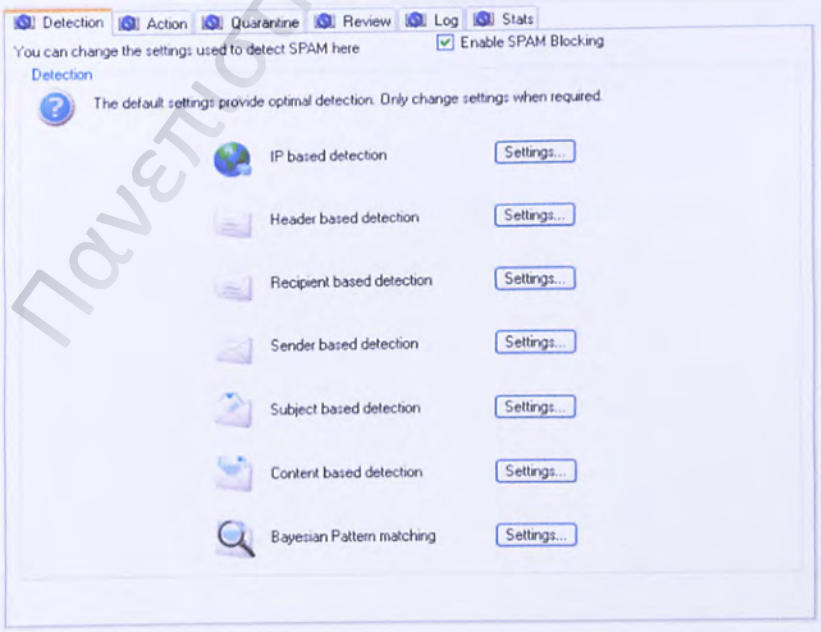
Για την αντιμετώπιση του κακόβουλου λογισμικού για λειτουργικά συστήματα Linux, κυκλοφορούν αρκετά «αντιβιοτικά» προγράμματα. Παρακάτω παρουσιάζονται μερικά από αυτά:

- ✓ F-secure Antivirus

  Το λογισμικό αυτό αποτελεί μία πολύ καλή λύση για την αντιμετώπιση κακόβουλου λογισμικού και είναι σε θέση να προστατεύσει υπολογιστές που χρησιμοποιούν Linux, αλλά και το υπόλοιπο δίκτυο από τα περισσότερα είδη απειλών (malware, spyware, riskware κ.λ.π.

✓ Hexamail Guard

Είναι λογισμικό που προστατεύει ένα σύστημα με Linux από κακόβουλο λογισμικό. Η εταιρία Hexamail που το αναπτύσσει, έχει δώσει έμφαση στην προστασία από spam που προέρχονται μέσω του ηλεκτρονικού ταχυδρομείου.



✓ Panda Antivirus for Linux

Πρόκειται για δωρεάν λογισμικό αντιμετώπισης ιών για ηλεκτρονικούς υπολογιστές (προσωπικούς ή εξυπηρετητές) που χρησιμοποιούν Linux. Μπορεί να ελέγξει και να «καθαρίσει» το ίδιο το σύστημα, αλλά και συστήματα που είναι συνδεδεμένα σε αυτό, ακόμα και αν εκείνα χρησιμοποιούν windows. Το λογισμικό αυτό μπορεί να ελέγξει αρχεία Word, Java applets και συμπιεσμένα αρχεία. Δεν διαθέτει γραφικό περιβάλλον, ο έλεγχός του γίνεται αποκλειστικά από τη γραμμή εντολών.

Σύγκριση παραμέτρων ασφαλείας Windows - Linux

Μέθοδος Σύγκρισης Λειτουργιών Ασφαλείας των Λειτουργικών Συστημάτων Windows – Linux

Σκοπός της σύγκρισης των λειτουργιών ασφαλείας των λειτουργικών συστημάτων Windows και Linux είναι η εξεύρεση των διαφορών τους στον τομέα της ασφάλειας και σε καμία περίπτωση η εύρεση του πιο ασφαλούς λειτουργικού συστήματος.

Η Σύγκριση πραγματοποιείται σε επιμέρους χαρακτηριστικά της ασφάλειας των λειτουργικών συστημάτων και αποσκοπεί στην συγγραφή ενός εγχειριδίου, το οποίο να δύναται να κατατοπίσει κάποιο χρήστη, ο οποίος γνωρίζει τι χαρακτηριστικά θέλει να έχει το σύστημά του, για το ποιο εκ' των λειτουργικών συστημάτων που συγκρίνονται, είναι το ιδανικότερο για την περίπτωσή του.

Συστήματα Αρχείων

Στον παρακάτω πίνακα φαίνεται συνοπτικά η σύγκριση μεταξύ των συστημάτων αρχείων που αναλύθηκαν παραπάνω και που χρησιμοποιούνται κατά κόρον από τους χρήστες των λειτουργικών συστημάτων Windows και Linux. Στη συνέχεια αναλύεται κάθε χαρακτηριστικό ξεχωριστά.

Σύστημα Αρχείων	Μέγιστο μέγεθος αρχείου	Μέγιστο μέγεθος μέσου αποθήκευσης	Αποθήκευση ονόματος ιδιοκτήτη αρχείου	Αποθήκευση ημ/νίας κ' ώρας δημιουργίας αρχείου	Αποθήκευση τελευταίας πρόσβασης σε αρχείο	Αποθήκευση τελευταίας τροποποίησης αρχείου	Λίστες Ελέγχου πρόσβασης	Αποθήκευση αλλαγών (Journaling)	Κρυπτογράφηση δεδομένων
ext3	16 GB – 2TB (1)	2 TB – 32 TB (2)	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΟΧΙ
ReiserFS	8 TB (v 3.6) 4 GB (v 3.5)	16 TB	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ	ΝΑΙ
JFS	4 PB	32 PB	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ	ΟΧΙ	ΟΧΙ
FAT16	2 GB	2 GB	ΟΧΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ
Fat 32	4 GB	8 TB	ΟΧΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ
NTFS	16 TB	256 TB	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ

Συνοπτική σύγκριση συστημάτων αρχείων

(1) Το μέγιστο μέγεθος αρχείου στο σύστημα αρχείων εξαρτάται από το μέγιστο μέγεθος του τομέα (cluster) που επιτρέπεται να δημιουργηθεί στο μέσο αποθήκευσης.

