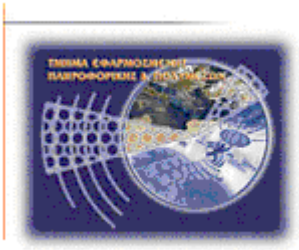
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων



Πτυχιακή εργασία

Επιθέσεις και αντίμετρα σε συστήματα Windows

Άντρια Νεοκλέους (ΑΜ: 2072)
(andriaenrique@hotmail.com)
Γιώργος Νεάρχου (ΑΜ: 2054)
(georgenearchou@hotmail.com)

Ηράκλειο – 20.1.2011

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

<u>Υπεύθυνη Δήλωση</u>:
Βεβαιώνουμε ότι είμαστε συγγραφείς αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχαμε για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχουμε αναφέρει τις όποιες πηγές από τις οποίες κάναμε χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνουμε ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμάς προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Εφαρμοσμένης Πληροφορικής και Πολυμέσων του Τ.Ε.Ι. Κρήτης.

Νεοκλέους Άντρια
Νεάρχου Γιώργος

Ευχαριστίες

Θα θέλαμε να ευχαριστήσουμε τον επιβλέποντα καθηγητή Δρ.Χαράλαμπο Μανιφάβα για την πολύτιμη και ουσιαστική καθοδήγηση του, για την αμέριστη συμπαράσταση, τις κατευθύνσεις που μας έδωσε σε σχετικές συναντήσεις, τις εποικοδομητικές ιδέες και τη βοήθεια του κατά την διάρκεια της πτυχιακής μας εργασίας.

Θεωρούμε χρέος να ευχαριστήσουμε τις οικογένειες μας που μας στήριξαν και μας συμπαραστάθηκαν σε όλη μας την προσπάθεια. Επιπλέον τους φίλους μας Χριστόδουλο, Χριστίνα, Αγγελική, Αυγουστίνο, Ασημίνα και Μαρία για την κατανόηση και την πίστη σε εμάς.

Ιστορικό εκδόσεων

Ημερομηνία	Έκδοση	Λεπτομέρειες
26/01/2011	Version 1.6	Κεφ1,Κεφ2,Κεφ3, Κεφ4,Κεφ5.
20/01/2011	Version 1.5	Κεφ1,Κεφ2,Κεφ3, Κεφ4,Κεφ5.
02/01/2011	Version 1.4	Κεφ1,Κεφ2,Κεφ3, Κεφ4,Κεφ5.
03/09/2010	Version 1.3	Κεφ4,Κεφ5.
12/06/2010	Version 1.2	Κεφ1,Κεφ2,Κεφ3.
18/03/2010	Version 1.1	Κεφ1,Κεφ2.
20/02/2010	Version 1.0	Κεφ1.

Περίληψη

Η πτυχιακή εργασία αυτή επικεντρώνεται κυρίως σε επιθέσεις και αντίμετρα σε συστήματα Windows. Η φράση "ασφάλεια των πληροφοριών" έχει επεκτείνει σημαντικά την έννοια της κατά την διάρκεια της τελευταίας δεκαετίας. Ο όρος αυτός έχει επεκταθεί τώρα και δεν αφορά μόνο την προστασία των μυστικών διαφόρων σημαντικών εταιρειών και κυβερνήσεων, αλλά συμπεριλαμβάνει πλέον και το μέσο καταναλωτή. Οι πιο εμπιστευτικές πληροφορίες αποθηκεύονται online σε τεράστιες ποσότητες. Καθώς αυξάνεται η κοινότητα των εγκληματιών του κυβερνοχώρου, αυξάνονται και οι κίνδυνοι για τα δίκτυα και τις κοινόχρηστες πληροφορίες από το ηλεκτρονικό έγκλημα, γι αυτό κι εμείς θα αναφερθούμε και θα αναλύσουμε κάποιες από τις υπάρχουσες απειλές ώστε να αντιμετωπιστούν μερικά από τα προβλήματα ασφάλειας.

