Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων

Πτυχιακή εργασία

Τίτλος:

Μελέτη και δοκιμαστική λειτουργία των μηχανισμών ασφάλειας που παρέχει η πλατφόρμα Microsoft Windows XP

ΚΟΥΡΟΣ ΚΩΝΣΤΑΝΤΙΝΟΣ (Α.Μ. 355)

Ηράκλειο - Ημερομηνία

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

Περιεχόμενα

Εισαγωγή

Σκοπός μελέτης

Το λειτουργικό σύστημα Microsoft Windows XP είναι το πλέον διαδεδομένο, τόσο σε προσωπική/οικιακή όσο και επαγγελματική/εμπορική χρήση. Οι νεότερες εκδόσεις του λειτουργικού συστήματος Windows, ικανοποιώντας τις απαιτήσεις των χρηστών, ενσωματώνουν όλο και περισσότερες εφαρμογές ή επιλογές που σκοπό έχουν να αυξήσουν την ασφάλεια που αυτό το σύστημα παρέχει. Η προστασία του χρήστη είναι ακρογωνιαίος λίθος στην δημιουργία ενός κλίματος εμπιστοσύνης, απαραίτητο για την εισαγωγή νέων τεχνολογιών με τα οφέλη που αυτές συνεπάγονται.

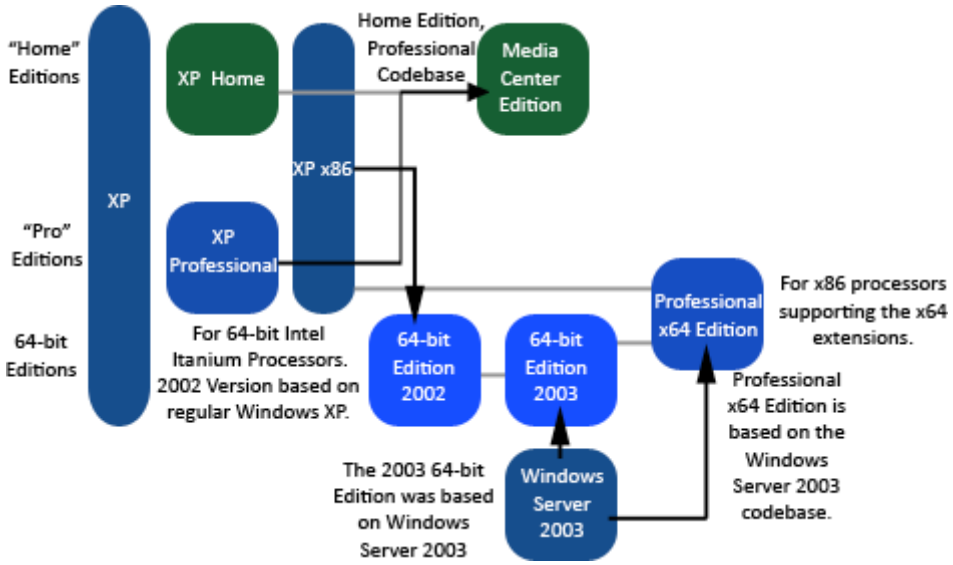
Η πτυχιακή εργασία μελετά και δοκιμάζει στην πράξη τις περισσότερες δυνατότητες που τα MS Windows XP παρέχουν στους χρήστες για την προστασία της ταυτότητάς τους, των δεδομένων τους, καθώς και των επικοινωνιών τους.

Λίγα λόγια για τα Windows XP

Τα Windows XP είναι ένα λειτουργικό σύστημα εξελιγμένο για υπολογιστές γενικών χρήσεων, μπορεί να χρησιμοποιηθεί στο σπίτι, στο γραφείο, σε φορητούς υπολογιστές καθώς και σε συστήματα αναπαραγωγής πολυμέσων. Τα γράμματα XP συμβολίζουν την λέξη εμπειρία (eXPerience). Είναι ο απόγονος των Windows 2000 και Windows Me, και είναι το πρώτο, προορισμένο για το κοινό, σύστημα φτιαγμένο από την Microsoft που είναι χτισμένο πάνω στην αρχιτεκτονική και τον πυρήνα (Kernel) των Windows NT.στην αγορά πρωτοεμφανίστηκαν τις 25 Οκτώβρη 2001, και πάνω από 400 εκατομμύρια αντίτυπα είναι σε χρήση ανά τον κόσμο, σύμφωνα με μια εκτίμηση του Ιανουαρίου του 2006 από έναν αναλυτή της IDC (International Data Corporation).

Οι πιο διαδομένες εκδόσεις των XP είναι η Home edition, που στοχεύει στους υπολογιστές που βρίσκονται σε σπίτια, και η XP Professional, που έχει επιπλέον στοιχεία όπως υποστήριξη για Windows Server domains και διπλούς επεξεργαστές, και στοχεύει σε έμπειρους χρήστες και επιχειρήσεις. Η έκδοση Windows XP Media Center έχει επιπλέον στοιχεία για αναπαραγωγή πολυμέσων βελτιώνοντας τις δυνατότητες προβολής και εγγραφής τηλεόρασης, ταινιών DVD, και μουσικής. Η Windows XP Tablet PC έκδοση είναι σχεδιασμένη να τρέχει την Tablet PC πλατφόρμα. Τέλος υπάρχουν δύο εκδόσεις για επεξεργαστές με λέξη μνήμης 64-bit, η Windows XP 64-bit για IA-64 (Itanium) επεξεργαστές και Windows XP Professional x64 για x86-64 επεξεργαστές.

Ακολουθεί ένα σχεδιάγραμμα που δείχνει τις κυριότερες εκδόσεις των XP.Με γκρι βέλος φαίνεται η κατηγορία και με μαύρο ο κώδικας βάση (Codebase).



Τα Windows XP είναι γνωστά για την βελτιωμένη σταθερότητα και αποδοτικότητα σε σχέση με τι προηγούμενες εκδόσεις των Microsoft Windows. Παρουσιάζει μια επανασχεδιασμένη γραφική διεπαφή χρήστη, μια αλλαγή που η Microsoft διαφήμισε σαν πιο φιλική προς τον χρήστη σε σχέση με τις παλαιότερες εκδόσεις. Νέες δυνατότητες διαχείρισης λογισμικού αναπτύχθηκαν για να αποφευχθεί η κόλαση των DLL (DLL-Hell) που μάστιζε τις παλαιές πελατειακές εκδόσεις των Windows. Είναι επίσης η πρώτη έκδοση Windows που χρησιμοποιεί ενεργοποίηση προϊόντος (product activation) για να καταπολεμήσει την πειρατεία του λογισμικού, μια τεχνολογία που δεν άρεσε σε πολλούς χρήστες και σε κάποιους δικηγόρους.

Τέλος τα Windows XP έχουν προκαλέσει την κριτική για προβλήματα ασφάλειας, προβλήματα που αφορούν το μπλέξιμο των προγραμμάτων (integration of applications) όπως ο Internet Explorer και ο Windows Media Player, και για τομείς της διεπαφής χρήστη υπολογιστή.

Προβλήματα ασφάλειας

Τα Windows XP έχουν δεχτεί έντονη κριτική για την ασφάλεια που προσφέρουν, αυτό γιατί είναι ευπαθή σε malware, ιούς, Trojan horses, και σκουλήκια. Τα προβλήματα αυτά προκύπτουν από το γεγονός ότι οι χρήστες της έκδοσης Home έχουν από την αρχή έναν administrator λογαριασμό που τους παρέχει πλήρης πρόσβαση σε όλους του τομείς του συστήματος. Άρα αν σπάσει ο λογαριασμός αυτός τότε δεν υπάρχει όριο στο τι μπορεί να κάνει κανείς στο σύστημα. Επίσης υπάρχουν και άλλοι τομείς οι οποίοι είναι ευαίσθητοι σε επιθέσεις και απαιτούν την προσοχή του χρήστη και τον συνεχή έλεγχο. Στη συνέχεια θα εξετάσουμε τις περιοχές αυτές και θα δούμε πως μπορούμε να εκμεταλλευτούμε τα κενά ασφάλειας στο σύστημα ώστε να βρούμε τρόπους προστασίας, επίσης θα τρέξουμε και κάποια εργαλεία τα οποία προσφέρουν ή πρόσθετη ασφάλεια ή διάγνωση του επιπέδου ασφάλειας του συστήματος. Το σύστημα στο οποίο θα δουλέψουμε τρέχει Windows XP professional

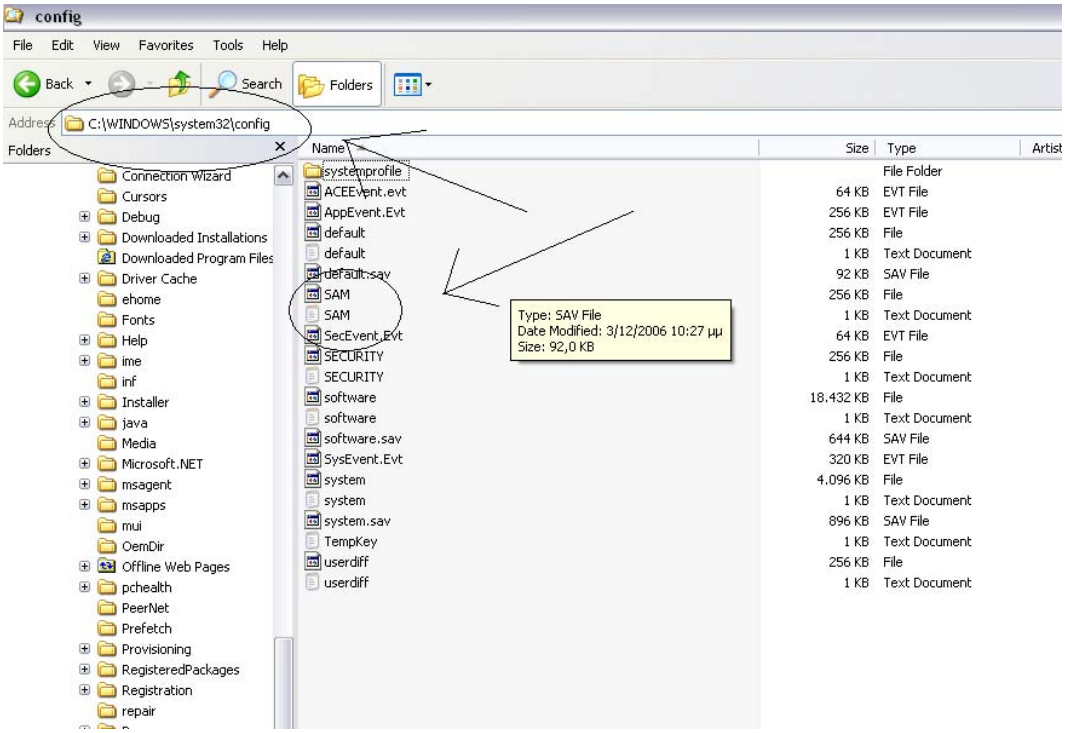
με Service pack 2 και Office 2003, το επιλέξαμε διότι αποτελεί την επιλογή λειτουργικού που αποτελεί την πλειοψηφεία των συστημάτων την παρούσα χρονική περίοδο.

Τα passwords και η λειτουργία τους

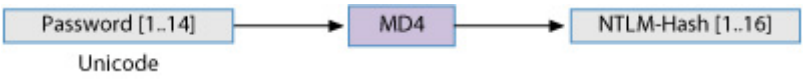
Windows Passwords

PASSWORDS

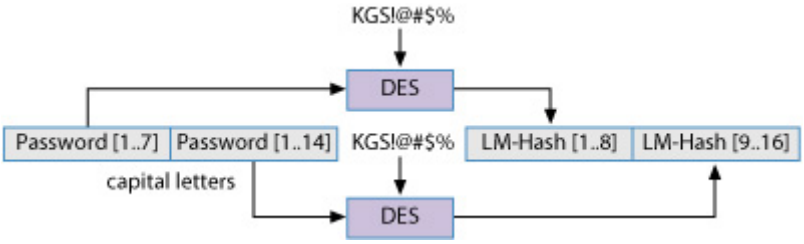
Τα passwords στα windows XP και 2K είναι αποθηκεμένα στο SAM file το οποίο βρίσκεται στο c:\windows\system32\config .



Τα passwords είναι μεγέθους 14 byte και μετατρέπονται σε Unicode.Το Unicode είναι ένα πρότυπο σχεδιασμένο να επιτρέπει κείμενο και σύμβολα από όλα τα γραφικά συστήματα στον κόσμο να αναγνωρίζονται και να διαχειρίζονται από υπολογιστές .Αποτελείται από ένα ρεπερτόριο χαρακτήρων ,μια μεθοδολογία κωδικοποίησης και ένα σετ από standard κωδικοποιήσεις χαρακτήρων, ένα σετ από γραφήματα κωδικών για οπτική αναφορά, μια αρίθμηση των χαρακτήρων για να διαχωρίζονται οι ιδιότητες τους, όπως κεφαλαία και μικρά, ένα σετ από αρχεία δεδομένων υπολογιστή για λόγους αναφοράς και κανόνες για απλούστευση , διαχείριση και μετατροπή .Αυτό γίνεται για να διατηρηθεί ο διαχωρισμός μεταξύ κεφαλαίων και μικρών, έπειτα με την βοήθεια του αλγόριθμου MD4 ή MD5 δημιουργείται ένα 16- byte (128 - bit) NTLM hash και αποθηκεύεται σε ένα κομμάτι .



Επίσης για λόγους συμβατότητας δημιουργείται και αποθηκεύεται και το LM (LAN Manager) hash, το οποίο χρησιμοποιείται όταν θέλουμε να κάνουμε το σύστημα μας μέλος ενός domain, και τα δύο αποθηκεύονται στο SAM file. Το hash που δημιουργείται είναι one-way άρα για να το σπάσεις πρέπει να δημιουργήσεις το ακριβώς ίδιο hash.Αυτή η μέθοδο ενώ προσφέρει ασφάλεια από brute force προσπάθειες κάποιου που έχει κλέψει το SAM file είναι αδύναμη σε άλλες μεθόδους εισβολής, τις οποίες θα αναλύσουμε παρακάτω, επίσης ένα ακόμα αδύναμο σημείο είναι το LM hash που δημιουργείται από το password, γιατί είναι case insensitive και ενώ έχει μέγεθος 14 characters, για passwords μεγαλύτερα από 7 χαρακτήρες δημιουργούνται δυο αδύναμα hash 7 χαρακτήρων το ένα και τα υπόλοιπα στο άλλο.



Τέλος ένα ακόμα σημείο που πρέπει να προσέξουμε είναι ότι τα windows σε μικρά passwords συμπληρώνουν μηδενικά άρα τα hashes μπορούν να προϋπολογιστούν γιατί δεν χρησιμοποιούνται random αξίες για την δημιουργία τους.

RECOVERY-CRACKING

Υπάρχουν διάφοροι τρόποι για να σπάσεις το password, ας τους εξετάσουμε.
Μπορείς χρησιμοποιώντας ένα bootable cd να κάνεις Reset το password, ξεκινάς κατεβάζοντας ένα Linux boot diskette
http://home.eunet.no/%7Epnordahl/ntpasswd/bootdisk.html
ή κάποιο άλλο πρόγραμμα που μπορεί να κάνει reset τα τοπικά win2k/xp passwords (Passware's password recovery kit, CIA commander, Offline NT password & registry editor, etc),γράφεις το image σε μια δισκέτα και ξεκινάς τον υπολογιστή κάνοντας boot από την δισκέτα και ακολουθώντας τις οδηγίες μπορείς να σβήσεις ή να αλλάξεις το password και μετά να ξεκινήσεις τα windows και να βάλεις το νέο password..Αυτές οι μεθόδους ενώ είναι πολύ απλές και γρήγορες, έχουν το μειονέκτημα ότι δεν θα μάθεις ποτέ το password και δεν δουλεύουν πάντα. Ένας άλλος τρόπος είναι να χρησιμοποιήσεις μια password reset disk εφόσον έχεις δημιουργήσει μια. Για να το κάνεις πας στο account manager και επιλέγεις prevent a forgotten password


Forgotten Password Wizard
Welcome to the Forgotten Password Wizard
This wizard helps you create a "password reset" disk. If you forget the password for this user account and are unable to log on, you can use this disk to create a new password.
Note: No matter how many times you change your password, you only need to create this disk once.
Warning: Anyone can use this disk to reset the password, and therefore have access to this account.
To continue, click Next.
< Back
Next >
Cancel

Πατάς Next,


Forgotten Password Wizard
Create a Password Reset Disk
The wizard will save password information about this user account to the disk in the drive below.
I want to create a password key disk in the following drive:
3.5 Floppy (A:)
< Back
Next >
Cancel

Βάζεις μια κενή δισκέττα και πατάς Next,

Πληκτρολογείς το password σου και συνεχίζεις,

Και η δισκέττα σου είναι έτοιμη,

Τώρα ας δούμε πως μπορείς να σπάσεις το password σε κάποιο σύστημα και όχι να το αλλάξεις.Αυτό μας ενδιαφέρει περισσότερο γιατί εξετάζουμε την ασφάλεια του συστήματος μας ενώ οι παραπάνω τρόποι είναι για περιπτώσεις που έχεις ξεχάσει κάποιο password και όχι για να αποκτήσεις πρόσβαση σε κάποιο προστατευμένο σύστημα.

Λοιπόν πρώτα από όλα πρέπει να αποκτήσεις το SAM file που είναι αποθηκευμένα τα password και μετά να το σπάσεις. Το SAM file μέσα από το περιβάλλον των Windows είναι κλειδωμένο, ένα άλλο SAM file το οποίο μπορείς να πάρεις υπάρχει στον φάκελο

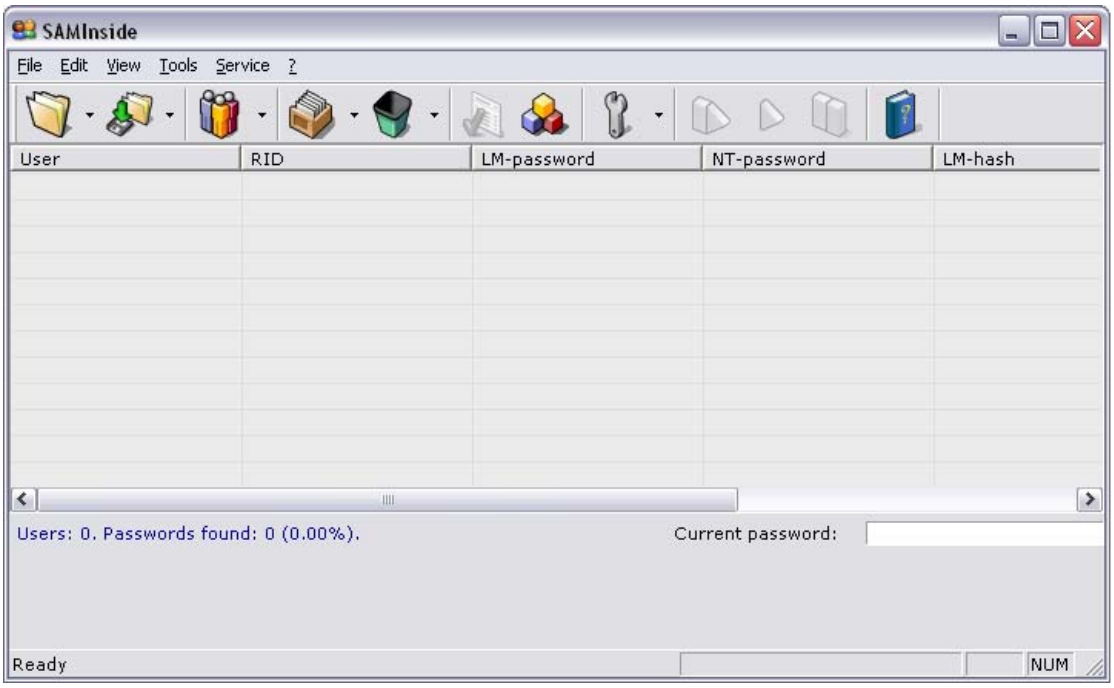
C:\WINDOWS\repair

Αλλά είναι το Default SAM file, άρα δεν έχει όλα τα passwords, οπότε πρέπει να αποκτήσουμε το πρώτο SAM file.

Ας δούμε κάποιους τρόπους για να κάνουμε αυτό.

Για τον πρώτο τρόπο χρειαζόμαστε το SamInside

http://www.topshareware.com/SAMInside-download-5188.htm.



Ένα εργαλείο που σου επιτρέπει να βγάλεις τα hashes από ένα κρυπτογραφημένο με syskey SAM file. Το syskey είναι μια προσπάθεια της Microsoft να βελτιώσει την ασφάλεια, αυτό που κάνει είναι να προσθέτει ένα κλειδί 128-bit στα hashes. Ένα bootcd με κάποιο πρόγραμμα όπως π.χ. το knoppix

http://www.knoppix-std.org/

και ένα USB flashdrive

Ξεκινάς το σύστημα του οποίου το password θέλεις να πάρεις κάνοντας boot με το knoppix και βάζεις το USB flashdrive στο σύστημα. Στην συνέχεια κάνεις mount το drive σε έναν φάκελο

```
mount -rw /dev/sda1 /mnt/sda1
```

και τον σκληρό δίσκο σε άλλον φάκελο

```
mount -rw /dev/hda1 /mnt/hda1
```

Έπειτα πληκτρολογείς

```
cd /mnt/hda1/windows/system32/config/
```

για να πας στο c:\windows\system32\config\ folder που βρίσκεται το SAM file και το αντιγράφεις μαζί με το system file στο USB σου

cp sam /mnt/sda1/,cp system /mnt/sda1.

Παίρνεις το USB και το βάζεις στο δικό σου σύστημα, τρέχεις το samInside και επιλέγεις το SAM και το SYSTEM file όταν σου ζητηθούν, μετά πατάς <ctrl>+<s> για να σώσεις τα hashes σε ένα textfile.

Ένας άλλος τρόπος είναι να ξεκινήσεις τον υπολογιστή με μια NTFS dos δισκέττα, όταν ξεκινήσει πήγαινε στο C:\windows(\winnt)\system32\config και αντέγραψε το SAM file σε μια δισκέττα. Τώρα που έχεις το SAM μπορείς να χρησιμοποιήσεις το samdump για να διώξεις το md5 hash, αυτό το κάνεις αν σε command prompt πληκτρολογήσεις

samdump C:\sam>>sammd5.txt.

Άρα σου μένει να σπάσεις τα md5 passwords.

Ένας πιο περίπλοκός τρόπος είναι ο παρακάτω:

Θα χρειαστούμε πρόσβαση σε ένα PC και ένα account (guest ή κάποιον άλλο), 4 ή περισσότερες δισκέττες, το chntpw και SCSI drivers, το pwdump2 ή v.3 και το NTFS dos

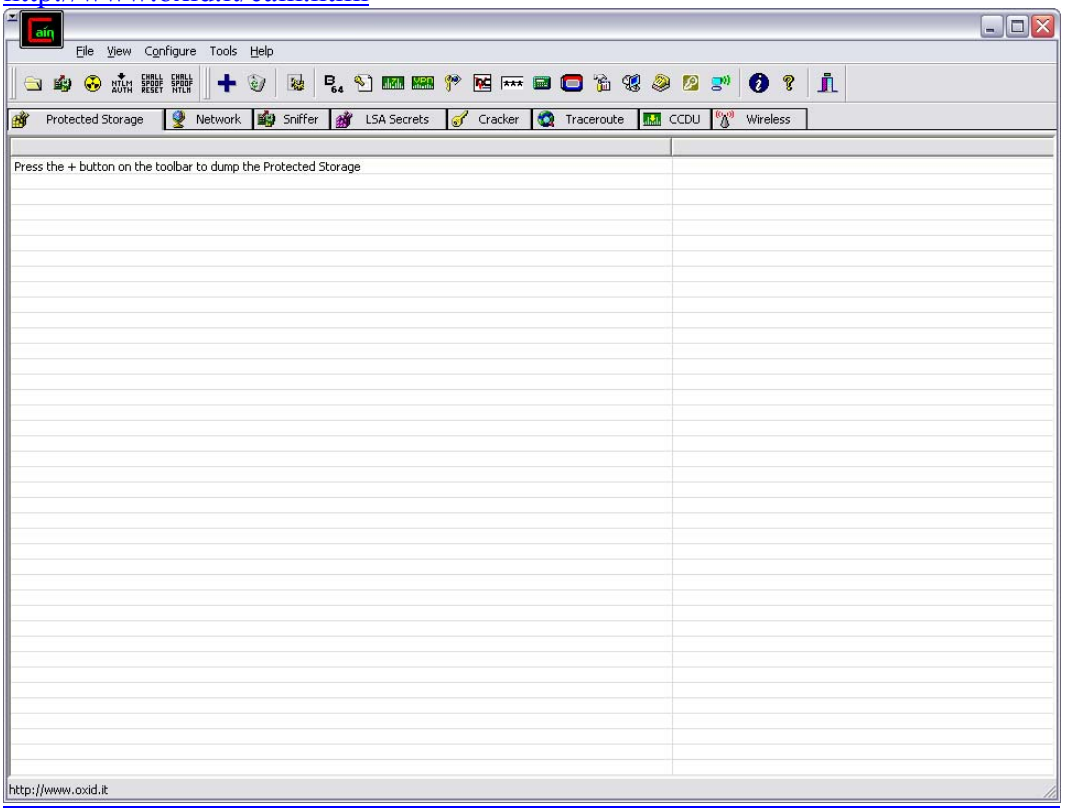
.Στην πρώτη δισκέττα φορτώνουμε το chntpw, στην δεύτερη τους SCSI drivers, για τις δύο πρώτες χρησιμοποιούμε το rawrite2, και στις δύο άλλες το NTFS dos (μια bootable και στην άλλη το πρόγραμμα).
Ξεγίναμε το PC με το NTFS dos βρίσκουμε το SAM file και το αντιγράφουμε στην δισκέττα. Κάνουμε restart το pc και βάζουμε την chntpw δισκέττα (χρεισημοποιούμε τους SCSI drivers όπου χρειαστεί). Έπειτα θέτουμε το HKML\System\CurrentControlSet\Control\Lsa\SecureBoot σε 1. Προφανώς δεν θέλουμε να αλλάξουμε το admin password, θέλουμε να αναβαθμίσουμε ένα άλλο account (π.χ. guest,test). Γράφουμε RID για το guest και γράφουμε @ για το νέο password (πρέπει να είναι @), και έτσι ο guest account ανήκει στο admin group.
Στη συνέχεια βγαίνεις, κάνεις reboot, και μπαίνεις στο guest account χωρίς password, τώρα τρέχεις το pwdump2
http://razor.bindview.com/tools/desc/pwdump2_readme.html
(αυτό μπορείς να το κάνεις μόνο αν είσαι admin και κάνει την ίδια δουλεία με το samdump), αντιγράφεις τα hashes σε μια δισκέττα και τα παίρνεις. Όμως πριν φύγεις πρέπει να πειράξεις το LOG file για να σβήσεις τα ίχνη σου και να ξεκινήσεις το NTFSdos ξανά και να αντικαταστήσεις το αλλαγμένο SAM file με το παλιό που έχεις στην δισκέττα.
Με τους παραπάνω τρόπους αποκτήσαμε το SAM file και τα hashes τώρα μας μένει να δούμε με ποιους τρόπους μπορούμε να τα σπάσουμε και να βρούμε τον καλύτερο.

Από τα προγράμματα που χρησιμοποιούνται για να σπάσουμε τους κωδικούς τα πιο γρήγορα και πιο δημοφιλή είναι τα LC5, John-the-Ripper, Cain & Abel και ένας σχετικά καινούργιος τρόπος είναι το Rainbow tables που θα το συζητήσουμε λίγο στο τέλος.
Το πιο γνωστό εργαλείο είναι το LC5 το οποίο χρησιμοποιείται για να τεστάρεις την ποιότητα των κωδικών, για να σου θυμίσει έναν κωδικό που ξέχασες και φυσικά για επιθέσεις όταν έχεις τα LM και NTLM hashes.Με το LC5 μπορείς να έχεις πρόσβαση

στο SAM εφόσον χρησιμοποιείς admin account, αλλιώς μπορείς να έχεις πρόσβαση στο backup copy του SAM που είναι στο repair folder. Αλλιώς μπορείς να πάρεις το SAM με έναν από τους τρόπους που είπαμε παραπάνω και μετά να τρέξεις το LC5 σε άλλον υπολογιστή, τέλος μπορεί να κάνει sniffing το τοπικό δίκτυο για να πιάσει hashes που μεταδίδονται όπως Login, file sharing, printer sharing etc .

-Πως δουλεύει το LC5.

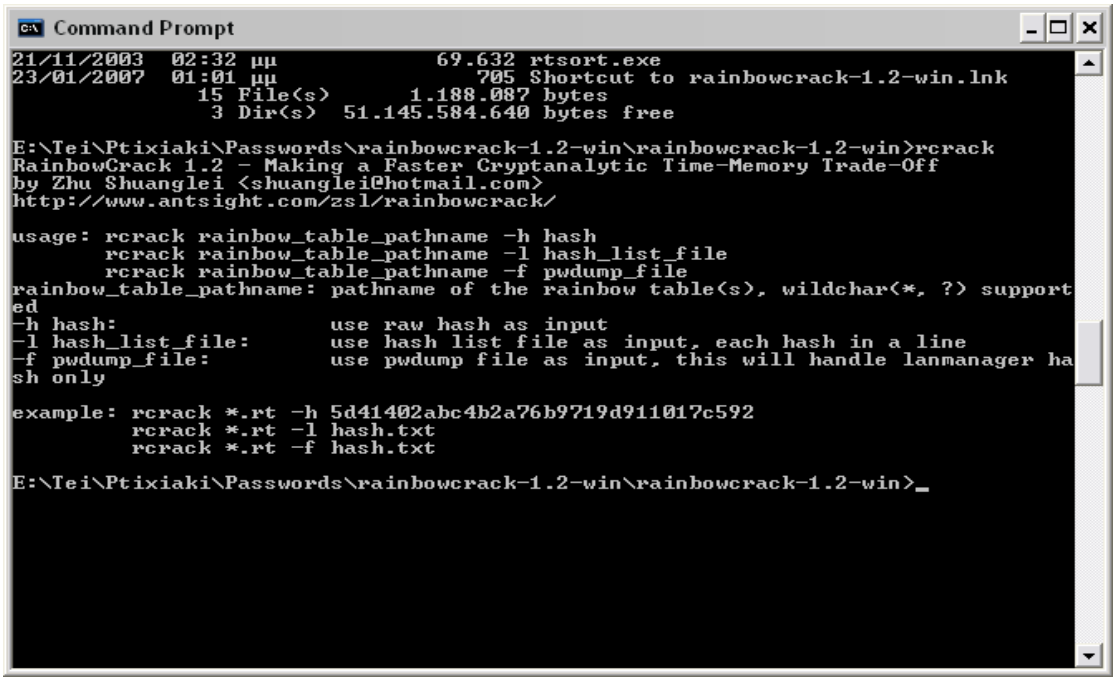
Πρώτα ξεκινάει κάνοντας μια επίθεση συντακτικού εναντίον των hashes διαβάζοντας από λίστα με διάφορες λέξεις. Έτσι τα αδύναμα password μπορούν να σπάσουν σε ένα σχετικά μικρό χρονικό διάστημα. Αν αυτή η μέθοδος αποτύχει τότε εξαπολύεται μια επίθεση τύπου brute-force, και όσο μεγαλώνει η λέξη δοκιμάζονται όλοι οι συνδυασμοί χαρακτήρων και αριθμών καθώς και ειδικών χαρακτήρων. Όπως είναι λογικό μια τέτοια επίθεση παίρνει περισσότερο χρόνο ειδικά αν τα passwords έχουν επιλεχθεί προσεκτικά. Τέλος υπάρχει και η δυνατότητα της αναμειγμένης επίθεσης (Hybrid attack), κατά την οποία το LC5 συνδυάζει στοιχεία από την λίστα των λέξεων με επιπλέον χαρακτήρες, και της προεπιλεγμένης επίθεσης (precomputed Attack) ,κάτι που υπάρχει μόνο στο LC5, και συγκρίνει το hash με διάφορα άλλα που έχει σε μια λίστα. Αυτή η επίθεση είναι πολλή γρήγορη αλλά πρέπει να υπάρχει το hash που ψάχνουμε στην λίστα.
Τα John-the-Ripper
http://www.openwall.com/john/
και Cain & Abel
http://www.oxid.it/cain.html



ενώ έχουν παρόμοιες λειτουργίες για σπάσιμο κωδικών και είναι πολύ ισχυρά εργαλεία, δεν προσφέρουν την επιλογή της πηγής των hashes όπως το LC5

Επίσης το LC5 είναι πιο γρήγορο από τα άλλα και πιο αξιόπιστο, όμως τα άλλα δύο προσφέρονται δωρεάν.

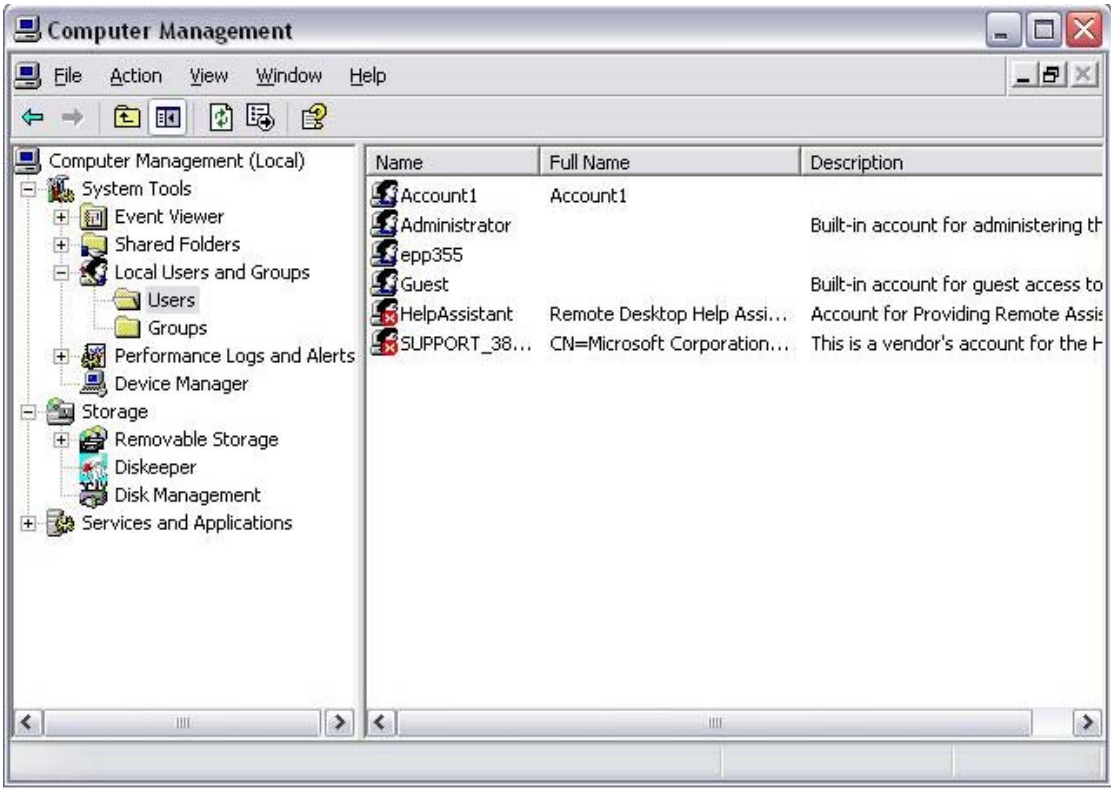
Ένας ακόμα τρόπος είναι να χρησιμοποιήσεις κάποια υπηρεσία στο internet που σπάει passwords, συνήθως με ένα μικρό αντίτιμο αν θέλεις γρήγορα αποτελέσματα, κάτι τέτοιο είναι τα εξής
http://www.loginrecovery.com/instructions.html , http://passcracking.ru/
Τέλος ας αναφερθούμε λίγο στην μέθοδο των Rainbow tables http://www.antsight.com/zsl/rainbowcrack/
η οποία είναι κατά την προσωπική μου εκτίμηση η καλύτερη και ευκολότερη μέθοδος. Πρώτα υπολογίζει κάθε πιθανό συνδυασμό κωδικών και μετά σπάει το md5 password σε δευτερόλεπτα.το βασικό μειονέκτημα είναι ότι κατά των υπολογισμό μπορεί να καταναλώσει 3 giga και κάνει έως και 26 μέρες αν έχουμε αργό υπολογιστή. Όμως υπάρχει η δυνατότητα να αγοράσεις τους πίνακες έτοιμους από το internet, το www.secureit.co.il έχει έναν πίνακα που θα σπάσει κάθε κωδικό md5.



LC5 βήμα προς βήμα

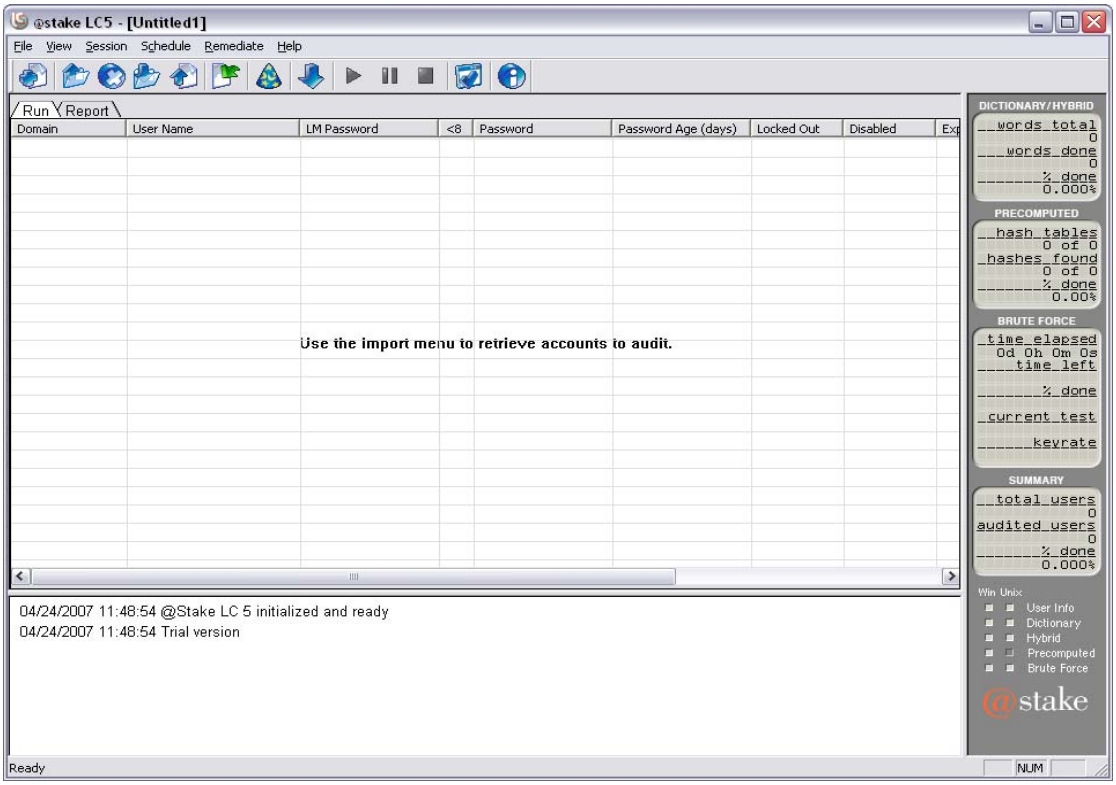
Ας δούμε ένα παράδειγμα του πως δουλεύει το LC5, ξεκινάμε δημιουργώντας στον υπολογιστή μας μερικά accounts και με την χρήση του LC5 θα σπάσουμε τα passwords .