(2) Το μέγιστο μέγεθος του μέσου αποθήκευσης στο σύστημα αρχείων εξαρτάται από το μέγιστο μέγεθος του τομέα (cluster) που επιτρέπεται να δημιουργηθεί σε αυτό.

Μέγιστο Μέγεθος Αρχείου

Σε ότι αφορά το μέγιστο μέγεθος ενός αρχείου που μπορεί να αποθηκευτεί σε ένα αποθηκευτικό μέσο, όπως φαίνεται και από τον παραπάνω πίνακα, το JFS υπερέχει σαφώς με 4 PB, ενώ και τα NTFS και ReiserFS (v 3.6) υποστηρίζουν πολύ μεγάλα αρχεία, 16 και 8 TB αντίστοιχα. Στο σύστημα αρχείων ext3, μπορούν να αποθηκευτούν αρχεία με μέγεθος μέχρι και 2 TB υπό συνθήκες. Τέλος, οι εκδόσεις του FAT, υστερούν στον τομέα αυτό καθώς επιτρέπουν αρχείο μέγιστου μεγέθους μέχρι 4GB η έκδοση 32 και 2GB η έκδοση 16.

Μέγιστο Μέγεθος Μέσου Αποθήκευσης

Αντίστοιχες με το μέγιστο μέγεθος αρχείου είναι και οι επιδόσεις στο μέγιστο μέγεθος του αποθηκευτικού μέσου που μπορεί να χρησιμοποιηθεί.

Το JFS υποστηρίζει μέγιστο μέγεθος αποθηκευτικού μέσου 32 PB, ενώ το NTFS 256 TB κάτι που τα καθιστά να υπερέχουν για χρήση σε συστήματα με πολύ μεγάλο φόρτο δεδομένων.

Τα ReiserFS και το ext3 υποστηρίζουν αποθηκευτικά μέσα 16 TB και 32 TB (υπό προϋποθέσεις και πάλι), αντίστοιχα.

Τέλος το FAT 32 υποστηρίζει αποθηκευτικά μέσα έως και 8 TB, ενώ το FAT 16 υστερεί κατά πολύ με μόλις 2GB.

Αποθήκευση Ιδιοκτήτη Αρχείου

Η αποθήκευση στο σύστημα αρχείων του ονόματος του ιδιοκτήτη ενός αρχείου, χρησιμεύει στην απόδοση δικαιωμάτων σε μεμονωμένο χρήστη για τη χρήση του. Έτσι είναι εφικτό για παράδειγμα να μη μπορεί να διαγράψει κανείς το συγκεκριμένο αρχείο εκτός από τον ιδιοκτήτη του.

Η λειτουργία αυτή υποστηρίζεται και από τα τρία συστήματα αρχείων του Linux που μελετώνται σε αυτή την εργασία, αλλά μόνο από το NTFS όσον αφορά στα συστήματα αρχείων που χρησιμοποιούν τα Windows.

Αποθήκευση Ημ/νίας κ' Ώρας Δημιουργίας Αρχείου

Εκτός από το δημιουργό κάθε αρχείου είναι πολύ χρήσιμο, όπως αναλύθηκε και παραπάνω, σε ότι αφορά την ασφάλεια ενός συστήματος και των δεδομένων που είναι αποθηκευμένα σε αυτό, να γνωρίζουμε και τον ακριβή χρόνο δημιουργίας του αρχείου.

Η λειτουργία αυτή, παρέχεται από όλα τα συστήματα αρχείων που χρησιμοποιούνται από τα λειτουργικά συστήματα Windows και Linux και που εξετάζονται σε αυτή την εργασία.

Αποθήκευση τελευταίας πρόσβασης σε αρχείο

Για την ασφάλεια των δεδομένων, μία πολύ σημαντική παράμετρος που πρέπει ο διαχειριστής κάθε συστήματος να γνωρίζει, είναι πότε πραγματοποιήθηκε η τελευταία ανάγνωση σε κάθε αρχείο

Η παράμετρος αυτή, αποθηκεύεται από όλα τα συστήματα αρχείων που χρησιμοποιούν τα Microsoft Windows καθώς και αυτά του Linux, τα οποία εξετάζονται.

Αποθήκευση τελευταίας τροποποίησης αρχείου

Μία ακόμα πολύ σημαντική παράμετρος για την ασφάλεια των δεδομένων είναι η γνώση του διαχειριστή του χρόνου της τελευταίας τροποποίησης κάθε αρχείου.

Η παράμετρος αυτή, αποθηκεύεται από όλα τα συστήματα αρχείων που χρησιμοποιούν τα Microsoft Windows, ενώ από τα συστήματα αρχείων του Linux που εξετάζονται, τα ReiserFS και ext3 παρέχουν τη λειτουργία αυτή, σε αντίθεση με το JFS το οποίο δεν την παρέχει.

Λίστες Ελέγχου πρόσβασης

Όπως αναφέρθηκε και παραπάνω, μία λίστα ελέγχου πρόσβασης καθορίζει εάν ένας χρήστης δικαιούται να χρησιμοποιήσει πόρους του συστήματος και εάν ναι, ποιους. Οι πόροι αυτοί μπορεί να είναι:

- Αρχεία
- Φάκελοι
- Κλειδιά Μητρώου (Registry Keys)
- Υπηρεσίες
- Αρχεία Λειτουργιών (System logs)
- Διεργασίες
- Η σειρά με την οποία εκτελούνται κάποιες διεργασίες (Named pipe)
- Περιοχές μνήμης δεσμευμένες από τον πυρήνα του συστήματος (Kernel objects)
- Πόρτες Δικτύου

Η λειτουργία αυτή, του περιορισμού της πρόσβασης χρηστών σε πόρους του συστήματος, παρέχεται στα ext3 και JFS σε ότι αφορά τα συστήματα αρχείων του Linux και στο NTFS σε ότι αφορά τα συστήματα αρχείων των Windows.