Στην εργασία αυτή παρουσιάζονται γνωστοί τύποι απειλών και επιθέσεων καθώς και το κύριο θέμα μας η αντιμετώπιση τους. Δεν μπορούμε να αγνοήσουμε τον πειρασμό που υπάρχει για εκείνους που διαθέτουν τη γνώση και τα εργαλεία ώστε να έχουν πρόσβαση στα εμπιστευτικά δεδομένα μας. Θέλουμε να εκπαιδεύσουμε αυτούς που θα ήθελαν να ασχοληθούν με την ασφάλεια των πληροφοριακών συστημάτων ώστε να υπερασπίσουμε τα έθνη μας, τα εκπαιδευτικά ιδρύματα μας, τις τράπεζες, τους εμπόρους μας, τις εταιρείες κοινής ωφέλειας μας, τις υποδομές μας και τις οικογένειες μας.

Είτε το θέλουμε είτε όχι είμαστε σε μια συνεχή πάλη εναντία στο ηλεκτρονικό έγκλημα. Για να επιτύχουμε καλή ασφάλεια σε οποιοδήποτε περιβάλλον, είναι ουσιαστικό να αναπτύσσουμε συνεχώς τις τεχνικές ικανότητες μας.

Πίνακας Περιεχομένων

Πίνακας Εικόνων

Πίνακας Πινάκων

Κεφάλαιο 1 Εισαγωγή

1.1 Γενικά

Με την πάροδο του χρόνου παρατηρούμε ότι η ασφάλεια της Microsoft άρχισε να ωριμάζει σε σχέση με τα προηγούμενα χρόνια. Αρχικά έπρεπε να σταματήσει η εκμετάλλευση των αδυναμιών της διαμόρφωσης που έδωσαν χώρο σε πιο σύνθετη επίθεση, όπως και επιθέσεις κατά των τελικών χρηστών μέσω του Internet Explorer. Η Microsoft έχει υπολογίσει κατά μέσο όρο περίπου 70 ενημερωτικά δελτία ασφαλείας ανά έτος σε όλα τα προϊόντα της από το 1998. Όμως, παρά τις μειώσεις στον αριθμό των δελτίων για κάποια συγκεκριμένα προϊόντα, δεν υπάρχει κανένα σημάδι επιβράδυνσης του ρυθμού εμφάνισης τους.

Η Microsoft έχει επιδιορθώσει επιμελώς τα περισσότερα προβλήματα που έχουν προκύψει και έχει ενισχύσει σταδιακά τα Windows με νέες λειτουργίες ασφάλειας. Αυτό είχε συνήθως το αποτέλεσμα να μεταφερθεί η εστίαση κυρίως σε διαφορετικές περιοχές του συστήματος των Windows κατά την διάρκεια του χρόνου από τις υπηρεσίες δικτύων για τους kernel drivers στις εφαρμογές. Όμως καμία λύση δεν βρέθηκε για να μειώσει ριζικά το πλήθος των αδυναμιών στην πλατφόρμα, μόνο έμμεσα μέσω της συνεχούς ροής των δελτίων και συμβούλων ασφαλείας από την Redmond (Microsoft).

Παρατηρώντας την ασφάλειας των Windows κατά τη διάρκεια πολλών ετών, έχουμε περιορίσει τις περιοχές με τους υψηλότερους κινδύνους σε δύο παράγοντες: **δημοτικότητα** και **πολυπλοκότητα**.

Η δημοτικότητα έχει δύο όψεις για αυτούς που χρησιμοποιούν τεχνολογίες της Microsoft. Από τη μια πλευρά, οι προγραμματιστές έχουν μεγάλη υποστήριξη, υπάρχει σχεδόν παγκόσμια αποδοχή από τους χρήστες και ένα ισχυρό παγκόσμιο σύστημα υποστήριξης. Από την άλλη πλευρά, η κυρίαρχη κουλτούρα των Windows παραμένει ο στόχος που προτιμούν οι hackers, για να επεξεργάζονται περίπλοκες εκμεταλλεύσεις τρωτών σημείων και στη συνέχεια να τις διανέμουν σε παγκόσμια κλίμακα (τα σκουλήκια του internet που βασίζονται στις αδυναμίες των Windows όπως τα Code Red, Nimda, Slammer, Blaster, Sasser, Netsky, Gimmiv κ.λπ., πιστοποιούν όλα την παραμονή αυτού του προβλήματος). Θα είναι ενδιαφέρον να μάθετε εάν ή πώς αλλάζει αυτή η δυναμική καθώς άλλες πλατφόρμες (όπως στα όλο και πιο ευρέως προϊόντα της Apples) συνεχίζουν να αποκτούν μεγαλύτερη δημοτικότητα και επίσης εάν διάφορες λειτουργίες όπως το Address Space Layout Randomization (ASLR), που περιλαμβάνεται σε νεότερες εκδόσεις των Windows θα έχουν κάποια επίδραση στο πρόβλημα αυτό.