Ο υπολογιστής στον οποίο θα εργαστούμε τρέχει windows XP Service pack 2, μέσω του Computer manager δημιουργούμαι τα accounts

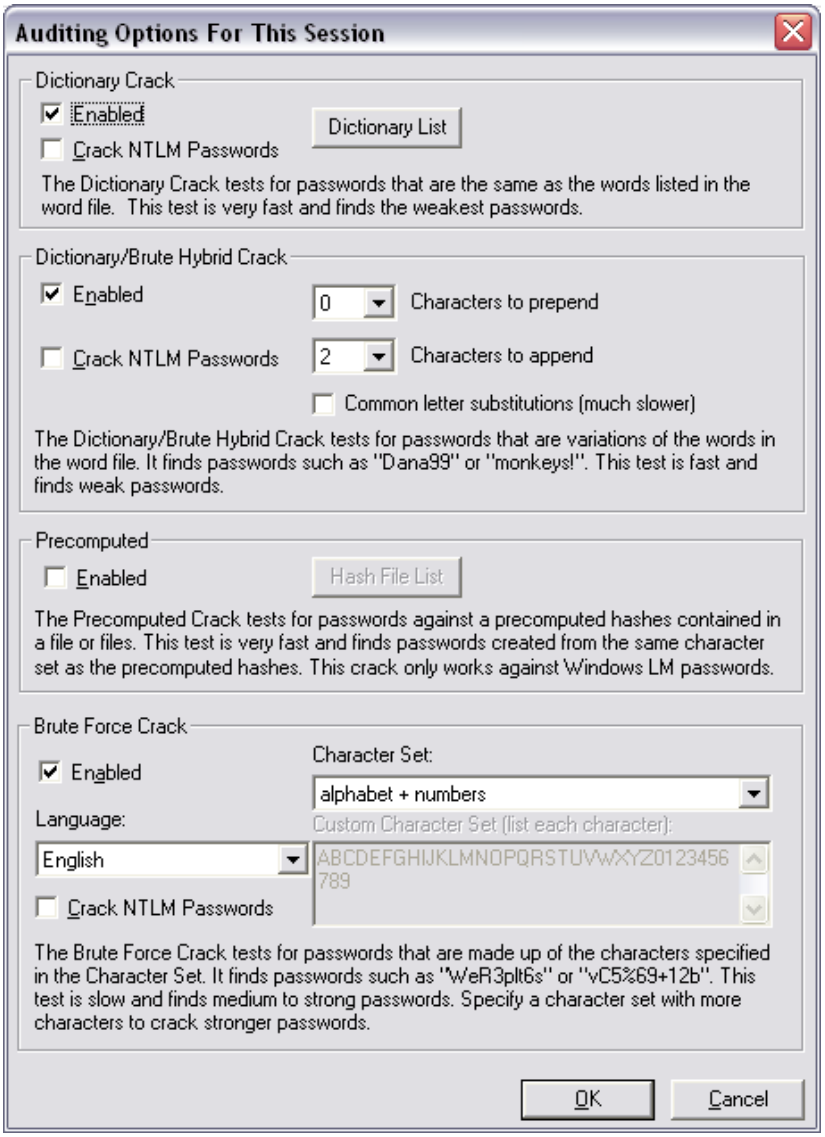


Στο παραπάνω παράθυρο πατώντας δεξί κλικ και επιλέγοντας New User μας παρουσιάζεται το παρακάτω παράθυρο

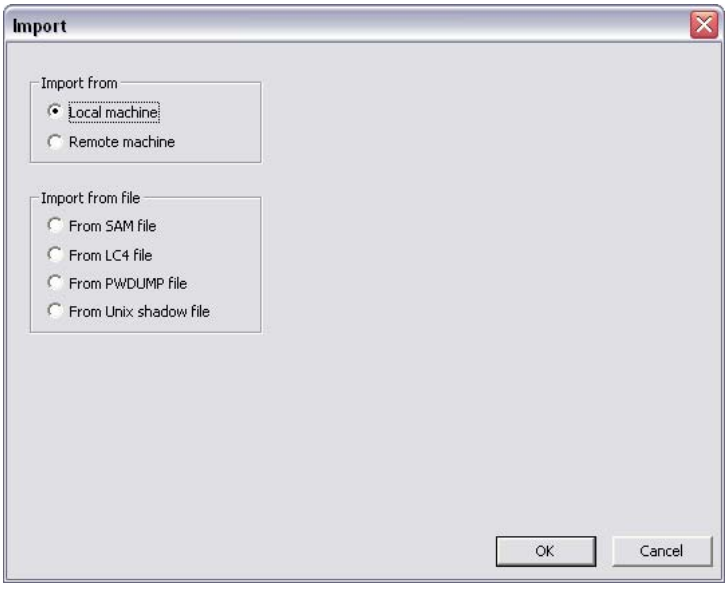
Αφού δημιουργήσαμε τα accounts είμαστε έτοιμοι να τρέξουμε το LC5. Η έκδοση που θα χρησιμοποιήσουμε είναι μια trial 15 ημερών, για την πλήρης έκδοση πρέπει να αγοράσεις ένα cd-key, την trial μπορείς να την κατεβάσεις από το http://sectools.org/tools2.html.
Ξεκινώντας το LC5 βλέπουμε την ακόλουθη οθόνη

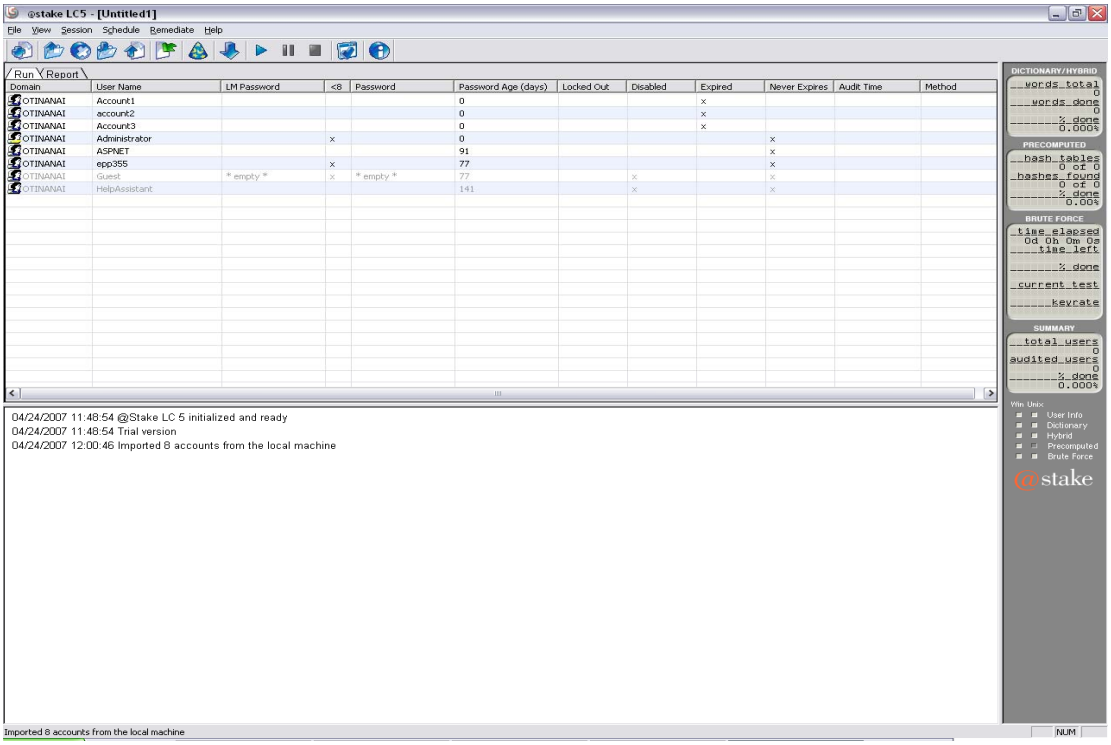


Στο μενού Session -> Session options υπάρχουν οι μέθοδοι auditing που μπορούμε να χρησιμοποιήσουμε. Αυτές είναι η Dictionary, η Hybrid, η Precomputed, και η Brute Force. Το τι τρόπο λειτουργίας έχουν το αναφέραμε παραπάνω, και από το παράθυρο που βλέπουμε μπορούμε να επιλέξουμε την διαδικασία που θα ακολουθήσουμε και τις επιμέρους ρυθμίσεις.

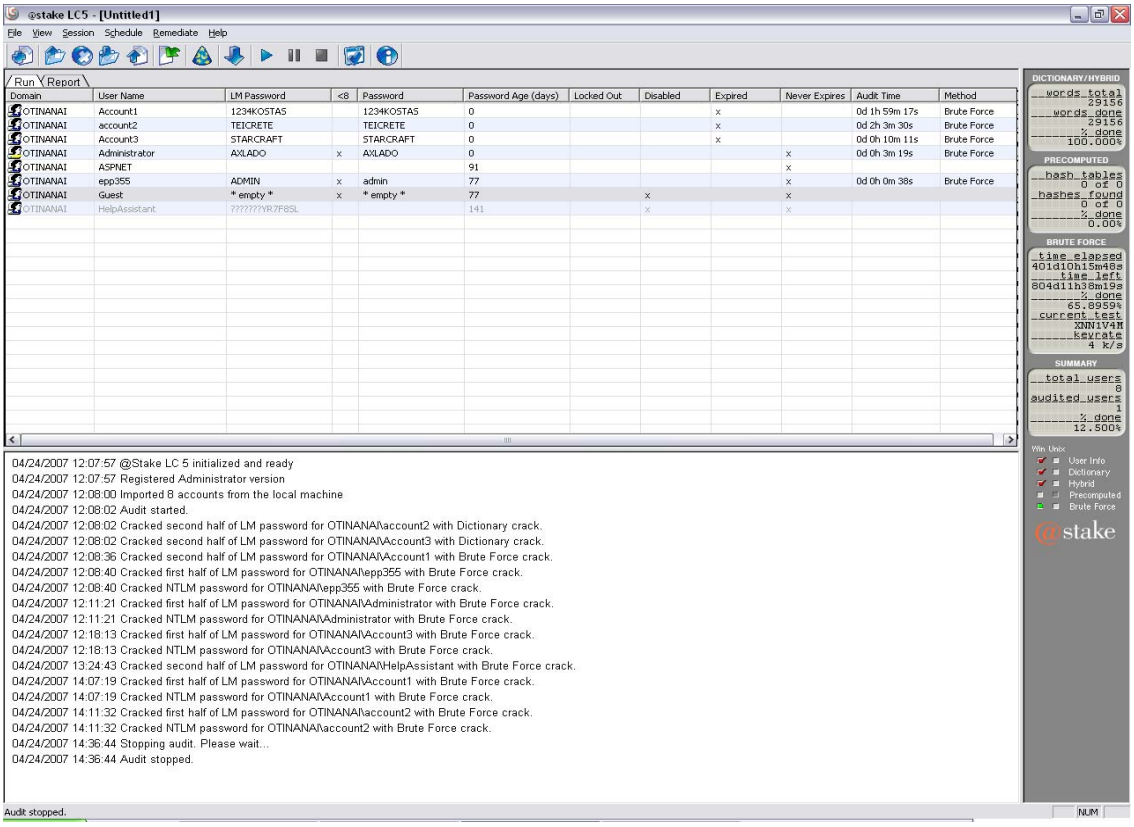


Στην συνέχεια επιλέγουμε από το μενού Session το Import και από τις επιλογές που βλέπουμε το Local Machine.





Βλέπουμε ότι αμέσως το LC5 εντοπίζει πόσα accounts έχουμε στο σύστημα, ποια έχουν password, ποια password είναι μεγαλύτερα από 8 ψηφία, και πόσον ημερών είναι. Στο πλάι δεξιά βλέπουμε τα στατιστικά της κάθε μεθόδου. Στην συνέχεια πατάμε το play και περιμένουμε τα αποτελέσματα, ανάλογα με το password ο χρόνος αναμονής διαφέρει. Με το πέρας της διαδικασίας βλέπουμε τα αποτελέσματα, και στο κάτω μισό την πρόοδο της διαδικασίας με τις χρονικές στιγμές που έσπασε ο κάθε κωδικός.



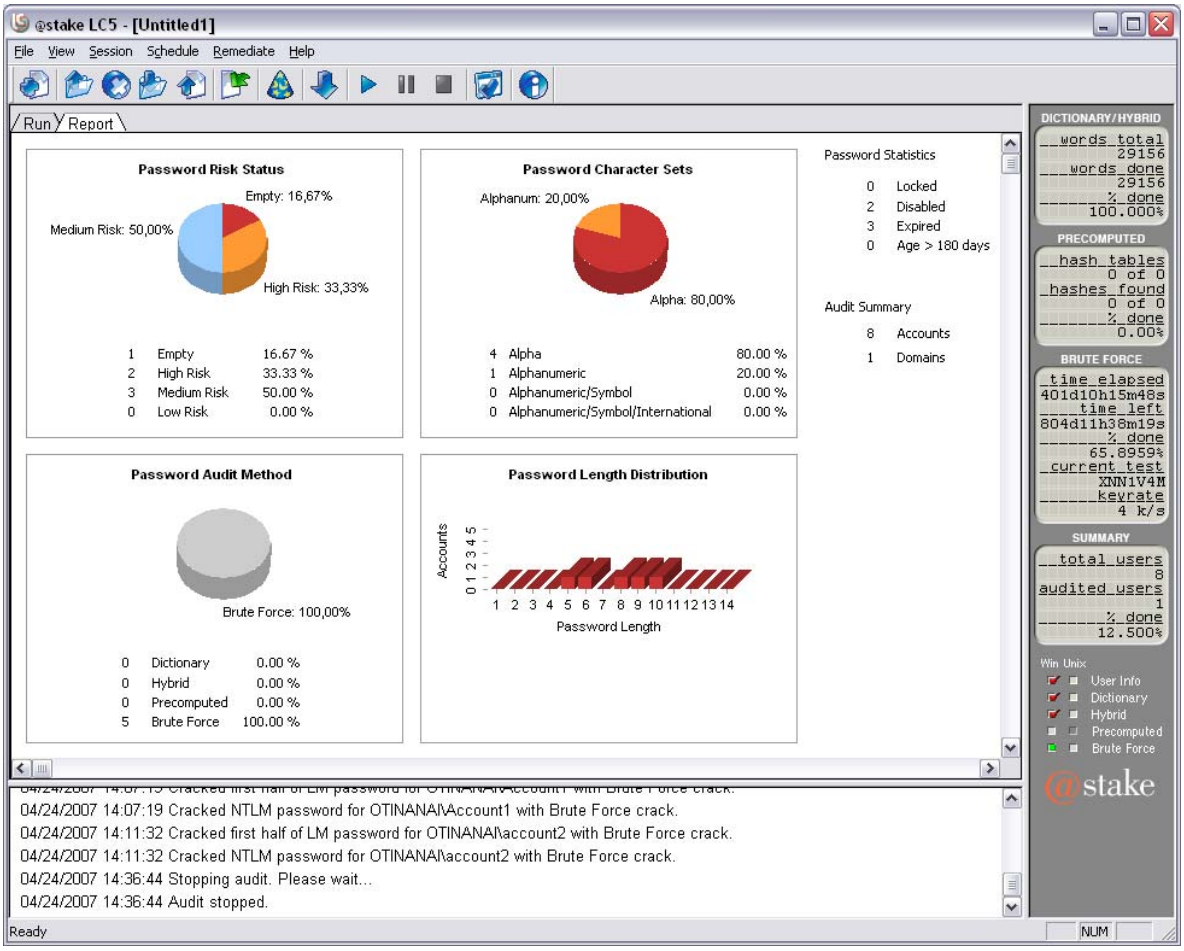
Και πιο αναλυτικά τα αποτελέσματα, στους τομείς που μας ενδιαφέρουν.

DOMAIN	**USERNAME**	**LANMAN PASSWORD**	**LESS THAN EIGHT**	**NTLM PASSWORD**	**LANMAN HAS**
OTINANAI-B0D879	Account1	1234KOSTAS		1234kostas	8F402E6F7F634436C0DD54996D50FB5D
OTINANAI-B0D879	account2	TEICRETE		τeicrete	A6DC59B1D2A0093017306D272A9441BB
OTINANAI-B0D879	Account3	STARCRAFT		StarCraft	B9AC99193D1831041FD352BDD2352014
OTINANAI-B0D879	Administrator	AXLADO	x	axlado	757CF155F2036FE7AAD3B435B51404EE
OTINANAI-B0D879	epp355	ADMIN	x	admin	F0D412BD764FFE81AAD3B435B51404EE
OTINANAI-B0D879	Guest	* empty *	x	* empty *	AAD3B435B51404EEAAD3B435B51404EE
OTINANAI-B0D879	HelpAssistant				B7231445F36D1417E6997D7B148A51EE

NTLM HASH	**CHALLENGE**	**PASSWORD AGE**	**CRACK TIME**	**CRACK METHOD**
F02F2F9705B8908DE6EC209EA9EA2F83		0	0d 1h 59m 17s	Brute Force
82FCCE78BB229E924E4C6C6232172576		0	0d 2h 3m 30s	Brute Force
D49101667E534E829B2C5B30C760CACF		0	0d 0h 10m 11s	Brute Force
AA19A4EE8D870AD07396C5156E33F742		0	0d 0h 3m 19s	Brute Force
209C6174DA490CAEB422F3FA5A7AE634		77	0d 0h 0m 38s	Brute Force
31D6CFE0D16AE931B73C59D7E0C089C0		77		
CFD23E7782EA9D470128E0246D1EE55B		141		

Βλέπουμε τα password, τα hashes, και όλες τις πληροφορίες που χρειαζόμαστε.

Τέλος να πούμε ότι το LC5 δημιουργεί και σχηματικές παραστάσεις των αποτελεσμάτων και των μεθόδων.



Βλέπουμε τα σχήματα που μας δείχνουν τον βαθμό δυσκολίας των password, τι χαρακτήρες χρησιμοποιούν, την μέθοδο με την οποία έσπασαν, και την κατανομή μεγέθους.

Παρατηρήσεις και Προτάσεις

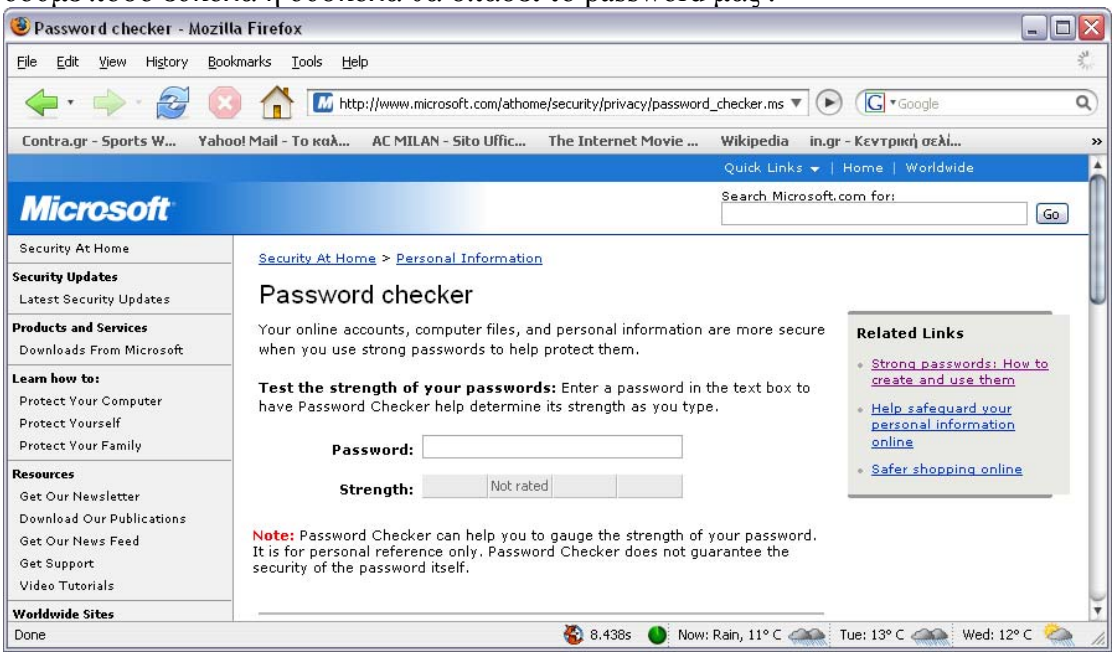
Τα συμπεράσματα που προκύπτουν είναι ότι τα password δεν πρέπει να είναι μικρά, κοινά ή system default, ακόμα πρέπει να αποφεύγονται αυτά που είναι λέξεις, ονόματα η παραλλαγές αυτών, τέλος εύκολα σπάνε στοιχεία από την προσωπική ζωή του χρήστη, όπως γενέθλια, ονόματα κατοικίδιων κ.α.

Παραδείγματα αδύναμων password:

* admin
* 1234
* susan
* password
* p@ssw0rd
* rover
* 12/3/75
* December12'.
* nbusr123
* asdf

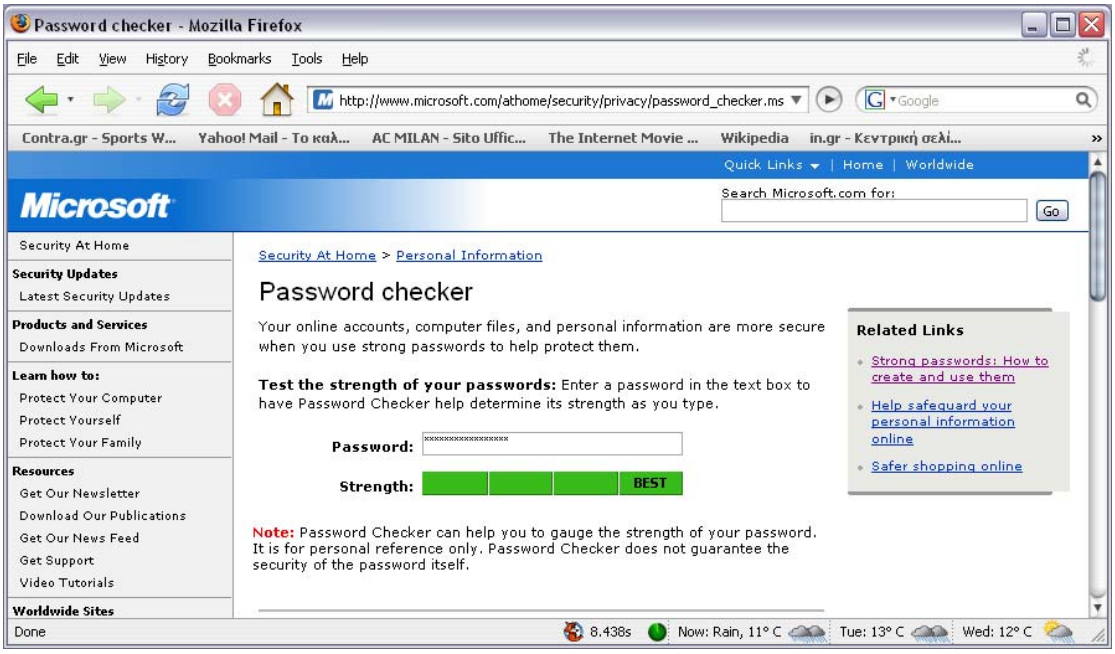
Οπότε τα password πρέπει να είναι μεγάλα, να περιέχουν νούμερα και χαρακτήρες και να μην μπορεί κάποιος να τα μαντέψει. Επίσης πρέπει να περιέχουν και κεφαλαία και μικρά.
Ορίστε μερικά παραδείγματα:
* t3wahSetyeT4
* 4pRte!ai@3
* #3kLfN2x
* MoOoOfIn245679
* Convert_100£ to Euros!

Όπως βλέπουμε από το τελευταίο παράδειγμα μπορούν να είναι και προτάσεις που είναι μεγάλες, μπορείς να τις θυμάσαι και περιέχουν διάφορους χαρακτήρες, επίσης μπορεί να χρησιμοποιηθεί ένας passwordchecker
http://www.microsoft.com/athome/security/privacy/password_checker.mspx ώστε να δούμε πόσο εύκολα ή δύσκολα θα σπάσει το password μας .



Απλά βάζουμε το password,

Και βλέπουμε τα αποτελέσματα,



Ακόμα τα password πρέπει να αλλάζουν σε τακτά χρονικά διαστήματα και να είναι αυστηρώς προσωπικά, τέλος όταν κάποιος σταματάει να εργάζεται ή κάνει κάποιο διάλλειμα, πρέπει οπωσδήποτε να κάνει log off ή lock στο σύστημα στο οποίο εργάζεται. Όταν κάποιος απομακρύνεται από την εταιρία ή τον οργανισμό πρέπει να αλλαχθούν όλα τα password που γνωρίζει ώστε να αποφευχθούν δυσάρεστες εκπλήξεις .

Ο administrator πρέπει να φροντίσει να κλειδώσει ευαίσθητες περιοχές του συστήματος ώστε να εξασφαλίσει την ασφαλή λειτουργία, όπως να μην επιτρέπει να κάνουν install οι χρήστες προγράμματα χωρίς την άδεια του. Πρέπει να κλειδώσει το

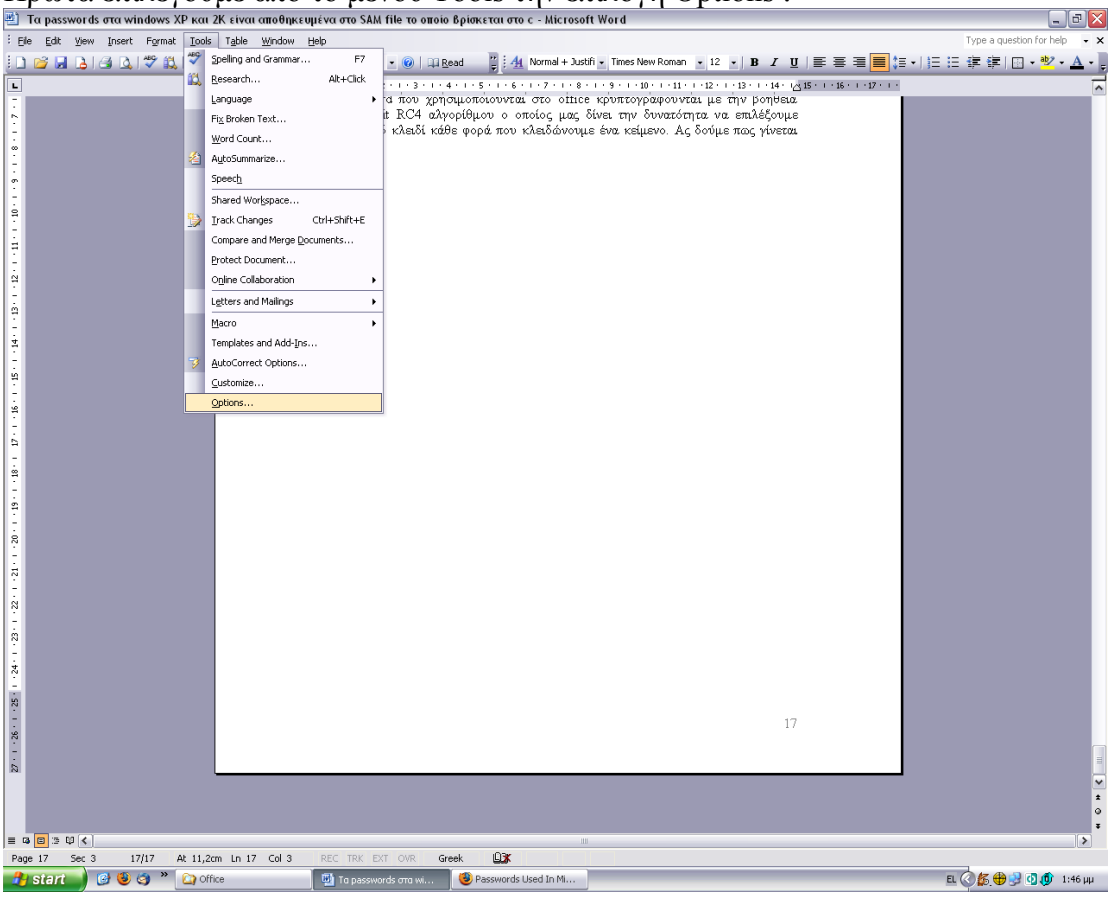
BIOS ώστε να αποφευχθούν αλλαγές στην boot sequence του συστήματος, και να ασφαλίσει το δίκτυο ώστε να μην γίνει προσπάθεια Snifing των κωδικών. Πρέπει να κρατάει logs από το ποιος χρησιμοποιεί τα συστήματα και πόσο χρόνο ώστε τυχόν ύποπτες κινήσεις να εντοπιστούν νωρίς. Να προστατεύεις με password το Screensaver, ώστε να μην υπάρχουν μηχανήματα ευάλωτα. Να αποφεύγεις γραφικά ή OpenGL screensaver που τρώνε μνήμη και χρησιμοποιούν πολύ την CPU, προτίμησε κενό ή το logo των windows, τέλος επέλεξε χρόνο ενεργοποίησης 5 λεπτά ή λιγότερο. Χρησιμοποίησε NTFS σε όλα τα partition γιατί υποστηρίζει file level security και κάποιος δεν μπορεί να χρησιμοποιήσει dos bootable floppys για να αποκτήσει πρόσβαση στο σύστημα σου. Τέλος απενεργοποίησε την δυνατότητα να κάνει κάποιος boot ο δισκέτα ή CD-ROM, αν χρειαστεί βγάλε τις συσκευές από το σύστημα σου.

Office passwors

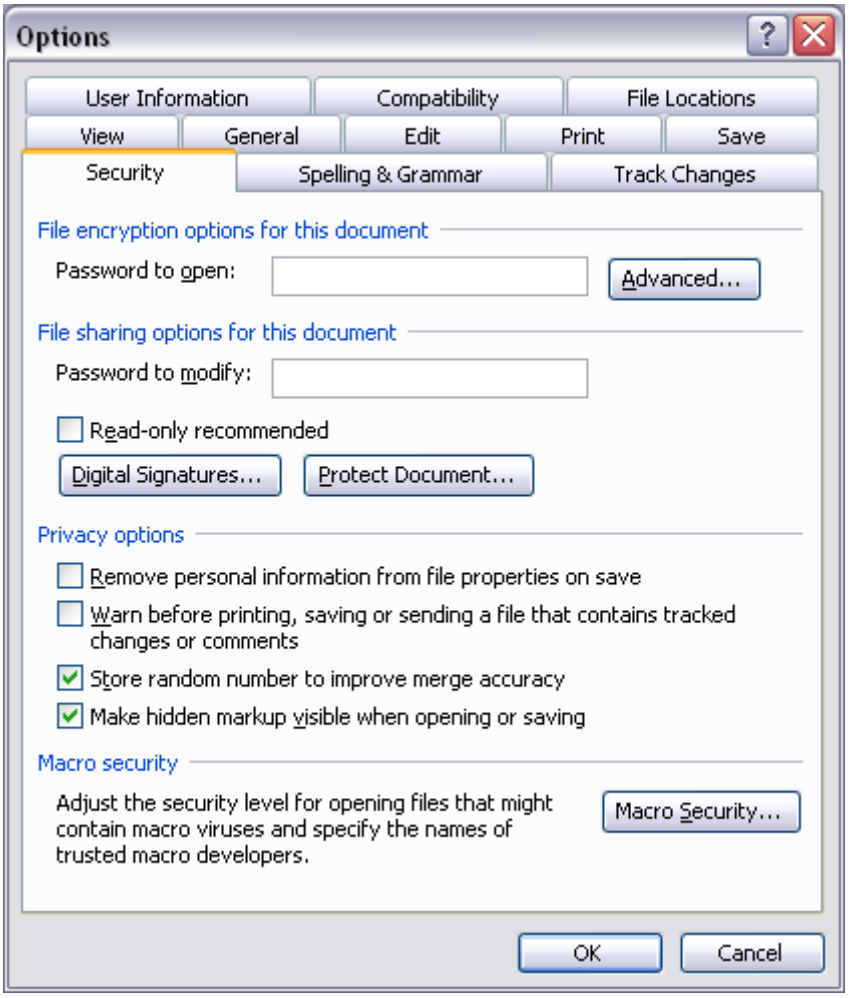
Passwords

Τα password που χρησιμοποιούνται στο office κρυπτογραφούνται με την βοήθεια ενός 128-bit RC4 αλγορίθμου ο οποίος μας δίνει την δυνατότητα να επιλέξουμε διαφορετικό κλειδί κάθε φορά που κλειδώνουμε ένα κείμενο. Αυτά που θα πούμε ισχύουν για το Word, το Excel και το PowerPoint ,εμείς θα χρησιμοποιήσουμε σαν παράδειγμα το Word. Ας δούμε πως γίνεται αυτό:

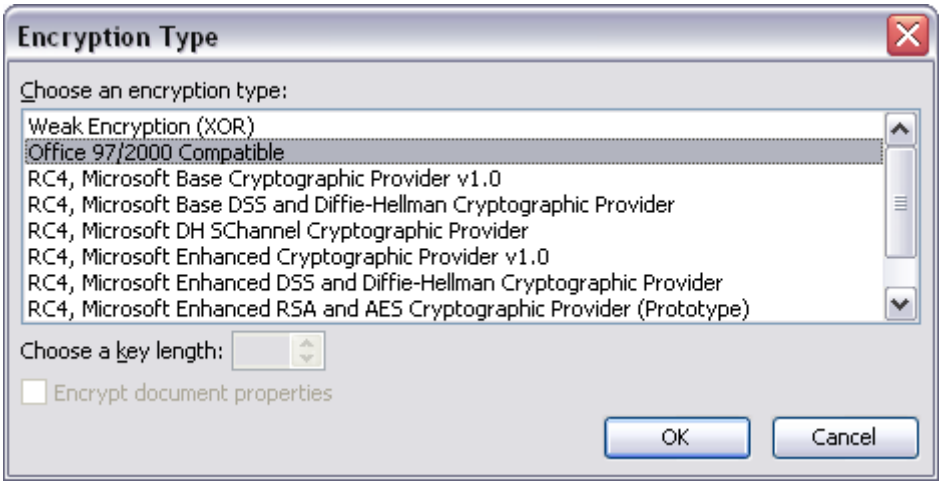
Πρώτα επιλέγουμε από το μενού Tools την επιλογή Options .



Στην συνέχεια επιλέγουμε στο παράθυρο που εμφανίζεται το tab Security.



Βλέπουμε ότι έχουμε την δυνατότητα να βάλουμε password ώστε να μην μπορεί κάποιος να ανοίξει το κείμενο (Password to open) ή να μην μπορεί να κάνει edit (Password to modify) αλλά το δεύτερο είναι πολύ εύκολο να σπάσει γιατί βασίζεται σε μια απλή μέθοδο κρυπτογράφησης. Το πρώτο όμως είναι δύσκολο γιατί μέσω της επιλογής Advanced μπορούμε να επιλέξουμε το κλειδί που θέλουμε.



Το πόσο δύσκολο είναι να σπάσει ένα password του office εξαρτάται κυρίως από το μέγεθος του, ένα μικρό σπάει γρήγορα , αντίθετα ένα μεγάλο θα πάρει χρόνο. Όμως ο

RC4 αν και ευρέως διαδεδομένος σε δημοφιλή προτώκολλα όπως τα Secure Sockets Layer (SSL) και WEP (to secure wireless networks) και ενώ είναι εντυπωσιακός στην απλότητα του δεν ικανοποιεί πια τα ψηλά στάνταρ που έχουν θέσει οι κρυπτογράφοι και έτσι η χρήση του μπορεί να οδηγήσει σε ανασφαλή κρυπτοσυστήματα

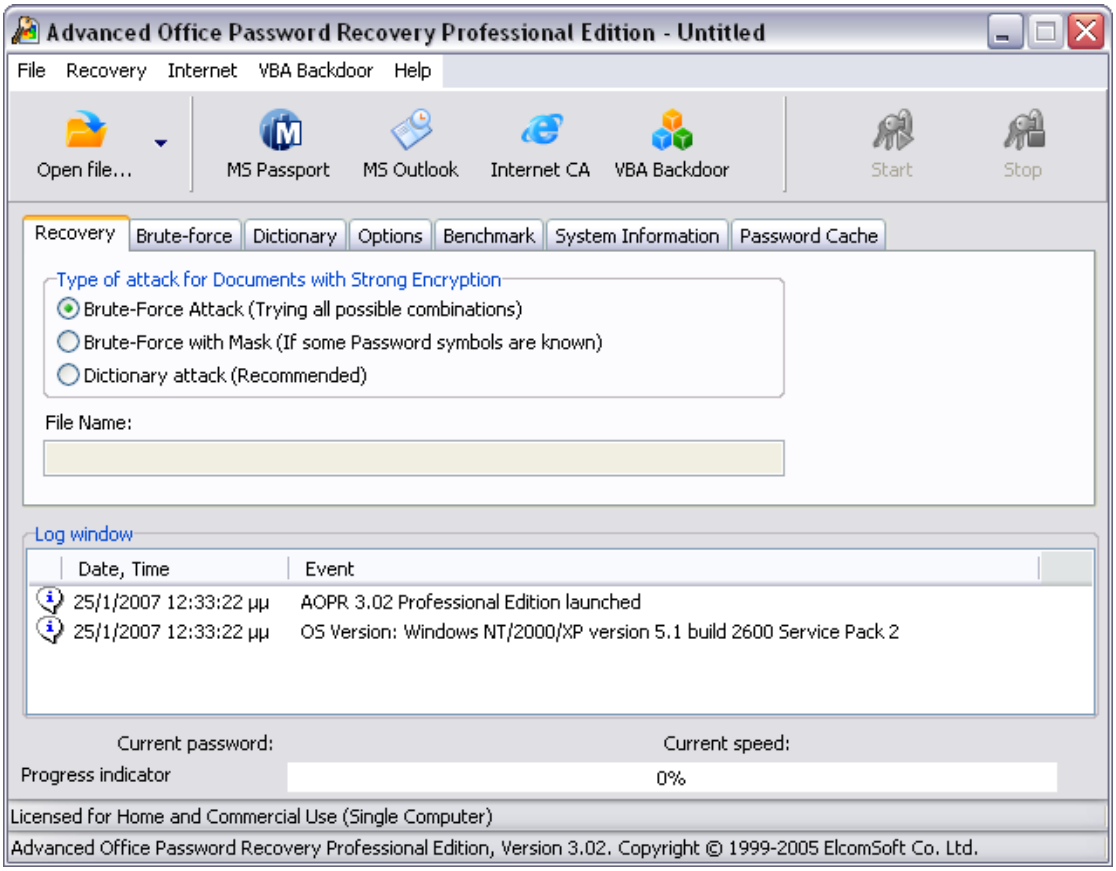
Εμείς παρακάτω θα εξετάσουμε μερικά εργαλεία ώστε να πάρουμε μια ιδέα το πώς λειτουργούν και πόσο χρόνο χρειάζονται για να σπάσουν.

Cracking

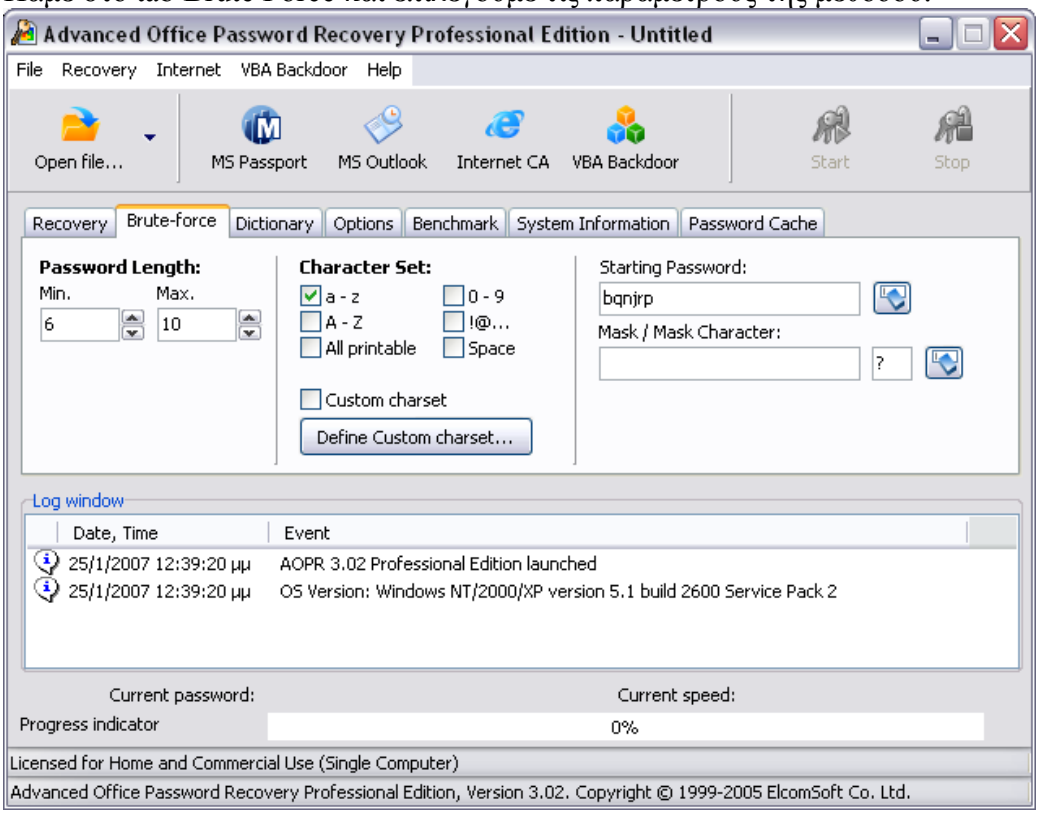
Κλειδώνουμε ένα αρχείο Word με το password axladof και με κλειδί RC4, Microsoft Base Cryptographic Provider v1.0 .

Πρώτα θα χρησιμοποιήσουμε το Advanced Office Password Recovery της Elcosoft το οποίο μπορεί κάποιος να το κατεβάσει από το http://www.freedownloadscenter.com/ ή από το site της εταιρίας www.**elcosoft**.com/. Δεν είναι δωρεάν αλλά με ένα μικρό αντίτιμο μπορείς να εκμεταλλευτείς όλες τις δυνατότητες του. Το εγκαθιστούμε ακολουθώντας τα βήματα του wizard και είμαστε έτοιμοι.

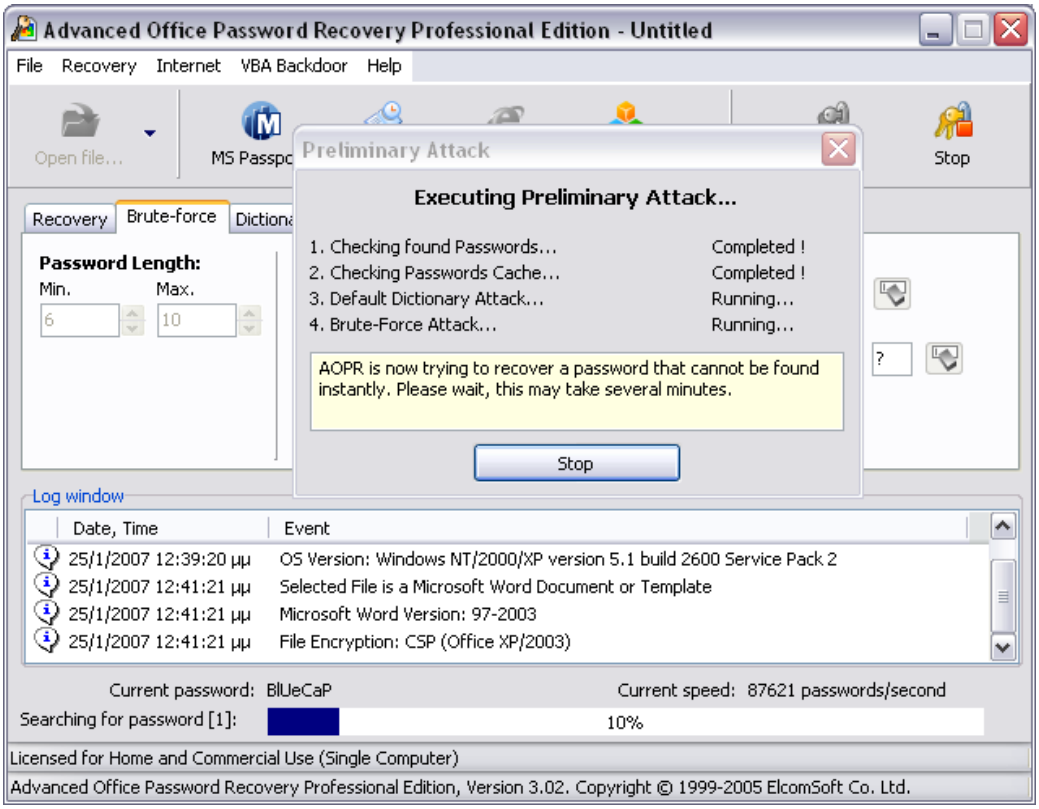
Στην αρχική οθόνη επιλέγουμε μπορούμε να επιλέξουμε τα settings της μεθόδου που θέλουμε να ακολουθήσουμε στα tabs που υπάρχουν .



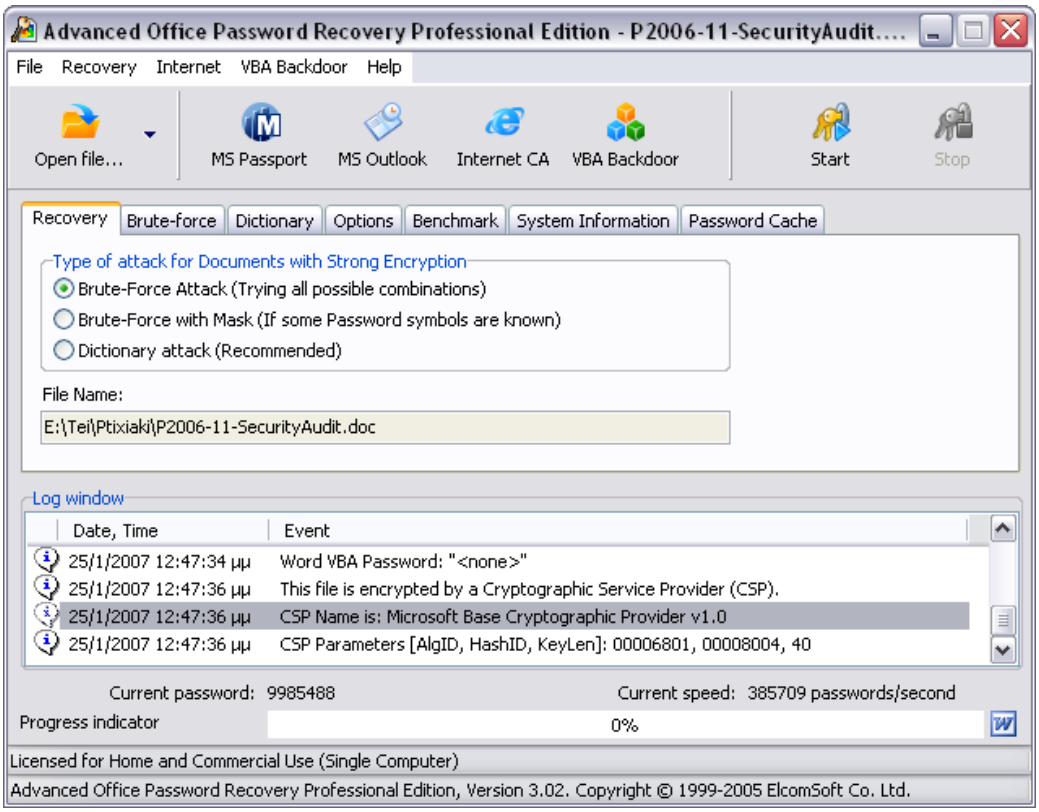
Πάμε στο tab Brute Force και επιλέγουμε τις παραμέτρους της μεθόδου.