Στα συστήματα αρχείων FAT 16, FAT 32 και ReiserFS, ο περιορισμός των χρηστών με τη χρήση λιστών ελέγχου πρόσβασης, δεν υποστηρίζεται.

Αποθήκευση αλλαγών (Journaling)

Το "Journaling" ή η αποθήκευση αλλαγών σε ελεύθερη μετάφραση, αφορά στην καταγραφή σε ένα αρχείο λειτουργιών (Journal) οποιαδήποτε αλλαγή πραγματοποιείται στο σύστημα αρχείων, **πριν όμως αυτή εφαρμοστεί**.

Η λειτουργία του "Journaling" δεν παρέχεται στο σύστημα αρχείων JFS σε ότι αφορά το Linux, καθώς και στις δύο εκδόσεις του FAT (16 kai 32).

Αντιθέτως, η λειτουργία αυτή παρέχεται τόσο από τα ReiserFS και ext3 του Linux, όσο και από το NTFS των Windows.

Κρυπτογράφηση Δεδομένων

Η κρυπτογράφηση των δεδομένων που αφορά στο επίπεδο του συστήματος αρχείων παρέχεται μόνο από τα ReiserFS και NTFS.

Φυσικά, κρυπτογράφηση δεδομένων μπορεί να γίνει σε οποιοδήποτε σύστημα αρχείων, με τη χρήση ειδικού λογισμικού, όμως η κρυπτογράφηση στο επίπεδο του συστήματος αρχείων παρέχει κάποια πλεονεκτήματα:

- Ευέλικτος τρόπος διαχείρισης κλειδιών, κάτι που καθιστά απλό κάθε αρχείο ή ομάδα αρχείων να κρυπτογραφείται με διαφορετικό κλειδί.
- Τα αρχεία μπορούν να αντιμετωπίζονται μεμονωμένα, κάτι που καθιστά απλή τη διαδικασία αντιγραφών ασφαλείας.

- Η κρυπτογράφηση μπορεί να καταστεί διαφανής στο χρήστη, δηλαδή τα αρχεία να αποκρυπτογραφούνται όταν κάποιος χρήστης με δικαίωμα ανάγνωσης ανοίγει ένα αρχείο και να επανακρυπτογραφούνται όταν κλείνει το αρχείο, χωρίς αυτή η διαδικασία να γίνεται αντιληπτή από το χρήστη.

Πύρινα Τείχη Προστασίας (Firewalls)

	IPtables / Netfilter	IPFilter	Windows XP / Windows Server 2003 Firewall	Windows Vista / Windows Server 2008 Firewall
Λειτουργικό Σύστημα	Linux	Linux	Windows	Windows
Φιλτράρισμα εισερχόμενων πακέτων	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ
Φιλτράρισμα εξερχόμενων πακέτων	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ
Αλλαγή πολιτικής με έναν κανόνα (rule)	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ
Φιλτράρισμα πακέτων βάσει της IP διεύθυνσης προορισμού	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ
Φιλτράρισμα πακέτων βάσει της IP διεύθυνσης αφετηρίας	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ
Φιλτράρισμα πακέτων βάσει της MAC διεύθυνσης προορισμού	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΟΧΙ
Φιλτράρισμα πακέτων βάσει της MAC διεύθυνσης αφετηρίας	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΟΧΙ
Φιλτράρισμα πακέτων βάσει της TCP / UDP πόρτας του προορισμού	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ
Φιλτράρισμα πακέτων βάσει της TCP / UDP πόρτας της αφετηρίας	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ

Λειτουργία στο 4° στρώμα του OSI (stateful firewall)	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ
Λειτουργία στο 7° στρώμα του OSI (application inspection)	ΝΑΙ	Μερική (Λειτουργεί μόνο με ορισμένα πρωτόκολλα)	ΟΧΙ	ΟΧΙ
Λειτουργία DMZ	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΟΧΙ
Φιλτράρισμα βάσει της ώρας	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΟΧΙ
Φιλτράρισμα βάσει των δικαιωμάτων του χρήστη	ΝΑΙ	ΟΧΙ	ΟΧΙ	ΝΑΙ
Όριο κίνησης / QOS	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΟΧΙ
Δυνατότητα κεντρικοποιημένης διαχείρισης σε ένα δίκτυο	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ
Υποστήριξη πακέτων IPv6	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ
Καταγραφή ιστορικού (Logging)	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ

Στον παραπάνω πίνακα απεικονίζονται οι λειτουργίες που υποστηρίζονται από τα πύρινα τείχη προστασίας των Windows (XP, Vista, Server 2003, Server 2008), καθώς και από τα IPtables, NetFilter και IPFilter του Linux.

Φιλτράρισμα εισερχόμενων πακέτων

Ο έλεγχος των εισερχόμενων πακέτων είναι η βασικότερη λειτουργία ενός τείχους προστασίας. Όλα τα τείχη προστασίας που κυκλοφορούν στην αγορά παρέχουν αυτή τη λειτουργία και φυσικά μέσα σε αυτά είναι και αυτά που εξετάζονται στη συγκεκριμένη εργασία.

Φιλτράρισμα εξερχόμενων πακέτων

Ο έλεγχος των εξερχόμενων πακέτων θεωρείται πολύ σημαντικός σε ένα σύγχρονο Η/Υ ή ένα δίκτυο Η/Υ. Το μόνο από τα τείχη προστασίας που δεν υποστηρίζει αυτή τη λειτουργία είναι αυτό που συμπεριλαμβάνονταν με τις εκδόσεις XP και Server 2003 των Windows και είναι ο κύριος λόγος για τον οποίο τα δύο αυτά προϊόντα δεν είχαν την επιθυμητή επιτυχία στην αγορά. Τα δύο τείχη προστασίας του Λ.Σ. Linux που εξετάζονται, παρέχουν τη λειτουργία αυτή.