Η πολυπλοκότητα είναι πιθανώς μια άλλη αιτία των τρωτών σημείων της Microsoft. Έχει δημοσιευτεί ευρέως ότι ο πηγαίος κώδικας για το λειτουργικό σύστημα έχει αυξηθεί κατά προσέγγιση δέκα φορές από τα NT 3.51 έως τα Vista. Μέρος αυτής της αύξησης ήταν πιθανώς αναμενόμενη (και ίσως να παρέχει και επιθυμητές βελτιώσεις) αν ληφθούν υπόψη οι διαφοροποιημένες απαιτήσεις των χρηστών και η πρόοδος της τεχνολογίας. Ωστόσο, μερικές πτυχές της αυξανόμενης πολυπλοκότητας των Windows φαίνονται ιδιαίτερα εχθρικές για την ασφάλεια: η προς τα πίσω συμβατότητα και ένα νέο σύνολο λειτουργιών.

Η προς τα πίσω συμβατότητα είναι ένα σύμπτωμα της μακρόχρονης επιτυχίας των Windows που είναι εγκατεστημένα σε πολλές διαφορετικές τεχνολογίες, απαιτώντας υποστήριξη για μία όλο και μεγαλύτερη σειρά από λειτουργικότητες που παραμένουν πάντα διαθέσιμες στο στόχαστρο των κακόβουλων hackers. Μια μεγάλη ευχαρίστηση για τους hackers ήταν η συνεχής εμπιστοσύνη των Windows σε κληροδοτούμενες λειτουργίες που είχαν κληρονομηθεί από τα LAN και είχαν μείνει ανοιχτές σε μερικές απλές επιθέσεις. Φυσικά, αυτή η κληροδοτούμενη υποστήριξη ενεργοποιείται συνήθως στις έτοιμες διαμορφώσεις για να εξασφαλίσει τη μέγιστη δυνατή συμβατότητα.

Τέλος, αυτό που κρατά τα Windows στο στόχαστρο των hacker είναι ο συνεχής πολλαπλασιασμός των λειτουργιών που είναι ενεργοποιημένες εξ ορισμού στην πλατφόρμα. Για παράδειγμα, χρειάστηκαν τρεις γενιές λειτουργικών συστημάτων ώστε να συνειδητοποιήσει η Microsoft ότι εγκατάσταση και η ενεργοποίηση των επεκτάσεων (IIS- Internet Information Services) των Windows αφήνουν εξ ορισμού τους πελάτες της εκτεθειμένους στην πλήρη μανία των δημόσιων δικτύων (π.χ., των σκουληκιών Code Red και Nimda που είχαν σαν στόχο τον IIS). Η Microsoft φαίνεται να μην έχει μάθει ακόμα αυτό το μάθημα με τον Internet Explorer.