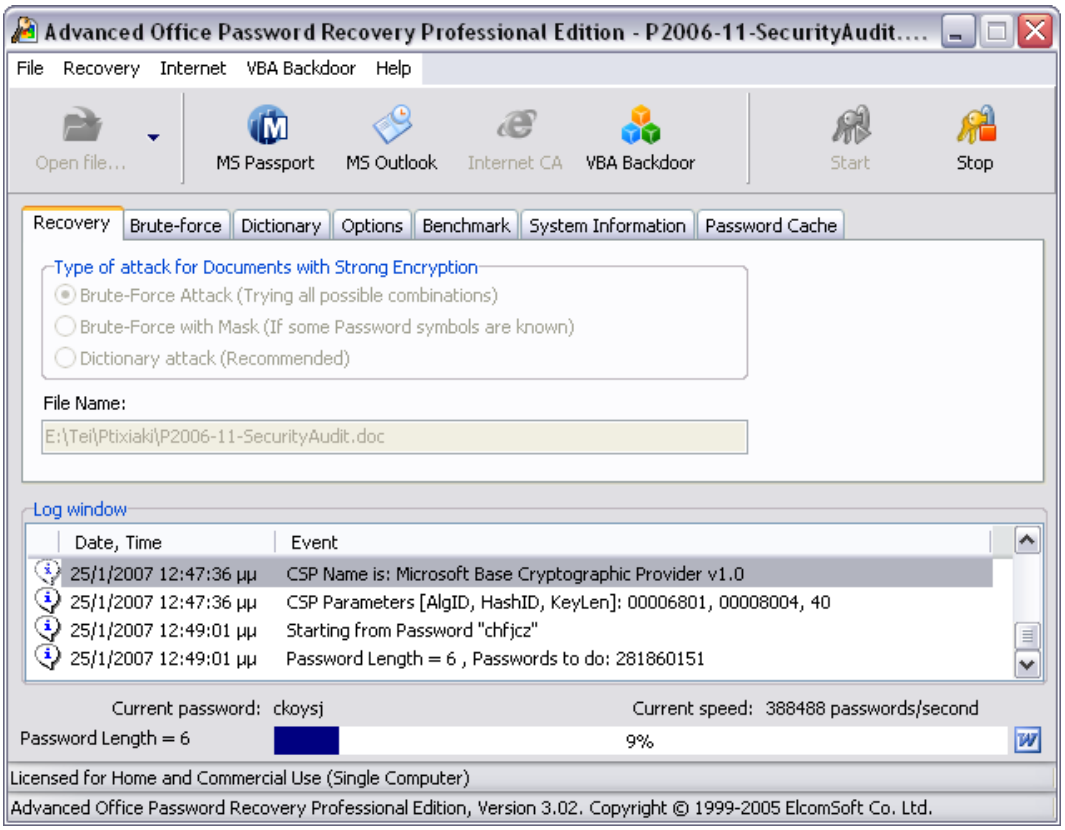
Στην συνέχεια επιλέγουμε το Open file και βρίσκουμε το αρχείο που μας ενδιαφέρει, και αμέσως ξεκινάει η διαδικασία σπασίματος.



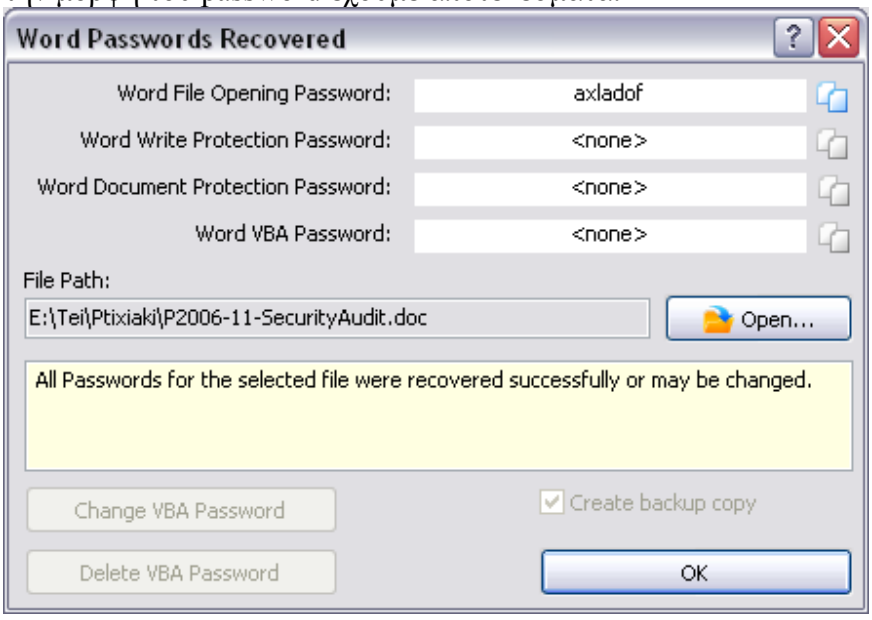
Παρατηρούμε ότι βρήκε ποιο Word είναι και με τη παραλλαγή του RC4 το κλειδώσαμε



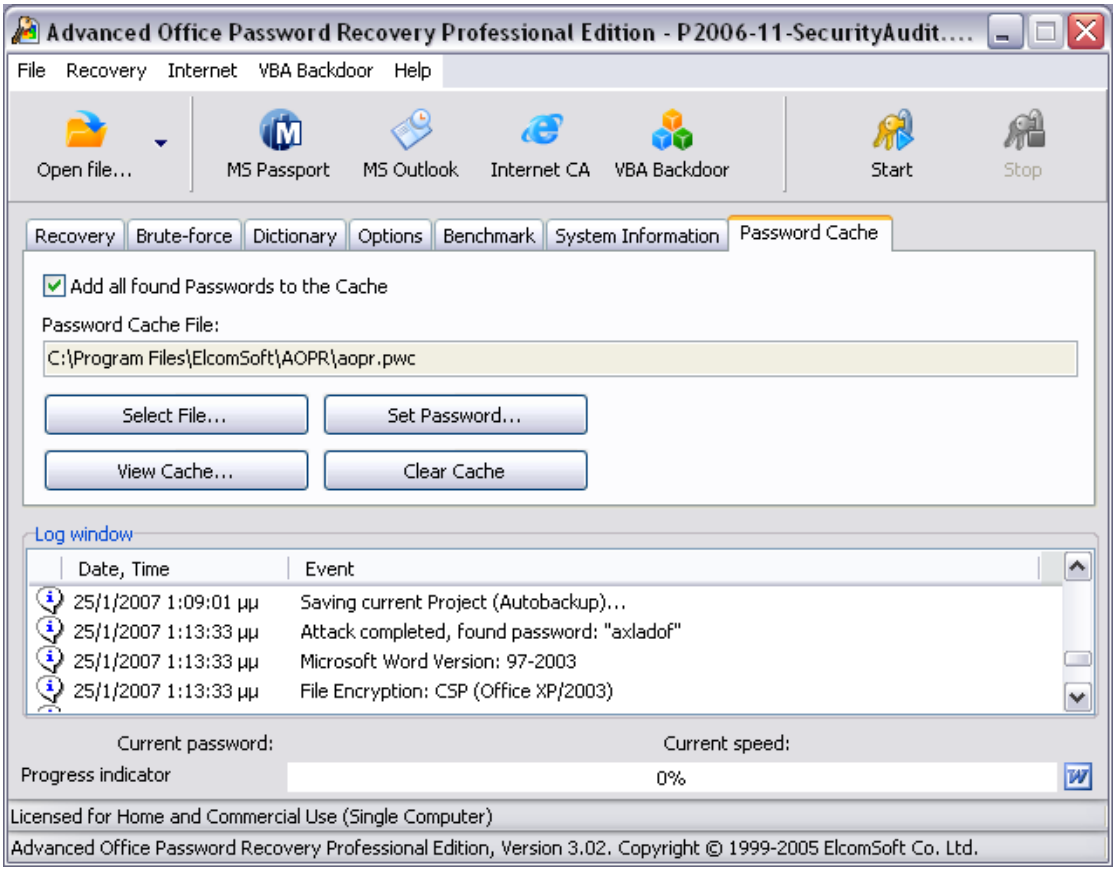
Στην συνέχεια εφόσον έχουμε επιλέξει τις παραμέτρους του Brute Force πατάμε το Start



Έπειτα από κάποιο χρονικό διάστημα το οποίο διαφέρει ανάλογα με το μέγεθος και την μορφή του password έχουμε αποτελέσματα.

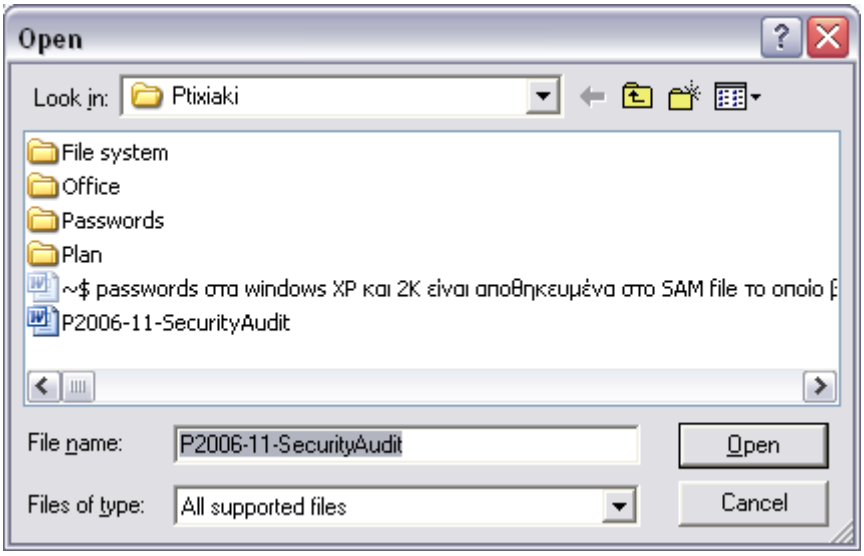


Και το εργαλείο αυτό μας δίνει την δυνατότητα να αποθηκεύσουμε το password για μελλοντική χρήση .

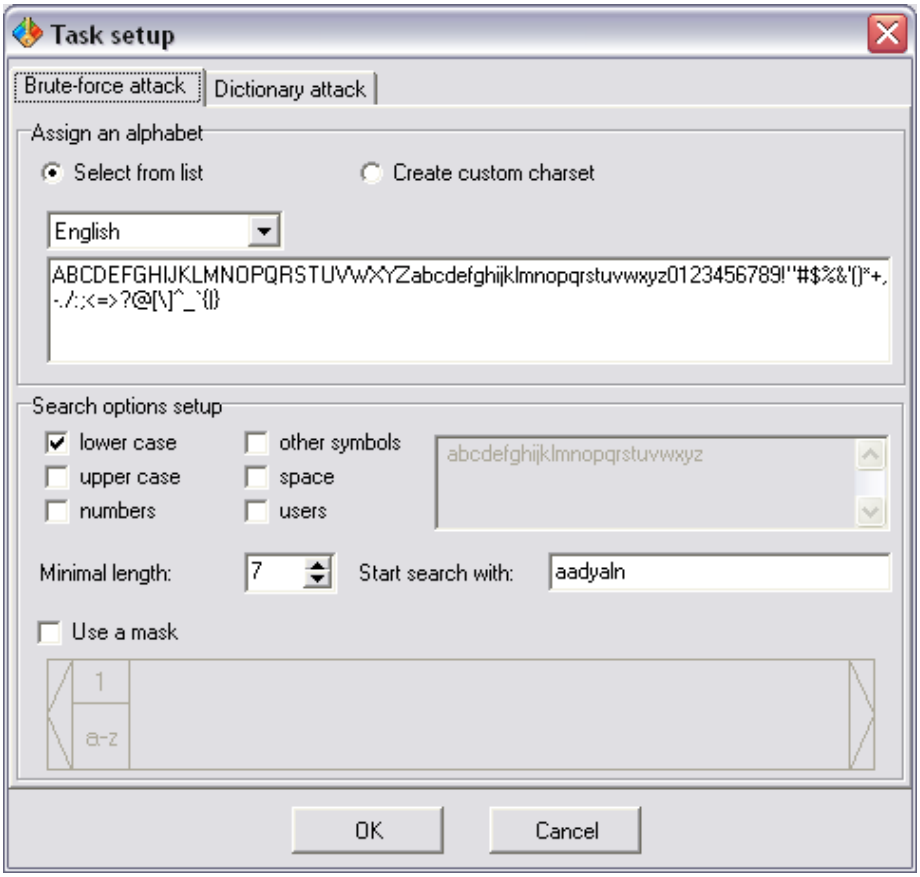


Ας εξετάσουμε τώρα άλλο ένα εργαλείο για την ίδια δουλειά, το Accent Office Password Recovery, το οποίο μπορούμε να κατεβάσουμε από το http://www.passwordrecoverytools.com/ ή το http://www.freedownloadscenter.com/ και αυτό δεν είναι δωρεάν αλλά πάλι το αντίτιμο είναι μικρό .
Ας το δούμε σε λειτουργία.

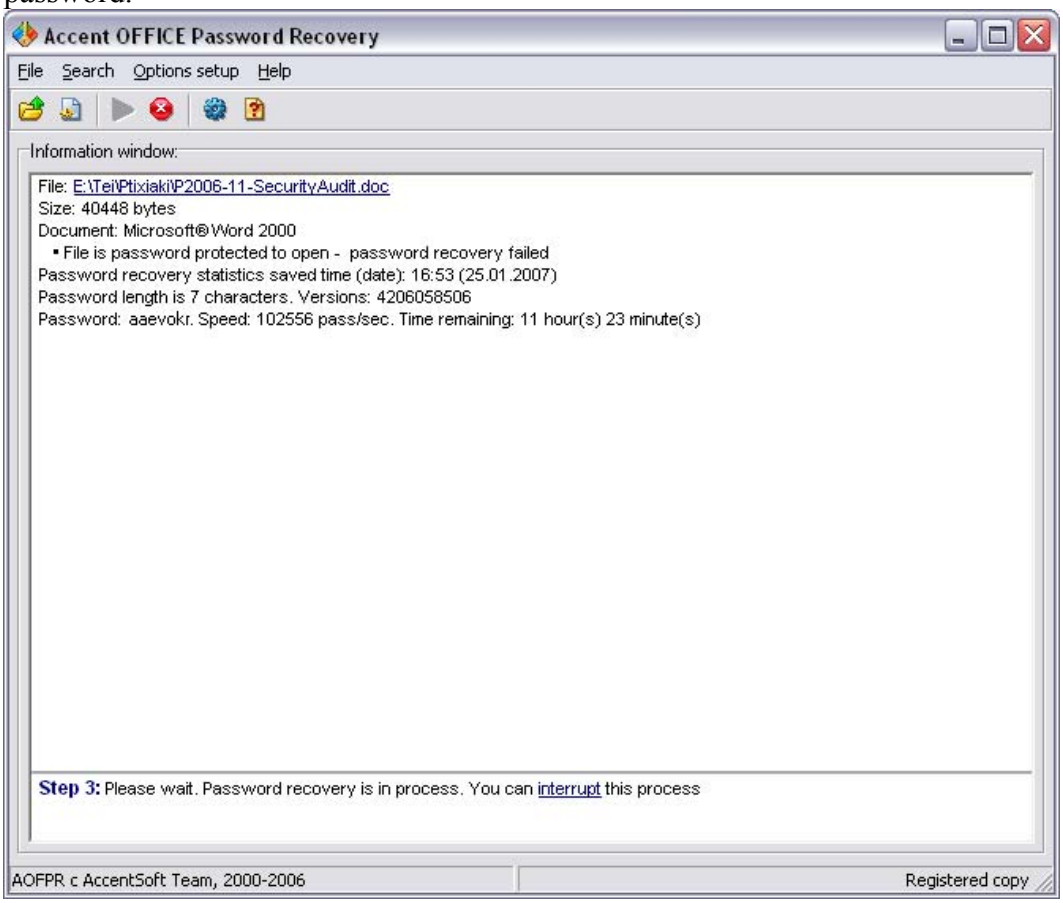
Επιλέγουμε το αρχείο που θέλουμε να ανοίξουμε από την επιλογή file.



Όταν επιλέξουμε το Start θα μας εμφανιστεί ένα παράθυρο με τις παραμέτρους της μεθόδου .



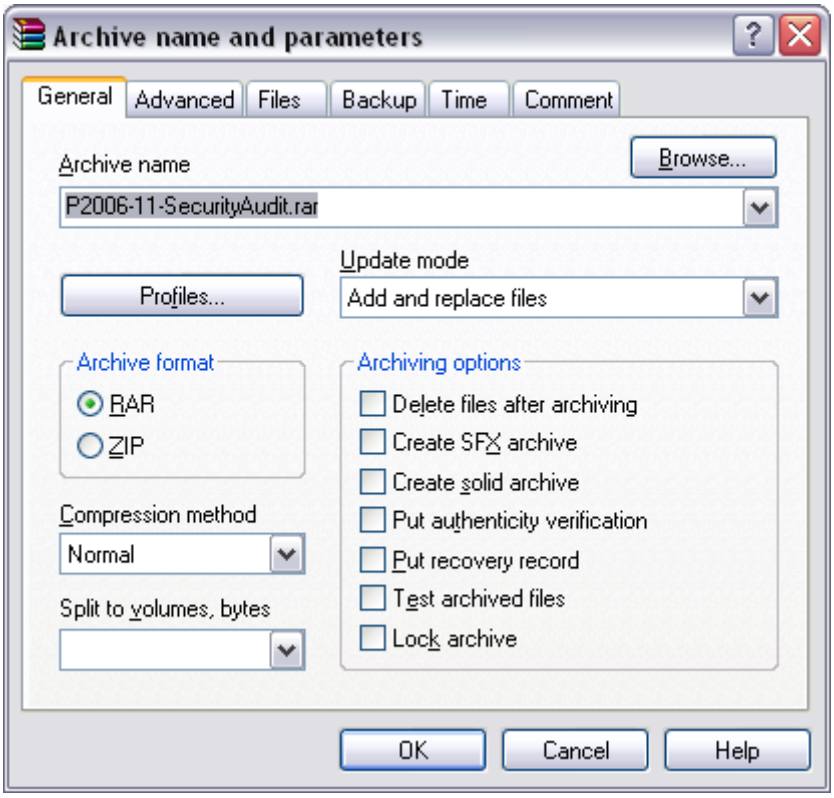
Αφού κάνουμε τις ρυθμίσεις πατάμε OK και ξεκινάει η διαδικασία ανεύρεσης του password.



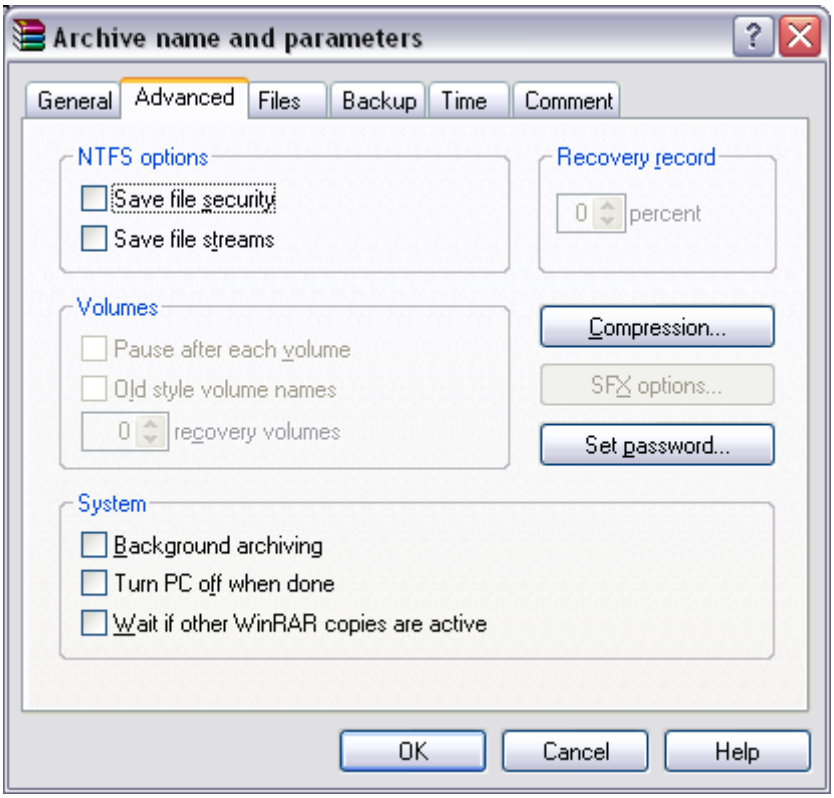
Όμως αυτό το εργαλείο κάνει πολύ περισσότερο χρόνο για να βρει αποτέλεσμα σε σχέση με το προηγούμενο, ενώ το πρώτο για τον κωδικό 7 ψηφίων έκανε 1 ώρα και κάτι λεπτά το δεύτερο προέβλεπε 23 ώρες .Βεβαία υπάρχουν και άλλα εργαλεία τα οποία κάνουν την ίδια δουλειά, εμείς χρησιμοποιήσαμε αυτά γιατί είναι τα πιο διαδομένα .

Παρατηρήσεις και Προτάσεις

Βλέπουμε ότι και εδώ όσο αναφορά το πόσο δύσκολο είναι ένα password ισχύουν τα ίδια με όσα ισχύουν και στο password των windows. Μια λύση όμως που έχουμε εδώ είναι να κλειδώσουμε τα αρχεία μας με την βοήθεια κάποιου άλλου προγράμματος, όπως το WinRar ή το WinZip τα οποία έχουν καλύτερες μεθόδους κρυπτογράφησης και η διαδικασία σπασίματος τους είναι πολύ πιο χρονοβόρα. Για να το κάνουμε αυτό διαλέγουμε το αρχείο και πατάμε δεξί κλικ, στο μενού που εμφανίζεται επιλέγουμε Add to Archive και μας εμφανίζεται το εξής μενού .



Επιλέγουμε το tab Advanced και βρίσκουμε την επιλογή Set Password που θα μας επιτρέψει να κλειδώσουμε το αρχείο.



Αυτό το κάνουμε γιατί το WinRar χρησιμοποιεί τον αλγόριθμο AES 128-bit που είναι πολύ πιο σύγχρονος και ασφαλής από τον RC4 που χρησιμοποιεί το Office. Ο AES δημιουργήθηκε το 2002 και αποτελεί στάνταρ από το 2006, ενώ ο RC4 δημιουργήθηκε το 1960 και έχει ξεπεραστεί.

Ψηφιακές ταυτότητες και υπογραφές

Microsoft Outlook

Εισαγωγή

Το Microsoft Outlook είναι ένας μάνατζερ προσωπικών πληροφοριών από την Microsoft και είναι μέρος του Microsoft Office. Χρησιμοποιείται περισσότερο σαν εφαρμογή διαχείρισης e-mail, όμως διαθέτει και χρονοδιάγραμμα, εφαρμογές διαχείρισης γεγονότων και επαφών, δημιουργία σημειώσεων και ημερολόγιο. Μπορεί να χρησιμοποιηθεί σαν stand-alone εφαρμογή, αλλά μπορεί να λειτουργήσει και σε συνεργασία με το Microsoft Exchange Server ώστε να προσφέρει διευρυμένες υπηρεσίες σε πολλαπλούς χρήστες σε έναν οργανισμό, όπως κοινά mailboxes και χρονοδιαγράμματα , δημόσιους φακέλους και ώρες συναντήσεων.

Ακολουθεί ένα πινακάκι με τις εκδόσεις του Microsoft Outlook

Outlook for MS-DOS	Μαζί με τον Exchange Server 5.5
Outlook for Macintosh	Μαζί με τον Exchange Server 5.5
Outlook 97	Κυκλοφόρησε Ιανουάριος 16, 1997, Επίσης μαζί με τον Exchange Server 5.5
Outlook 98	Κυκλοφόρησε Ιούνιος 21, 1998
Outlook 2000 or "Outlook 9"	Κυκλοφόρησε Ιούλιος 7, 1999
Outlook 2002 or "Outlook 10" or "Outlook XP"	Κυκλοφόρησε Μάιος 31, 2001
Office Outlook 2003 or "Outlook 11"	Κυκλοφόρησε Οκτώβριος 21, 2003
Office Outlook 2007 or "Outlook 12"	Κυκλοφόρησε Νοέμβριος 30, 2006

Εμείς θα ασχοληθούμε με το Outlook 2003 που σε θέματα ασφάλειας, σύμφωνα με την Microsoft, ήταν ένα μεγάλο βήμα μπροστά.

Προβλήματα παλαιοτέρων εκδόσεων

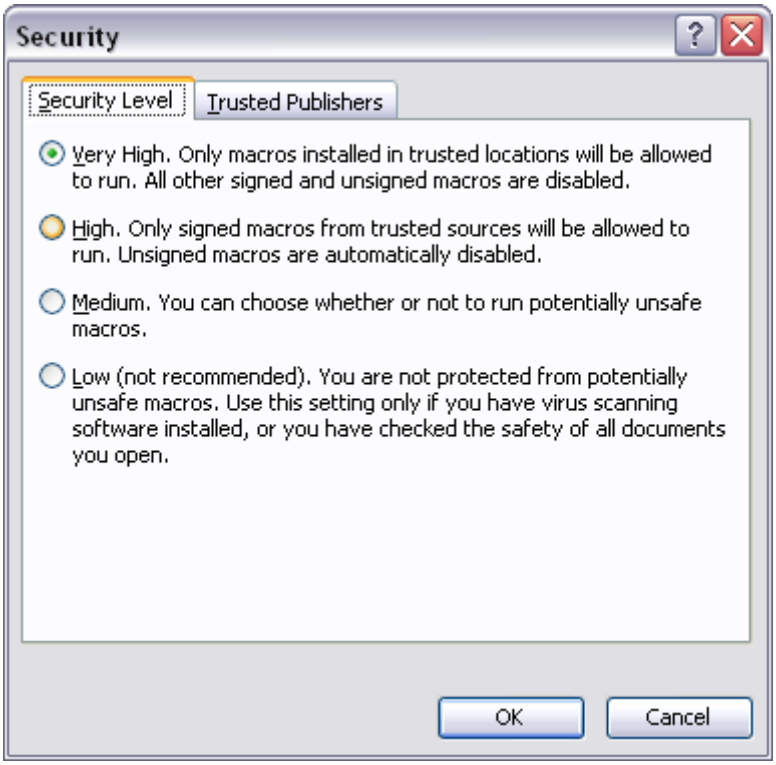
Ένα από τους στόχους της Microsoft για το πρόγραμμα διαχείρισης e-mail είναι η ευκολία στην χρήση. Όμως η εγκατεστημένη αυτοματοποίηση και η έλλειψη

προδιαγραφών ασφάλειας σε σχέση με τον ανταγωνισμό έχουν γίνει στόχοι εκμετάλλευσης από hackers μέσω ιών e-mail. Οι ιοί παίρνουν την μορφή ενός e-mail attachment που εκτελείται στον υπολογιστή στόχο, αναπαράγει τον εαυτό του και τον στέλνει σε όλες τις διευθύνσεις που βρίσκονται στην λίστα του χρήστη ή του Exchange Server. Παραδείγματα τέτοιων ιών είναι το Melisa και το Sobin Worms .Άλλα προγράμματα έχουν εκμεταλλευτεί τις HTML e-mail δυνατότητες του Outlook να εκτελεί κακοπροαίρετο κώδικα ή να δέχεται Spam-mail. Η ποικιλία των net-worms και άλλων ιών έχουν οδηγήσει στο συμπέρασμα ότι το Outlook είναι ένα πολύ ανασφαλές πρόγραμμα.

Ο προγραμματιστής Unix Bill Joy έχει δηλώσει ότι το Outlook είναι ανασφαλές λόγω του ότι έχει γραφτεί κυρίως σε C, κάνοντας εύκολο να γραφτούν προγράμματα που το εκμεταλλεύονται. Επίσης πίστευε ότι η εξάπλωση του Outlook είναι από τους κυριότερους λόγους που οδήγησε στην εξάπλωση του Spam

Outlook 2003

Ας εξετάσουμε τώρα τις προδιαγραφές ασφάλειας του Outlook 2003. Πρώτα από όλα στις προηγούμενες εκδόσεις έπρεπε οι χρήστες να θέσουν τις παραμέτρους στο επίπεδο ασφάλειας για να πετύχουν την μέγιστη δυνατή ασφάλεια, ενώ τώρα οι παράμετροι είναι σεταρισμένοι για την υψηλότερη δυνατή ασφάλεια by default. Το Outlook 2003 μας δίνει την δυνατότητα να απενεργοποιήσουμε τα Macros (Κώδικας κρυμμένος μέσα σε ένα κείμενο ή e-mail που μπορεί να περιέχει ένα ιό). Κάθε μη αναγνωρίσιμο macros δεν θα τρέξει αυτόματα, άσχετα με το αν ο χρήστης έχει επιλέξει να τα μπλοκάρει.



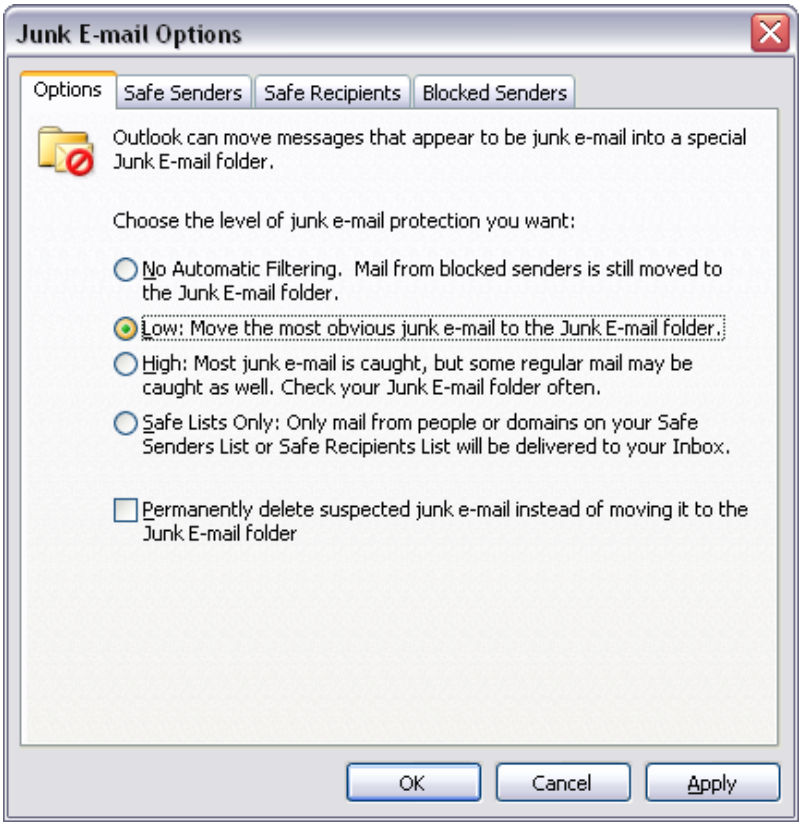
Αν το Outlook 2003 τρέχει σε μηχάνημα με Windows XP, οι χρήστες ή οι administrator μπορούν να στήσουν μια λίστα από ασφαλείς εκδότες (Trusted publishers). Macros ή εκτελέσιμα αρχεία που δεν προέρχονται από αυτές τι πηγές δεν θα εκτελούνται.

Το Outlook 2003 έχει και αναβαθμισμένη ασφάλεια όσο αναφορά την προστασία των προσωπικών δεδομένων κυρίως λόγω του antispam φίλτρου του και των δυνατοτήτων προστασίας από ιούς. Δίνει στον χρήστη την δυνατότητα να μπλοκάρει τα e-mailed HTML δεδομένα, πράγμα το οποίο φέρνει σε ένα τέλος τα animated junk mail που περιέχουν φωτεινούς τίτλους, προϊόντα που χορεύουν κτλ .

Ακόμα το να μπλοκάρεις το HTML επίσης σε προστατεύει από Web ιούς, μικρά γραφικά που περιέχουν κώδικα που μπορεί να μπει σ ένα e-mail επιτρέποντας σε τρίτους να συλλέγουν προσωπικές πληροφορίες όταν κάποιος ανοίξει το μήνυμα.

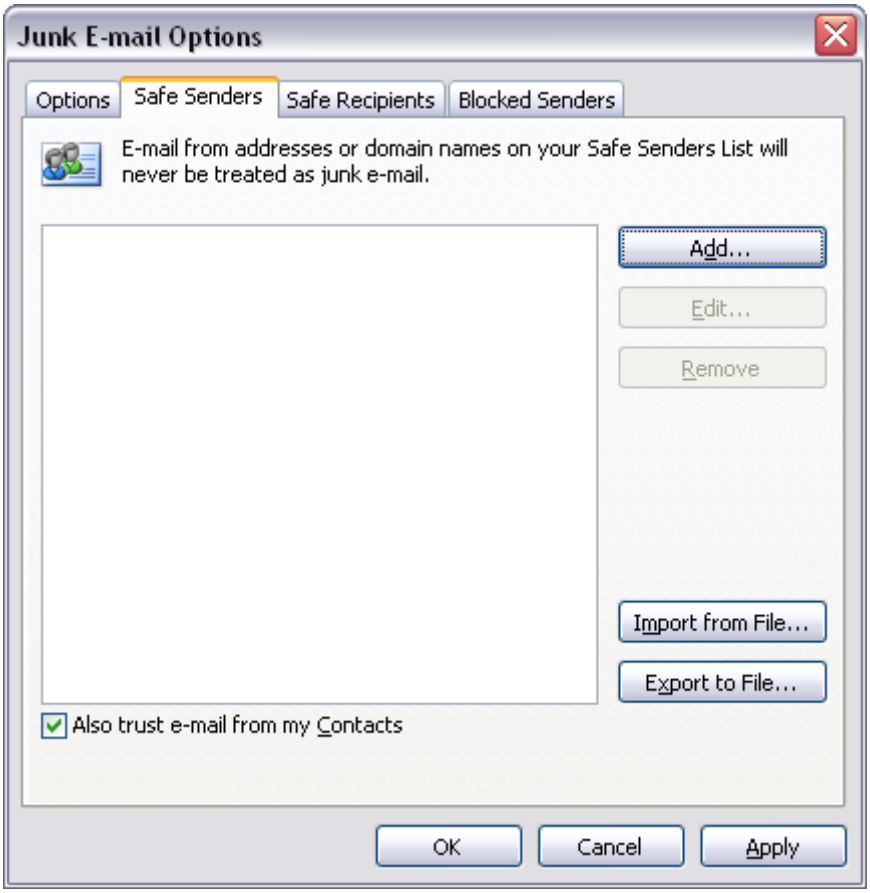
Η πιο σημαντική αναβάθμιση στο Outlook 2003 είναι το junk mail φίλτρο του. Αυτό χρησιμοποιεί την Microsoft SmartScreen Technology η οποία είναι βασισμένη σε μια machine-learning Bayesian technology δηλαδή μια μηχανή που παίρνει αποφάσεις, μια απλή μορφή τεχνίτης νοημοσύνης, που μαθαίνει τον εαυτό της να αναγνωρίζει τα junk mail. Λαμβάνει υπόψη του παράγοντες όπως την ώρα αποστολής και τα περιεχόμενα και την δομή του μηνύματος. Επίσης το φίλτρο μαθαίνει να ξεχωρίζει τα spam βασισμένο στο ποια ξεχωρίζει ο χρήστης σαν junk στα εισερχόμενα και ποια μηνύματα που θεωρεί κανονικά καταλήξανε στον φάκελο junk-mail κατά λάθος.

Παρακάτω βλέπουμε το παράθυρο επιλογών επιπέδου ασφάλειας του φίλτρου.

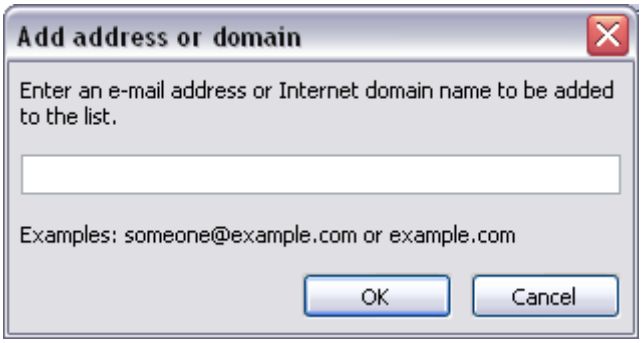


Παρατηρούμε τις επιλογές επιπέδου και τα tabs μέσω των οποίων μπορούμε να προσθέσουμε ποιους θεωρούμε ασφαλείς αποστολείς και ποιους ανασφαλείς.

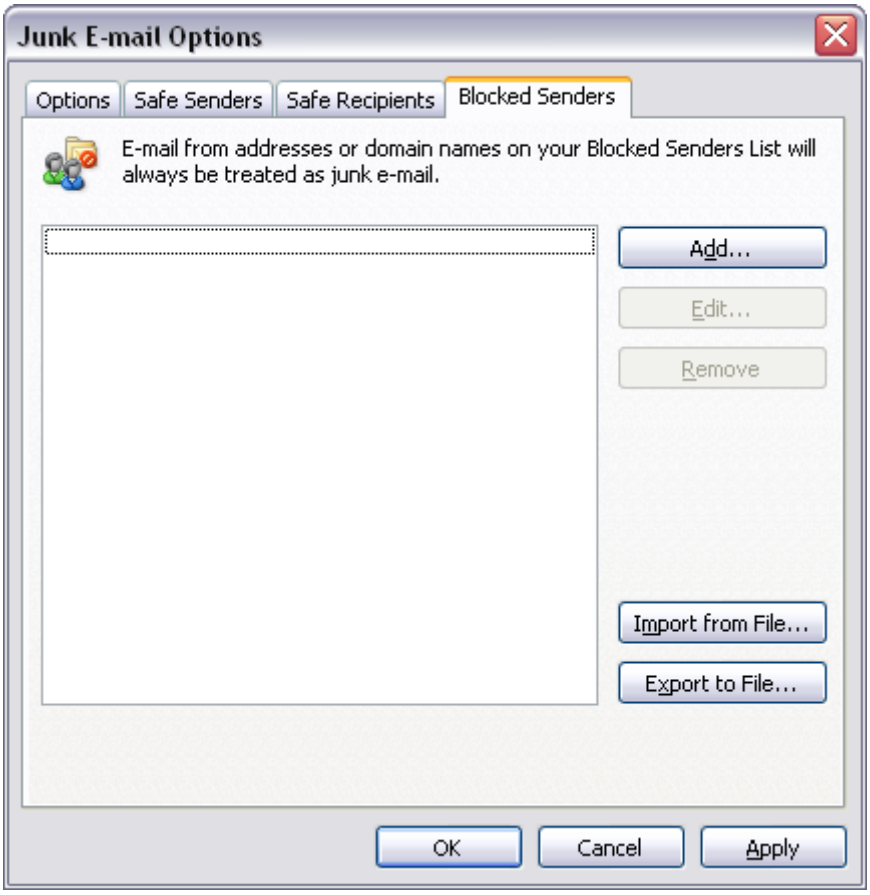
Επιλέγουμε Safe Senders για να δούμε την λίστα των ασφαλών .

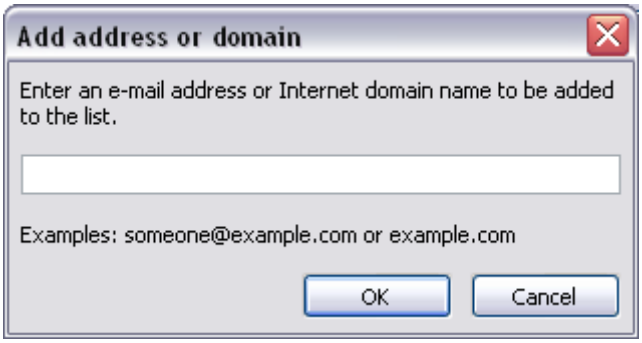


Και επιλέγοντας Add προσθέτουμε και άλλους



Αντίστοιχα στο tab Blocked Senders βάζουμε πηγές που δεν εμπιστευόμαστε , και πάλι επιλέγοντας την επιλογή Add μπορούμε να προσθέσουμε και άλλους.





Σε ένα τεστ μιας εβδομάδας του νέου φίλτρου, ρυθμισμένο σε ένα μέσο επίπεδο ασφάλειας , η δυνατότητα του Outlook 2003 να αναγνωρίζει και να μπλοκάρει junk e-mail έχει βελτιωθεί πάρα πολύ σε σχέση με το Outlook 2002. Κατάφερε να μπλοκάρει το 85% του Spam μιας μέρας σε σχέση με το 65% του Outlook 2002.\

Ψηφιακές Ταυτότητες

Εισαγωγή

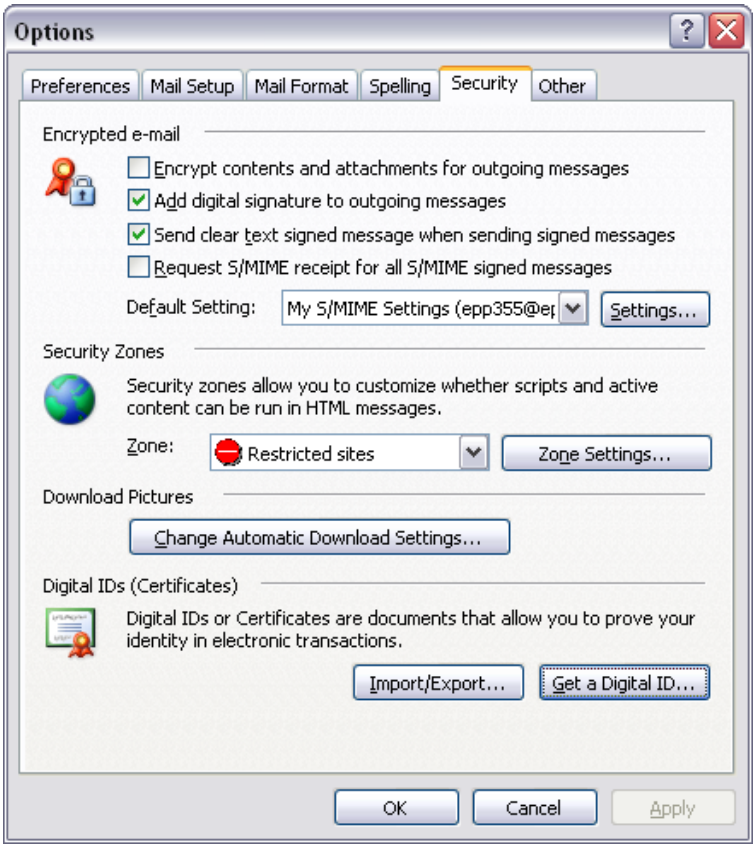
Στην κρυπτογραφία η ψηφιακή υπογραφή είναι μια μορφή ασύμμετρης κρυπτογραφίας που χρησιμοποιείται για να εξομοιώσει την ασφάλεια μιας υπογραφής. Οι διαδικασίες ψηφιακών υπογραφών συνήθως δίνουν δύο αλγόριθμους, ένα για υπογραφή (χρησιμοποιεί το κρυφό προσωπικό κλειδί του χρήστη) και ένα για επιβεβαίωση των υπογραφών (χρησιμοποιεί το δημόσιο κλειδί). Το αποτέλεσμα της διαδικασίας υπογραφής επίσης λέγεται ψηφιακή υπογραφή.