Αλλαγή πολιτικής με έναν κανόνα (rule)

Η δυνατότητα ενός τείχους προστασίας να διατηρεί διαφορετικά προφίλ, ώστε σε περίπτωση που ένας Η/Υ συνδέεται σε δύο ή περισσότερα διαφορετικά δίκτυα δεν είναι μόνο θέμα ευχρηστίας. Κατά την εναλλαγή μεταξύ διαφορετικών δικτύων, είναι πιθανό να ξεχαστεί κάτι κατά τη ρύθμιση του τείχους προστασίας και συνεπώς να δημιουργηθεί τρύπα στην ασφάλεια του συστήματος.

Η λειτουργία αυτή παρέχεται από τα IPtables, Netfilter και IPfilter σε ότι αφορά το Linux καθώς και από το τείχος προστασίας των Windows Vista και Windows Server 2003.

Φιλτράρισμα πακέτων βάσει της IP διεύθυνσης (είτε του προορισμού είτε της αφετηρίας)

Ο έλεγχος της κίνησης με βάση την IP διεύθυνση (είτε του προορισμού είτε της αφετηρίας) δεν παρέχεται μόνο από το τείχος προστασίας των Windows XP. Αντιθέτως, τα IPtables, Netfilter, IPfilter και Windows Vista Firewall / Windows Server 2003 Firewall παρέχουν αυτή τη δυνατότητα.

Φιλτράρισμα πακέτων βάσει της MAC διεύθυνσης (είτε του προορισμού είτε της αφετηρίας)

Η δυνατότητα ελέγχου των εισερχόμενων και των εξερχόμενων πακέτων βάσει της διεύθυνσης MAC, παρέχεται από τα τείχη προστασίας του Linux, ενώ αντιθέτως, δεν παρέχεται από τα τείχη προστασίας των Windows.

Φιλτράρισμα πακέτων βάσει της TCP / UDP πόρτας.

Σε ότι αφορά την πόρτα (TCP ή UDP) του προορισμού, αυτή μπορεί να ενταχθεί σε κανόνες από όλα τα τείχη προστασίας που εξετάζονται. Σε ότι αφορά την πόρτα της αφετηρίας, αυτή δεν μπορεί να ελεγχθεί από το τείχος προστασίας των Windows XP / Windows Server 2003, αφού όπως αναφέρθηκε και παραπάνω, το τείχος προστασίας αυτό δεν υποστηρίζει τον έλεγχο των εξερχόμενων πακέτων.

Λειτουργία στο 4ο στρώμα του OSI

Τα τείχη προστασίας που λειτουργούν στο 4ο στρώμα του OSI, δηλαδή στο επίπεδο μεταφοράς, ονομάζονται "stateful firewalls", ανήκουν στην τρίτη γενιά τειχών προστασίας και θεωρούνται ασφαλέστερα από όλα τα είδη που κυκλοφορούν στην αγορά. Τα τείχη προστασίας που ανήκουν στην κατηγορία αυτή συγκρατούν στη μνήμη του υπολογιστή την κατάσταση (state) κάθε σύνδεσης που έχει πραγματοποιηθεί και εξετάζουν αν κάθε πακέτο που εισέρχεται στον υπολογιστή συνάδει με τους κανόνες που έχουν οριστεί.

Και τα τέσσερα τείχη προστασίας που εξετάζονται στην εργασία αυτή λειτουργούν στο επίπεδο μεταφοράς.

Λειτουργία στο 7ο στρώμα του OSI

Τα τείχη προστασίας που λειτουργούν στο 7ο επίπεδο του OSI, δηλαδή το επίπεδο εφαρμογής (stateless firewall ή application inspection firewall) ανήκουν στη δεύτερη γενιά τειχών προστασίας. Μειονεκτούν ως προς τα τείχη προστασίας τρίτης γενιάς στο ότι δεν υποστηρίζουν τον έλεγχο των πακέτων ως προς την πόρτα και είναι σαφώς πιο αργά.

Η λειτουργία στο 7ο στρώμα του OSI παρέχεται στα IPtables / Netfilter και IPfilter (μερικώς) του Linux, ενώ αντίθετα στα τείχη προστασίας των Windows δεν παρέχεται. Παρόλα αυτά, το γεγονός αυτό δεν επηρεάζει την αποτελεσματικότητα των τελευταίων, καθώς είναι κάτι που προσφέρεται συμπληρωματικά από τα τείχη προστασίας του Linux.

Λειτουργία DMZ (Demilitarized Zone)

Σε ένα δίκτυο, οι υπολογιστές που είναι πιο ευπαθείς σε επιθέσεις, είναι συνήθως αυτοί που παρέχουν κάποια υπηρεσία σε άλλους υπολογιστές εκτός του τοπικού δικτύου. Η συνήθης πρακτική για την αντιμετώπιση πιθανών επιθέσεων είναι η τοποθέτηση των υπολογιστών αυτών σε ένα υποδίκτυο ώστε να προστατευθούν οι υπόλοιποι υπολογιστές του τοπικού δικτύου.

Οι υπολογιστές που βρίσκονται στο DMZ έχουν κανόνες επικοινωνίας και με το εσωτερικό δίκτυο (το υπόλοιπο) αλλά και με το εξωτερικό. Η λειτουργία αυτή επιτυγχάνεται με την εγκατάσταση ενός επιπλέον τείχους προστασίας ανάμεσα στο υποδίκτυο DMZ και το υπόλοιπο δίκτυο.

Η δημιουργία ενός DMZ υποστηρίζεται από τα τείχη προστασίας IPtables / Netfilter και IPfilter του Linux ενώ αντιθέτως δεν υποστηρίζεται από αυτά των Windows (XP SP2 / Server 2003 και Vista / Server 2008). Η Microsoft, για τη δημιουργία DMZ διαθέτει τον ISA Server, ο οποίος όμως σε καμία περίπτωση δεν μπορεί να θεωρηθεί κομμάτι του λειτουργικού συστήματος.