Παρά τις διάφορες προβληματικές περιοχές, όπως τον Internet Explorer, υπάρχουν μερικά σημάδια ότι το μήνυμα έχει αρχίσει να λαμβάνεται. Πλέον τα Windows XP Service Pack 2 και Vista στέλνονται με μειωμένες προεπιλεγμένες υπηρεσίες δικτύων και με ένα firewall ενεργοποιημένο εξ ορισμού. Διάφορες νέες λειτουργίες, όπως το User Account Control (UAC), αρχίζουν να δείχνουν σε χρήστες και προγραμματιστές τα πρακτικά οφέλη και τις συνέπειες των ελάχιστων δικαιωμάτων. Αν και, όπως πάντα, η Microsoft τείνει να ακολουθεί παρά να οδηγεί με τέτοιες βελτιώσεις (από αλλού ξεκίνησαν αρχικά τα firewall σε κύριους υπολογιστές και η εναλλαγή της κατάστασης των χρηστών), είναι αξιοθαύμαστη η κλίμακα, στην οποία έχουν αναπτυχθεί αυτές οι λειτουργίες. Ασφαλώς, θα ήμαστε οι πρώτοι που θα αναγνωρίσουμε ότι η επίθεση σε ένα δίκτυο των Windows που αποτελείται από Vista και Windows Server 2008 (στις προεπιλεγμένες διαμορφώσεις τους) είναι πολύ πιο δύσκολη απ' την αντίστοιχη επίθεση σε προηγούμενες εκδόσεις τους.

1.2 Σκοπός

Η ασφάλεια των δικτύων στα Windows έχει επεκτείνει σημαντικά την έννοια της κατά την διάρκεια της τελευταίας δεκαετίας. Καθημερινά εμφανίζονται νέα εργαλεία, τεχνικές, μέθοδοι, script και αυτοματοποιημένες εισβολές από τους hacker που επιτίθενται σε όλο τον κόσμο.

Καθώς αυξάνεται η κοινότητα των εγκληματιών του κυβερνοχώρου, αυξάνονται και οι κίνδυνοι ,οι απειλές για τα δίκτυα και τις κοινόχρηστες πληροφορίες από το ηλεκτρονικό έγκλημα.

Η πτυχιακή αυτή ασχολείται με την ασφάλεια των Windows, συγκεκριμένα αναλύονται οι επιθέσεις και τα αντίμετρα για τα πιο κάτω θέματα:

- Μη πιστοποιημένες επιθέσεις (Επιθέσεις χωρίς πιστοποίηση/μη εξουσιοδοτημένη πρόσβαση εξ αποστάσεως).

- Επιθέσεις με πιστοποίηση (Κλιμάκωση δικαιωμάτων, Εξαγωγή και διάρρηξη κωδικών πρόσβασης, Έλεγχος από απόσταση και Πίσω Πόρτες, Ανακατεύθυνση θυρών και Κάλυψη των ιχνών).

- Λειτουργίες ασφάλειας των Windows(Firewall των Windows, Αυτοματοποιημένες ενημερώσεις, Κέντρο ασφάλειας, Πολιτική ασφάλειας και πολιτική ομάδας, bitlocker και EFS, Προστασία πόρων των Windows, Επίπεδα ακεραιότητας ,UAC και LoRIE, DEP, Θωράκιση Υπηρεσιών και Βελτιώσεις βασισμένες σε μεταγλωττιστή).

Αυτή η εργασία βασίζεται στο βιβλίο «Ασφάλεια Δικτύων» έκτη έκδοση των Stuart McClure, Joel Scambray και George Kurtz. Στα πλαίσια αυτής της πτυχιακής εργασίας θα παρουσιαστούν και θα εκτελεστούν στην πράξη προγράμματα που χρησιμοποιούν συχνά οι hacker καθώς και μερικά κομμάτια κώδικα που παραβιάζουν μέσω δικτύου τα περιβάλλοντα των Windows.

Σκοπός είναι η θωράκιση των δικτύων με τον καλύτερο δυνατό τρόπο, η αντιμετώπιση και η διόρθωσή έτσι ώστε να αποτραπούν πολλές σημαντικές και επικίνδυνες επιθέσεις.

1.3 Συνοπτική Περιγραφή

Έχουμε οργανώσει αυτή την πτυχιακή σε τρία σημαντικά κεφάλαια:

• **Μη πιστοποιημένες επιθέσεις**. Σε αυτή την ενότητα καλύπτετε η εκμετάλλευση τρωτών σημείων σε απομακρυσμένα δίκτυα.