Οι ψηφιακές υπογραφές, όπως και οι γραπτές, χρησιμοποιούνται για να δώσουν αυθεντικότητα του μηνύματος. Το μήνυμα μπορεί να είναι οτιδήποτε, από e-mail έως ένας σύνδεσμος, ή απλά ένα μήνυμα σταλμένο σε μια πιο περίπλοκη κρυπτογραφική μορφή. Οι ψηφιακές υπογραφές χρησιμοποιούνται για να δημιουργήσουμε υποδομές δημοσίου κλειδιού (public key infrastructure (PKI)) στις οποίες το δημόσιο κλειδί ενός χρήστη (Για χρήσεις όπως public-key encryption, ψηφιακές υπογραφές, ή οποιαδήποτε άλλη) σχετίζεται με τον χρήστη μέσω ενός πιστοποιητικού ψηφιακής ταυτότητας που εκδίδεται από μια αρχή (certificate authority). Ο στόχος των υποδομών PKI είναι να δέσουν τις πληροφορίες για τον χρήστη στο δημόσιο κλειδί, έτσι ώστε αυτό να μπορεί να χρησιμοποιηθεί σαν μια μορφή αναγνώρισης.

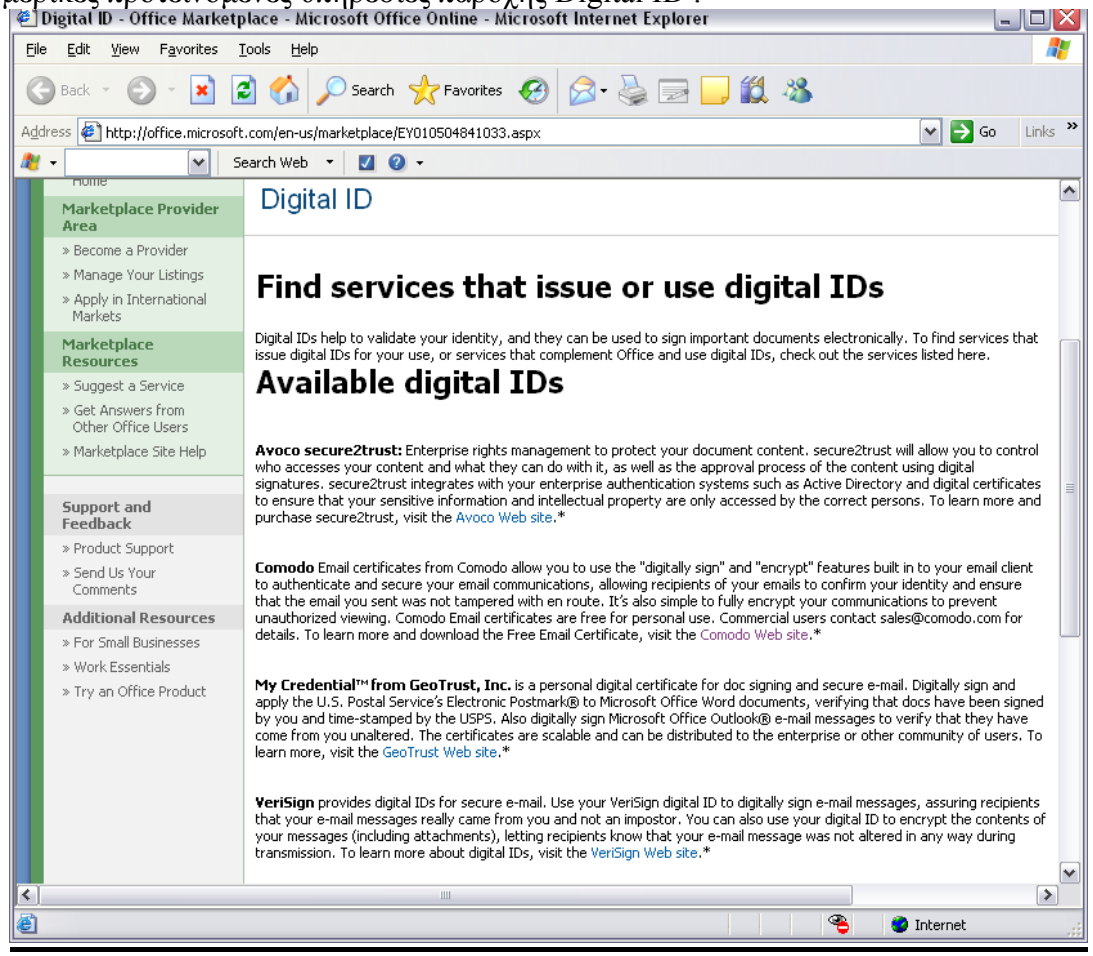
Οι ψηφιακές υπογραφές είναι ένα είδος ηλεκτρονικής υπογραφής, ενός πιο διευρυμένου όρου που καλύπτει όλες τις μορφές ηλεκτρονικών δεδομένων που χρησιμοποιούνται από το internet σαν υπογραφές, αλλά δεν είναι όλες οι ηλεκτρονικές υπογραφές και ψηφιακές υπογραφές. Σε κάποιες χώρες, συμπεριλαμβανομένων των Ηνωμένων Πολιτειών και της Ευρωπαϊκής Ένωσης, οι ηλεκτρονικές υπογραφές έχουν νομική υπόσταση .

Digital ID στο Outlook

Στο outlook στο μενού Tools επιλέγουμε το Options έπειτα στο παράθυρο που ανοίγει επιλέγουμε το Tab Security, στο οποίο βλέπουμε την επιλογή ‘Add digital signature to outgoing message’ και το ‘Encrypt contents and attachments for outgoing messages’. Για να μπορέσουμε να χρησιμοποιήσουμε το πρώτο πρέπει να έχουμε αποκτήσει ψηφιακή ταυτότητα ενώ για το δεύτερο πρέπει να έχει και ο παραλήπτης για να μπορέσει να αποκρυπτογραφήσει το μήνυμα. Για να αποκτήσουμε ψηφιακή ταυτότητα κάνουμε κλίκ στο κουμπί Get a Digital ID.

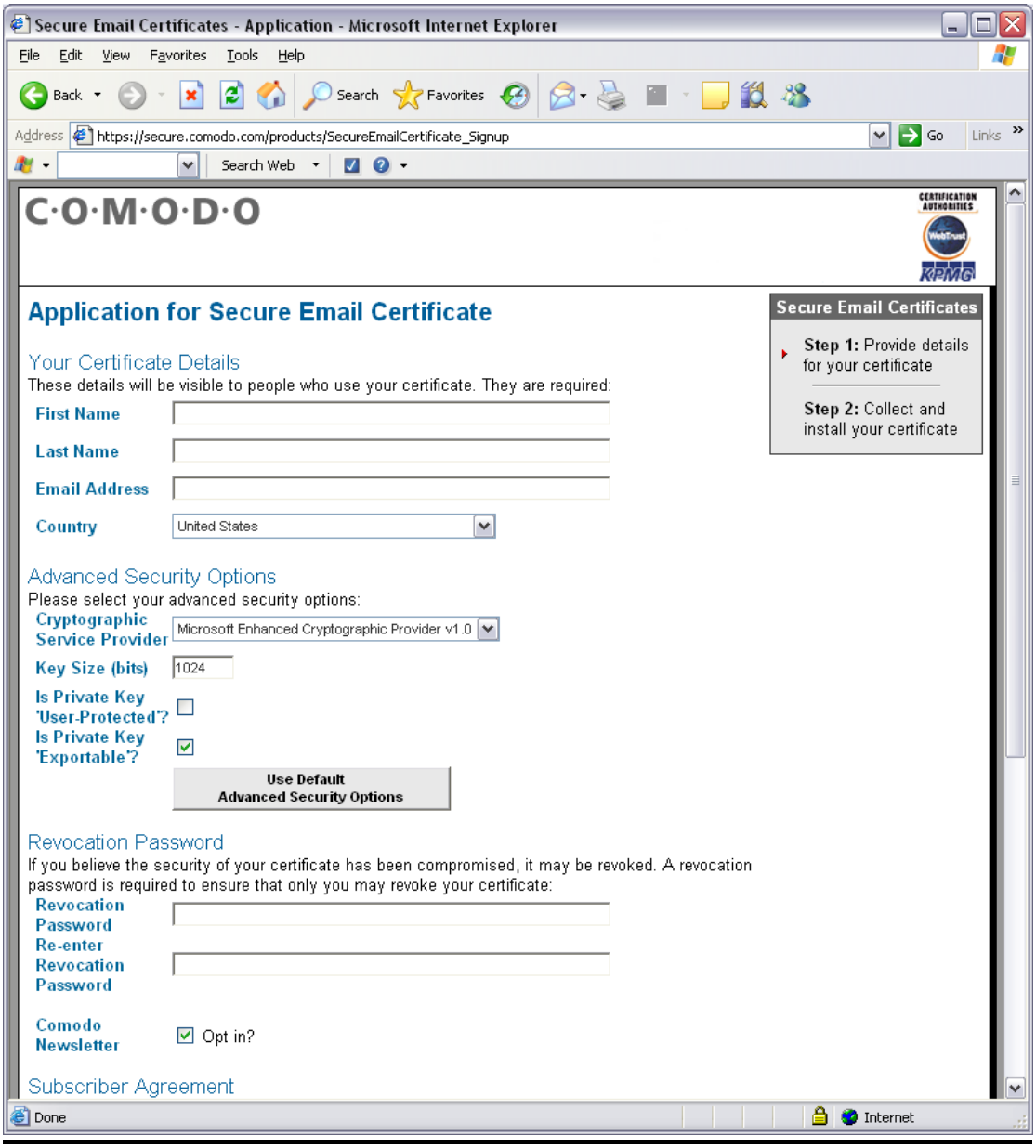


Μόλις το πατήσουμε μας παραπέμπει στην web page του Microsoft office που έχει μερικές προτεινόμενες υπηρεσίες παροχής Digital ID .

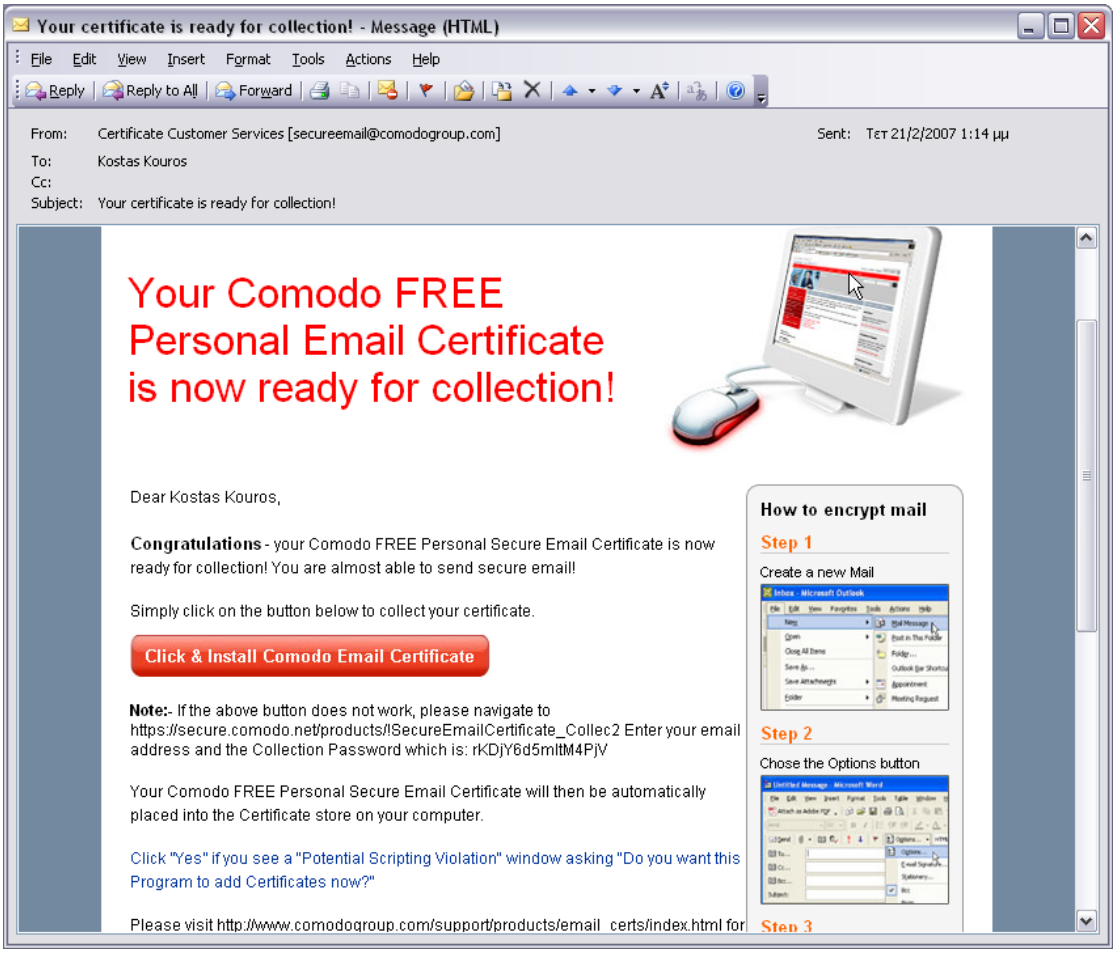


Από αυτές εμείς προτιμήσαμε την Comodo γιατί παρέχει την υπηρεσία δωρεάν για χρήση με το Outlook και τα άλλα προγράμματα του Microsoft Office. Αρχικά σε οδηγεί στην σελίδα της Comodo

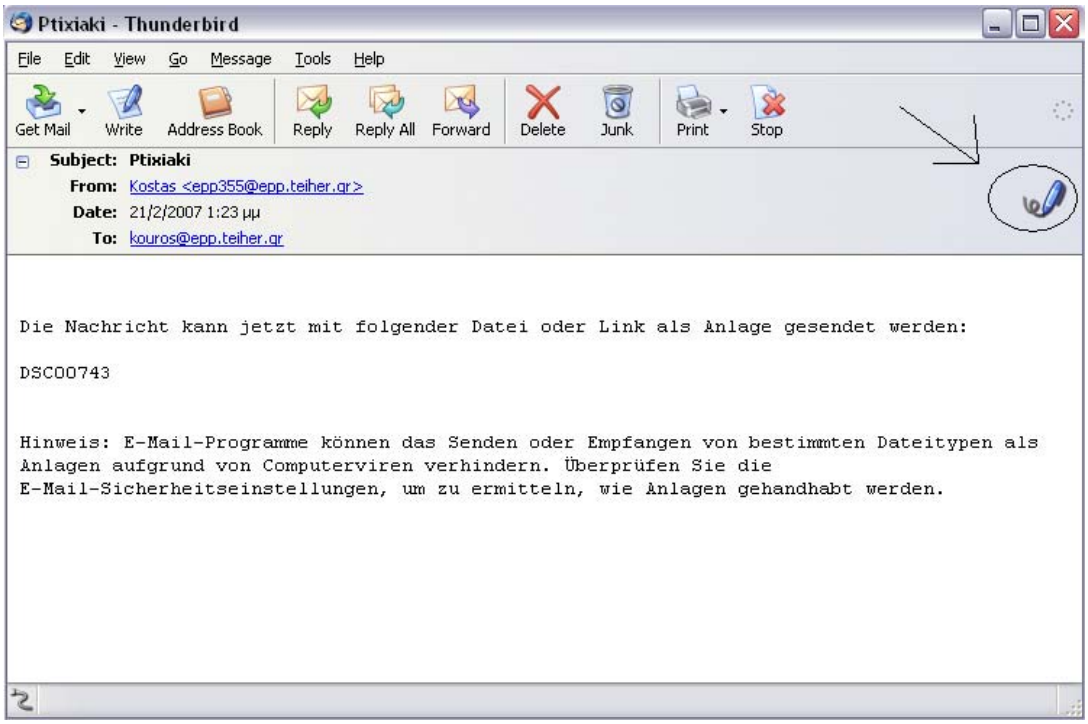
Επιλέγεις το ‘Get your e-mail cert now‘ οδηγείσαι σε μια φόρμα που συμπληρώνεις τα στοιχεία σου και επιλέγεις το επίπεδο ασφάλεια.



Μετά από αυτό σου στέλνουν ένα E-mail με την ψηφιακή σου υπογραφή και τις απαραίτητες οδηγίες για εγκατάσταση και χρήση .

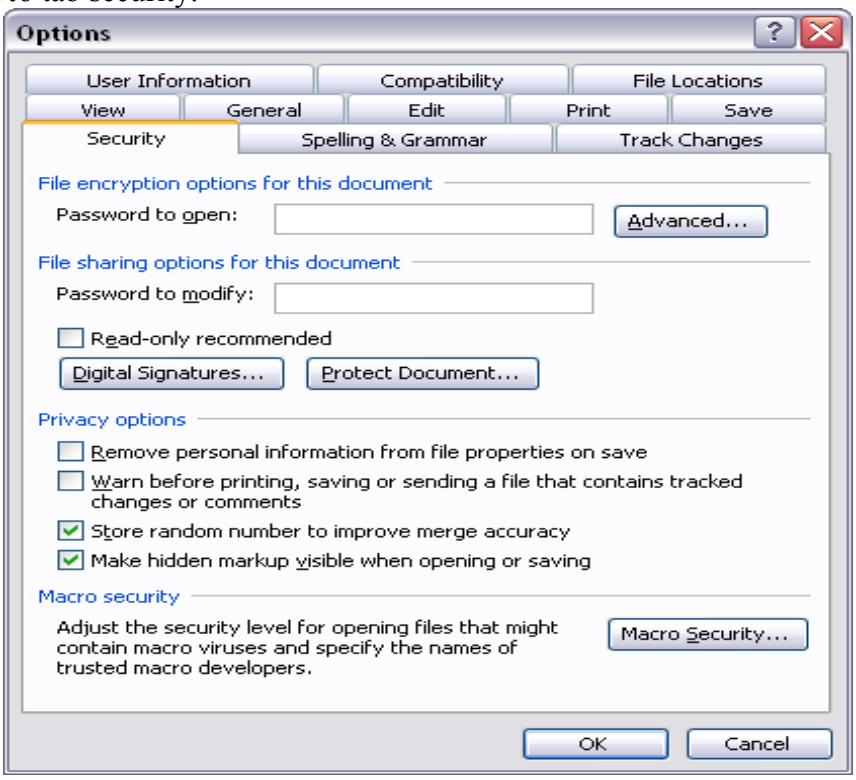


Τώρα έχεις ψηφιακή ταυτότητα και μπορείς να υπογράφεις τα e-mail σου, ώστε να φαίνεται η αυθεντικότητα και αν κάποιος έχει αλλοιώσει το μήνυμα.
Δείτε στο παρακάτω mail πως φαίνεται ότι είναι υπογεγραμμένο και άρα αυθεντικό

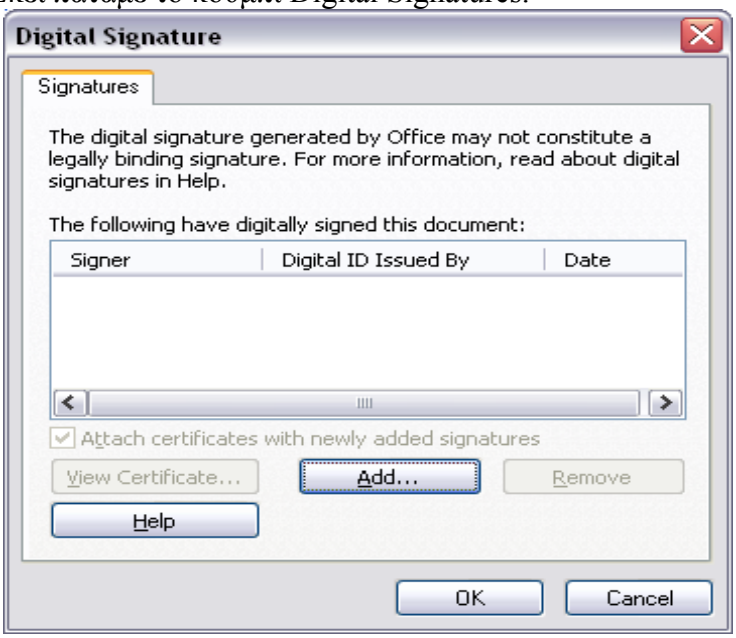


Digital ID στα Word και Excel

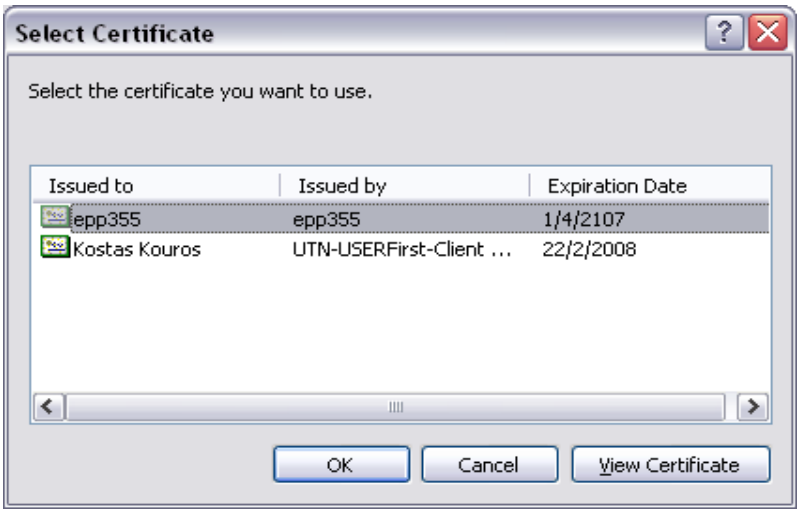
Η ψηφιακή υπογραφή μπορεί να χρησιμοποιηθεί για να υπογράψουμε έγγραφα του Word και του Excel, ώστε να ήμαστε βέβαιοι για τον δημιουργό του εγγράφου, και να καταλάβουμε αν έγιναν αλλαγές.Ας δούμε πρώτα πως μπορούμε να υπογράψουμε ένα έγγραφο του Word. Επιλέγουμε από το μενού Tools την επιλογή Options, και πάμε στο tab security.



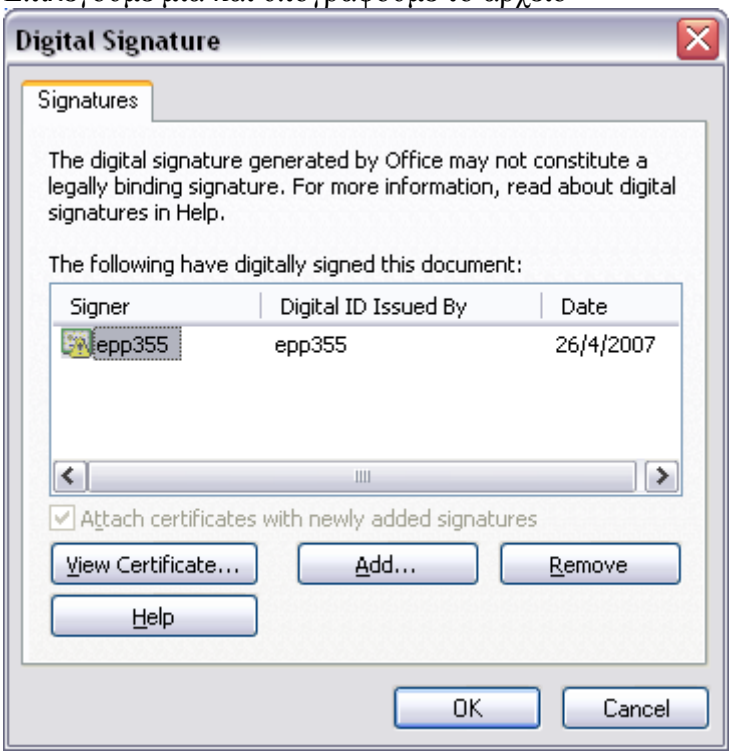
Εκεί πατάμε το κουμπί Digital Signatures.



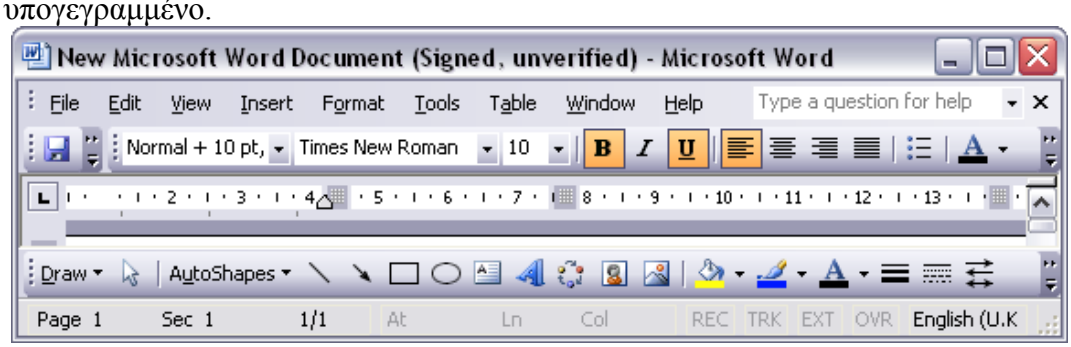
Στην συνέχεια επιλέγουμε το Add και βλέπουμε τις διαθέσιμες υπογραφές.



Επιλέγουμε μια και υπογράφουμε το αρχείο



Όταν ανοίγουμε το αρχείο, δίπλα στο όνομα του θα φαίνεται ότι είναι υπογεγραμμένο.



Τώρα αν σβήσουμε κάτι από το αρχείο και επιλέξουμε save ή exit θα μας εμφανιστεί το εξής μήνυμα.

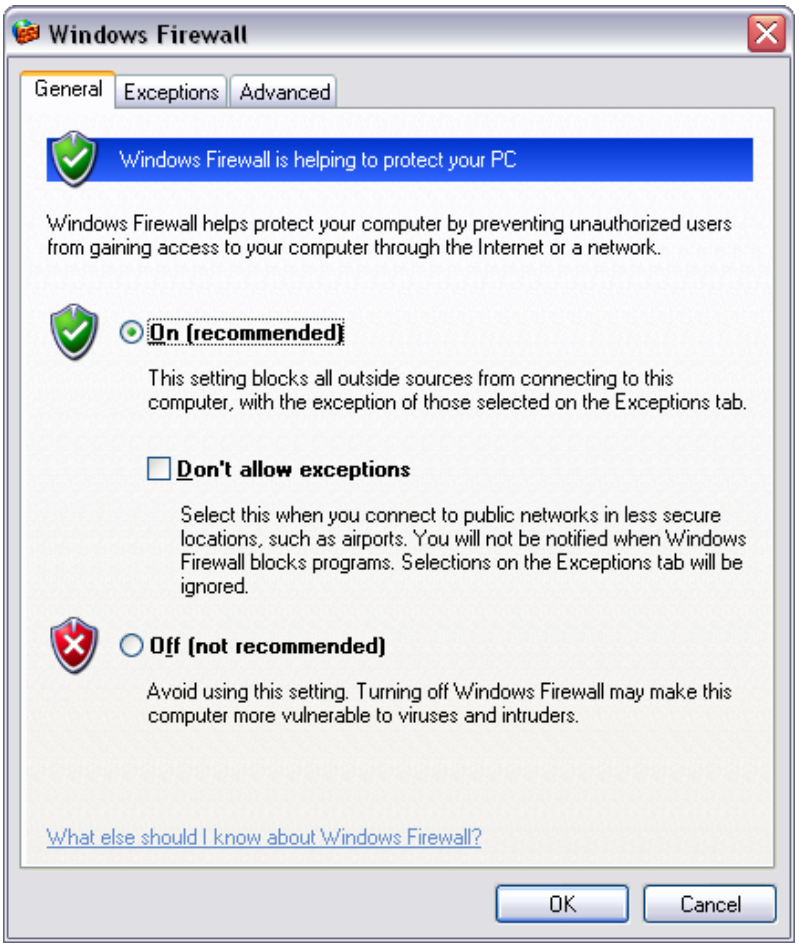
Άρα αν πάω να αλλάξω κάτι, θα χαθεί η υπογραφή και έτσι ο δημιουργός ή ο παραλήπτης θα ξέρει ότι έχει αλλαχθεί.
Με τον ίδιο τρόπο μπορούμε να χρησιμοποιήσουμε την ψηφιακή υπογραφή και στο Excel.

Εργαλεία ανίχνευσης προβλημάτων ασφάλειας

Windows Firewall

Γενικά

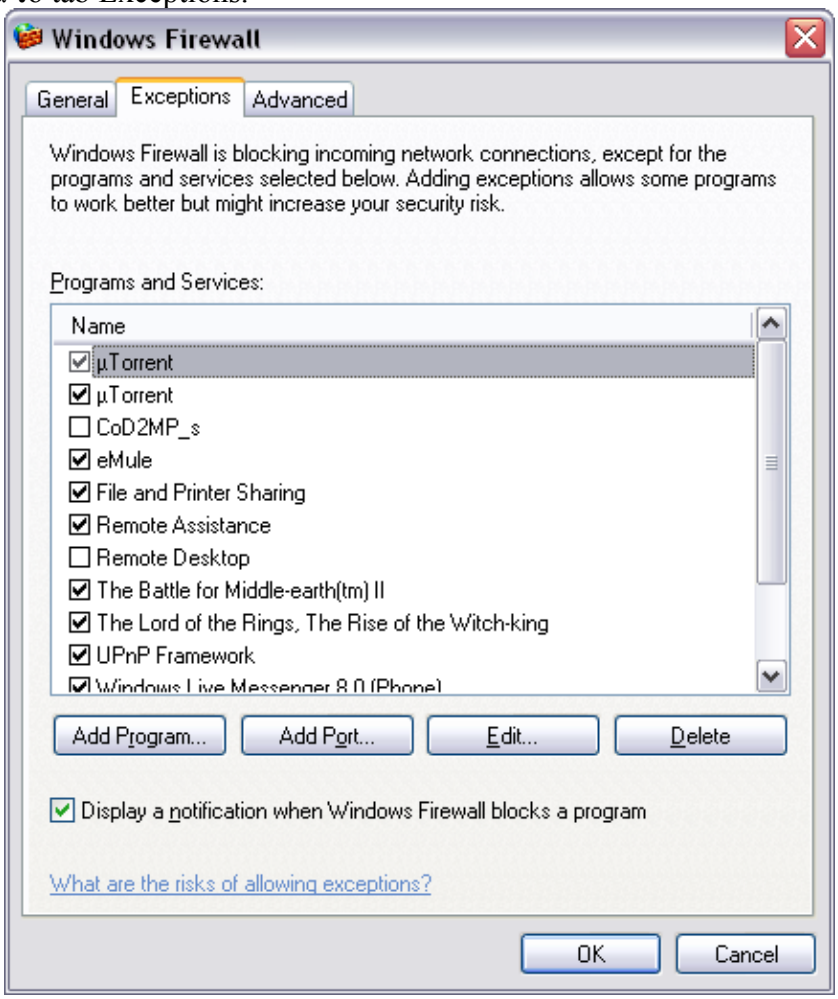
Όταν τα XP πρωτοεμφανιστήκαν τον Οκτώβρη του 2001, περιλάμβαναν ένα περιορισμένο firewall που λεγόταν “Internet connection Firewall”. Ήταν απενεργοποιημένο από προεπιλογή, και οι οθόνες ρυθμίσεων του ήταν κάπου θαμμένες στις ρυθμίσεις δικτύου, με αποτέλεσμα να μην το βλέπει κανείς και άρα να μην χρησιμοποιείται. Το 2003 το σκουλήκι Blaster επιτέθηκε σε πολλά μηχανήματα με Windows, εκμεταλλευόμενο τις αδυναμίες στην υπηρεσία RPC. Μερικούς μήνες μετά το σκουλήκι Sasser έκανε κάτι παρόμοιο.
Λόγω αυτών των περιστατικών και άλλων παρόμοιων, καθώς και έντονη κριτική προς την πλευρά της Microsoft για την προστασία των πελατών της, αποφασίστηκε να βελτιωθεί σημαντικά η λειτουργικότητα και το interface του firewall των Windows XP, και να μετονομαστεί σε Windows Firewall.



Το Firewall των Windows XP

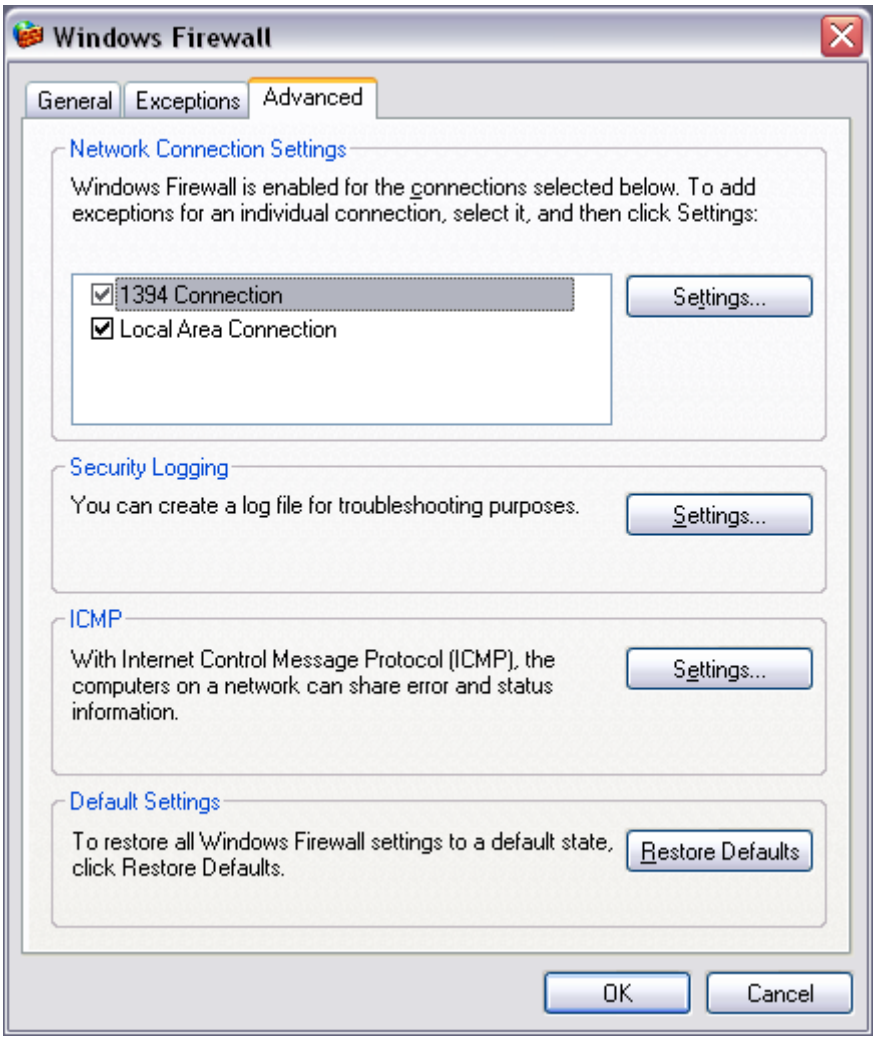
Πρώτα από όλα να πούμε ότι το firewall είναι μια εφαρμογή που ελέγχει την κίνηση στο δίκτυο από και προς το σύστημα μας. Το Windows Firewall εμφανίστηκε σαν μέρος του Service Pack 2 των Windows XP. Είναι ενεργοποιημένο από προεπιλογή σε κάθε τύπου σύνδεσης δικτύου ασύρματη ή ενσύρματη, με κάποιες προεπιλεγμένες εξαιρέσεις ώστε να επιτρέπει συνδέσεις από συστήματα στο τοπικό δίκτυο. Επίσης επιδιόρθωνε το πρόβλημα ενεργοποίησης των firewall policies, οι οποίες ενεργοποιούταν μερικά δευτερόλεπτα μετά την δημιουργία της σύνδεσης. Ακόμα μερικές προσθήκες έγιναν στο Group Policy, ώστε οι administrators να μπορούν να ρυθμίζουν το firewall σε επίπεδο εταιριών. Το Windows Firewall δεν μπορεί να μπλοκάρει εξωγενείς συνδέσεις, μπορεί μόνο να μπλοκάρει εσογενείς.
Ας δούμε τη επιλογές μας προσφέρει, εκτός από την αρχική οθόνη που είδαμε παραπάνω με τις επιλογές on και off, ας δούμε κει τις υπόλοιπες.

Πρώτα το tab Exceptions.



Εδώ μπορούμε να επιλέξουμε ποια προγράμματα και ποιες υπηρεσίες μπορούν να δημιουργούν συνδέσεις.

Και τέλος το tab Advanced.



Όπου μπορεί να διαλέξεις σε ποιες συνδέσεις θα είναι ενεργό, τις ρυθμίσεις του ICMP, το security Logging, και να επαναφέρεις τις αρχικές ρυθμίσεις σε περίπτωση λάθους.

Microsoft Baseline Security Analyzer

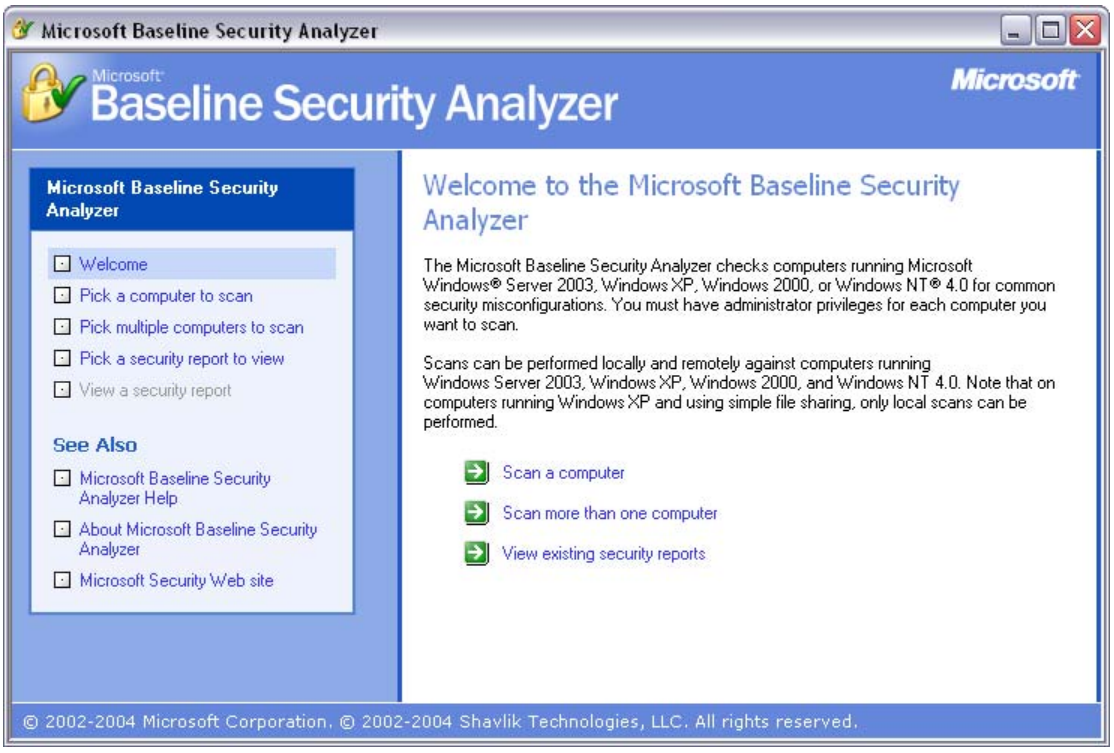
Εισαγωγή

Το Microsoft Baseline Security Analyzer (MBSA) είναι ένα εργαλείο φτιαγμένο από την Microsoft για να βοηθήσει στον εντοπισμό και την ανάλυση προβλημάτων ασφαλείας στα Microsoft Windows. Αυτό το επιτυγχάνει σκανάροντας το σύστημα για προβλήματα στα Windows, σε Windows components όπως οι εφαρμογές IIS Server, στο Microsoft SQL Server και στο Microsoft Office. Πρόβλημα ασφάλειας έχουμε π. χ. όταν τα permissions για ένα από τα directories στο wwwroot φάκελο του IIS Server είναι ένα επίπεδο πιο χαμηλά με αποτέλεσμα να επιτρέπονται ανεπιθύμητες μεταβολές σε αρχεία από εξωτερικούς παράγοντες.

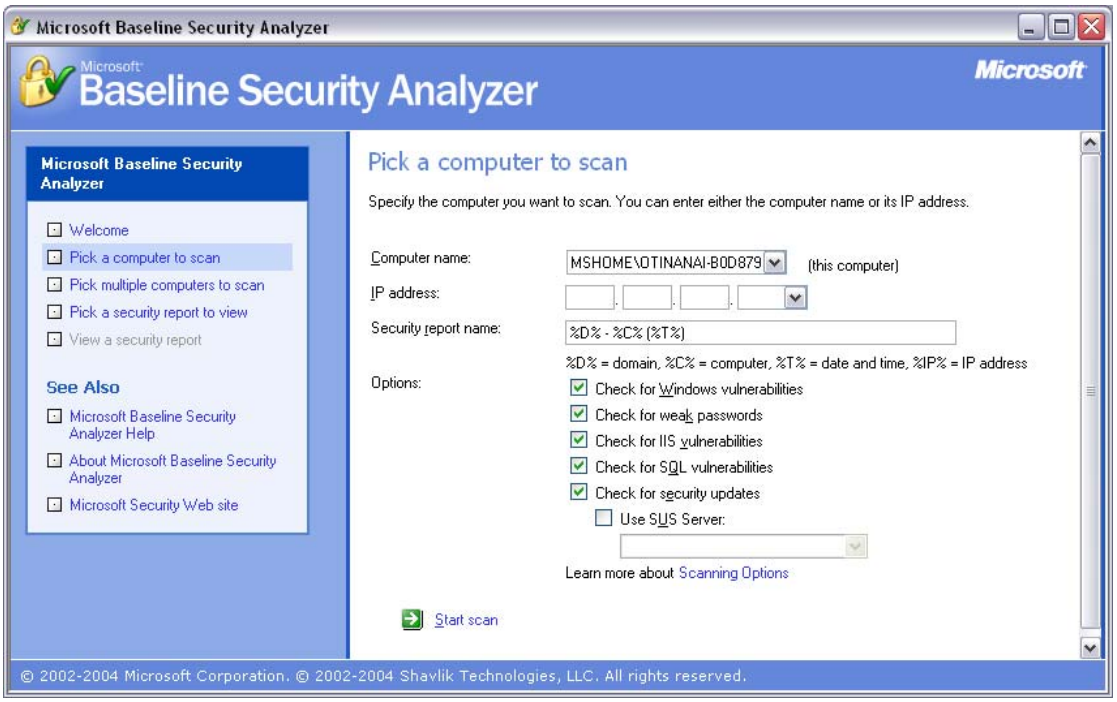
Λειτουργία

Εμείς θα τρέξουμε την έκδοση 1.2.1 του MBSA πάνω σε ένα σύστημα που τρέχει Windows XP και Office 2003

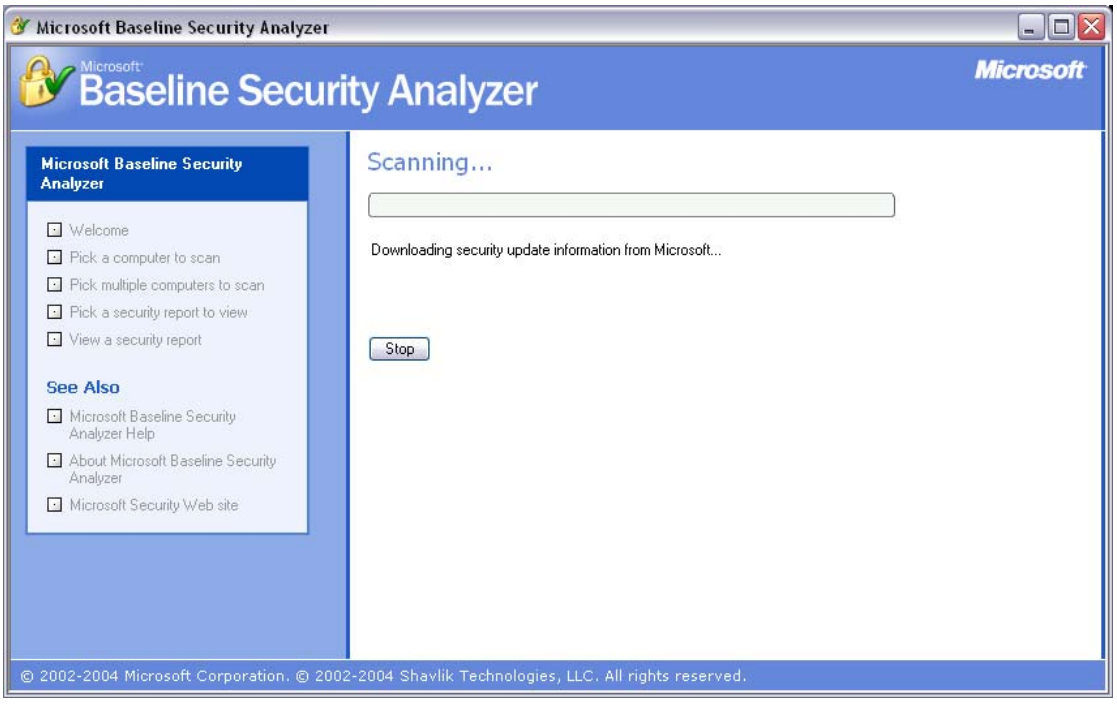
Στην αρχική οθόνη επιλέγουμε Scan a Computer για να ξεκινήσουμε την διαδικασία εντοπισμού.