Φιλτράρισμα βάσει της ώρας

Η δυνατότητα το τείχος προστασίας να συμπεριφέρεται διαφορετικά ανάλογα με την ώρα της ημέρας, από πολλούς δε θεωρείται σημαντικό προτέρημα. Παρόλα αυτά όμως, αξιολογείται ως λειτουργία ασφαλείας.

Και πάλι, τα τείχη προστασίας που μπορούν να λειτουργήσουν με κανόνα ώρας, είναι αυτά του Linux και για να επιτευχθεί κάτι αντίστοιχο στα Windows απαιτείται ο ISA Server ή κάποιο προϊόν τρίτου κατασκευαστή.

Φιλτράρισμα βάσει των δικαιωμάτων του χρήστη

Τα IPtables / Netfilter και Windows Vista / Server 2008 firewall δίνουν τη δυνατότητα παραμετροποίησης τους ανάλογα με το χρήστη που χρησιμοποιεί τον Η/Υ. Αντιθέτως τα Windows XP SP2 / Server 2003 firewall και IPfilter δεν υποστηρίζουν τη λειτουργία αυτή, κάτι που θεωρείται μεγάλο μειονέκτημα, καθώς είναι πολύ πιθανό να χρησιμοποιούν τον ίδιο υπολογιστή δύο ή περισσότερα άτομα που δε χρήζουν της ίδιας εμπιστοσύνης από το διαχειριστή του συστήματος.

Όριο κίνησης / QOS

Είναι πολύ συχνό φαινόμενο σε ένα δίκτυο, οι πόροι σε συγκεκριμένα χρονικά διαστήματα να μην επαρκούν για την εξυπηρέτηση όλων των λειτουργιών που ζητούνται να πραγματοποιηθούν. Αποτέλεσμα ενός τέτοιου φαινομένου μπορεί να είναι είτε η πολύ αργή εξυπηρέτηση είτε η πλήρης κατάρρευση του δικτύου.

Σε ότι αφορά τα τείχη προστασίας, αυτά του Linux, παρέχουν τη δυνατότητα ορισμού της μέγιστης κίνησης που επιτρέπεται να διακινείται, ώστε να αποφευχθεί μία τέτοια περίπτωση. Αντιθέτως, τα τείχη προστασίας

των Windows δεν παρέχουν τη δυνατότητα αυτή και κατά τη Microsoft, ο ISA Server προσφέρει και πάλι λύση στο πρόβλημα αυτό.

Δυνατότητα κεντρικοποιημένης διαχείρισης σε ένα δίκτυο

Η δυνατότητα τα τείχη προστασίας των υπολογιστών σε ένα δίκτυο να μπορούν να παραμετροποιούνται από έναν κεντρικό υπολογιστή παρέχεται και από τα τέσσερα που εξετάζονται.

Υποστήριξη πακέτων IPv6

Καθώς η ποσότητα των διαθέσιμων IPv4 έχει αρχίσει να μην επαρκεί, θεωρείται βέβαιο ότι σε σύντομο χρονικό διάστημα το IPv6 θα εδραιωθεί. Όταν αυτό συμβεί, ένα τείχος προστασίας που δε θα μπορεί να διαβάσει πακέτα αυτού του τύπου θα είναι τελείως άχρηστο.

Το μόνο τείχος προστασίας από αυτά που μελετώνται που δεν υποστηρίζει φιλτράρισμα πακέτων IPv6 είναι αυτό που συμπεριλαμβάνεται στα Windows XP και στα Server 2003

Καταγραφή ιστορικού (Logging)

Η καταγραφή γεγονότων θεωρείται πολύ σημαντική, όπως αναλύθηκε και παραπάνω, όχι μόνο για την καταστολή εν εξελίξει επιθέσεων αλλά και για την γρήγορη ανάκαμψη σε περίπτωση επιτυχημένης επίθεσης.

Φυσικά, και τα τέσσερα τείχη προστασίας που εξετάζονται παρέχουν τη δυνατότητα καταγραφής γεγονότων κι έτσι δεν τίθεται θέμα σύγκρισης.

Κακόβουλο λογισμικό

Το κακόβουλο λογισμικό (malware) διακρίνεται σε τρείς κύριες κατηγορίες:

- Δούρειοι ίπποι (Trojan horses)
- Ιοί (Viruses)
- Σκουλήκια (Worms)

Η σύγκριση πραγματοποιείται σε κάθε μία από τις παραπάνω κατηγορίες ξεχωριστά και αφορά τόσο στην ποσότητα και τη διάδοση όσο και στους τρόπους αντιμετώπισης.

Δούρειοι Ίπποι (Trojan horses)

Οι δούρειοι ίπποι είναι λογισμικό σχεδιασμένο ώστε να επιτρέπουν την απομακρυσμένη διαχείριση ενός υπολογιστή με σκοπό να πραγματοποιηθούν κάποιες διεργασίες σε αυτόν.

Ποσότητα

Σύμφωνα με τη Wikipedia, υπάρχουν μόλις 2 αναγνωρισμένοι δούρειοι ίπποι σχεδιασμένοι για να λειτουργούν σε περιβάλλον Linux, ενώ αντίθετα υπάρχουν εκατοντάδες αναγνωρισμένοι τύποι δούρειων ίππων για τις διάφορες εκδόσεις των Microsoft Windows, χωρίς κανείς να μπορεί να προσδιορίσει τον ακριβή αριθμό, καθώς η λίστα μεγαλώνει καθημερινά.

Ο ρυθμός διάδοσης των δούρειων ίππων στο Linux είναι σαφώς μικρότερη απ' ότι στα Windows. Αυτό οφείλεται κυρίως στο γεγονός ότι κάθε εταιρεία υποστηρίζει τη διανομή της μέσω κέντρων κατεβάσματος αρχείων (repositories), κάτι που εξασφαλίζει ότι το λογισμικό που εγκαθιστά ο χρήστης είναι «καθαρό» από κακόβουλο λογισμικό, κάτι που δε συμβαίνει με τα Windows λόγω της εμπορικότητας αυτού καθαυτού του προϊόντος όσο και των προϊόντων που απευθύνονται στους χρήστες του.

Τρόποι αντιμετώπισης

Για την αντιμετώπιση των δούρειων ίππων σε περιβάλλον Windows, δεν παρέχεται κάποιο εξειδικευμένο λογισμικό. Κρίνεται όμως απαραίτητη η χρήση λογισμικού τρίτου κατασκευαστή και η μόνη προστασία που παρέχεται από το ίδιο το λειτουργικό είναι η γνωστή ειδοποίηση «Ο υπολογιστής σας είναι πιθανό να κινδυνεύει».

Σε ότι αφορά τις εκδόσεις του λειτουργικού συστήματος Linux, επίσης δεν παρέχεται μαζί με τις διάφορες διανομές κάποιο λογισμικό προστασίας και αυτό συμβαίνει κυρίως λόγω του πολύ μικρού κινδύνου που αντιμετωπίζει ένας υπολογιστής με Linux, αλλά και λόγω της δυνατότητας αντιμετώπισης του δούρειου ίππου μεμονωμένα από τον πυρήνα του λογισμικού με μία πιθανή αναβάθμιση από την εταιρεία που παράγει τη διανομή.

Ιοί

Οι ιοί είναι κακόβουλο λογισμικό που μπορεί να αναπαράγεται και να μολύνει ηλεκτρονικούς υπολογιστές με σκοπό να βλάψει είτε τη λειτουργικότητα του ηλεκτρονικού υπολογιστή είτε τα αρχεία που βρίσκονται αποθηκευμένα σε αυτόν.

Ποσότητα

Και πάλι σύμφωνα με τη διαδικτυακή εγκυκλοπαίδεια Wikipedia, υπάρχουν περίπου 40 αναγνωρισμένοι ιοί για λειτουργικό σύστημα Linux. Για τα λειτουργικά συστήματα της Microsoft, ο αριθμός δεν μπορεί επακριβώς να προσδιοριστεί από κανέναν όμως είναι της τάξης των δεκάδων εκατομμυρίων ίσως και περισσότεροι.

Ο ρυθμός διάδοσης των ιών για τα λειτουργικά συστήματα Linux είναι πολύ μικρός σε αντίθεση με αυτούς που μολύνουν υπολογιστές με λειτουργικό σύστημα Windows, όπου η μόλυνση ενός απροστάτευτου υπολογιστή με σύνδεση στο διαδίκτυο είναι σχεδόν σίγουρη αν όχι στην πρώτη, μέσα στις πρώτες λίγες χρήσεις του.

Τρόποι αντιμετώπισης

Στα λειτουργικά συστήματα Linux, η χρήση λογισμικού αντιμετώπισης δεν κρίνεται από τους περισσότερους χρήστες απαραίτητη. Από τα "repositories" των εταιρειών που κατασκευάζουν τις διανομές δεν παρέχεται

τέτοιου είδους λογισμικό, παρόλα αυτά υπάρχουν εταιρείες που παράγουν λογισμικό αντιμετώπισης ιών για Linux.

Σε ότι αφορά τα Windows, η χρήση λογισμικού προστασίας και αντιμετώπισης ιών είναι κάτι παραπάνω από επιτακτική, καθώς οι ιοί για Windows έχουν κατακλύσει το διαδίκτυο και ένας υπολογιστής που δεν «τρέχει» τέτοιου είδους λογισμικό είναι σχεδόν απίθανο να μην προσβληθεί μέσα στις πρώτες λίγες ώρες λειτουργίας του. Και σε αυτόν τον τομέα, η Microsoft απλώς προειδοποιεί το χρήστη ότι δεν έχει εγκατεστημένο λογισμικό αντιμετώπισης ιών και δεν παρέχει με τα λειτουργικά της συστήματα ασφάλεια στον τομέα αυτό.

Σκουλήκια (Worms)

Τα σκουλήκια είναι κακόβουλο λογισμικό, που σε αντίθεση με τους ιούς, δεν μολύνουν αρχεία, αλλά καταναλώνουν πόρους του δικτύου, με σκοπό να το καταστήσουν μη λειτουργικό. Επίσης χρησιμοποιούν τα δίκτυα ηλεκτρονικών υπολογιστών για να διαδοθούν.

Ποσότητα

Σύμφωνα με τη διαδικτυακή εγκυκλοπαίδεια “Wikipedia”, για λειτουργικό σύστημα Linux έχουν εντοπιστεί συνολικά είκοσι περίπου σκουλήκια. Ο αριθμός των σκουληκιών που έχουν εντοπιστεί με στόχο λειτουργικά συστήματα Windows, αγγίζει τις 13,000.

Ο ρυθμός διάδοσης είναι αντίστοιχος της ποσότητάς τους, δηλαδή πολύ μικρός για λειτουργικά συστήματα Linux και πολύ μεγάλος για λειτουργικά συστήματα Windows.

Τρόποι αντιμετώπισης

Και σε αυτή την κατηγορία κακόβουλου λογισμικού, τα πράγματα είναι παρόμοια με τις δύο προηγούμενες, δηλαδή στα λειτουργικά συστήματα Linux, η χρήση λογισμικού αντιμετώπισης δεν κρίνεται από τους περισσότερους χρήστες απαραίτητη. Από τα “repositories” των εταιρειών που κατασκευάζουν τις διανομές δεν παρέχεται τέτοιου είδους λογισμικό, παρόλα αυτά υπάρχουν εταιρείες που παράγουν λογισμικό αντιμετώπισης σκουληκιών για Linux.

Αντιθέτως από το Linux, στα Windows είναι επιτακτική ανάγκη η χρήση λογισμικού αντιμετώπισης. Φυσικά, τέτοιο λογισμικό δεν παρέχεται από την Microsoft, ούτε μαζί με το λειτουργικό, αλλά ούτε και ως ξεχωριστό προϊόν. Σε

ειδικές περιπτώσεις, όπου η διάδοση ενός σκουληκιού είναι πολύ μεγάλη, τα λειτουργικά συστήματα υποστηρίζονται με αναβαθμίσεις, οι οποίες κλείνουν τις τρύπες στην ασφάλεια που εκμεταλλεύεται το σκουλήκι, όπως συνέβη το 2003 και το 2004 με τα γνωστά σκουλήκια Blaster και Sasser.