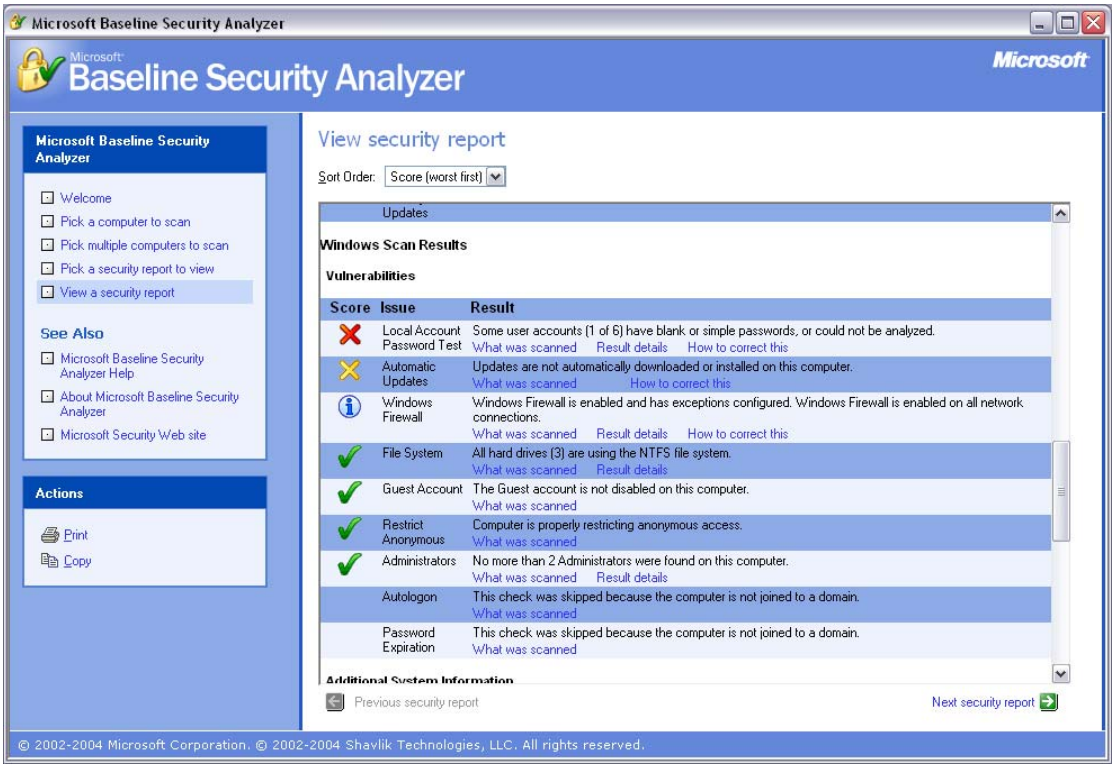
Στην επόμενη οθόνη δίνουμε τις παραμέτρους της αναζήτησης, δηλαδή σε ποιους τομείς να αναζητηθούν τα προβλήματα αν όχι σε όλους, σε ποιόν υπολογιστή θα δουλέψουμε και την μορφή του Report .



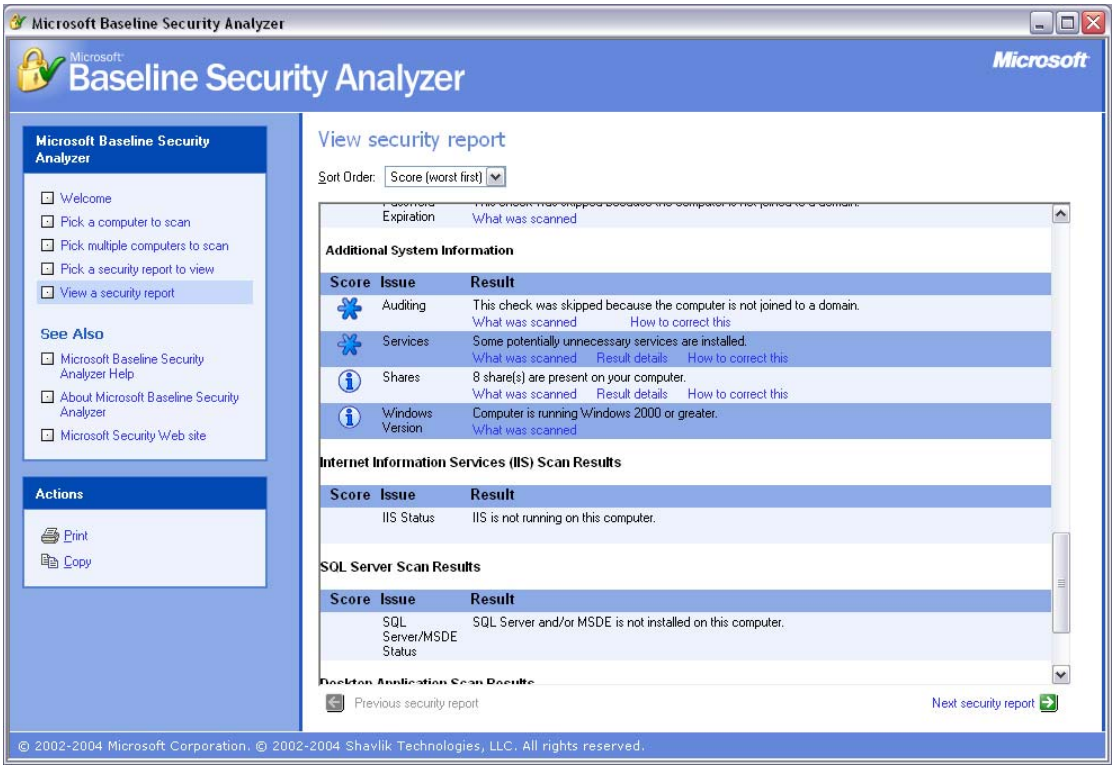
Περιμένουμε να ολοκληρωθεί η αναζήτηση

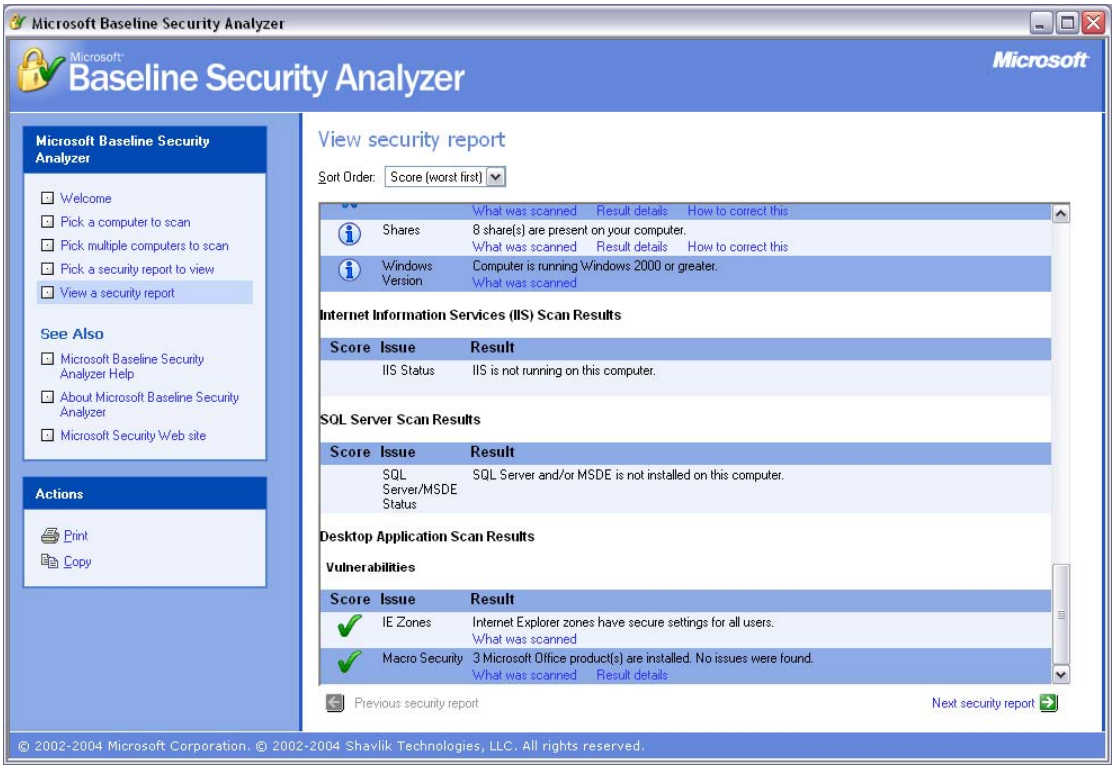


Και στην συνέχεια προκύπτει η αναφορά Πρώτα για προβλήματα στα Windows.

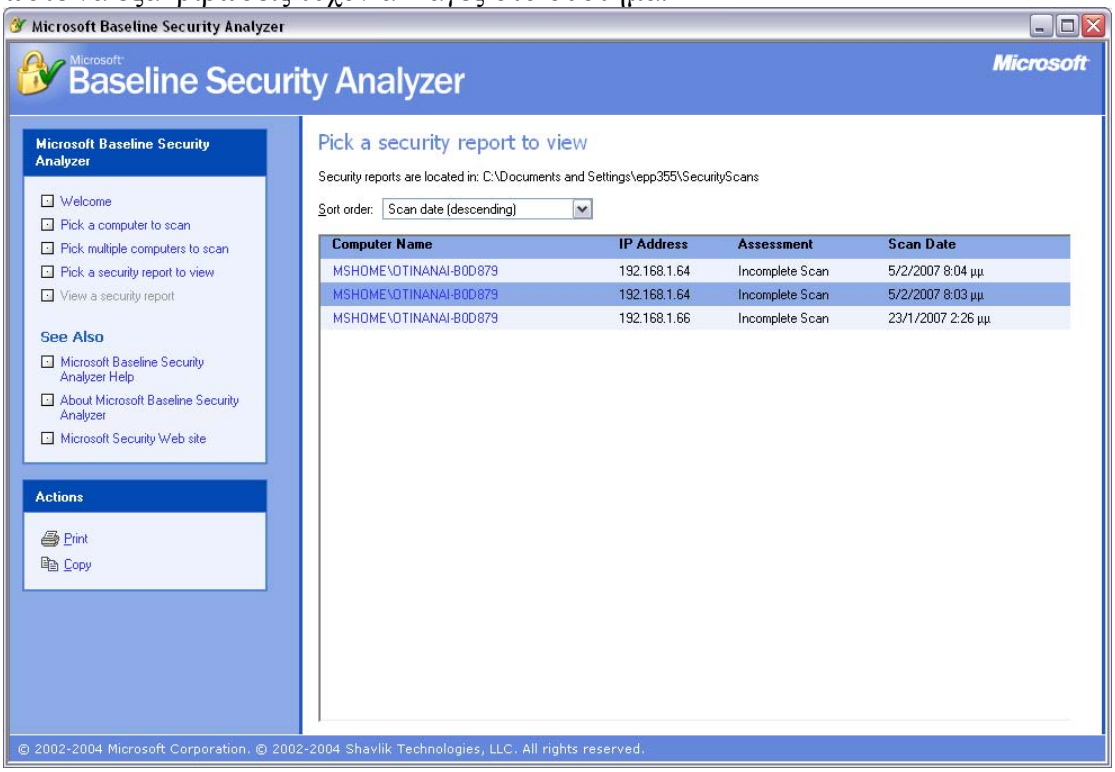


Έπειτα για τα διάφορους άλλους τομείς που είπαμε στην εισαγωγή





Επίσης σου δίνει την δυνατότητα να εξετάσεις και παλιές αναφορές και να συγκρίνεις ώστε να εξακριβώσεις τυχόν αλλαγές στο σύστημα.



Microsofts' Security Risk Self-Assessment Tool

Γενικά

Το Microsoft Security Assessment είναι μια διεπαφή αλληλεπίδρασης που χρησιμοποιεί το Microsoft Assessment Tool (MSAT) και περιλαμβάνει ένα ερωτηματολόγιο. Είναι μια διαδικασία υποκινούμενη από τον χρήστη που κρατάει από μια έως δύο ώρες, σκοπός της είναι να βοηθήσει τους χρήστες να καταλάβουν καλύτερα τα προβλήματα ασφαλείας που τυχόν έχουν.
Η διαδικασία αυτή παρέχει στους χρήστες μια καλύτερη εικόνα της εταιρίας και της οργάνωσης, και παρέχει ένα σχέδιο για την βελτίωση της ασφάλειας μέσα από ταξινομημένες εργασίες, λύσεις, και καθοδήγηση. Το MSAT είναι ένα εργαλείο που μπορεί κανείς να χρησιμοποιήσει πολλές φορές, και επικεντρώνει σε βασικές εργασίες βελτίωσης.
Όταν τελειώσει η διαδικασία ερωτήσεων, μας παρέχει μια λεπτομερείς αναφορά με τα ευρήματα και τις προτάσεις του όσο αναφορά τα θέματα ασφάλειας. Η αναφορά αυτή είναι σχεδιασμένη να κάνει τον χρήστη να κατανοήσει τα θέματα που σχετίζονται με την ασφάλεια και να του δώσει τα κατάλληλα βήματα για την βελτίωση της.

Λειτουργία

Τα τέσσερα σημεία που αναλύουν καλύτερα τον τρόπο λειτουργίας του MSAT είναι τα εξής.

Business Risk Profile.

Κατανοώντας την φύση των απειλών μπορεί να μας υποδείξει που να εστιάσουμε την προσοχή μας, ώστε να μειώσουμε τον κίνδυνο. Επίσης μπορεί να μας βοηθήσει στην πιο σωστή κατανομή του προϋπολογισμού ασφάλειας.

Defence – in – Depth.

Το "Defence – in - Depth" (DiD) σημείο αναφέρεται στην ανάλυση της άμυνας σε όλα τα επίπεδα, το τεχνικό, οργανωτικό, και επιχειρησιακό. Βασίζεται σε καθιερωμένα στάνταρ και τις καλύτερες τακτικές για μείωση κινδύνου σε IT περιβάλλον.

Αποτελέσματα και αναφορές.

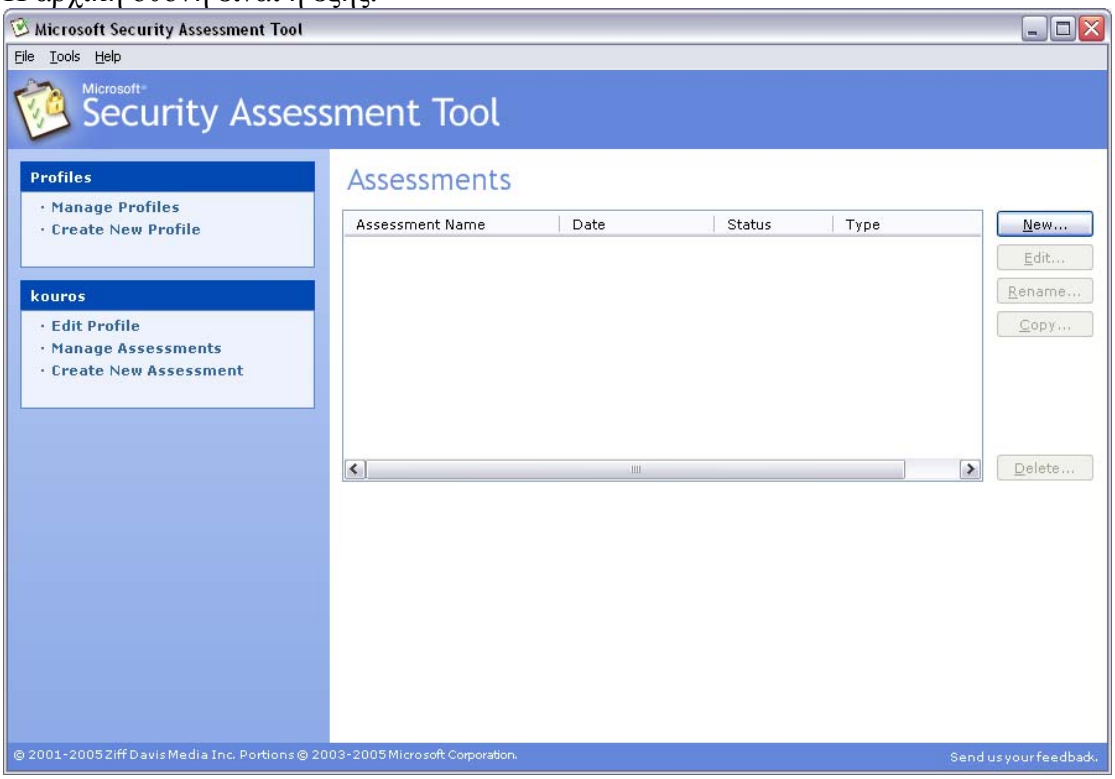
Μπορείς να δεις τα αποτελέσματα αμέσως μετά το πέρας της διαδικασίας. Η αναφορά σου δίνει την δυνατότητα να συγκρίνεις τα αποτελέσματα με αυτά των συναδέλφων σου, επίσης μπορείς να τα συγκρίνεις και με δικά σου παλαιότερα.
Ακόμα σου παρέχεται μια εκτενής αναφορά που περιγράφει το επίπεδο ασφάλειας της εταιρίας, βασισμένο στις απαντήσεις σου, και προτάσεις και τακτικές για την βελτίωση της. Τέλος η αναφορά αποθηκεύετε σαν κείμενο HTML για εκτύπωση και αποστολή μέσω e-mail.

Περιοχή Ανάλυσης.

Αντίθετα με το Microsoft Baseline Security Analyzer, που ελέγχει απευθείας το σύστημα σου, το MSAT είναι ένα λεπτομερές ερωτηματολόγιο που συμπληρώνεις ο ίδιος. Στη συνέχεια αναλύει τις απαντήσεις σου και προσφέρει λύσεις σε τομείς όπως η υποδομή, οι διεργασίες, τα προγράμματα που τρέχεις και το προσωπικό που χρησιμοποιεί τα συστήματα.

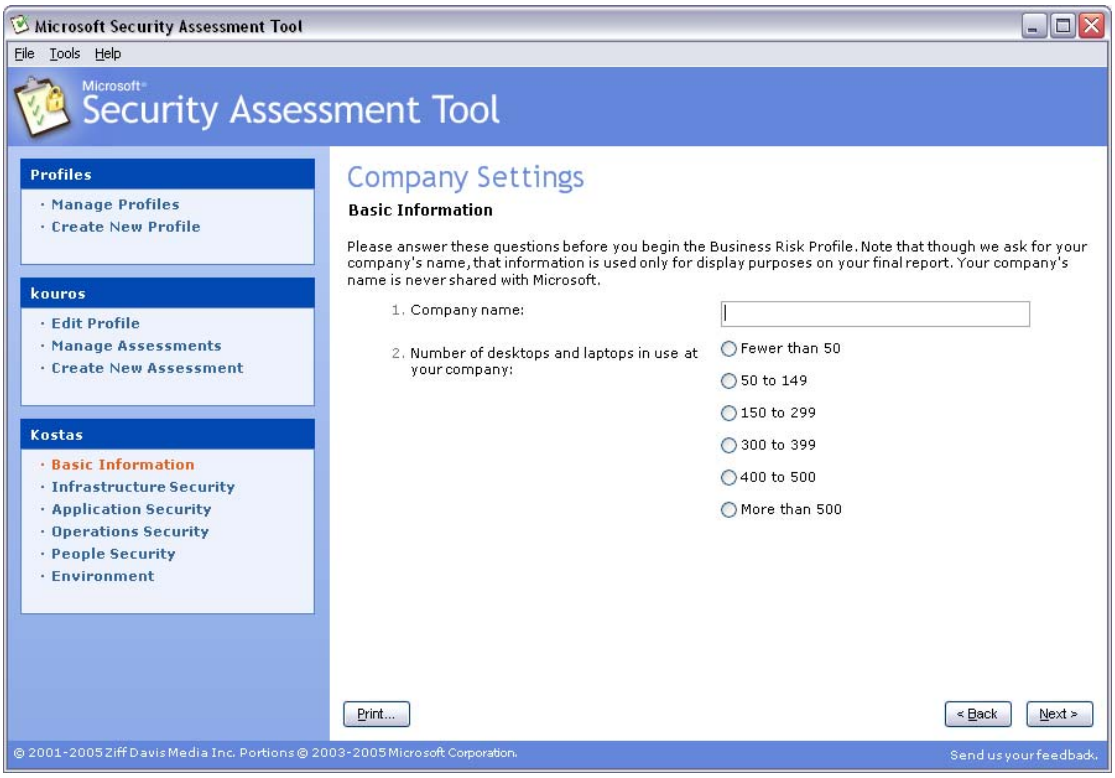
Στην Πράξη

Η αρχική οθόνη είναι η εξής.

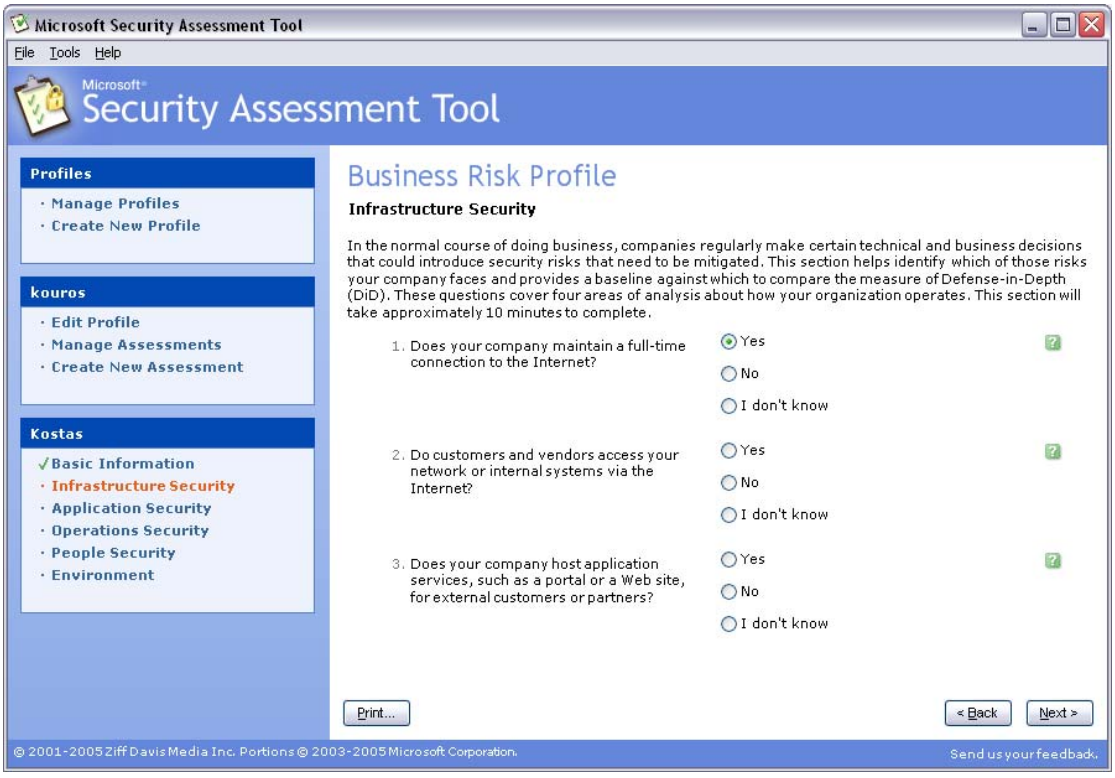


Ξεκινάμε επιλέγοντας το Create New Profile.

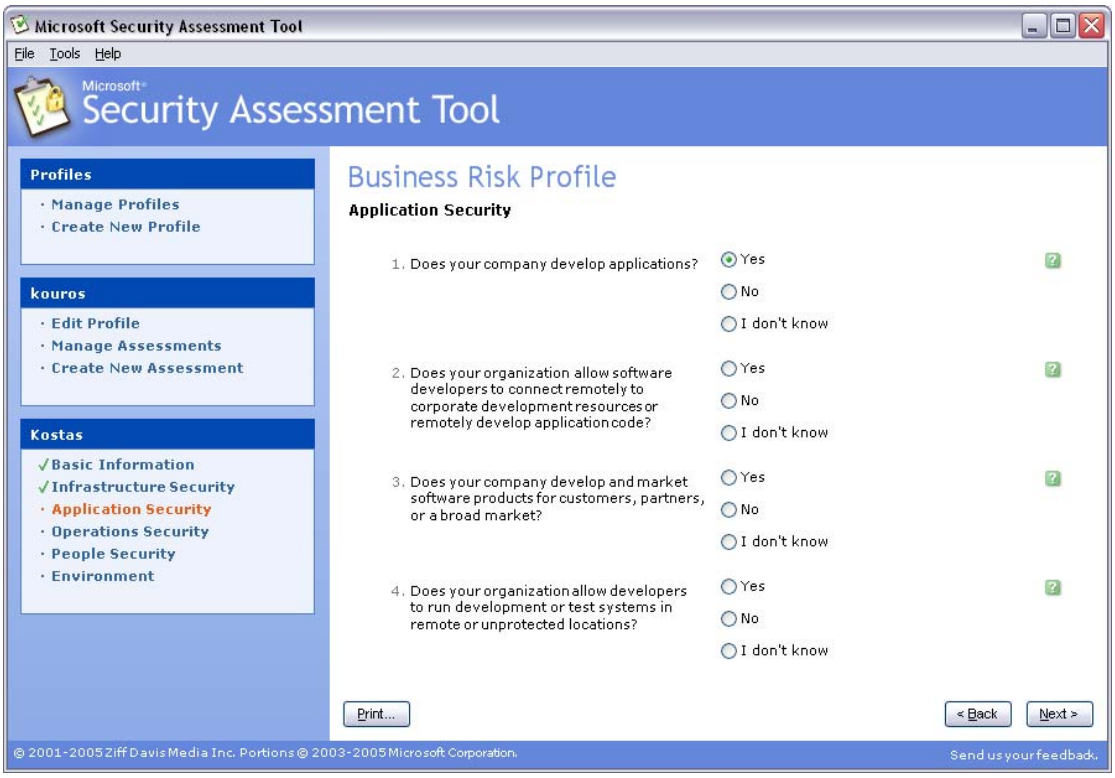
Στην συνέχεια πρέπει να συμπληρώσουμε μερικά στοιχεία για την εταιρία μας.



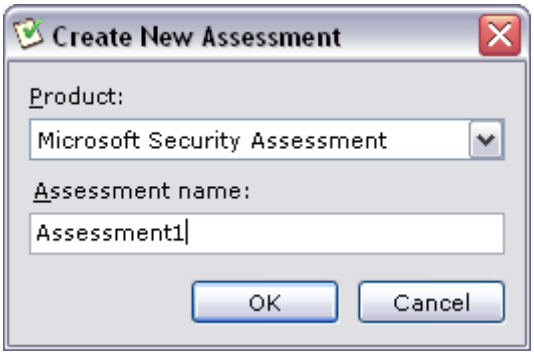
Στην συνέχεια προχωράμε στο στάδιο Business Risk Profile.



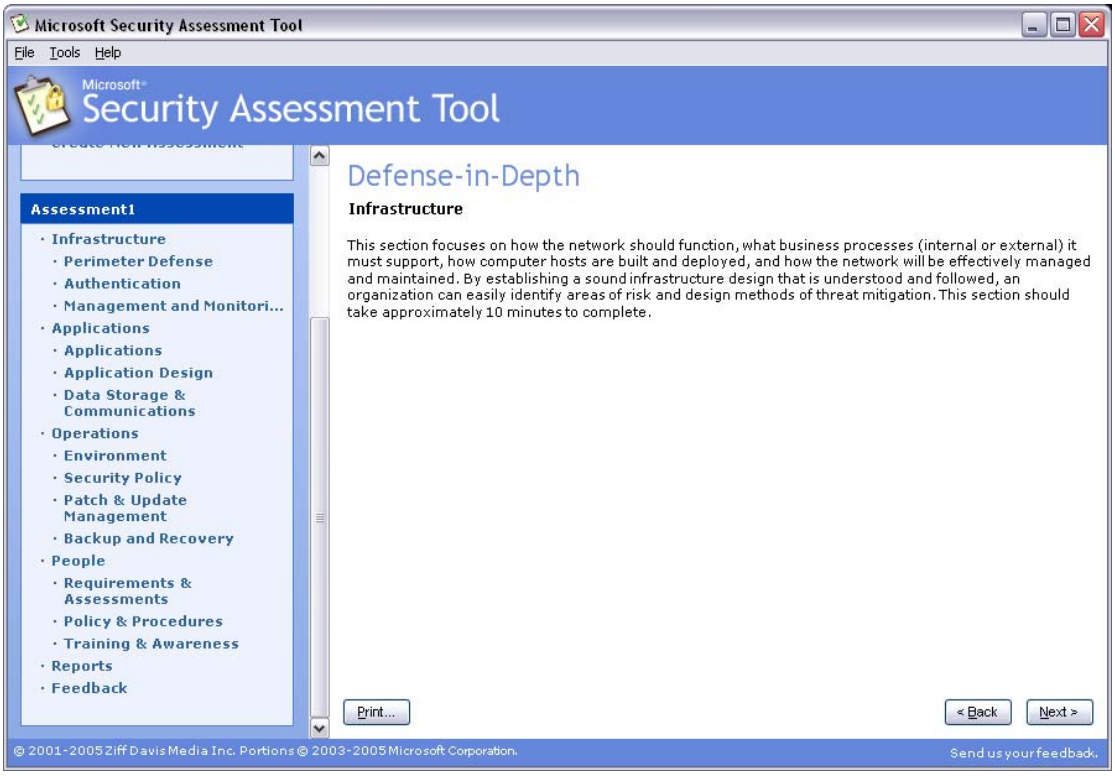
Στα αριστερά βλέπουμε τα στάδια της ανάλυσης και μαρκαρισμένα αυτά που έχουν συμπληρωθεί. Επίσης φαίνονται και κάτω από την επικεφαλίδα, όπως βλέπουμε εδώ είμαστε στο στάδιο Business Risk Profile – Application Security.



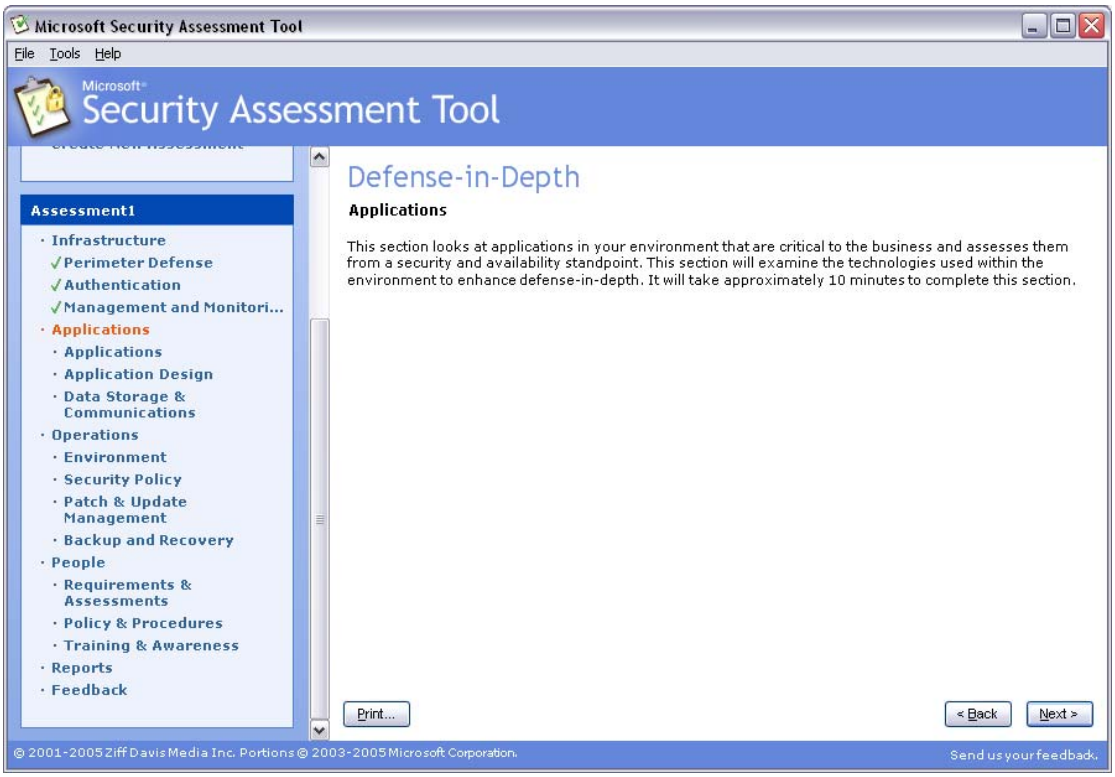
Αφού ολοκληρώσουμε αυτόν τον τομέα προχωράμε στο Assessment.



Στη συνέχεια αρχίζει το DiD στάδιο, πάλι με του επιμέρους τομείς να φαίνονται στο αριστερό μέρος της οθόνης. Τώρα είμαστε στο στάδιο Infrastructure.

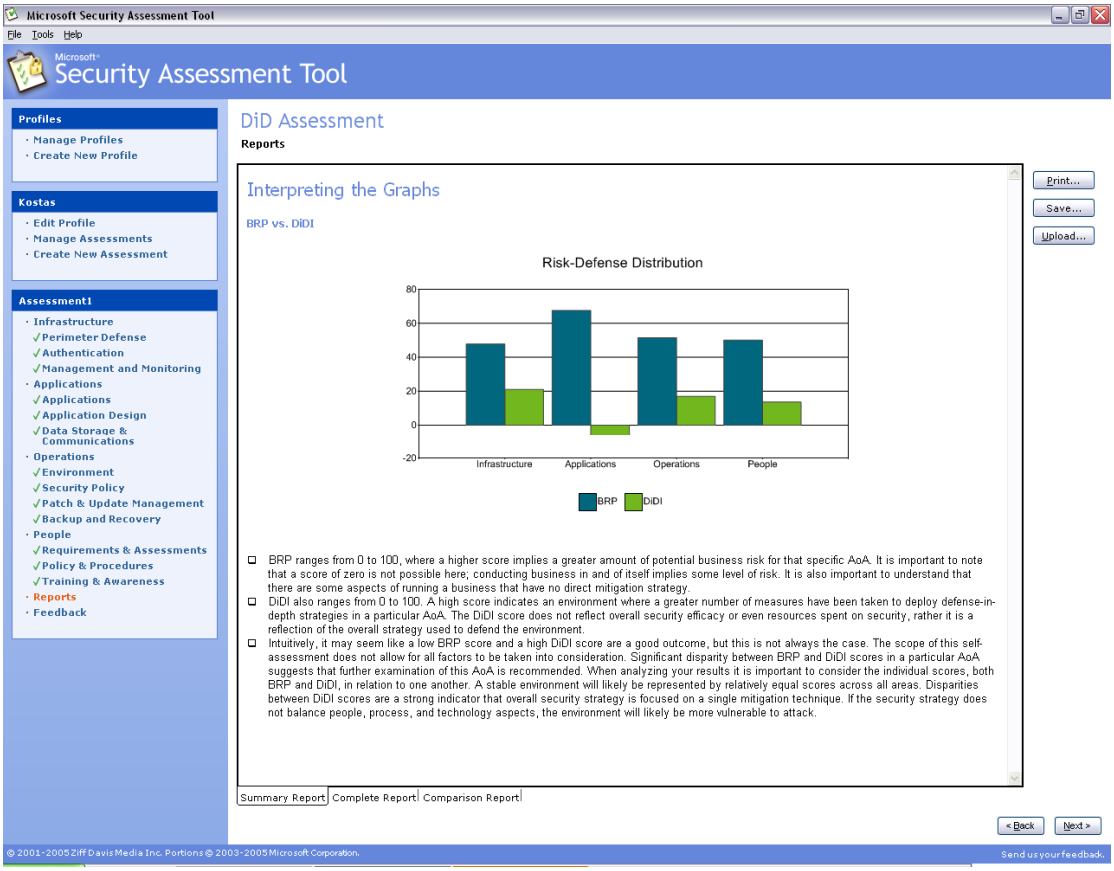


Στη συνέχεια είναι το στάδιο Applications και ούτω καθ' εξής.

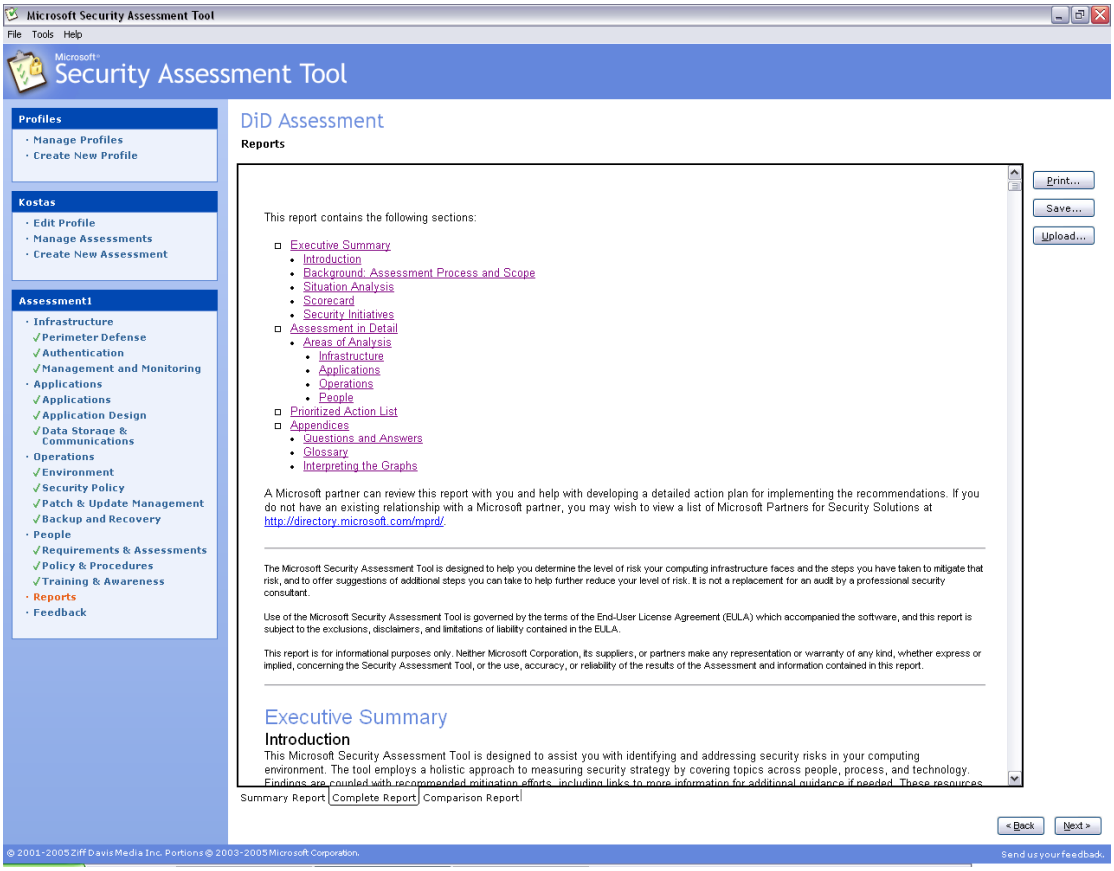


Αφού ολοκληρωθεί η διαδικασία μας προβάλετε αναφορά σε δύο μέρη, ένα περιληπτικό και ένα πλήρες.

Η περιληπτική.

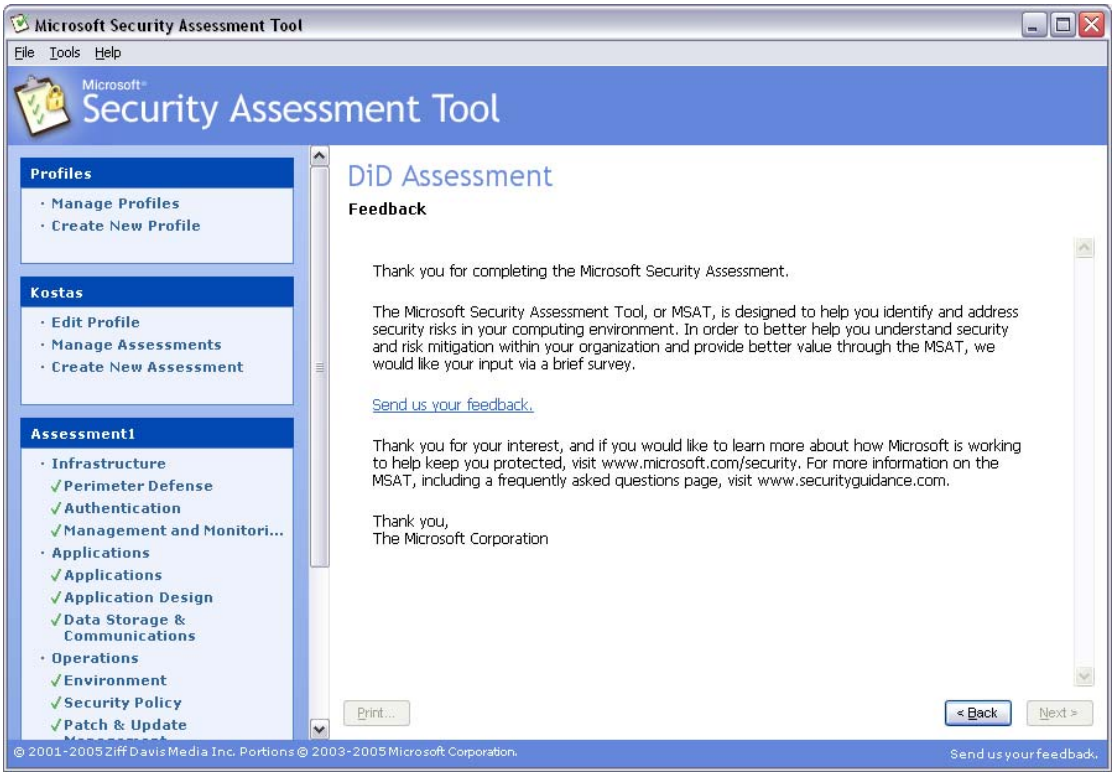


Και η πλήρης.



Από ότι βλέπουμε είναι ταξινομημένη και καλύπτει τους εξής τομείς.

Τέλος μας δίνεται η δυνατότητα να στείλουμε τα αποτελέσματα για έρευνα και καλύτερη υποστήριξη.