Spyware

Spyware είναι το λογισμικό αυτό που εγκαθίσταται σε ηλεκτρονικούς υπολογιστές χωρίς τη συγκατάθεση του χρήστη και έχει ως σκοπό τη συλλογή πληροφοριών για τον ίδιο το χρήστη. Οι πληροφορίες αυτές μπορεί να είναι από λιγότερο σημαντικές (π.χ. προτιμήσεις ιστοσελίδων) έως καταστροφικές (π.χ. αριθμός πιστωτικής κάρτας).

Ποσότητα

Είναι ίσως το πιο διαδεδομένο είδος κακόβουλου λογισμικού στις μέρες μας. Τα είδη και η ποσότητα του λογισμικού αυτού που έχει ως στόχο τα Windows είναι άγνωστα, οι συνέπειες όμως τεράστιες.

Αντιθέτως για Linux δε θεωρείται ότι υπάρχει κάποια γνωστή απειλή. Μέσα στην πάροδο των χρόνων έχουν υπάρξει λογισμικά με τα χαρακτηριστικά ενός Spyware αλλά έχουν αντιμετωπιστεί άμεσα με διορθώσεις σε κενά ασφαλείας από τις εταιρείες που υποστηρίζουν τις διανομές Linux.

Τρόποι αντιμετώπισης

Η Microsoft, έχοντας ανιχνεύσει την τεράστια απειλή του Spyware, από την έκδοση Vista και μετά των Windows, διαθέτει δωρεάν το Windows Defender, του οποίου αποκλειστική αρμοδιότητα είναι η προστασία του υπολογιστή από τέτοιου είδους λογισμικό.

Αντιθέτως στο Linux δεν παρέχεται κάποιο λογισμικό για την αντιμετώπιση του Spyware και αυτό οφείλεται στο ότι δεν υπάρχει πραγματική απειλή.

Ανίχνευση και αντιμετώπιση εισβολών

Η ανίχνευση και η αντιμετώπιση των εισβολών, έχει να κάνει με την παρακολούθηση ενός δικτύου και τον εντοπισμό κακόβουλων δραστηριοτήτων ή παραβιάσεων της πολιτικής του.

Όπως αναφέρθηκε και παραπάνω ο χειρισμός των εισβολών, μπορεί να πραγματοποιηθεί με δύο κύριους τρόπους:

- Ενεργή ανίχνευση εισβολών
- Παθητική αντιμετώπιση εισβολών

Στην ενεργή αντιμετώπιση εισβολών περιλαμβάνονται εκτός από την ανίχνευση και κάποιες αυτοματοποιημένες ενέργειες οι οποίες πραγματοποιούνται, όταν εντοπιστεί εισβολή, ενώ στην παθητική αντιμετώπιση, το λογισμικό που χρησιμοποιείται μόνο ανιχνεύει τις επιθέσεις και ειδοποιεί το διαχειριστή.

Στα λειτουργικά συστήματα Windows, δεν προσφέρεται λογισμικό για την ενεργή ανίχνευση εισβολών (active intrusion detection). Παρόλα αυτά όμως η ίδια η Microsoft στην ιστοσελίδα της τονίζει τη σημασία της παρακολούθησης και της ανίχνευσης εισβολών (Auditing and Intrusion Detection) αλλά προσφέρει μαζί με τα λειτουργικά της συστήματα όλα τα απαραίτητα εργαλεία για την παθητική ανίχνευση εισβολών (passive intrusion detection). Ακόμα και για την ανίχνευση όμως των εισβολών, απαιτούνται ενέργειες του διαχειριστή. Φυσικά, υπάρχουν διάφορα λογισμικά τρίτων κατασκευαστών στην αγορά, τα οποία φροντίζουν για την έγκαιρη ειδοποίηση, όσο και για την αντιμετώπιση των εισβολών.

Αντιθέτως, για λειτουργικά συστήματα Linux, διατίθεται κάθε είδους λογισμικό για την ανίχνευση και την αντιμετώπιση εισβολών. Επιγραμματικά αναφέρονται τα Snort, Kismet, Ethereal κ.α. τα οποία είτε μόνα τους, είτε σε συνδυασμό με άλλο λογισμικό μπορούν να λειτουργήσουν είτε ως παθητικά είτε ως ενεργητικά συστήματα ανίχνευσης εισβολών.

Στον παρακάτω πίνακα απεικονίζεται μία συνοπτική σύγκριση μεταξύ των διάφορων ειδών πακέτων.

Δυνατότητα	.msi (Windows)	.deb (Debian, Ubuntu)	.rpm (Red hat, Fedora, Suse, Mandriva)	.tgz (Slackware)	.pkg (Solaris)
Ψηφιακή υπογραφή	✔	✔	✔	✗	✗
Checksum	✔	✔	✔	✗	✔
Άδειες, Ιδιοκτήτης	✔	✔	✔	✔	✔
Όνομα	✔	✔	✔	✗	✔
Έκδοση	✔	✔	✔	✗	✔
Περιγραφή	✔	✔	✔	✔	✔
Εξαρτήσεις	✔	✔	✔	✗	✔
Συγκρούσεις	✔	✔	✔	✗	✔
Προτεραιότητα	✗	✔	✗	✗	✗

Ψηφιακή Υπογραφή

Η πιστοποίηση του δημιουργού του αρχείου, μέσω της ψηφιακής υπογραφής, είναι μία δυνατότητα που παρέχεται από τα πακέτα msi (Windows), deb (debian, Ubuntu) και rpm (Red hat, Fedora, Suse, Mandriva), ενώ αντιθέτως δεν παρέχεται από τα πακέτα είδους tgz (Slackware) και pkg (Solaris).