Microsoft Windows Defender

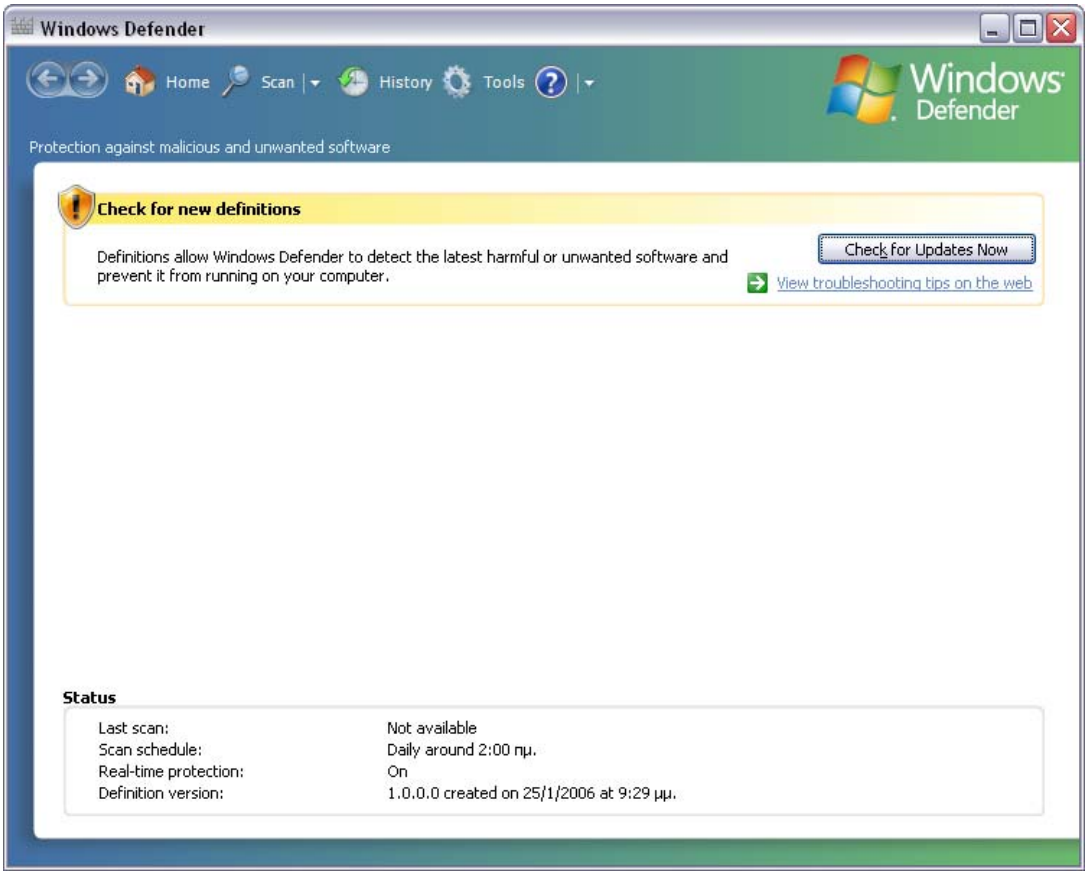
Εισαγωγή

Το Windows Defender, προηγουμένως γνωστό ως Microsoft Antispyware, είναι μια εφαρμογή που σχεδιάστηκε για να αποτρέψει, να απομακρύνει ή να περιορίσει spyware στο Microsoft Windows.
Είναι βασισμένο στο GIANT AntiSpyware που είχε δημιουργηθεί από την GIANT Company Software, Inc. Ενώ σαν GIANT AntiSpyware υποστήριζε παλαιότερες εκδόσεις των Windows, μόλις το απέκτησε η Microsoft η υποστήριξη για την σειρά Windows 9x λειτουργικών συστημάτων σταμάτησε.
Το Windows Defender περιέχει ένα σύστημα αναζήτησης (Scanning) παρόμοιο με άλλων εφαρμογών που υπάρχουν στην αγορά, αλλά περιέχει και έναν αριθμό από Real-Time Security Agents που παρακολουθούν διάφορες περιοχές των Widows για αλλαγές που μπορεί να προκλήθηκαν από spyware. Επίσης σου δίνει την δυνατότητα να αφαιρείς εύκολα Active X εφαρμογές που έχουν εγκατασταθεί. Τέλος υπάρχει υποστήριξη από το Microsoft Spynet network που επιτρέπει στους χρήστες να αναφέρουν στην Microsoft τι πιστεύουν ότι είναι Spyware και ποιες εφαρμογές και οδηγούς συσκευών επιτρέπουν να εγκατασταθούν στα σύστημα τους

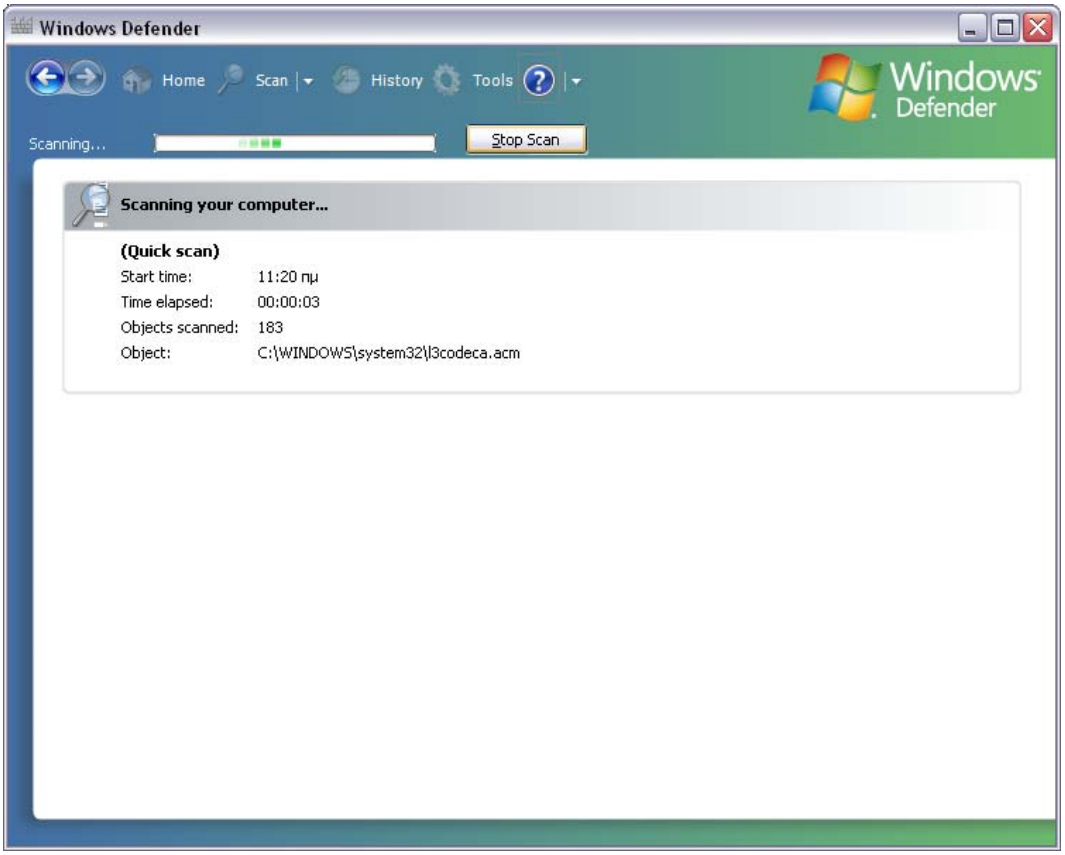
Λειτουργία

Τώρα θα δούμε το interface και τις επιλογές που μας προσφέρει ο Windows Defender.

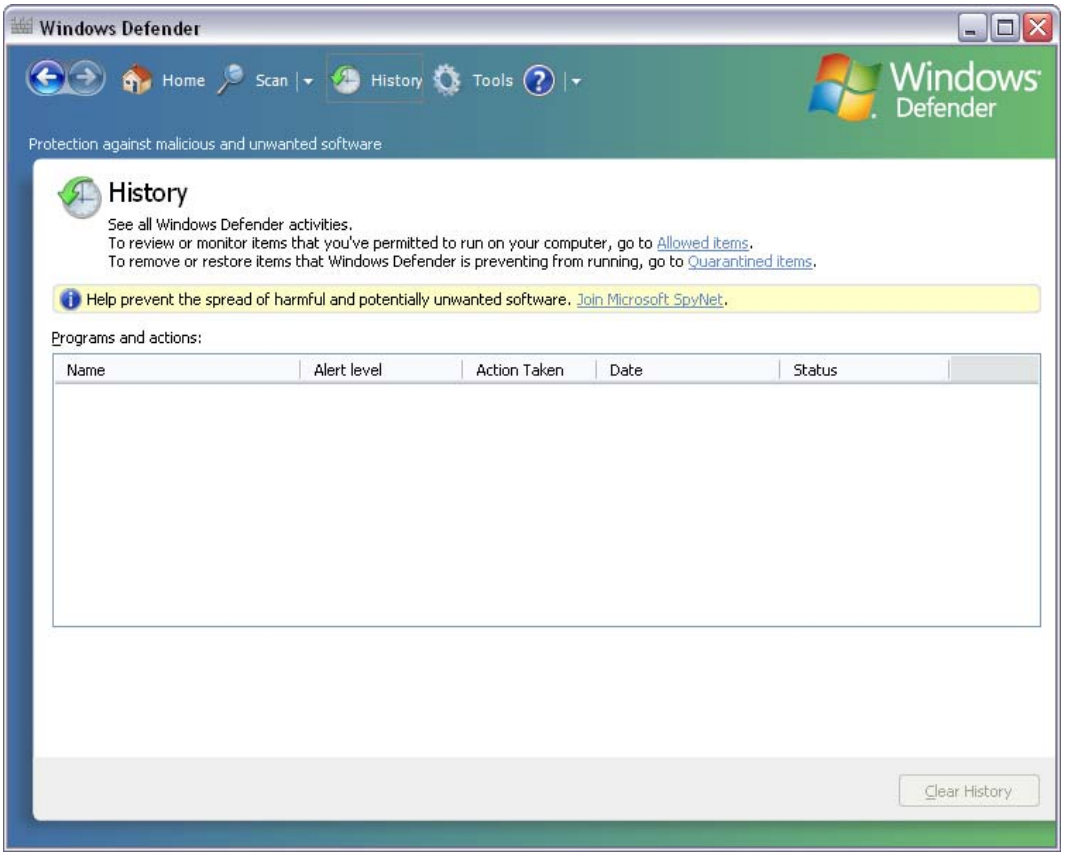
Η αρχική εικόνα είναι η εξής



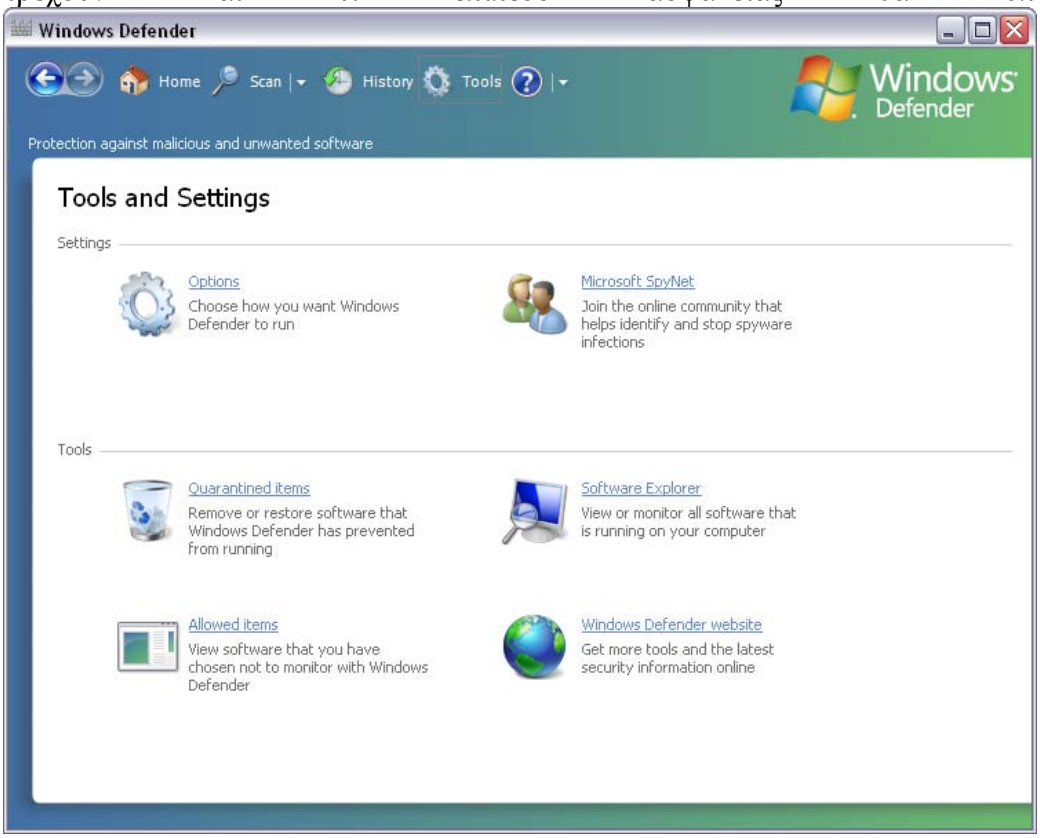
Τώρα ας εξετάσουμε τις επιλογές που υπάρχουν. Πρώτα στο tab Scan μπορούμε να κάνουμε ένα Full scan του συστήματος μας για να εντοπίσουμε τυχόν απειλές



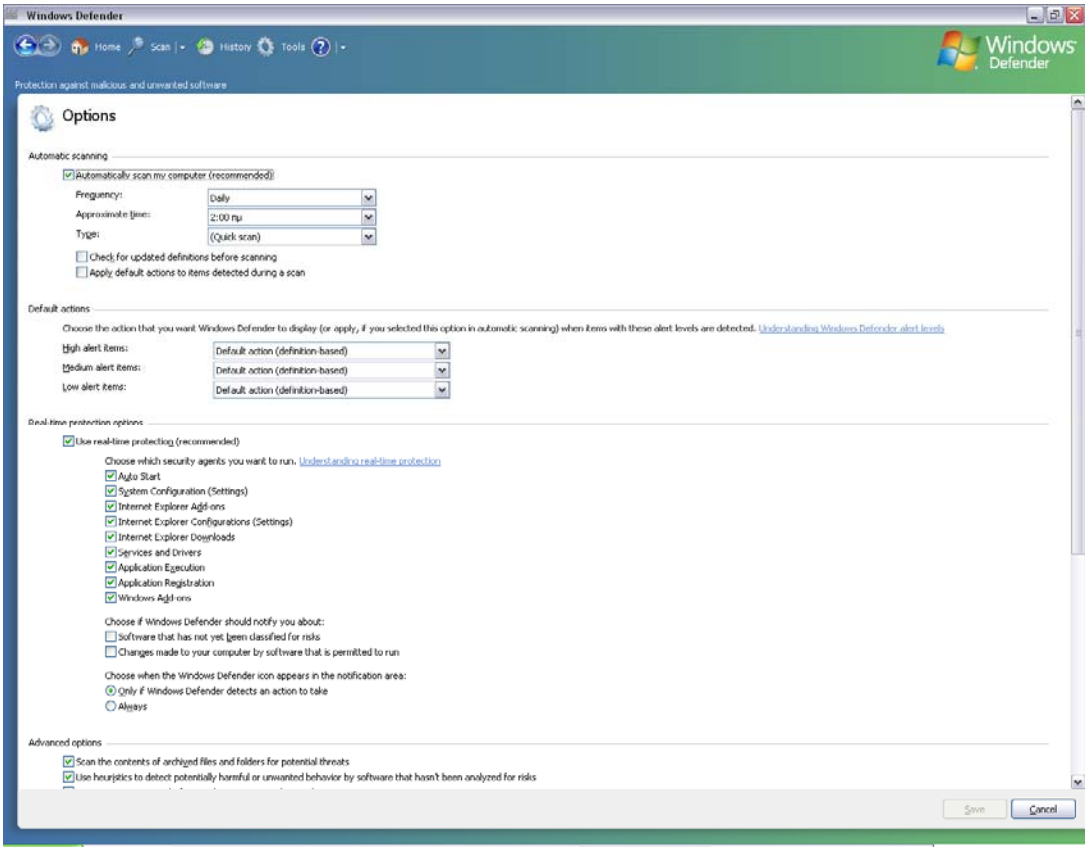
Στο tab History μπορούμε να δούμε ποιες εφαρμογές τρέχουν στο σύστημα μας και ποιες έχουμε αποκλείσει, επίσης μπορούμε να δούμε τα αρχεία που έχουμε στην καραντίνα.



Τέλος έχουμε το tab Tools στο οποίο υπάρχουν οι επιλογές για το ποια εργαλεία θα τρέχουν και τι επίπεδο ασφάλειας θα υπάρχει.



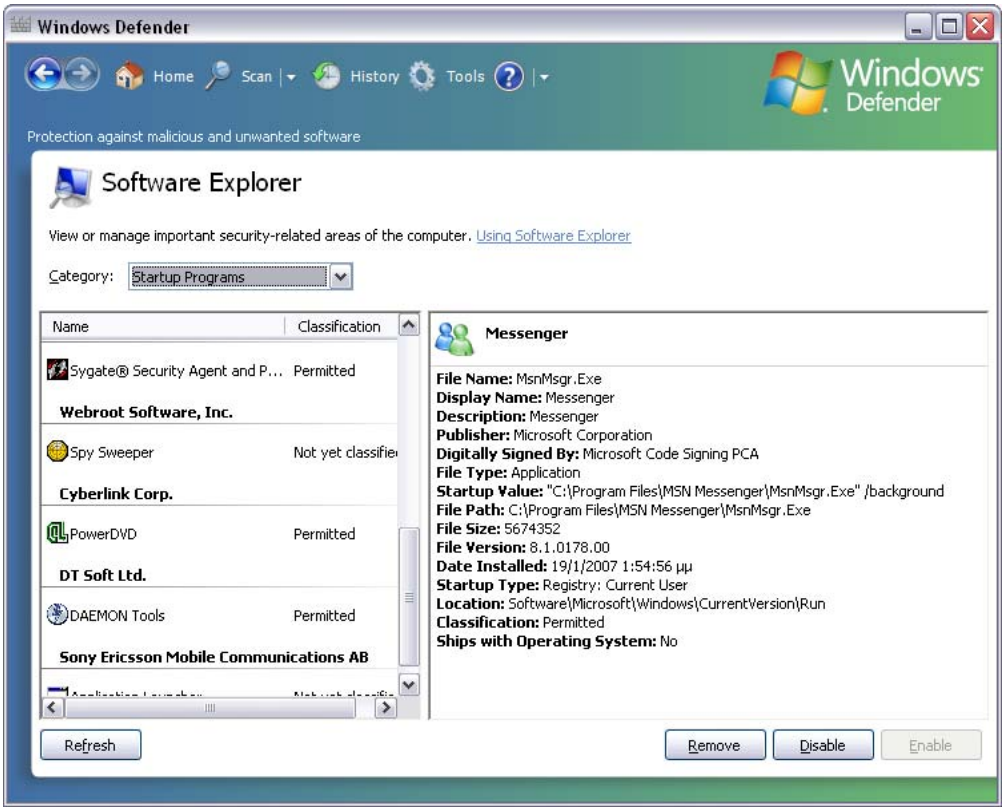
Ας δούμε το μενού options που μας ενδιαφέρει περισσότερο.



Από εδώ μπορούμε να επιλέξουμε κάθε πότε θα γίνεται Scan στο σύστημα, τον τύπο των συναγερμών σε περίπτωση που κάτι συμβεί και ποια εργαλεία εντοπισμού και καταστολής θα τρέχουν ανά πάσα στιγμή στο σύστημα μας (Real-time protection) .
Τα εργαλεία αυτά είναι.

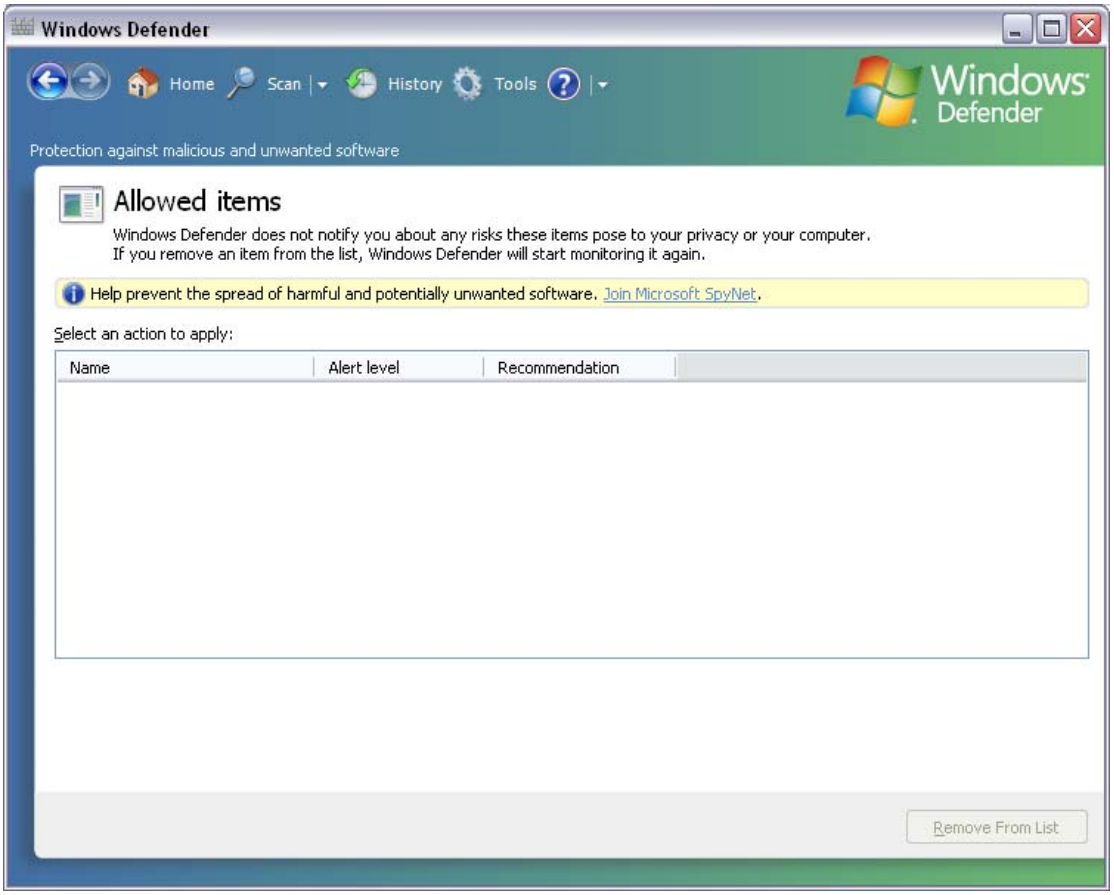
- *Auto Start* - Παρακολουθεί την λίστα των προγραμμάτων που τρέχουν όταν ξεκινάει το σύστημα.
- *System Configuration (settings)* – Παρακολουθεί τις ρυθμίσεις ασφάλειας των Windows .
- *Internet Explorer Add-ons* – Παρακολουθεί τα προγράμματα που τρέχουν όταν ανοίγεις τον Internet Explorer.
- *Internet Explorer Configurations (settings)* – Παρακολουθεί τις ρυθμίσεις ασφάλειας του browser.
- *Internet Explorer Downloads* – Παρακολουθεί αρχεία και προγράμματα που είναι σχεδιασμένα να συνεργάζονται με τον Internet Explorer.
- *Services and Drivers* – Παρακολουθεί υπηρεσίες και οδηγούς καθώς αλληλεπιδρούν με τα Windows και τα άλλα προγράμματα.
- *Application Execution* – Παρακολουθεί πότε ξεκινούν τα προγράμματα και τη εργασίες κάνουν ενώ δουλεύουν.
- *Application Registration* – Παρακολουθεί εργαλεία και αρχεία του λειτουργικού συστήματος που τα προγράμματα καταγράφουν για να τρέχουν ανά πάσα στιγμή.
- *Windows Add-ons* – Παρακολουθεί add-on προγράμματα των Windows (γνωστά και ως εφαρμογές λειτουργικού).

Τώρα ας εξετάσουμε τι άλλες επιλογές μας δίνει το Defender και τι εργαλεία μας προσφέρει. Πρώτα από όλα ας δούμε την επιλογή Software Explorer.



Μέσα από αυτό το εργαλείο μπορούμε να δούμε ποια προγράμματα τρέχουν στην έναρξη, ποια τρέχουν κατά την λειτουργία, ποια χρησιμοποιούν το δίκτυο, και υπηρεσίες που παρέχουν Winsock. Επίσης μας δίνει πληροφορίες για τον εκδότη του κάθε προγράμματος, την έκδοση, και τι άδειες πρόσβασης έχει.

Άλλο ένα εργαλείο είναι το Allowed Items, μέσω αυτού μπορούμε να ορίσουμε ποια προγράμματα εμπιστευόμαστε και δεν θέλουμε να παρακολουθούνται. Αν βγάλουμε κάποιο από την λίστα τότε αμέσως θα είναι υπό παρακολούθηση.



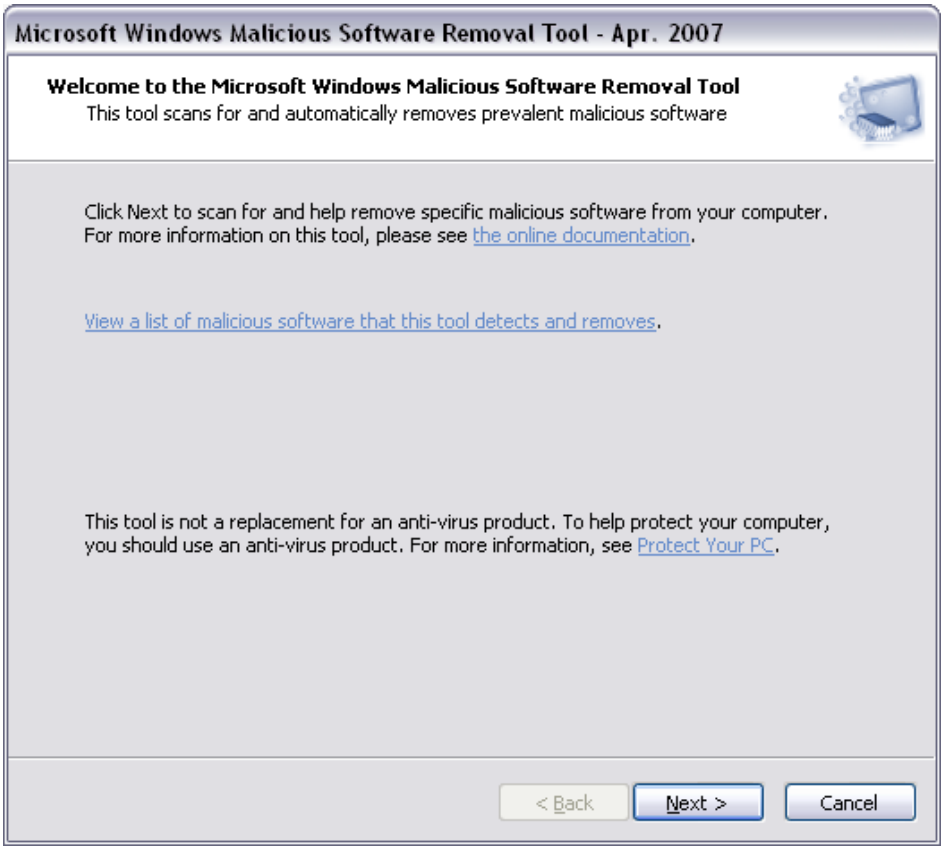
Windows Malicious Software Removal Tool

Γενικά

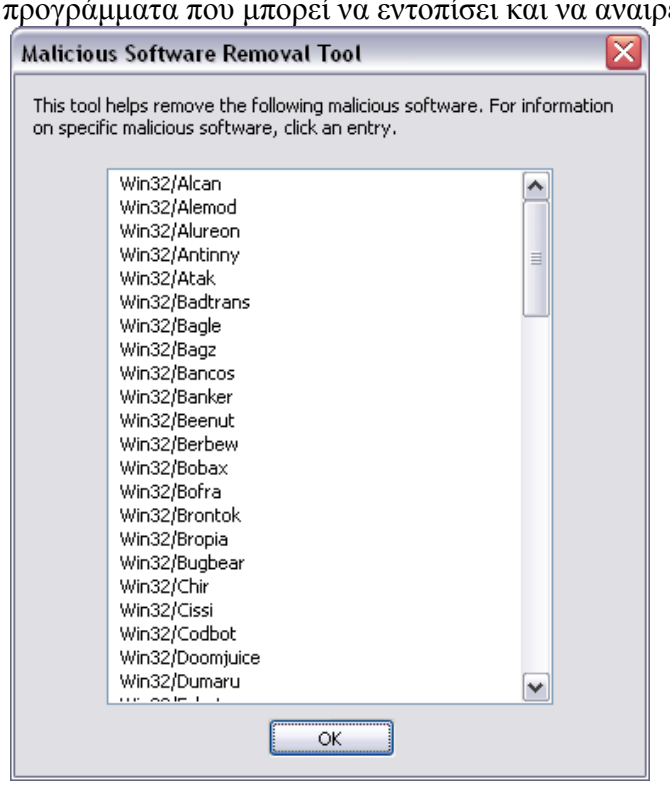
Το WMSRT είναι ένα εργαλείο ανεπτυγμένο από την Microsoft που διανέμεται δωρεάν. Κυκλοφόρησε τον Ιανουάριο του 2005, και αναβαθμίζεται κάθε δεύτερη Πέμπτη κάθε μήνα μέσω του Windows Update.
Το εργαλείο αυτό κυκλοφόρησε για απομάκρυνση ιών, δεν αντικαθιστά καθιερωμένα anti-virus εργαλεία όπως το Norton Antivirus και το McAfee Antivirus, αλλά είναι μια προσπάθεια της Microsoft να παρέχει ασφάλεια για ιούς στους χρήστες της. Επειδή το εργαλείο αυτό διανέμεται μέσω του internet, το έχουν προσέξει οι περισσότεροι χρήστες.
Το εργαλείο αυτό ελέγχει το σύστημα μας για μολύνσεις από συγκεκριμένα κακόβουλα προγράμματα, συμπεριλαμβανομένων των Blaster, Sasser και Mydoom, και τα αναιρεί. Όταν η διαδικασία εντοπισμού και αναίρεσης τελειώσει, μας παρουσιάζει μια αναφορά με τα αποτελέσματα της έρευνας.
Τέλος να πούμε ότι η έκδοση του WMSRT που διανέμεται μέσω του Windows Update τρέχει στο παρασκήνιο και αναφέρει αν βρει κάποια μόλυνση. Αν θέλει κάποιος να το τρέχει περισσότερες από μια φορά το μήνα, μπορεί να το κατεβάσει από το http://www.microsoft.com/downloads/details.aspx?FamilyID=ad724ae0-e72d-4f54-9ab3-75b8eb148356&displaylang=en

Λειτουργία

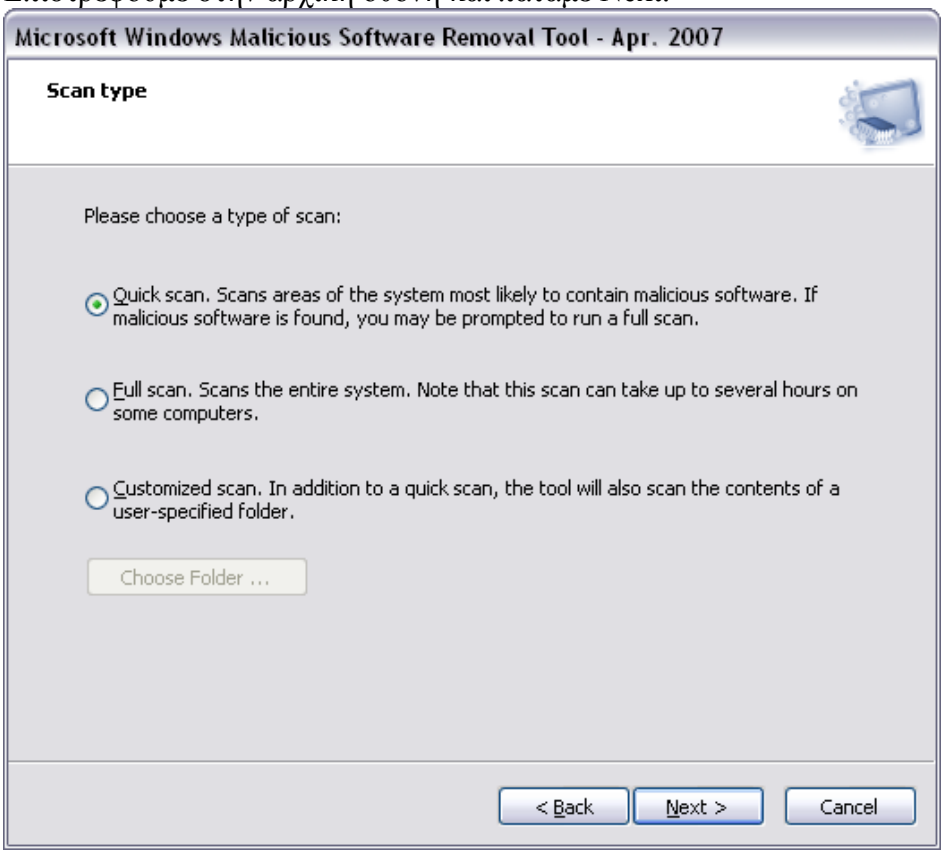
Αφού κατεβάσουμε το αρχείο που αναφέρουμε παραπάνω το τρέχουμε με διπλό κλίκ.



Βλέπουμε ότι μας λέει από την αρχή ότι δεν αντικαθιστά ένα anti-virus προϊόν. Επίσης μας δίνει την δυνατότητα να εξετάσουμε την λίστα με το κακόβουλα προγράμματα που μπορεί να εντοπίσει και να αναιρέσει.

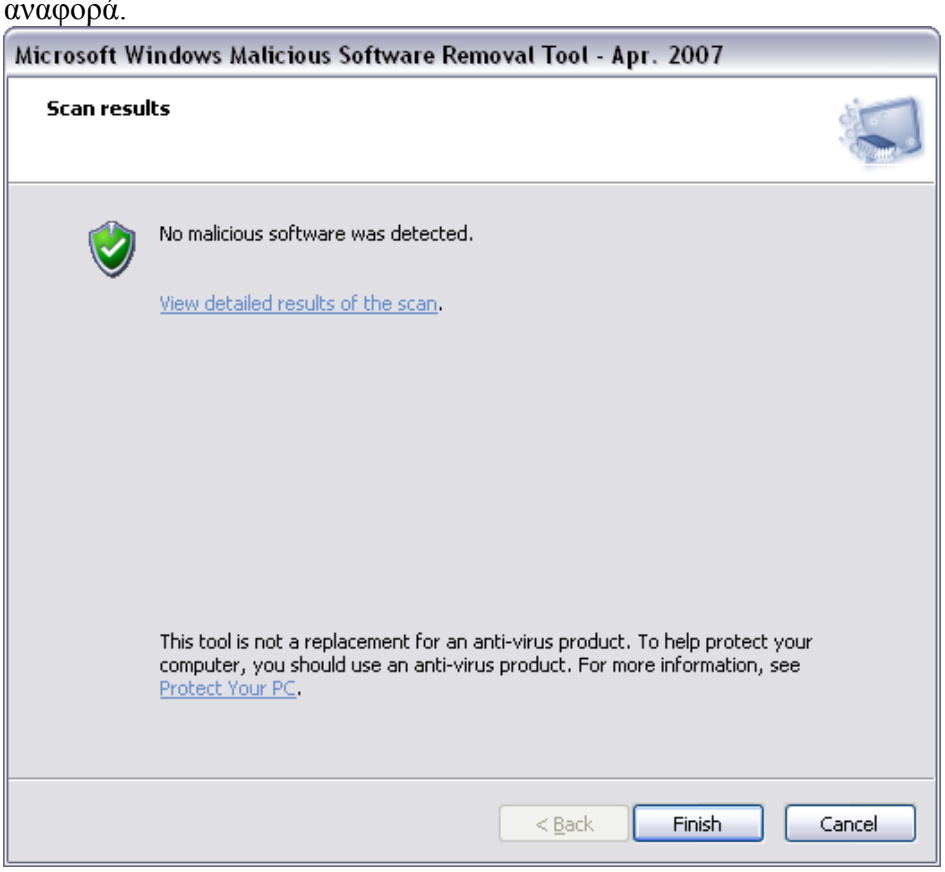


Τα ονόματα των οποίων λειτουργούν σαν links στο on-line λεξικό της Microsoft με πληροφορίες για το καθένα.
Επιστρέφουμε στην αρχική οθόνη και πατάμε Next.

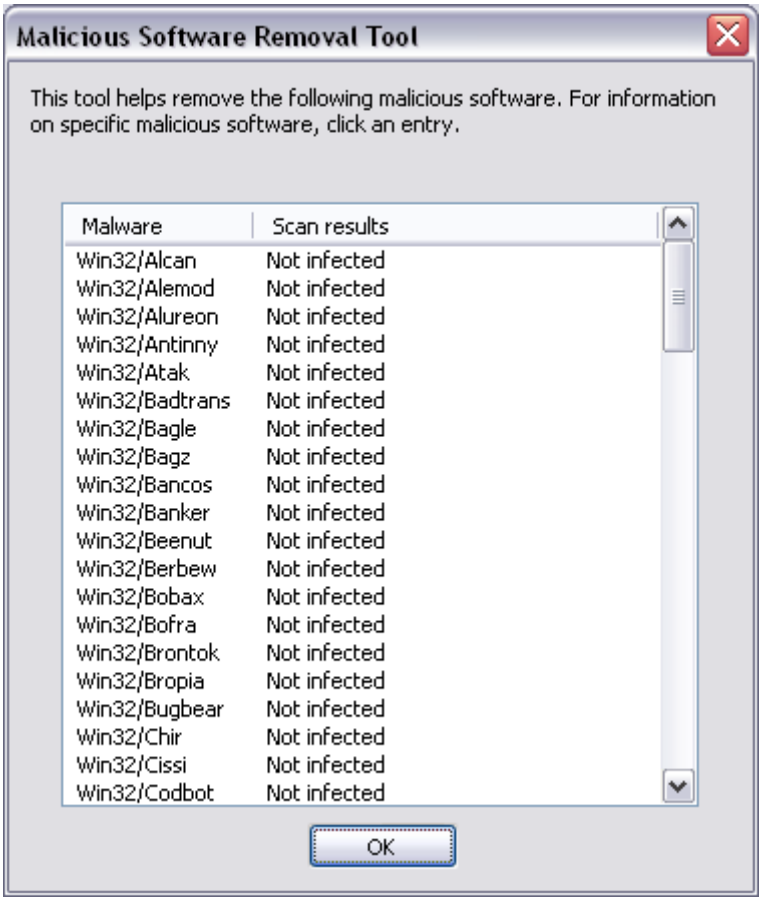


Βλέπουμε τις επιλογές αναζήτησης που έχουμε, γρήγορο, πλήρες, και την δυνατότητα να επιλέξουμε να γίνει αναζήτηση σε ένα συγκεκριμένο φάκελο.
Επιλέγουμε κάποιο και πατάμε Next.

Η διαδικασία αναζήτησης έχει ξεκινήσει και μόλις ολοκληρωθεί θα έχουμε την αναφορά.



Βλέπουμε ότι δεν εντοπίσθηκε καμία απειλή, και επιλέγοντας το View detailed results of the scan μπορούμε να δούμε αναλυτικά τα αποτελέσματα.



Windows Genuine Advantage

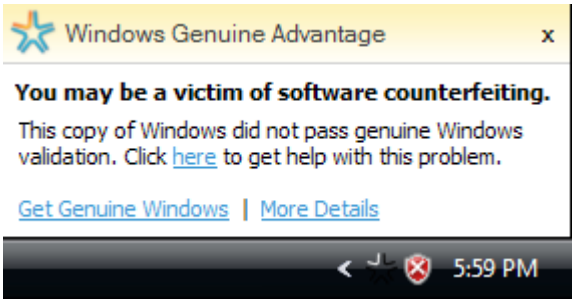
Γενικά

Το Windows Genuine Advantage (WGA) είναι ένα πρόγραμμα κατά της πειρατείας που ανέπτυξε η Microsoft που επιτρέπει στους χρήστες των XP να προσδιορίσουν την αυθεντικότητα του λειτουργικού τους συστήματος όταν χρησιμοποιούν διάφορες υπηρεσίες των Windows, όπως το Windows Update, και όταν κατεβάζουν από το Windows Download Centre. Αποτελεί μέρος του Service Pack 2 των Windows XP, ή μπορεί να κατεβάσει κανείς σε μορφή Update, από τον Ιούλιο του 2005 έγινε υποχρεωτικό για την χρήση των υπηρεσιών που αναφέραμε παραπάνω. Το πρόγραμμα αυτό εξελίχθηκε διότι στις περισσότερες χώρες λιγότερο από το 10% των Windows είναι γνήσια.

Λειτουργία

Όταν κάποιος εγκαταστήσει το WGA, εμφανίζεται ένα add-on του Internet Explorer που ονομάζεται Windows Genuine Advantage. Το πρόγραμμα αυτό χρησιμοποιεί είτε ένα αυτόνομο πρόγραμμα για να δημιουργήσει ένα κλειδί, είτε ένα ActiveX control για να ανακαλύψει αν το Licence Key είναι έγκυρο. Αν το WGA προσδιορίσει ότι κάποιο αντίγραφο δεν είναι γνήσιο και το CD εγκατάστασης είναι, τότε η Microsoft θα δώσει στον χρήστη ένα νέο CD. Αν όμως κάποιο σύστημα δεν περάσει τον έλεγχο του WGA δεν θα σταματήσει να λαμβάνει σημαντικά update ασφάλειας προς το παρόν και αυτό γιατί η Microsoft σκοπεύει να κάνει απαραίτητη την εγκατάσταση του για την λήψη updates.

Η Microsoft ξεκίνησε την παροχή του WGA τον Απρίλη του 2006 σαν critical update KB905474 στους χρήστες των Windows. Οι χρήστες με πειρατικά αντίτυπα άρχισαν να βλέπουν μηνύματα συναγερμού στην έναρξη, στο login και κατά την χρήση του λειτουργικού, ότι δεν έχουν γνήσιο αντίτυπο των XP.



Η τελευταία έκδοση του WGA έχει αλλαγμένη διαδικασία εγκατάστασης ώστε να ενημερώνει τον χρήστη για το τι κάνει το πρόγραμμα, και επίσης μπορεί να ρυθμιστεί ώστε να κάνει αυτόματα update σε νεότερη έκδοση. Ακόμα ενημερώνει τους χρήστες που έχουν ένα πειρατικό αντίτυπο γιατί η έκδοση των Windows τους φαίνεται ότι δεν είναι γνήσια.

Τα σημεία που ελέγχει το WGA είναι τα εξής:

- BIOS checksum
- MAC address
- Τον σειριακό αριθμό του σκληρού δίσκου
- Την έκδοση γλώσσας του λειτουργικού συστήματος
- Την έκδοση του λειτουργικού συστήματος
- Πληροφορίες για το BIOS του υπολογιστή (Κατασκευαστής, έκδοση, ημερομηνία)
- Τον κατασκευαστή του υπολογιστή
- Τις τοπικές ρυθμίσεις του χρήστη
- Τα αποτελέσματα της εγκατάστασης και της εξακρίβωσης
- Το κλειδί προϊόντος (product key) των Windows και Office
- Την ταυτότητα προϊόντος των Windows XP (product ID)

Η Microsoft συμπεριλαμβάνει την βιβλιοθήκη εξακρίβωσης του WGA και σε άλλα προϊόντα της, όπως το Windows Defender, τον Internet Explorer 7 και τον Windows Media Player 11 ώστε να εκτιμήσει την εγκατάσταση των Windows.

Προβλήματα

Το WGA έχει κατηγορηθεί ότι συμπεριφέρεται σαν spyware, επικοινωνώντας με την Microsoft σε καθημερινή βάση. Η Microsoft παραδέχτηκε το πρόβλημα, αλλά αρνήθηκε ότι η επικοινωνία ήταν τόσο συχνή ώστε να μοιάζει με spyware. Όμως μετά από πιέσεις ανακοίνωσε ότι στο μέλλον το πρόγραμμα θα επικοινωνεί μια φορά κάθε δύο εβδομάδες, αντί για κάθε μέρα. Επίσης έδωσε οδηγίες απεγκατάστασης για την έκδοση πιλότο του WGA.

Τέλος να αναφέρουμε ότι το WGA μπορεί να παρουσιάσει λανθασμένα αποτελέσματα, δηλαδή να χαρακτηρίσει ένα αυθεντικό αντίτυπο των Windows μη αυθεντικό. Αυτό συμβαίνει για διάφορους λόγους και για αυτό η Microsoft έχει δημιουργήσει ένα Forum για να βοηθάει τους χρήστες που έχουν προβλήματα.

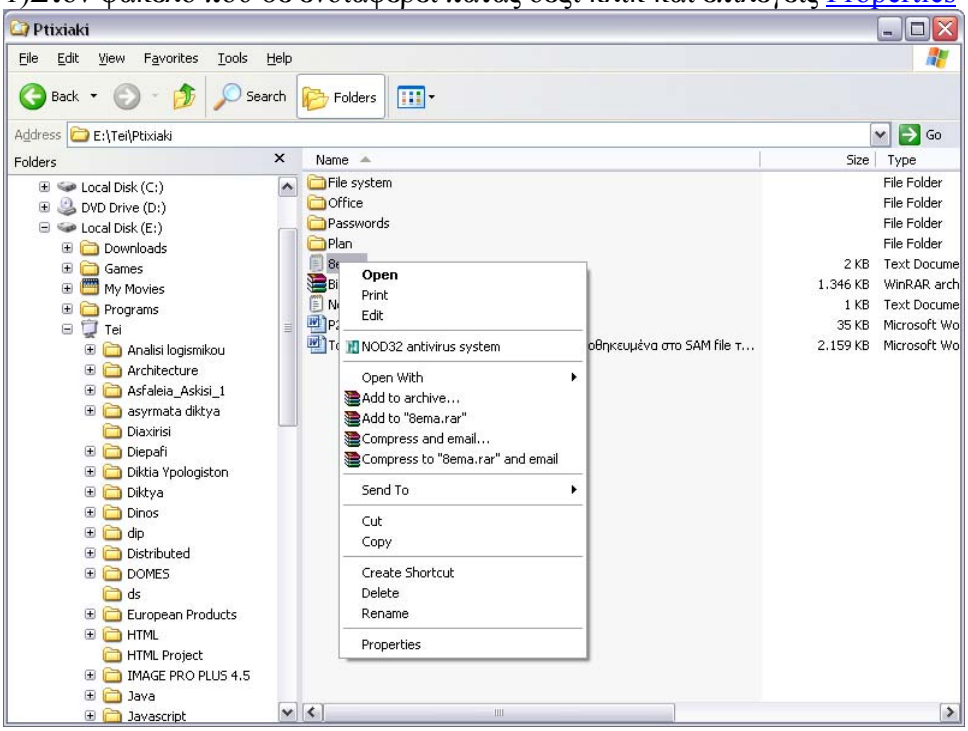
Windows Encrypted File System

Εισαγωγή

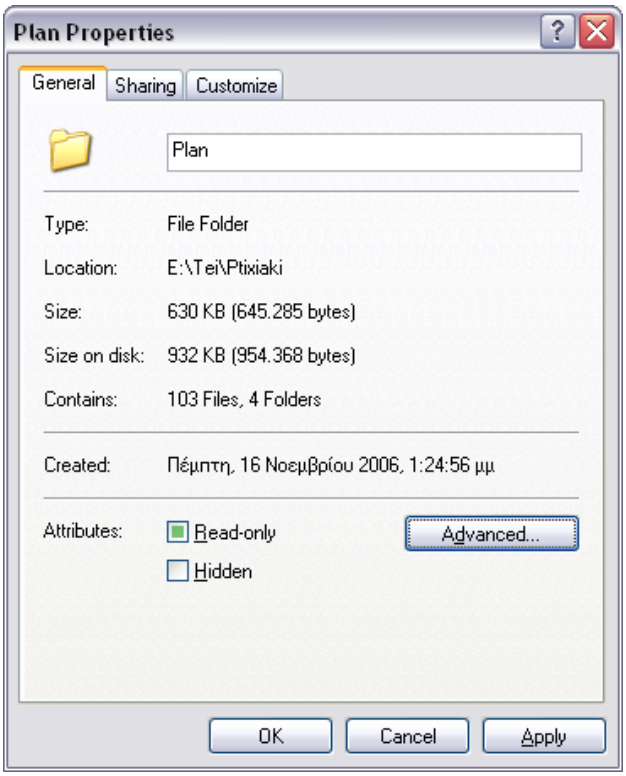
Το Encrypted File System (EFS) είναι ένα file system με filesystem-level encryption. Όπου filesystem-level encryption είναι μια μορφή κρυπτογράφησης δίσκου όπου ξεχωριστά αρχεία ή directories κρυπτογραφούνται από το file system , σε αντίθεση με την πλήρης κρυπτογράφηση δίσκου όπου ένα ολόκληρο partition ή δίσκος κρυπτογραφείτε όταν προστατεύουμε το file system.

Το EFS το συναντάμε από τα Windows 2000 και μετά, η τεχνολογία επιτρέπει αρχεία και φακέλους να αποθηκεύονται κρυπτογραφημένοι στο NTFS file system, ώστε να προστατευθούν δεδομένα από επιτιθέμενους με φυσική πρόσβαση στον υπολογιστή.
Ταυτοποίηση χρήστη και λίστες ελέγχου πρόσβασης μπορούν να προστατεύσουν αρχεία από μη εξουσιοδοτημένη πρόσβαση ένω το λειτουργικό σύστημα τρέχει, αλλά μπορούν εύκολα να τα παρακάμψουν αν αποκτήσουν φυσική πρόσβαση στο σύστημα. Μια λύση είναι να αποθηκεύεις τα αρχεία κρυπτογραφημένα στο δίσκο του υπολογιστή, Το EFS το κάνει αυτό χρησιμοποιώντας κρυπτογράφηση δημοσίου κλειδιού, και στοχεύει στο να σιγουρεύσει ότι το να αποκρυπτογραφήσεις τα αρχεία είναι πρακτικά αδύνατο χωρίς το σωστό κλειδί. Όμως το EFS δεν προστατεύει από brute-force επιθέσεις στο password του λογαριασμού του χρήστη, το συμπέρασμα είναι ότι το file encryption δεν προσφέρει και πολύ ασφάλεια αν το account password σπάει εύκολα.
Για να κλειδώσεις ένα φάκελο με την βοήθεια του EFS κάνεις το εξής:

1)Στον φάκελο που σε ενδιαφέρει πατάς δεξί κλικ και επιλέγεις Properties



2)Επειτα επιλέγεις Advanced

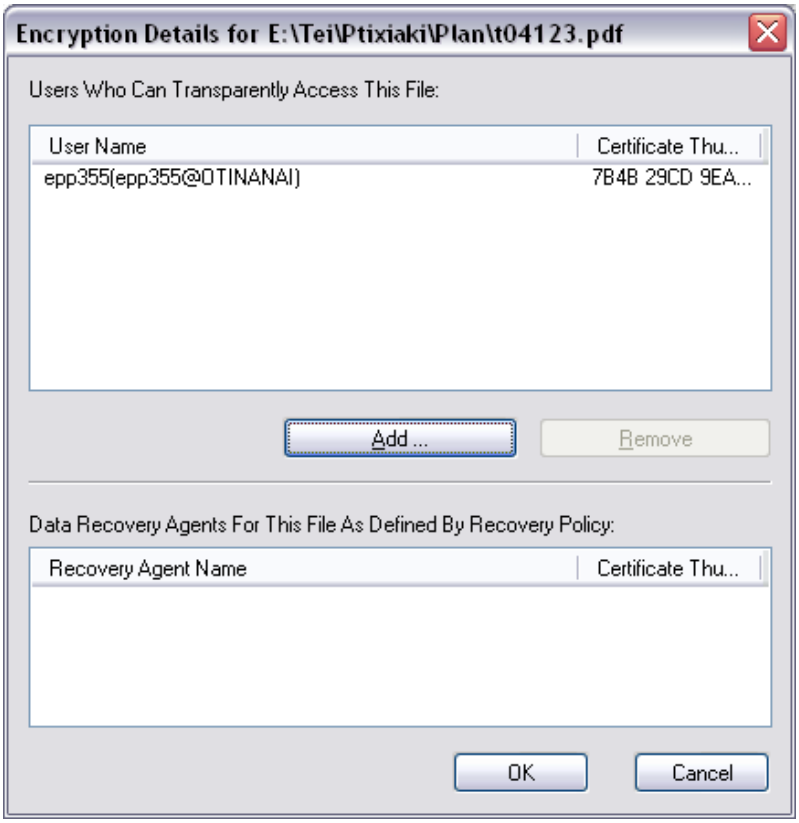


3)Και μετά στο παράθυρο που βγαίνει κλικάρεις την επιλογή Encrypt contents to secure data

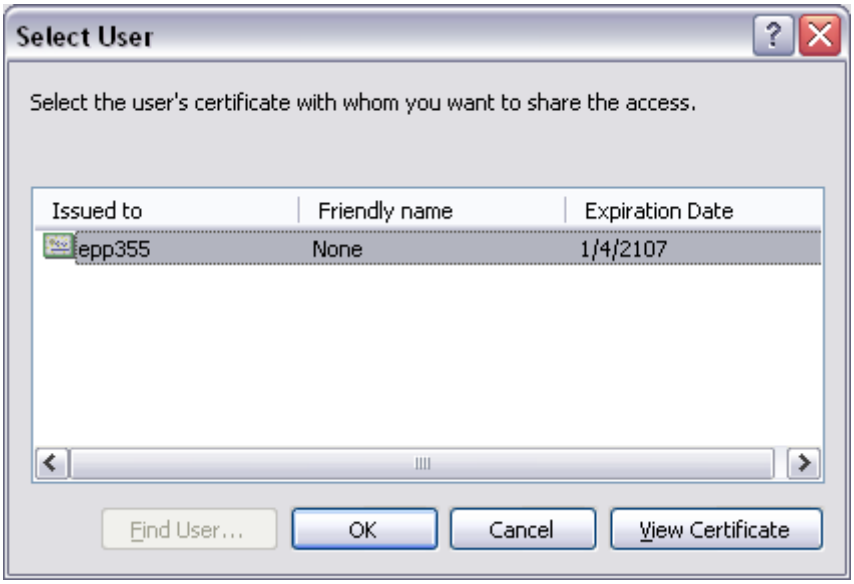
Αμέσως μετά θα σου ζητηθεί να επιλέξεις αν θέλεις να κρυπτογραφήσεις μόνο αυτό το αρχείο, ή όλο τον φάκελο που το περιέχει.

Στην συνέχεια θα δεις ότι το όνομα του φακέλου έχει πράσινο χρώμα.
Τώρα αν κάνεις Log-off και στην συνέχεια Log-on με άλλο account δεν μπορείς να κάνεις τίποτα σε αυτόν τον φάκελο.
Όμως μπορείς όταν έχεις κάνει encrypt ένα φάκελο να προσθέσεις και άλλους χρήστες που μπορούν να τον αλλάξουν. Επιλέγεις ξανά properties και στο advanced επιλέγεις Details

Στην συνέχεια ανοίγει ένα παράθυρο που σου δείχνει ποιοι χρήστες μπορούν να δούνε το αρχείο.

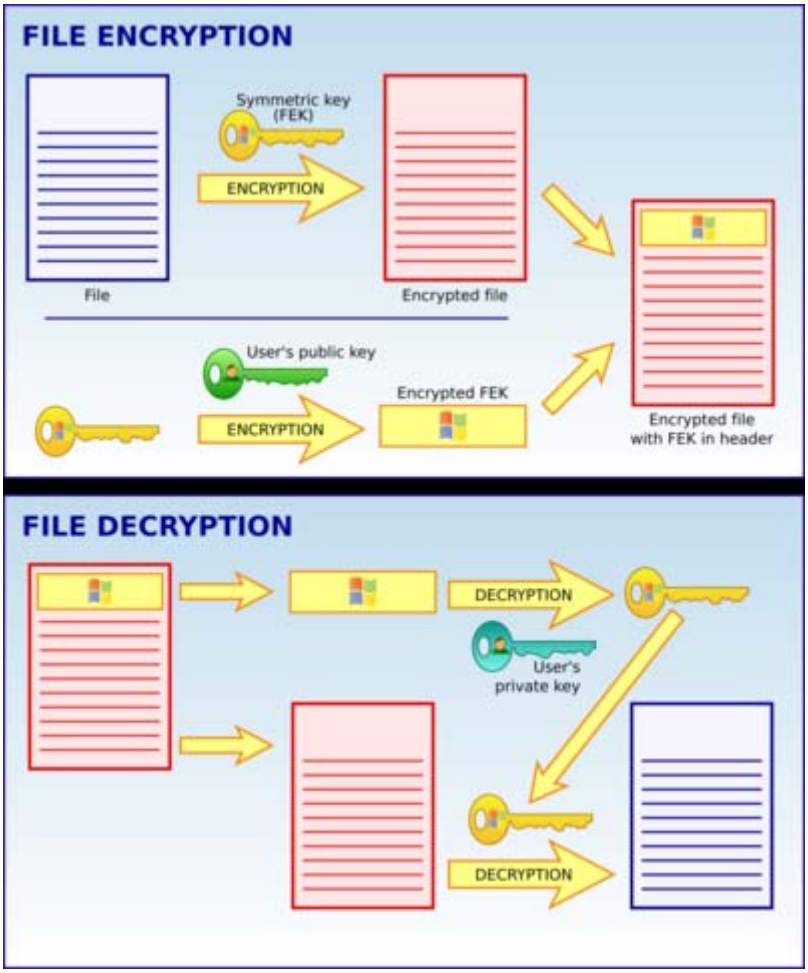


Επιλέγοντας add μπορείς να προσθέσεις και άλλους χρήστες, αρκεί να έχουν ψηφιακή ταυτότητα



Λειτουργία

Τα αρχεία και οι φάκελοι που είναι να κρυπτογραφηθούν από το file system πρέπει να σημαδευτούν με μια μεταβλητή κρυπτογράφησης. Όπως με τα permissions των φακέλων στο NTFS , εάν ένας φάκελος είναι σημαδεμένος για κρυπτογράφηση , τότε λόγω προεπιλογής όλοι οι υποφάκελοι και το περιεχόμενο τους θα κρυπτογραφηθούν. Όταν φάκελοι αντιγράφονται σε άλλον δίσκο που είναι Formatted με άλλο file system (π.χ. FAT32), τότε αποκρυπτογραφούνται πριν την αντιγραφή τους. Η μόνη εξαίρεση είναι όταν τους κάνουμε back-up, οπότε οι δεν αποκρυπτογραφούνται



Αυτό που κάνει το EFS είναι να κρυπτογραφεί τον φάκελο χρησιμοποιώντας ένα σκέτο συμμετρικό κλειδί (bulk symmetric key), που είναι επίσης γνωστό και σαν File Encryption Key (FEK), αυτό χρησιμοποιείται γιατί παίρνει ένα αρκετά μικρότερο χρονικό διάστημα να κρυπτογραφήσεις και να αποκρυπτογραφήσεις μεγάλες ποσότητες δεδομένων από ότι αν χρησιμοποιούσες έναν κρυπτοκώδικα ασύμμετρου κλειδιού. Το συμμετρικό κλειδί που χρησιμοποιείται για να κρυπτογραφήσουμε το αρχείο, στη συνεχεία κρυπτογραφείται και το ίδιο με την χρήση ενός δημόσιου κλειδιού που σχετίζεται με τον χρήστη που κρυπτογράφησε το αρχείο, και αυτό το κρυπτογραφημένο κλειδί αποθηκεύεται στην επικεφαλίδα του κρυπτογραφημένου

αρχείου. Για να αποκρυπτογραφήσουμε το αρχείο το file system χρησιμοποιεί το προσωπικό κλειδί του χρήστη για να αποκρυπτογραφήσει το συμμετρικό κλειδί που είναι αποθηκευμένο στην επικεφαλίδα του αρχείου. Έπειτα παίρνει το συμμετρικό κλειδί και το χρησιμοποιεί για να αποκρυπτογραφήσει το αρχείο. Επειδή αυτό γίνεται στο επίπεδο του File system ,η διαδικασία δεν γίνεται αντιληπτή από τον χρήστη.

Από τα Windows Vista το προσωπικό κλειδί ενός χρήστη μπορεί να αποθηκευτεί και σε μια smart card. Επίσης τα recovery keys του Windows Domain μπορούν και αυτά να αποθηκευτούν στην smart card του administrator

Ασφάλεια

Υπάρχουν δύο σημαντικά προβλήματα ασφάλειας στο EFS των Windows 2000

-Αποκρυπτογράφηση αρχείων με την χρήση του Administrator Login :
Στα Windows 2000, ο administrator είναι ο προεπιλεγμένος υπεύθυνος ανάκτησης, ικανός να αποκρυπτογραφήσει όλους τους φακέλους που έχει κλειδώσει το EFS. Τα Win2k δεν μπορούν να λειτουργήσουν χωρίς έναν υπεύθυνο ανάκτησης, άρα υπάρχει πάντα κάποιος που μπορεί να αποκρυπτογραφήσει τα αρχεία όλων των χρηστών. Από τα WinXP και μετά δεν υπάρχει προεπιλεγμένος υπεύθυνος ανάκτησης και δεν χρειάζεται να υπάρχει. Θέτοντας το Syskey σε mode2 ή παραπάνω (Syskey που πληκτρολογούμε κατά την εκκίνηση ή το αποθηκεύουμε σε δισκέττα) θα αποτρέψουμε την επίθεση, γιατί τα ιδιωτικά κλειδιά θα είναι αποθηκεμένα σε ένα κρυπτογραφημένο SAM φάκελο που ο επιτιθέμενος δεν μπορεί να αποκρυπτογραφήσει γιατί δεν ξέρει το Syskey passphrase/keyfile.

-Resseting των δεδομένων των ιδιωτικών κλειδιών
Στα Win2k το ιδιωτικό κλειδί εν είναι αποθηκεμένο σε μια πραγματικά κρυπτογραφημένη μορφή. Εάν ένας επιτιθέμενος μπορεί να αποκτήσει φυσική πρόσβαση σε ένα σύστημα και κάνει reset τα passphrases ενός χρήστη , μπορεί να κάνει μπει σαν αυτόν τον χρήστη και να αποκτήσει πρόσβαση στο ιδιωτικό κλειδί του και να αποκρυπτογραφήσει όλους τους φακέλους. Από τα WinXP και έπειτα το ιδιωτικό κλειδί κρυπτογραφείται με την χρήση του hash της passphrase του χρήστη και το user name, έτσι είναι αδύνατο να ανακτήσεις το ιδιωτικό κλειδί χωρίς να ξέρεις το passphrase του χρήστη. Επίσης πάλι θέτοντας το Syskey σε mode2 ή παραπάνω (Syskey που πληκτρολογούμε κατά την εκκίνηση ή το αποθηκεύουμε σε δισκέττα) θα αποτρέψουμε την επίθεση, γιατί τα ιδιωτικά κλειδιά θα είναι αποθηκεμένα σε ένα κρυπτογραφημένο SAM φάκελο που ο επιτιθέμενος δεν μπορεί να αποκρυπτογραφήσει γιατί δεν ξέρει το Syskey passphrase/keyfile.

Σχετικά θέματα

Τα Windows μπορούν να αποθηκεύουν παραλλαγές απλού κειμένου των password των χρηστών, επίσης αποθηκεύουν από προεπιλογή τα LM hash των password τα οποία ένας επιτιθέμενος μπορεί να σπάσει σχετικά εύκολα. Ακόμα αποθηκεύει τα NTLM Hash των password, τα οποία πάλι μπορούν να σπάσουν με τις μεθόδους που είδαμε παραπάνω. Για να αποτρέψουμε αυτές τις επιθέσεις πρέπει να ρυθμίσουμε τα Windows (από το Security policy) να μην αποθηκεύουν ποτέ ή να στέλνουν τα LM/NTLM hashes ή παραλλαγές απλού κειμένου των password, και οπωσδήποτε να απενεργοποιήσουμε το automatic login (Γιατί αποθηκεύονται τα password στην registry). Επίσης τα να χρησιμοποιούμαι password πάνω από 14 χαρακτήρες αποτρέπει την καταγραφή του LM hash και κάνει τις επιθέσεις στο NTLM hash πιο δύσκολες. Φυσικά αν λάβουμε υπόψη μας ότι το EFS χρησιμοποιεί Triple DES ή AES για να κρυπτογραφήσει τους φακέλους , πρέπει να έχουμε password με σωστό μέγεθος (πάνω από 20 χαρακτήρες) .

Όταν κρυπτογραφούμαι φακέλους με το EFS, τα αρχεία απλού κειμένου δεν καταστρέφονται απλά σβήνονται, αυτό σημαίνει ότι μπορούν εύκολα να ανακτηθούν εκτός αν έχουν γραφτεί από πάνω. Για να χρησιμοποιήσουμε σωστά το EFS ,πρέπει να σημαδεύουμε ολόκληρους φακέλους για κρυπτογράφηση (έτσι ώστε όλα τα προσωρινά αρχεία σαν τα backup του Word θα κρυπτογραφούνται), και όταν θέλεις να κρυπτογραφήσεις συγκεκριμένα αρχεία, αντέγραψε τα σε ένα φάκελο, και μετά κατάστρεψε τις παραλλαγές απλού κειμένου. Μπορείς να χρησιμοποιήσεις το Windows Cipher Utility για να καταστρέψεις αρχεία με ασφάλεια.

Οποιοσδήποτε με προνόμια administrator μπορεί να κάνει τον εαυτό του υπεύθυνο ανάκτησης. Αυτό είναι ένα πολύ σοβαρό θέμα, αφού ένας επιτιθέμενος μπορεί απλά να σπάσει το administrator account (όπως είδαμε παραπάνω), να κάνει τον administrator υπεύθυνος ανάκτησης και να περιμένει. Όταν οι χρήστες μπουν στο σύστημα το ιδιωτικά τους κλειδιά αυτόματα θα κρυπτογραφηθούν στο δημόσιο κλειδί του admin. Ο επιτιθέμενος πρέπει μόνο να χρησιμοποιήσει το σύστημα άλλη μια φορά σαν administrator για να αποκτήσει full πρόσβαση σε όλους τους EFS – κρυπτογραφημένους φακέλους. Ακόμα και αν χρησιμοποιήσουμε SYSKEY mode2 ή 3 δεν μας προστατεύει από την επίθεση, γιατί ο επιτιθέμενος μπορεί να προσπεράσει το SYSKEY και να αποκτήσει πρόσβαση admin και να δημιουργήσει καινούργια κλειδιά για admin, να επαναφέρει το SYSKEY σε λειτουργία και να περιμένει τους χρήστες να μπουν στο σύστημα. Βέβαια αν ο επιτιθέμενος μπορεί να έχει φυσική πρόσβαση στο σύστημα όλα τα χαρακτηριστικά ασφάλειας είναι αδιάφορα γιατί μπορεί να εγκαταστήσει rootkits, software ή ακόμα hardware keyloggers .

Ανάκτηση

Οι φάκελοι που κρυπτογραφούνται με το EFS μπορούν να ανακτηθούν μόνο με τα κλειδιά κρυπτογράφησης, που είναι με την σειρά τους κρυπτογραφημένα με το login password. Το να ανοίξεις κρυπτογραφημένους φακέλους έξω από περιβάλλον Windows π.χ. Linux είναι αδύνατο. Επίσης το να χρησιμοποιήσεις ειδικά εργαλεία για να κάνεις reset το login password καθιστά κάθε κρυπτογραφημένο φάκελο για αυτό το login άχρηστο.

Ασφαλείς διαμόρφωση (Hardening Windows)

Υπηρεσίες των Windows

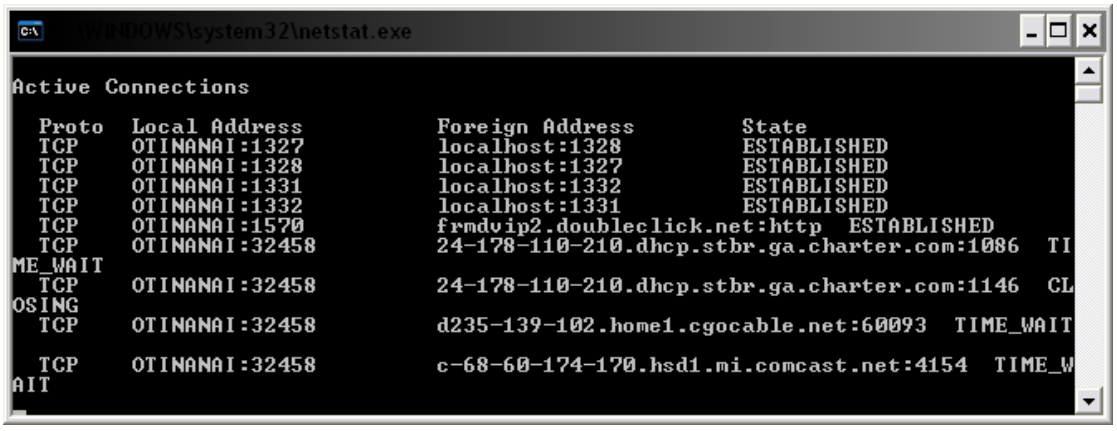
Εισαγωγή

Σε αυτή την ενότητα θα πάρουμε ένα σύστημα με φορτωμένα πάνω τα WinXP με SP2 και τίποτα άλλο από software, ώστε να δούμε ποιες υπηρεσίες τρέχουν by default. Οι περισσότερες από αυτές δεν χρειάζονται, και πολλές φορές είναι και επικίνδυνες σε μηχανήματα που είναι συνδεμένα στο internet. Η by default ενεργοποίηση τους είναι μια μικρή επιβάρυνση για τους διαχειριστές, που πρέπει να απενεργοποιήσουν ότι δεν χρειάζονται, και μεγάλη πηγή προβλημάτων για home users, που δεν γνωρίζουν τι υπηρεσίες χρειάζονται, ή πώς να θωρακίσουν τα συστήματα τους απενεργοποιώντας τι επικίνδυνες.

Το Service pack 2 απενεργοποιεί μερικές υπηρεσίες που σχετίζονται με την δικτύωση και δεν έχουν απενεργοποιηθεί, που είναι σίγουρα μια βελτίωση. Δυστυχώς όμως πολλές υπηρεσίες παραμένουν, κάτι πολύ ζημιογόνο για τους home users.

Υπηρεσίες

Σύμφωνα με το εργαλείο netstat,



στο μηχάνημα μας οι ακόλουθες υπηρεσίες ακούνε στο internet από προεπιλογή:

- DCE endpoint resolution (epmap), port 135. Αυτή είναι βασικά η UNIX/BSD/Linux υπηρεσία χαρτογράφησης port (portmap daemon), άχρηστη στα μηχανήματα σπιτιών.

- NetBIOS name service, port 137. Αυτή είναι WINS (Windows Internet Naming Service) server για ένα NetBIOS δίκτυο, άχρηστη στα μηχανήματα σπιτιών.

- NetBIOS datagram service, port 138. Αυτή χρησιμοποιείται από την SMB (Server Message Block) υπηρεσία αναζήτησης, άχρηστη στα μηχανήματα σπιτιών.

- Microsoft-ds (Server Message Block), port 445. Το SMB μπορεί να τρέχει απευθείας πάνω από TCP/IP, χωρίς το NetBT χρησιμοποιώντας αυτήν την υπηρεσία, άχρηστη στα μηχανήματα σπιτιών.

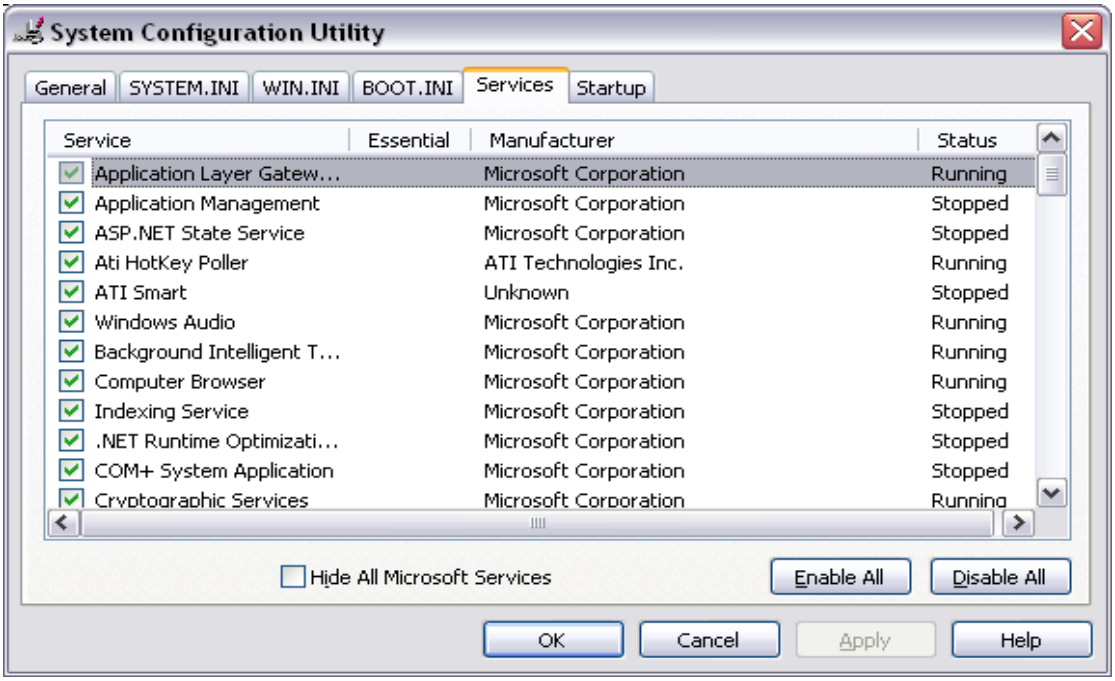
- NetBios Session, port 139. Αυτή χρησιμοποιείται για την κοινή χρήση φακέλων και εκτυπωτών, άχρηστη στα περισσότερα μηχανήματα σπιτιών, και εξαιρετικά επικίνδυνη σε οποιοδήποτε μηχάνημα με σύνδεση στο δίκτυο έκτος αν ο χρήστης ξέρει πώς να την τρέχει με ασφάλεια.

- Η αναφορά σφαλμάτων είναι ενεργοποιημένη από προεπιλογή. Όμως δεν υπάρχει λόγος για να επικοινωνεί με τον κατασκευαστή ένα μηχάνημα όποτε κάνει σφάλμα. Καλύτερα να απενεργοποιηθεί.

- Οι αυτόματες αναβαθμίσεις (Automatic Updates) είναι απενεργοποιημένες από προεπιλογή. Η υπηρεσία αυτή καλύτερα να μείνει κλειστή και οι χρήστες να επιλέγουν οι ίδιοι τις αναβαθμίσεις που θέλουν, ώστε να επιλέγουν ποιες χρειάζονται και τι επιλογές τους προσφέρουν.

Στη συνέχεια θα κοιτάξουμε το παράθυρο υπηρεσιών ώστε να δούμε ποιες δεν χρειάζονται και τι ρυθμίσεις έχουν (Σημείωση: ¨υποκινουμένη¨ σημαίνει ότι ξεκινάει αν υποκινηθεί από τον χρήστη, από μια εφαρμογή, ή μια άλλη υπηρεσία, ενώ ¨αυτόματη¨ ότι θα ξεκινήσει με την εκκίνηση του υπολογιστή άσχετα αν χρειάζεται ή όχι).

Το παράθυρό επιλογής βγαίνει αν στο Run πληκτρολογήσουμε msconfig και επιλέξουμε το tab Services.



ClipBook (χρησιμοποιείται για να αποθηκεύσει πληροφορίες, αποκοπή/επικόλληση, και κοινή χρήση με άλλους υπολογιστές) απενεργοποιημένο.

DCOM Server Process Launcher, αυτόματη. Ο εκτελεστής υπηρεσιών εννοεί ότι το DCOM τρέχει (περισσότερα παρακάτω).

DHCP Client, αυτόματη. Δεν χρειάζεται στα περισσότερα μηχανήματα σπιτιών. Θα πρέπει να απενεργοποιηθεί, έκτος αν έχουμε ADSL σύνδεση με LAN Router.

DNS Client, αυτόματη. Ισχύουν τα ίδια με το DHCP Client.

NetMeeting Remote Desktop sharing, υποκινουμένη. Δεν χρειάζεται στα περισσότερα μηχανήματα σπιτιών, απενεργοποιημένο από προεπιλογή.

Network DDE, απενεργοποιημένο.

Network DDE DSDM, απενεργοποιημένο.

Remote Access Connection Manager, υποκινουμένη. Δεν χρειάζεται στα περισσότερα μηχανήματα σπιτιών, θα πρέπει να είναι απενεργοποιημένο.

Remote Desktop Help Session Manager, υποκινουμένη. Δεν χρειάζεται στα περισσότερα μηχανήματα σπιτιών, θα πρέπει να είναι απενεργοποιημένο.

Remote procedure call (RCP), αυτόματη. Αυτό είναι μια από τις μεγαλύτερες τρύπες ασφάλειας . Το RCP επιτρέπει σε ένα μηχάνημα να εκτελεί κώδικα απομακρυσμένα σ ένα άλλο. Στα UBIX/BSD/Linux, ,μπορεί να απενεργοποιηθεί με ασφάλεια. Στα Windows δεν απενεργοποιείται γιατί μια πληθώρα υπηρεσιών το χρειάζεται. Πρέπει να μπλοκάριστει με ένα Firewall.

Remote Registry, αυτόματη (επιτρέπει σε χρήστες να κάνουν αλλαγές στην Registry απομακρυσμένα).Άχρηστη και επικίνδυνη στα περισσότερα μηχανήματα σπιτιών, θα πρέπει να είναι απενεργοποιημένο και να ενεργοποιείται μόνο όταν χρειάζεται.

Routing and Remote Access, απενεργοποιημένη.

Secondary Logon, αυτόματη (επιτρέπει να ξεκινάν διεργασίες κάτω από εναλλακτικά διαπιστευτήρια). Δεν χρειάζεται στα περισσότερα μηχανήματα σπιτιών, θα πρέπει να είναι απενεργοποιημένο.

SSDP Disovery Service (UPnP discovery), υποκινουμένη. Δεν χρειάζεται στα περισσότερα μηχανήματα σπιτιών, θα πρέπει να είναι απενεργοποιημένο.

TCP/IP NetBIOS Helper, αυτόματη (επιτρέπει υποστήριξη για NetBIOS πάνω από TCP/IP (NetBT) υπηρεσίες και NetBIOS ανάλυση ονομάτων). Δεν χρειάζεται στα περισσότερα μηχανήματα σπιτιών, θα πρέπει να είναι απενεργοποιημένο.

Telnet, υποκινουμένη. Δεν χρειάζεται στα περισσότερα μηχανήματα σπιτιών, θα πρέπει να είναι απενεργοποιημένο. Όσοι θέλουν να το χρησιμοποιήσουν ας το ενεργοποιήσουν.

Universal Plug and Play Device Host, υποκινούμενη. Δεν χρειάζεται στα περισσότερα μηχανήματα σπιτιών, θα πρέπει να είναι απενεργοποιημένο.

WebClient, αυτόματη (επιτρέπει σε προγράμματα των Windows να δημιουργούν, να έχουν πρόσβαση, και να αλλάζουν αρχεία δικτύου). Δεν χρειάζεται στα περισσότερα μηχανήματα σπιτιών, θα πρέπει να είναι απενεργοποιημένο.

Τέλος να πούμε ότι η DCOM (Distributed COM) είναι ενεργοποιημένη από προεπιλογή ενώ δεν χρειάζεται στα περισσότερα μηχανήματα σπιτιών, και θα πρέπει να απενεργοποιείται έκτος αν την χρειαζόμαστε. Είναι η υπηρεσία που εκμεταλλεύτηκε το Blaster Worm για να πάρει μια RPC.

Secure Service on Windows XP

Εισαγωγή

Σε αυτήν την ενότητα θα δούμε τι πρέπει να κάνει κανείς προκειμένου να τρέξει μια secure service που πρέπει να κοιτάει συνέχεια στο internet, π.χ. έναν web server. Για το παράδειγμα μας θα εγκαταστήσουμε έναν web server και θα δούμε μια προς μια τις ενέργειες που πρέπει να γίνουν ώστε να μην απειλείται το σύστημα μας από επιθέσεις, μια καλή ιδέα είναι να κάνουμε ένα backup των Windows πρώτα, ώστε σε περίπτωση λάθους να ελαχιστοποιήσουμε την ζημία.

Τι πρέπει να γίνει

Ας δούμε τι πρέπει να κάνουμε ώστε να ασφαλίσουμε το σύστημα μας βήμα προς βήμα. Για όλες τις ρυθμίσεις που αναφέρονται στα παρακάτω βήματα, καθώς και αναλυτικές οδηγίες για το που βρίσκονται αυτές οι ρυθμίσεις θα βρείτε στο **http://www.gregthatcher.com/** .

1. **Να βεβαιωθούμε ότι τα Automatic Updates είναι ενεργοποιημένα να κάνουν αυτόματη εγκατάσταση.**
   Αυτό το κάνουμε για να βεβαιωθούμε ότι θα έχουμε στο σύστημα μας όλα τα Critical updates και τα Service packs. Οι περισσότερες επιθέσεις γίνονται σε συστήματα που δεν έχουν τα πιο καινούργια updates εγκατεστημένα.

2. **Απενεργοποιούμε και παρακολουθούμε τα παρακάτω αρχεία: ftp.exe, tftp.exe, command.com, cmd.exe, telnet.exe, wscript.exe, και cscript.exe.**
   Αυτό που επιδιώκει κάποιος ώστε να επιτεθεί είναι να τρέξει στο μηχάνημα σου τον κώδικα του. Τα παραπάνω αρχεία μπορούν να χρησιμοποιηθούν για να εγκαταστήσει κάποιος κάτι ή και να το τρέξει.
   Απενεργοποιώντας αυτά τα αρχεία γλιτώνεις από τις επιθέσεις, και παρακολουθώντας τα βλέπεις τις δραστηριότητες του επιτιθέμενου στο Event Viewer ώστε να εντοπίζεις τις επιθέσεις.

   Όμως δεν πρέπει να ξεχνάμε ότι όταν κάνουμε updates να τους ενεργοποιούμε γιατί ορισμένες βελτιώσεις γράφουν σε αυτούς. Επίσης κάποια προγράμματα εγκατάστασης και κάποια development tools απαιτούν πρόσβασή στο cmd.exe, άρα το ενεργοποιούμε σε τέτοιες περιπτώσεις.

3. **Αλλάζουμε το όνομα του Administrator Account και απενεργοποιούμε τον Guest Account.**

Από προεπιλογή τα Windows δημιουργούν δυο accounts που αναζητούν οι επιτιθέμενοι στον υπολογιστή, τον Guest και τον Administrator. Αν το σύστημα σου είναι μέλος ενός domain αυτό πρέπει να κάνεις και στο σύστημα σου και στο Active Directory.

4. **Χρησιμοποιούμε δυνατά Account Policies**

Ο ευκολότερος τρόπος να μπει κάποιος στο δίκτυο σου είναι μέσω αδύναμων password και account policies. Χρησιμοποιώντας το "Local Security Settings" θα πρέπει να επιλέξεις τα παρακάτω.

Password Policies

- Enforce password history: 24 passwords remembered.
- Maximum password age: 42 μέρες.
- Minimum password age: 2 μέρες.
- Minimum password length: 8 χαρακτήρες.
- Τα password πρέπει να πληρούν τους κανόνες πολυπλοκότητας.
- Απενεργοποιούμε την αποθήκευση password χρησιμοποιώντας αναστρέψιμη κρυπτογράφηση (reversible encryption).

Account policies

- Account lockout duration: 60 λεπτά.
- Account lockout threshold: 3 αποτυχημένες προσπάθειες.
- Reset account lockout counter after: 60 λεπτά.

5. **Παρακολουθούμε το σύστημα μας.**

Αυτό το κάνουμε χρησιμοποιώντας εργαλεία που έχουν τα Windows.

Event viewer - - Security Log: Τα Windows XP έχουν ένα εργαλείο που λέγεται Event Viewer (Βρίσκεται στο Programs – Administrate tools). Αυτό το εργαλείο κρατάει ένα Log με τις διεργασίες, τις ενέργειες συστήματος, και τα γεγονότα συστήματος και ασφάλειας. Πρέπει όμως να ενεργοποιήσουμε το Security Auditing εμείς.

Είναι καλύτερα αν κάνουμε τις ακόλουθες ρυθμίσεις μέσω του "Local Security Policy" ή του "Active Directory Group Policy" αν είμαστε μέλος domain.

- Audit account logon events: Failure
- Audit account management: Success/Failure
- Audit logon events: Failure
- Audit object Access: Failure
- Audit policy change: Success/Failure
- Audit privilege use: Failure
- Audit system events: Success/Failure

Είναι πολύ σημαντικό περιοδικά να ανανεώνουμε το **Event Viewer Security log.** Επίσης πρέπει να κρατάμε όλα τα Log αρχεία και να επιλέξουμε στα Event Logs να μην σβήνουν εγγραφές.

Τέλος μπορούμε να χρησιμοποιούμε και τα Log files της υπηρεσίας που έχουμε εγκαταστήσει.

6. Απενεργοποιούμε υπηρεσίες και drivers που δεν χρειάζονται

- **Απενεργοποιούμε το ftp service**:
  Το ftp στέλνει τα password σε μορφή cleartext, αυτό το κάνει εύκολο για να έναν επιτιθέμενο να τα αποκτήσει.
- **Απενεργοποιούμε το SNMP**:
  Πρόσφατα βρέθηκαν πολλά αδύναμα σημεία στην λειτουργία του SNMP. Επίσης κάποιος μπορεί να πάρει πληροφορίες για το σύστημα μας χρησιμοποιώντας το Public Community String που τρέχει το SNMP
- **Απενεργοποιούμε την υπηρεσία περιεχομένων (Indexing Service)**:
  Αυτή επιτρέπει σε εμάς (και στους επιτιθέμενους) να βρίσκουμε αρχεία και φακέλους γρήγορα. Αν ο web server μας δεν χρησιμοποιεί αυτήν την υπηρεσία για να κάνει Site Search στο website μας, είναι καλύτερα να την απενεργοποιήσουμε.
- **Απενεργοποιούμε τις απλές υπηρεσίες TCP/IP:**
  Αυτές οι υπηρεσίες εγκαθιστούνται από προεπιλογή και πολλοί Admins τις αφήνουν γιατί περιλαμβάνουν αστείες εφαρμογές, όπως το ρητό της μέρας και άλλα. Όμως είναι και οι αγαπημένοι στόχοι ενός επιτιθέμενου.
- **Απενεργοποιούμε τον Network Monitor Driver:**
  Αυτός ο driver χρησιμοποιείται από το Network Monitor και από το SMS για να αναλύει την κίνηση στο μηχάνημα μας.