Άθροισμα ελέγχου λάθους (Checksum)

Η δυνατότητα επαλήθευσης του περιεχομένου του πακέτου μέσω του αθροίσματος ελέγχου λάθους (Checksum) μπορεί σε μεγάλο βαθμό να εξασφαλίσει ότι το πακέτο δεν έχει υποστεί αλλοίωση. Η πολύ σημαντική αυτή λειτουργία ασφαλείας δεν παρέχεται μόνο από τα πακέτα τύπου tgz των διανομών Slackware.

Άδειες, Ιδιοκτήτης

Η αποθήκευση του ονόματος του ιδιοκτήτη του αρχείου καθώς και πληροφορίες για την άδεια χρήσης του, μπορεί να γίνει από όλα τα είδη πακέτων τα οποία εξετάζονται στην εργασία.

Όνομα

Η επιβεβαίωση του ονόματος του πακέτου παρέχεται από όλα τα είδη πακέτων που μελετώνται, πλην αυτών που έχουν επέκταση tgz και ανήκουν στις διανομές Slackware.

Έκδοση

Σε όλα τα είδη πακέτων που απευθύνονται είτε για λειτουργικά Windows είτε για Linux, εκτός αυτών που προορίζονται για διανομές Slackware, είναι δυνατή η αποθήκευση, μέσα στο ίδιο το πακέτο, της έκδοσης του λογισμικού που περιλαμβάνει.

Περιγραφή

Σε όλα τα είδη πακέτων που απευθύνονται είτε για λειτουργικά Windows είτε για Linux είναι δυνατή η αποθήκευση, μέσα στο ίδιο το πακέτο, της περιγραφής του λογισμικού που περιέχει.

Εξαρτήσεις

Και σε αυτόν τον τομέα, μόνο τα πακέτα μορφής tgz του Slackware linux υστερούν. Σε όλες τις υπόλοιπες μορφές, είναι δυνατή η αποθήκευση εξαρτήσεων του συγκεκριμένου πακέτου από άλλα, τα οποία πρέπει να βρίσκονται εγκατεστημένα στο σύστημα, ώστε να μη δημιουργούνται προβλήματα κατά την εγκατάστασή του.

Συγκρούσεις

Σε κάποιες περιπτώσεις, εκτός από τα πακέτα που πρέπει να βρίσκονται εγκατεστημένα στο σύστημα, ώστε να μπορέσει να εγκατασταθεί ένα πακέτο, υπάρχει και ο περιορισμός πακέτων που δεν πρέπει να βρίσκονται εγκατεστημένα, ώστε να μη δημιουργούνται συγκρούσεις.

Και εδώ μόνο τα πακέτα μορφής tgz του Slackware linux δεν παρέχουν αυτή τη δυνατότητα. Τόσο τα πακέτα μορφής msi (Windows) όσο και τα deb, rpm, pkg την παρέχουν.

Προτεραιότητα

Στα πακέτα τύπου deb των διανομών Debian και Ubuntu, αποθηκεύεται πληροφορία σχετικά με την προτεραιότητα κάθε πακέτου. Πακέτα με υψηλή προτεραιότητα είναι εκείνα τα πακέτα που πρέπει να εγκατασταθούν οπωσδήποτε από το χρήστη για να λειτουργήσει το σύστημα σωστά, ενώ πακέτα με χαμηλή προτεραιότητα δε χρήζουν εγκατάστασης, εκτός και αν ο ίδιος ο χρήστης επιθυμεί να την πραγματοποιήσει.

Τόσο στις διάφορες εκδόσεις Windows, όσο και στις υπόλοιπες εκδόσεις Linux, η δυνατότητα αυτή δεν παρέχεται, τουλάχιστον όχι με αυτόν τον τρόπο.

Επίλογος

Στο χώρο της πληροφορικής, η διαμάχη μεταξύ των υποστηρικτών των λειτουργικών συστημάτων Linux και των υποστηρικτών των Windows μαίνεται εδώ και πολλά χρόνια και δεν αναμένεται να κοπάσει σύντομα.

Στην εργασία αυτή αναλύθηκαν ξεχωριστά αλλά και κατ' αντιπαράθεση οι σημαντικότερες λειτουργίες ασφαλείας διαφόρων διανομών του Linux αλλά και διαφόρων εκδόσεων των Windows.

Όπως αναφέρθηκε πολλές φορές μέσα στην εργασία, σκοπός της δεν ήταν η εύρεση του καλύτερου λειτουργικού συστήματος όσον αφορά στην ασφάλεια, αλλά η αντιπαράθεση λειτουργιών ασφαλείας που πραγματοποιούνται από τα δύο είδη λειτουργικών συστημάτων. Γι' αυτό το λόγο πουθενά δεν αναφέρεται υπεροχή του ενός ως προς το άλλο παρά μόνο ελλείψεις όπου αυτές εντοπίστηκαν.

Ευχαριστώ τον καθηγητή κ. Σωκράτη Κάτσικα για το χρόνο που αφιέρωσε για να με βοηθήσει στην εκπόνηση της πτυχιακής αυτής εργασίας τόσο ως προς τη δομή της, όσο και ως προς το υλικό που χρησιμοποιήθηκε.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Βιβλία

1) Windows Vista Security (Roger A. Grimes, Jesper M Johansson)
2) Πλήρες Εγχειρίδιο UNIX (Kate Wrightson, Joe Merlino)
3) Microsoft Encyclopedia of Networking (Mitch Tulloch)
4) Σύγχρονα Λειτουργικά Συστήματα Α' Τόμος (A.S. Tanenbaum)
5) Σύγχρονα Λειτουργικά Συστήματα Β' Τόμος (A.S. Tanenbaum)

Διαδικτυακοί Τόποι

1) http://www.wikipedia.org
2) http://www.tech-faq.com/
3) http://tldp.org/HOWTO/Security-HOWTO/
4) http://www.linuxtopia.org/LinuxSecurity/index.html
5) http://www.microsoft.com
6) http://www.kaspersky.com
7) http://www.ntfs.com/ntfs_vs_fat.htm
8) http://linux.about.com/
9) http://Novell.com