7. Default WinXP Installation Directories

Πολλοί επιτιθέμενοι βασίζονται στο προεπιλεγμένο file system των windows για να επιτεθούν. Ξέρουν π.χ. ότι σβήσουν τους φακέλους και τα αρχεία στον C δίσκο, πρέπει να τρέξουν την ακόλουθη εντολή: **..\..\windows\system32\cmd.exe /C del c:*.***

Για αυτό όταν εγκαθιστούμε οτιδήποτε στο μηχάνημα μας πρέπει να αλλάζουμε τα προεπιλεγμένα directory με δικά μας. Το ίδιο ισχύει και για τα windows, δηλαδή αντί να τα εγκαταστήσουμε στο c:\windows ή στο c:\winnt να τα εγκαταστήσουμε στο c:\winxpKourosDir.

8. Ενεργοποιούμε την παρακολούθηση στα Web και Ftp directories για άδεια εγγραφής, μετατροπής, και διαγραφής.

Αυτό το κάνουμε με τα εξής δύο βήματα

A. Ενεργοποιούμε το “Audit object access” στο “Local Security Settings” ή στο “Group Policy”.

B. Ενεργοποιούμε την παρακολούθηση για φακέλους και directories.

Αυτό το κάνουμε σε φακέλους και directories που δεν αλλάζουν συχνά, και δεν ξεχνάμε να ελέγχουμε τακτικά το Event viewer – Security Log.

9. Ελέγχουμε όλες τις ανοιχτές TCP/IP πόρτες.

Πρώτα έλεγξε ποιες πόρτες είναι ανοιχτές στο σύστημα σου, και βρες ποιες υπηρεσίες τις διαχειρίζονται. Αυτό μπορείς να το βρεις μέσω του "netstat –an" ή κάποιας άλλης εφαρμογής.

Στη συνέχεια τρέξε ένα PortScan στο σύστημα σου από έναν άλλο υπολογιστή που είναι έξω από το Firewall σου, ώστε να δεις ποιες πόρτες φαίνονται αν κάποιος σκανάρει το σύστημα σου.

Αν δεις οτιδήποτε υπηρεσίες που δεν χρειάζεσαι να τρέχουν, απλά απενεργοποίησε τες για περισσότερη ασφάλεια .

10. Διάφορες ενέργειες

- Οι Server των XP περιλαμβάνουν ένα χρήσιμο εργαλείο, το "Security Configuration and Analysis Tool". Περισσότερα για το πώς το χρησιμοποιούμε υπάρχουν στο site που ανέφερα στην αρχή του κεφαλαίου.

- Πρέπει να απενεργοποιήσουμε το "Enumeration of SAM accounts and Shares (by anonymous users)". Ανάλογα με τις ρυθμίσεις μας, κάποιος μπορεί να πάρει μια λίστα με τα usernames και τα share names του συστήματος χρησιμοποιώντας μια "Null Session Vulnerability". Με αυτές τις πληροφορίες είναι πιο εύκολο για κάποιον να σπάσει τα password.

11. Απενεργοποιούμε το RDS (Remote Data Services)

Το RDS επιτρέπει σε έναν επιτιθέμενο να τρέξει αρχεία στο σύστημα μας. Τα περισσότερα websites δεν το χρησιμοποιούν οπότε μπορούμε να το απενεργοποιήσουμε με ασφάλεια.

12. Απενεργοποιούμε το ODBC Shell Access

Κάποιοι Server είναι πιθανό να δεχτούν επίθεση μέσω του Jet Database Engine που μπορεί να επιτρέψει σε κάποιον να τρέξει προγράμματα σε έναν Server.

13. Ελέγχουμε τα αρχεία έναρξης

Τα Windows έχουν πολλές μεθόδους για να ξεκινάνε προγράμματα να τρέχουν με την εκκίνηση του λειτουργικού. Είναι πολύ πιθανό κακόβουλα προγράμματα (π.χ. Trojans) να εκμεταλλεύονται κάποια από αυτές τις μεθόδους. Για αυτό πρέπει πάντα πριν κλείσουμε τον υπολογιστή μας να ελέγχουμε ποια προγράμματα θα εκκινήσουν με την επανέναρξη.

14. **<u>Χρησιμοποιούμε τα permissions του NTFS για να μπλοκάρουμε τα δικαιώματα εγραφής.</u>**

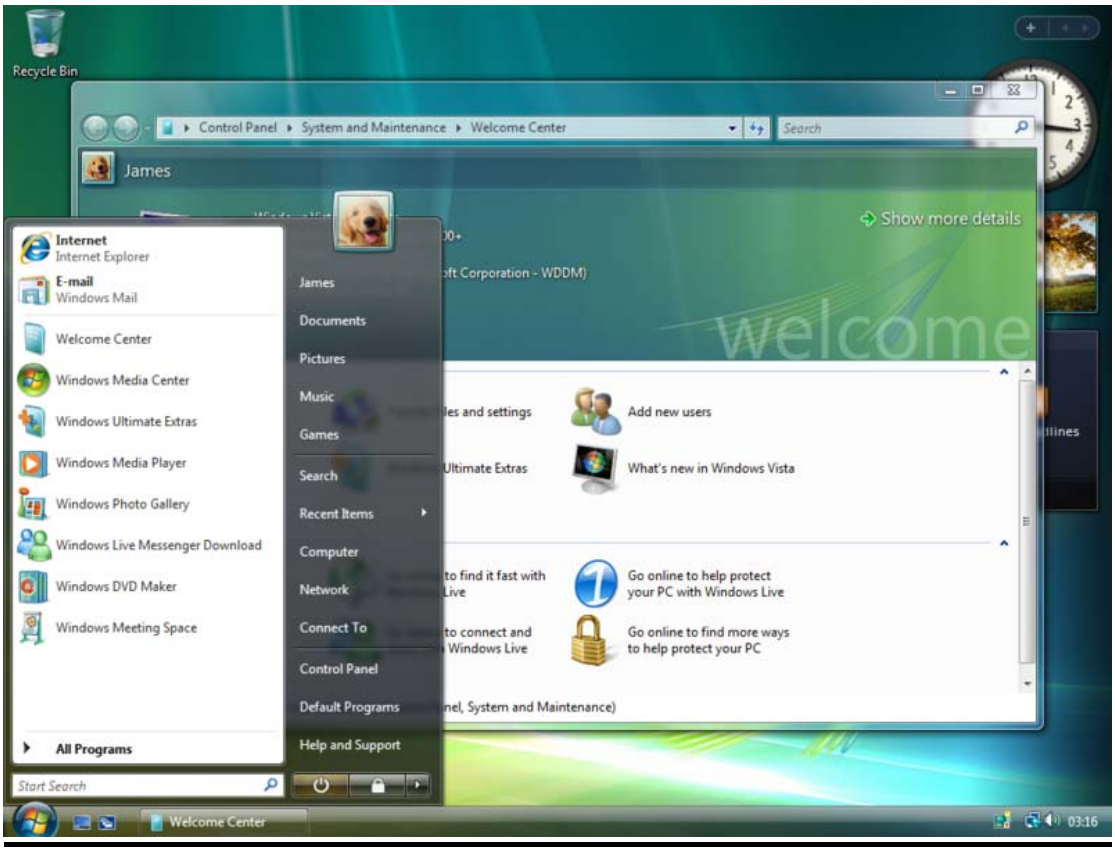
    Χρησιμοποιώντας το NTFS μπορούμε να περιορίσουμε τα δικαιώματα εγγραφής στο γκρουπ "Everyone", έτσι αν κάποιος καταφέρει να αποκτήσει πρόσβαση στο σύστημα μας, δεν θα μπορεί να αλλάξει κάτι.

15. **<u>Απενεργοποιούμε την απομακρυσμένη πρόσβαση στον υπολογιστή μας</u>**

Τέλος μην ξεχνάμε ότι πρέπει να κάνουμε και ρυθμίσεις στην εφαρμογή που θέλουμε να τρέξουμε, οι οποίες ποικίλουν ανάλογα με την μορφή της εφαρμογής. Μόνο όταν ρυθμίσουμε και την εφαρμογή θα έχουμε ένα ασφαλές σύστημα.

Μια Ματιά στο μέλλον

Microsoft Windows Vista



Εισαγωγή

Τα Windows Vista είναι το νεότερο μέλος της σειράς των Microsoft Windows . Τα Vista σύμφωνα με την Microsoft έχουν πάρα πολλές βελτιώσεις και εκατοντάδες νέες εφαρμογές. Μερικές από τις πιο σημαντικές είναι η αναβαθμισμένη γραφική διεπαφή χρήστη, νέα εργαλεία δημιουργίας πολυμεσικών εφαρμογών, ανασχεδιασμένη μέθοδο δυκτίωσης και πολλά άλλα. Όμως εμείς θα ασχοληθούμε με την βελτίωση της ασφάλειας, γιατί υπήρξε το κυριότερο σημείο κριτικής του XP και των προκατόχων του. Για αυτόν τον λόγο η Microsoft δημιούργησε το 2002 την εταιρία 'Trustworthy Computing initiative' που σκοπός της ήταν να μελετήσει την ασφάλεια σε κάθε πλευρά της ανάπτυξης του λογισμικού. Αυτό σύμφωνα με την Microsoft οδήγησε στην βελτίωση της ασφάλειας του Windows XP και του Windows Server 2003 και για αυτό καθυστέρησαν τα Vista, για να ληφθούν υπόψη όλα τα συμπεράσματα που βγήκαν

Προηγμένη Ασφάλεια

Η προηγμένη ασφάλεια ήταν ένας από του κυριότερους στόχους για τα Vista. Με την βοήθεια της 'Trustworthy Computing' η προσπάθεια οδήγησε σε έναν αριθμό νέων εφαρμογών ασφάλειας και πρόληψης .

Πρώτα από όλα ας δούμε το **User Account Control** που είναι η πιο σημαντική και πιο εμφανής από τις αλλαγές. Αυτή είναι μια τεχνολογία ασφάλειας που επιτρέπει στους χρήστες να χρησιμοποιούν τον υπολογιστή τους με λιγότερα δικαιώματα εξαρχής. Αυτό ήταν συχνά δύσκολο σε προηγούμενες εκδόσεις των Windows, γιατί ο παλιός λογαριασμός περιορισμένων δικαιωμάτων ήταν πολύ περιοριστικός και μη συμβατός με ένα μεγάλο ποσοστό εφαρμογών, ακόμα απέτρεπε κάποιες βασικές λειτουργίες όπως το άνοιγμα του ημερολογίου στην μπάρα ειδοποιήσεων (notification tray). Στα Windows Vista όταν πρέπει να γίνει μια ενέργεια που απαιτεί δικαιώματα administrator, ο χρήστης θα πρέπει να δώσει administrator name και password, σε περίπτωση που ο χρήστης είναι administrator, πρέπει να επιβεβαιώσει την ενέργεια που θα γίνει. Το **User Account Control** ζητάει επιβεβαίωση στοιχείων σε Secure Desktop λειτουργία, όπου η οθόνη γίνεται μαύρη, προσωρινά απενεργοποιημένη και φαίνεται μόνο το παράθυρο επιβεβαίωσης. Αυτό γίνεται για να αποτρέψει έναν κακοπροαίρετο πρόγραμμα να αποκτήσει κωδικούς administrator.

Μια ακόμα σημαντική νέα προσθήκη είναι το **BitLocker Drive Encryption**, μια μέθοδος προστασίας δεδομένων που συμπεριλαμβάνεται στις Enterprise και Ultimate εκδόσεις των Vista που σου επιτρέπει να κρυπτογραφήσεις όλο τον δίσκο του λειτουργικού. Το BitLocker μπορεί να δουλέψει σε συνεργασία με ένα Trusted Platform Module chip που θα βρίσκεται στην motherboard του υπολογιστή ή με ένα USB κλειδί.

Αναλυτικά το **BitLocker Drive Encryption** έχει τρεις επιλογές λειτουργίας .Στις δύο πρώτες χρειάζεται το Trusted Platform Module chip και ένα συμβατό BIOS:

- **Transparent operation mode :** Σε αυτή την μορφή εκμεταλλεύεται τις δυνατότητες του TPM 1.2 υλισμικού για να μας δώσει μια αδιαφανής λειτουργία, ο χρήστης μπαίνει στο λειτουργικό κανονικά. Το κλειδί που χρησιμοποιείται για την κρυπτογράφηση είναι σφραγισμένο από το TPM chip και αποκαλύπτεται στο κωδικό εκκίνησης του λειτουργικού μόνο αν τα αρχικά αρχεία φόρτωσης είναι αμετάβλητα.
- **User authentication mode :** Αυτή η λειτουργία προϋποθέτει από τον χρήστη να δώσει κάποια στοιχεία επιβεβαίωσης στο pre-boot περιβάλλον ώστε να μπορέσει να φορτώσει το λειτουργικό. Δύο μέθοδοι επιβεβαίωσης υποστηρίζονται, ένα pre-boot PIN που δίνεται από τον χρήστη ή με μια USB συσκευή που περιέχει το απαιτούμενο κλειδί.

Η τελευταία επιλογή δεν χρειάζεται ένα TPM chip:

- **USB-Key :** Ο χρήστης πρέπει να εισάγει μια USB συσκευή που περιέχει ένα startup κλειδί στον υπολογιστή για να μπορεί να εκκινήσει το προστατευμένο

λειτουργικό. Για αυτή την επιλογή πρέπει το BIOS του υπολογιστή να υποστηρίζει διάβασμα USB στο pre-OS περιβάλλον.

Το **Windows Defender** έχει ενσωματωθεί στο λειτουργικό, παρέχοντας προστασία απέναντι σε ιούς, spyware και άλλες απειλές. Αλλαγές σε ρυθμίσεις μπλοκάρονται εκτός αν ο χρήστης τις επιτρέπει.

Στη συνέχεια ας αναφερθούμε στις αλλαγές στον Internet Explorer 7 που περιλαμβάνουν ένα phishing φίλτρο, IDN με anti-spoofing δυνατότητες, και συνεργασία με όλο το σύστημα. Για περισσότερη ασφάλεια, τα ActiveX controls είναι απενεργοποιημένα εξαρχής. Επίσης ο Internet Explorer λειτουργεί σε προστατευμένη λειτουργία, που σημαίνει ότι δίνει λίγα δικαιώματα στον χρήστη, και δουλεύει σε απομόνωση από άλλες διεργασίες, ώστε να τις αποτρέψει από το να γράψουν ή να αλλάξουν οτιδήποτε εκτός από το Temporary Internet Files κατάλογο. Τέλος ο Internet Explorer δεν είναι πια μπλεγμένος με το shell του Explorer, οπότε τοπικοί φάκελοι ανοίγουν με τον Explorer και Web Sites με τον default web browser.
Στα Vista υπάρχει μια πληθώρα από τεχνικές περιορισμού δικαιωμάτων. Ένα παράδειγμα είναι το σκηνικό των επιπέδων ακεραιότητας (integrity levels) στις διεργασίες του χρήστη, όπου μια διεργασία με χαμηλό επίπεδο δεν μπορεί να αλληλεπιδράσει με μια διεργασία υψηλοτέρου επιπέδου. Οι περιορισμοί ασφάλειας των υπηρεσιών των Windows είναι πιο καλορυθμισμένες, ώστε οι υπηρεσίες δεν έχουν την ικανότητα να αλληλεπιδρούν με μέρη του λειτουργικού που δεν χρειάζονται. Τέλος εφαρμογές όπως τα address space layout randomization και Kernel Patch Protection χρησιμοποιούνται για να δυσκολέψουν το έργο των κακοπροαίρετων προγραμμάτων (malware).

Πριν κλείσουμε θα αναφερθούμε και στην αναβάθμιση του **Windows Firewall** σαν μέρος του ανασχεδιασμού της αρχιτεκτονικής δικτύου. Έχει νέα μέθοδο φιλτραρίσματος για την εισερχόμενη και την εξερχόμενη κίνηση. Βελτιωμένοι κανόνες φιλτραρίσματος πακέτων μπορούν να δημιουργηθούν που μπορούν να αρνηθούν επικοινωνία σε συγκεκριμένες υπηρεσίες.
Αναλυτικά τα σημεία που βελτιώθηκαν είναι τα εξής:

- **IPv6** φιλτράρισμα σύνδεσης
- Εκτός ορίων φιλτράρισμα πακέτων, μειώνει τις ανησυχίες για spyware και υιούς που προσπαθούν να επικοινωνήσουν.
- Με το προηγμένο φιλτράρισμα μπορούμε να θεσπίσουμε κανόνες για τις IP διευθύνσεις του αποστολέα και παραλήπτη καθώς και την εμβέλεια των θυρών.
- Κανόνες μπορούν να ρυθμιστούν για υπηρεσίες λαμβάνοντας υπόψη λίστες ονομάτων , χωρίς να χρειάζεται να δώσουμε ολόκληρο το path file name.
- Το IPsec είναι πλήρως αναβαθμισμένο, επιτρέποντας σε συνδέσεις να ανοιχτούν ή να καταργηθούν βασισμένο μόνο σε ψηφιακά πιστοποιητικά, Kerberos εξακρίβωση, κ.τ.λ.. Η κρυπτογράφηση μπορεί να χρησιμοποιηθεί για κάθε είδους σύνδεση.
- Μια νέα κονσόλα διαχείρισης, η *Windows Firewall with Advanced Security* που παρέχει πρόσβαση σε πολλές προηγμένες εφαρμογές, και επιτρέπει απομακρυσμένη πρόσβαση.
- Δυνατότητα να έχουμε διαφορετικά firewall προφίλ όταν οι υπολογιστές είναι μέλη ενός domain ή συνδεμένοι σε ένα ιδιωτικό ή δημόσιο δίκτυο.

Υποστήριξη για την δημιουργία κανόνων που προβλέπουν απομόνωση του Server ή του domain.

Τα Vista προσθέτουν νέες SSL και TLS κρυπτογραφικές επεκτάσεις , που παρέχουν υποστήριξη για AES και μερικές από τις νέες ECC μεθόδους κρυπτογράφησης.

Ακόμα μια σημαντική βελτίωση είναι το **Code signing,** η βασική ιδέα είναι ότι όλα τα αρχεία συστήματος έχουν υπογραφτεί ψηφιακά από την Microsoft. Αυτό επιτρέπει στα Vista να ελέγχουν την αυθεντικότητα των αρχείων και κατά συνέπεια να προστατεύουν την δομή του λειτουργικού. Ο λόγος που αυτό είναι σημαντικό είναι γιατί πολλές φορές κακοπροαίρετες εφαρμογές αντικαθιστούν κανονικά αρχεία συστήματος με υιούς ή οτιδήποτε άλλο. Έτσι τα καταστροφικά αρχεία είναι δύσκολο να εντοπιστούν γιατί αντικαθιστούν αρχεία που πρέπει να είναι εκεί. Επίσης τα αρχεία που αντικαθιστούν είναι έμπιστα για το λειτουργικό και πολλές φορές τρέχουν με πολλά προνόμια, πράγμα που επιτρέπει στον κακοπροαίρετο αντικαταστάτη να κάνει ότι θέλει.

Τα Vista περιέχουν και μια εφαρμογή που μπορεί να αποτρέψει έναν client με Vista να συνδεθεί στο προσωπικό μας δίκτυο αν δεν έχει τα τελευταία security updates, τα πιο ενημερωμένα virus definitions ή απλά δεν έχει τις απαιτούμενες προδιαγραφές. Αυτό είναι το **Network Access Protection (NAP)** και μπορεί να χρησιμοποιηθεί για να προστατέψει το σύστημα μας από clients απομακρυσμένης πρόσβασης καθώς και τοπικού δικτύου. Το NAP αναφέρει την κατάσταση των Vista σε ένα Server-based αντίστοιχο NAP που αποφασίζει αν θα δώσει άδεια ώστε ο client να μπει στο δίκτυο μας.

Τέλος το **Windows Service Hardening** δεν επιτρέπει σε κρίσιμες υπηρεσίες των Windows να κάνουν ύποπτες δραστηριότητες στο file system, την registry, το δίκτυο, ή σε άλλες περιοχές που μπορεί να χρησιμοποιηθούν ώστε mallware να εγκαταστήσει τον εαυτό του ή να επιτεθεί σε άλλα συστήματα. Για παράδειγμα μπορούμε να αποτρέψουμε την Remote Procedure Call (RPC) υπηρεσία από το να αντικαταστεί αρχεία συστήματος ή να μεταβάλει την registry

Public Key Infrastructure

Γενικά

Στην κρυπτογραφία το public key infrastructure (PKI) είναι ένας διακανονισμός που παρέχει βεβαιώσεις για τις ταυτότητες των χρηστών. Επιτρέπει την ταυτοποίηση των δημόσιων κλειδιών με τους χρήστες. Αυτό συνήθως γίνεται με την συνεργασία ενός προγράμματος σε ένα κεντρικό σημείο με άλλα σε κατανεμημένες τοποθεσίες, τα κλειδιά είναι σε πιστοποιητικά.
Ο όρος αυτός χρησιμοποιείται για να περιγράψει και την αρχή έκδοσης πιστοποιητικών και τους επιμέρους διακανονισμούς, όπως και την χρήση του αλγόριθμου δημόσιου κλειδιού στις ψηφιακές επικοινωνίες.
Το PKI επιτρέπει στους χρήστες να επιβεβαιώνουν την ταυτότητα τους, και να χρησιμοποιούν τις πληροφορίες στις ψηφιακές τους ταυτότητες για να κρυπτογραφούν μηνύματα. Γενικά το PKI αποτελείται από λογισμικό client, λογισμικό Server όπως μια αρχή έκδοσης και ελέγχου πιστοποιητικών, υλισμικό (π.χ. smart cards) και κανόνες λειτουργίας. Ένας χρήστης μπορεί να υπογράψει μηνύματα χρησιμοποιώντας το ιδιωτικό κλειδί και κάποιος άλλος μπορεί να ελέγξει την υπογραφή χρησιμοποιώντας το δημόσιο κλειδί που έχει εκδώσει κάποια αρχή μέσα από το PKI. Αυτό επιτρέπει σε δύο ή περισσότερους χρήστες να επικοινωνούν με ασφάλεια και εμπιστοσύνη χωρίς να χρειάζεται να ανταλλάξουν κρυφές πληροφορίες από πρίν.

What's New in Windows Server 2003

Version 2 Certificate Templates

Στα Windows 2000 και στα Windows XP Professional το PKI χρησιμοποιούσε σχέδια πιστοποιητικών που ήταν αποθηκεμένα στο Active Directory. Τα σχέδια αυτά είχαν τα προεπιλεγμένα περιεχόμενα μιας αίτησης πιστοποιητικού σε μια αρχή έκδοσης εταιρίας.
Η αρχή έκδοσης εταιρίας χρησιμοποιεί αυτά τα σχέδια για να εντοπίσει την αυθεντικότητα, το format του πιστοποιητικού, τον παροχέα υπηρεσίας κρυπτογράφησης, το μέγεθος του κλειδιού, και τις απαιτήσεις της X. 509 επέκτασης.

Version 1 and Version 2 Certificate Templates

Version 1 Templates

Στα Windows 2000 Server και Windows 2000 Professional οι clients υποστηρίζουν ένα προεπιλεγμένο σέτ από templates (σχέδια) πιστοποιητικών στο Active Directory που δεν μπορεί να αλλαχθεί ή να αυξηθεί. Αυτά είναι τα πρώτης έκδοσης templates, αυτά μπορούν να χρησιμοποιηθούν όπως ορίζονται ή να αντιγραφτούν.

Version 2 Templates

Στο Windows Server 2003 επεκτείνεται ο αριθμός των ρυθμίσεων που μπορείς να κάνεις σε ένα template. Έχεις την δυνατότητα να κάνεις τα εξής:

Να δημιουργήσεις νέα certificate templates

Να αντιγράψεις τα υπάρχοντα templates

Να αναβαθμίσεις templates already σε χρήση

Χρησιμοποιώντας Windows 2003 Server, τα Version 2 templates μπορούν να αλλαχθούν για να ικανοποιούν ανάγκες διάφορων εφαρμογών, και όταν αντιγράψουμε ένα Version 1 template αμέσως αναβαθμίζεται σε Version 2 template..

Enrollment and Certificate Issuance in Version 2

Οι ακόλουθες βελτιώσεις έχουν γίνει στα Version 2 templates. Παρέχουν επιπρόσθετη λειτουργικότητα κατά την ένταξη και έκδοση τους, όπως:

Customization of enrollment policies

Certificate authorization

Domain authentication

Certificate administrator

Enrollment agent signed

Key creation

Key type and CSP type

Certificate contents

Validity, issuance, and application policies—and key usages

Key archiving

Creating and Customizing Certificate Templates

Τα templates πιστοποιητικών μπορούν να δημιουργηθούν και να ρυθμιστούν ώστε να καλύπτουν τις ανάγκες του κάθε χρήστη, οι χρήστες μπορούν να αναβαθμιστούν εύκολα και γρήγορα, απλά με την έκδοση ενός νέου πιστοποιητικού ή με την αναβάθμιση ενός υπάρχοντος. Αυτό μας γλιτώνει από το άγχος να πρέπει να αλλάξουμε ή να αναβαθμίσουμε πιστοποιητικά πριν την λήξη τους.

Παράρτημα

Πλήρης οδηγός για προστασία Home User σε περιβάλλον Windows

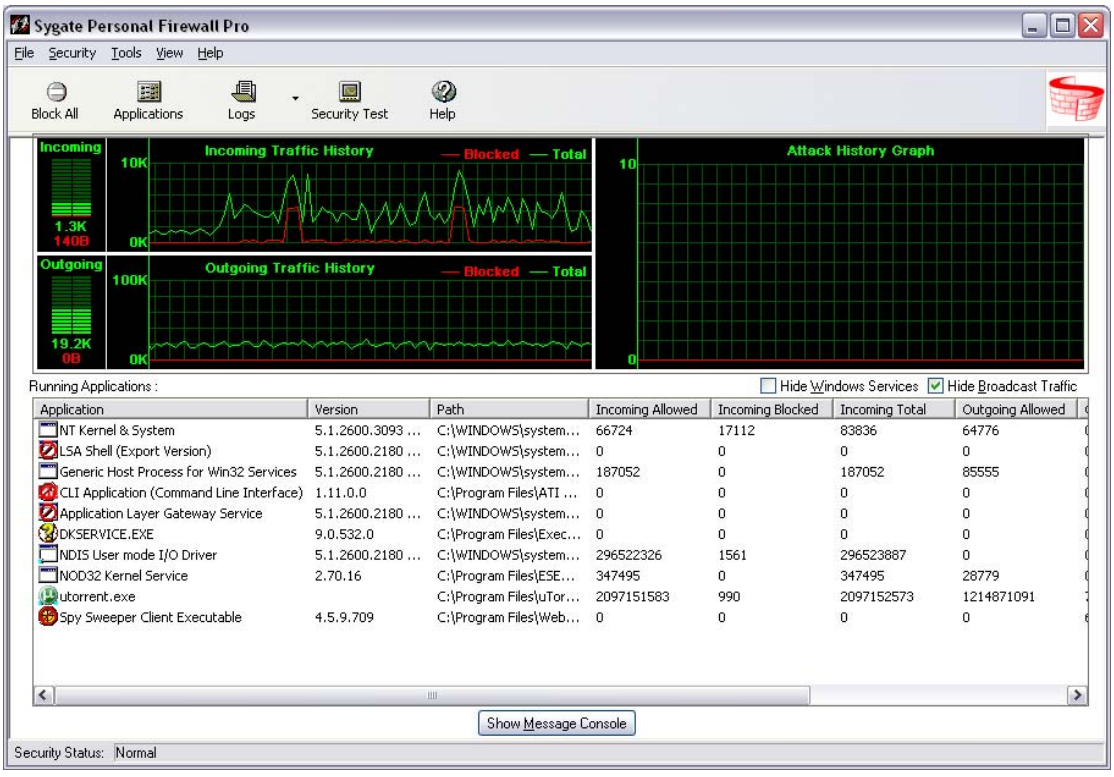
Σε αυτό το κομμάτι της εργασίας υπάρχουν οδηγίες ώστε κάποιος να ασφαλίσει τον υπολογιστή του ακολουθώντας μερικά απλά βήματα. Έτσι ώστε να μπορέσει να έχει ένα ασφαλές σύστημα και να γλιτώσει από πολλά προβλήματα που μπορεί να προκληθούν.

Εντοπίζοντας και εξολοθρεύοντας απειλές

1. Εγκατάσταση ενός Firewall.

Ένα Firewall χρειάζεται για τον έλεγχο των εισερχομένων και εξερχομένων πακέτων.

Πρόταση:
Ενώ τα Windows XP έχουν το δικό τους Firewall, δεν είναι αρκετό, οπότε καλύτερα να χρησιμοποιήσετε και κάποιο άλλο, όπως τα Sygate, BitDefender, Zone Alarm.

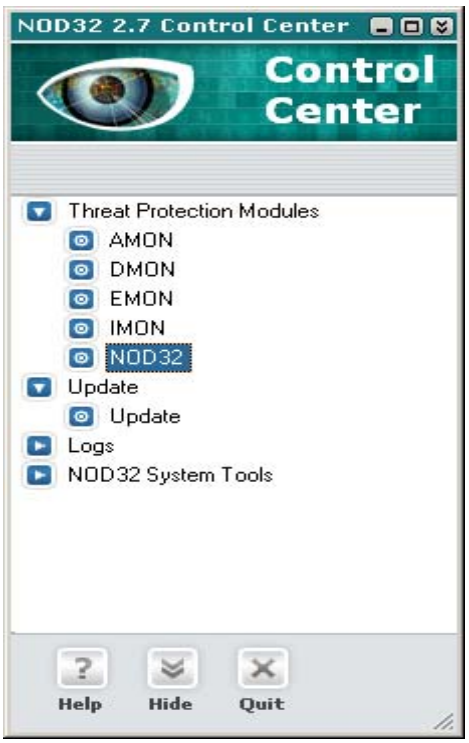


2. Εγκατάσταση και ενημέρωση Antivirus

Ένα πολύ καλό Firewall δεν είναι αρκετό, ώστε να αντιμετωπιστούν malwares όπως viruses, worms και Trojan horses. Ενώ ένα Firewall είναι ικανό να αντιμετωπίσει εξωτερικές απειλές ένα antivirus θα αντιμετωπίσει απειλές που βρίσκονται ήδη μέσα στον υπολογιστή ή θα προσπαθήσουν να εισέλθουν από κάποιο site, κάποιο e-mail attachement σκανάροντας πρώτα το αρχείο και μετά διαγράφοντας το.

Πρόταση:

Το NOD32 είναι ότι καλύτερα για antivirus. Πολύ συχνά updates, on-line προστασία και πολλά άλλα χαρακτηριστικά.

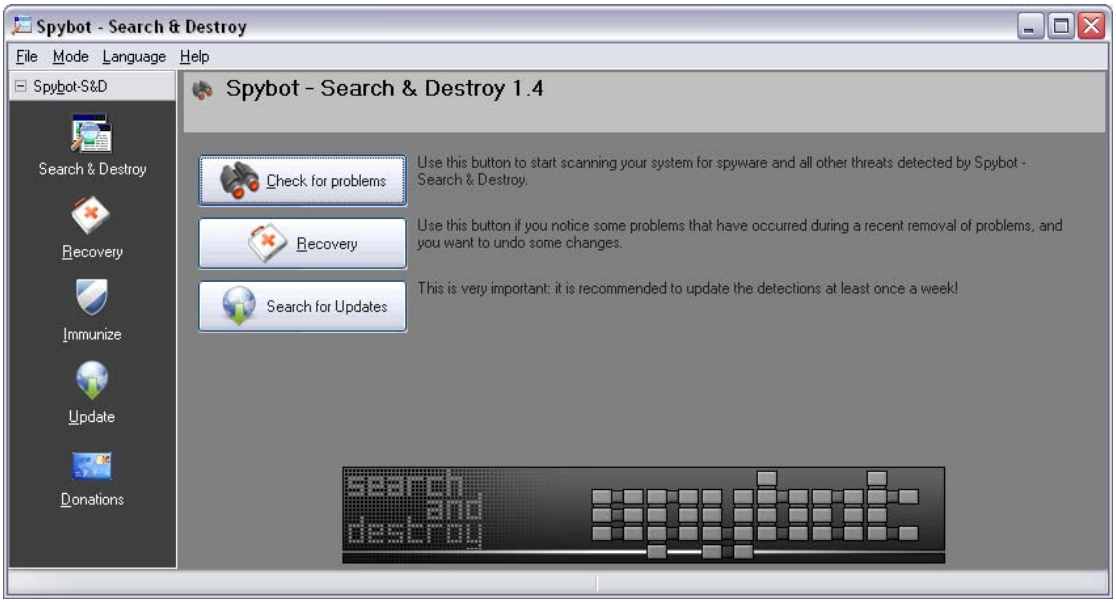


3. Χρησιμοποίηση anti-spyware

Κάποιο antispyware μπορεί να σας δώσει μεγαλύτερη προστασία από ότι φαντάζεστε καθώς τα antispywares είναι ικανά να βρίσκουν απειλές οι οποίες δεν σχετίζονται άμεσα με κάποιον τύπο virus αλλά μπορούν να αποδειχτούν εξίσου επικίνδυνες.Μία πρόσφατη έρευνα έδειξε ότι 9 στους 10 υπολογιστές που είναι συνδεδεμένοι με το Internet είναι μολυσμένοι με κάποιας μορφής spyware. Τα spyware μπορούν να εμφανιστούν είτε σαν pop-ups, είτε να κλέψουν προσωπικές πληροφορίες, είτε να κάνουν hijack τον Browser κτλ.

Πρόταση:

Τα πιο φημισμένα spyware removal προγράμματα είναι της Lavasoft's το Ad-ware, το spybot και πλέον και το Windows Defender. Η σημαντικότερη προστασία που μπορεί να προσφέρει το καθένα από αυτά είναι ότι σε περίπτωση που κάτι πάει να αλλάξει στην registry θα ειδοποιήσει τον χρήστη και πλέον είναι στην ευθύνη του χρήστη αν θα πατήσει accept (αν γνωρίζει το πρόγραμμα κτλ) ή deny αν δεν γνωρίζει τι είναι.



4. Επιπρόσθετα μέτρα προστασίας

Αν παίζετε online games ή κάποια άλλα τυχερά παιχνίδια τότε μπορεί να είστε ευάλωτοι σε Rootkits. Σε αυτήν την περίπτωση θα πρέπει να χρησιμοποιήσετε κάποιο anti-rootkit πρόγραμμα για να ασφαλίσετε τον υπολογιστή σας.

Πρόταση:

Το RootkitRevealer είναι το ιδανικό για να βρείτε τυχόν rootkits που βρίσκονται στον υπολογιστή σας και να τα απομακρύνετε.

Διάφορες άλλες ρυθμίσεις και patches

Τώρα που έχετε εγκαταστήσει τα πιο βασικά security softwares θα πρέπει να κάνετε και κάποιες άλλες ρυθμίσεις με σκοπό να μειώσετε τα αδύναμα σημεία του υπολογιστή σας.

1. Web browser security

Σερφάρουμε στο Internet χρησιμοποιώντας κάποιον browser όπως Internet Explorer, Mozilla, Opera κτλ.Επειδή όμως υπάρχουν είτε διάφορα flaws,είτε διάφορα plugins που μπορούνε να εγκαταστήσουν διάφορα softwares χωρίς να το ξέρετε καν τα updates στον browser σας είναι μέτρο μεγάλης σημασίας.

Πρόταση:

Επειδή ο Internet Explorer είναι ο βασικός στόχος και κατά συνέπεια ο browser στον οποίον βγαίνουν οι περισσότερες απειλές θα ήταν προτιμότερο να σερφάρετε με κάποιον browser όπως Firefox ή ακόμα καλύτερα Opera για να μειώσετε αυτόν τον κίνδυνο.

2. Εγκατάσταση του τελευταίου OS Service pack

Κάθε μέρα βγαίνει κάποια αδυναμία ή κάποιο exploit για το λειτουργικό σύστημα των Windows κτλ. Συνεπώς είναι σημαντικό να κάνουμε αμέσως τα απαραίτητα updates είτε είναι patches, είτε service packs κτλ προκειμένου να είμαστε πιο σίγουροι ότι είμαστε ασφαλής. Η Microsoft κάνει releases patches και updates για τα λειτουργικά της μία φορά τον μήνα κάθε δεύτερη Τρίτη που ονομάζεται αυτήν η μέρα και σαν Patch Tuesday.

Πρόταση:

Κάθε δεύτερη τρίτη του μήνα λοιπόν να κοιτάτε πάντα για νέα διαθέσιμα updates και πάντα από το επίσημο site της Microsoft και από πουθένα αλλού καθώς υπάρχουν και μερικά fakes τα οποία μοιάζουν με το official και φυσικά δεν περιέχουν updates.

3. Προσοχή στο τι κατεβάζετε

Πολλά προγράμμα που διατίθενται free συχνά κρύβουν και κάποιο malware μέσα. Έτσι χωρίς να ξέρετε ότι μαζί με το πρόγραμμα που θέλετε περιέχει και το malware κατεβάζετε και αυτό.

Πρόταση:

Κατεβάστε πάντα από αξιόπιστα sites όπως ZDNet ή VNUNet ή από τα επίσημα των προγραμμάτων που θέλετε. Αν κατεβάζετε από torrents ή από peer2peers καλό θα ήταν μόλις πάρετε το αρχείο να το σκανάρετε πριν το τρέξετε.

E-mail Security

Το e-mail θεωρείτε ένας ασφαλής τρόπος ανταλλαγής αρχείων καθώς είναι κάτι προσωπικό και συχνά τα e-mails που έχετε είναι από γνωστούς σας. Παρόλα αυτά

είναι ακόμα ένα μέσο που πρέπει να λάβετε υπόψη σας για προστασία από hacker's και spammers.

1. Χρησιμοποίηση email client

Όλα τα email clients παραδίδουν τα email το θέμα είναι να χρησιμοποιήσετε κάποιο που να σας προσφέρει ένα επίπεδο προστασίας και εκεί όπως να έχουν κάποιο virus scanning για τα attachements ή να μπλοκάρουν/μετακινούν τα spam emails από το inbox σας.

Πρόταση:

Το Yahoo mail είναι ένα από τα καλύτερα web-based email clients που παρέχει στον χρήστη spam filtering και έχει virus scan στα attachments, αν όμως χρησιμοποιείται κάποιο άλλο μπορείτε να το κάνετε με το antivirus που έχετε.

2. Διαχείριση email attachments

Όταν κατεβάζετε κάποιο email attachment συνήθως το επιτρέπεται να κατέβει καθώς γνωρίζετε το τι μπορεί να είναι. Όμως τα attachements είναι ο πιο αποτελεσματικός τρόπος για να εισέλθει ένας ιός στον υπολογιστή σας.

Πρόταση:

Μην ανοίγετε attachments από αγνώστους ή ακόμα από εταιρείες όσο γνωστές και να είναι αυτές. Επίσης αν ο υπολογιστής ενός φίλου σας μολυνθεί τότε είναι πολύ πιθανό να λάβετε κάποιο email με κάποιο attachment που θα περιέχει κάποιο worm. Αν δεν περιμένετε κάποιο attachment από αυτό το πρόσωπο τότε καλύτερα να το καλέσετε στο skype, msn ή ακόμα και στο κινητό για να μάθετε αν όντως το email προήλθε από αυτόν.

3. Μην κάνετε κλικ σε τυχαία email links

Μία συνηθισμένη τεχνική phising είναι το να περιέχει κάποιο email που μοιάζει με αυθεντικό κάποιο link. Αυτά τα links το πιο πιθανό είναι να οδηγήσουν τον χρήστη σε κακόβουλα sites. Συνήθως μπορεί να ζητάνε επιβεβαίωση κάποιας οικονομικής συναλλαγής ή απλά να ζητάνε κάποιο unsubscribe από newsletter ή ακόμα χειρότερα link με κάποιο virus που θα εγκατασταθεί αμέσως στον υπολογιστή σας.

Πρόταση:

Μην κάνετε κλικ σε links που μπορεί να περιέχουν κάποιο ερώτημα και να ζητούν από εσάς επιβεβαίωση μέσω του link αυτού. Το καλύτερο που έχετε να κάνετε είναι να απενεργοποιήσετε το HTML στα email έτσι ώστε τα links που βρίσκονται μέσα στην HMTL σελίδα που μπορεί να σας στείλουν να μην λειτουργούν.

4. Εγκατάσταση email filters

Οι περισσότεροι ISPs παρέχουν και email filtering για να ελαχιστοποιήσουν το μέγεθος των spam emails που θα φτάσουν στο inbox σας. Για να φτάσετε τον αριθμό αυτόν κοντά στο 0 πρέπει να εγκαταστήσετε το δικό σας προσωπικό email filter.

Πρόταση:

Μπορείτε να χρησιμοποιήσετε κάποιο e-mail organizer από τον υπολογιστή σας, όπως το Outlook ή το Thunderbird που έχουν ρυθμίσιμα spam filters. Ένας άλλος τρόπος είναι ο εξής: το gmail σας επιτρέπει να δημιουργήσετε έναν αριθμό από email aliases που όλα θα γίνονται redirect στο email σας και θα σας επιτρέπει να χωρίσετε όλα τα email σας. Για παράδειγμα αν έχετε αυτήν την διεύθυνση

Code:
```
paris.hilton@gmail.com
```

μπορείτε να δώσετε στο site που θα μπαίνετε το παρακάτω

Code:
```
paris.hilton+fans@gmail.com
```

Και όλα τα email που προέρχονται από εκεί θα ομαδοποιηθούν σε έναν ξεχωριστό φάκελο. Τέλος μπορείτε πάντα να χρησιμοποιήσετε emails των 10 λεπτών για να αποφύγετε το spam.

Προστατεύοντας του κωδικούς σας

Φαντάζομαι ποτέ δεν θα σκεφτήκατε να βάλετε κάποιον κωδικό όπως 123κτλ ιδιαιτέρως για πράγματα που έχουν να κάνουν για οικονομικές συναλλαγές. Οπότε καλό θα ήταν για να μην μπείτε σε κίνδυνο να αποκτήσει κάποιος τον κωδικό σας να επιλέξετε κωδικούς που δεν είναι απλοί και να τους αλλάζετε συχνά.

1. Αφήστε τους hackers να ψάχνουν

Οι hackers χρησιμοποιούν ποικίλες τεχνικές για να βρίσκουν κωδικούς. Μία από τις πιο γνωστές είναι το λεγόμενο dictionary attack το οποίο ψάχνει για κοινούς συνδυασμούς λέξεων και έναν μεγάλο αριθμό συνδυασμών. Γνωρίζοντας τώρα αυτό θα πρέπει να βάλετε κωδικούς που είναι δύσκολο να βρεθούν από τέτοιες επιθέσεις.

Πρόταση:

Χρησιμοποιήστε δυνατούς κωδικούς τουλάχιστον 7 χαρακτήρων, με μία μίξη κεφαλαίων και μικρών γραμμάτων για παράδειγμα AxV37TtP0.Επίσης μην χρησιμοποιήσετε ποτέ συνηθισμένες λέξεις ή ονόματα και να αλλάζετε τους κωδικούς σας συχνά .

2. Χρησιμοποίηση διαφορετικών password

Επειδή είναι πιο βολικό να χρησιμοποιείται τα ίδια username και password για αρκετά sites και επειδή μπορεί κάποιο site να χτυπηθεί από κάποιον hacker και να έχει τον κωδικό σας, γνωρίζοντας ότι οι περισσότεροι χρήστες χρησιμοποιούν τους ίδιους κωδικούς είναι εύκολο να του δοκιμάσουν και σε άλλα sites ή σε online banking.

Πρόταση:

Χρησιμοποιείστε διαφορετικά passwords για κάθε web-based εφαρμογή, ή αν έχετε πρόβλημα να τα θυμηθείτε, να έχετε πάντα τουλάχιστον τρία password διαφορετικής πολυπλοκότητας, ώστε να χρησιμοποιείται ένα από τα τρία κάθε φορά. Εννοείται ότι θα τα αλλάζεται με νέα τρία σε τακτά χρονικά διαστήματα.