• **Πιστοποιημένες επιθέσεις.** Υποθέτοντας ότι έχουμε επιτύχει μια από τις προηγούμενες επιθέσεις εκμετάλλευσης τρωτών σημείων, ο επιτιθέμενος θα προσπαθήσει τώρα να αποκτήσει περισσότερα προνόμια εάν είναι απαραίτητο, αποκτώντας απομακρυσμένο έλεγχο του θύματος, υποκλέπτοντας κωδικούς πρόσβασης και άλλες χρήσιμες πληροφορίες, εγκαθιστώντας «πίσω πόρτες» και καλύπτοντας τα ίχνη του.

• **Λειτουργίες ασφάλειας των Windows.** Αυτή η τελευταία ενότητα παρέχει την πλήρη κάλυψη των ενσωματωμένων αντίμετρων του λειτουργικού συστήματος και των καλύτερων πρακτικών εναντίον της εκμετάλλευσης των πολλών τρωτών σημείων.

1.4 Σχεδιάγραμμα Αναφοράς

Κεφάλαιο 2 Μη Πιστοποιημένες Επιθέσεις

Τα αρχικά στοιχεία για την κατάληψη ενός συστήματος των Windows για απομακρυσμένη χρήση περιλαμβάνουν:

• **Εξαπάτηση κατά τον έλεγχο ταυτότητας** (Authentication spoofing): Ο αρχικός φύλακας της πρόσβασης σε συστήματα των Windows παραμένει ο ευπαθής κωδικός πρόσβασης. Επίσης, παραμένουν πραγματικές απειλές για τα δίκτυα Windows το συνηθισμένο μάντεμα των κωδικών πρόσβασης με την μέθοδο brute force/λεξικό, όπως και η ενδιάμεση εξαπάτηση κατά τον έλεγχο της ταυτότητας.

• **Υπηρεσίες Δικτύου** (Network services): Τα σύγχρονα εργαλεία κάνουν εύκολη την εκμετάλλευση αδυναμιών διαπερνώντας τις τρωτές υπηρεσίες που ακροάζονται στο δίκτυο.

• **Τρωτά σημεία λογισμικού πελάτη** (Client vulnerabilities): Κάποια προγράμματα-πελάτες (χρηστές) όπως ο Internet Explorer, το Outlook, ο Windows Messenger, το office και άλλα θα πρέπει να διερευνηθούν πολύ από τους επιτιθεμένους που ψάχνουν για άμεση πρόσβαση σε δεδομένα των τελικών χρηστών.

• **Οδηγοί συσκευών** (Device drivers): Η έρευνα συνεχίζει να εμφανίζει νέες δυνατότητες επίθεσης όπου το λειτουργικό σύστημα αναλύει ακατέργαστα δεδομένα από διάφορες συσκευές, όπως ασύρματες κάρτες δικτύων, USB μνήμης και εισαγόμενα μέσα όπως δίσκους CD-ROM.

Εάν προστατεύσουμε τα πιο πάνω, θα έχουμε κάνει μεγάλα βήματα προς το να είναι τα Windows πιο ασφαλή. Σε αυτή την ενότητα θα παρουσιάσουμε τις πιο σημαντικές αδυναμίες και στις δύο λειτουργίες, καθώς επίσης και την αντιμετώπιση τους.

2.1 Επιθέσεις Χωρίς Πιστοποίηση

Αν και δεν είναι τόσο εντυπωσιακή όσο η υπερχείλιση buffer, η υποκλοπή ή το μάντεμα ενός κωδικού πρόσβασης παραμένει ένας από τους ευκολότερους τρόπους να αποκτηθεί μη πιστοποιημένη πρόσβαση στα Windows.

2.1.1 Εύρεση κωδικών πρόσβασης εξ αποστάσεως

Ο παραδοσιακός τρόπος να παραβιάσουμε από εξ' αποστάσεως συστήματα Windows είναι να επιτεθούμε στην υπηρεσία κοινής χρήσης αρχείων και εκτύπωσης των Windows , η οποία λειτουργεί μέσω ενός πρωτοκόλλου που ονομάζεται Server Message Block (SMB). Το SMB προσπελάζεται μέσω δύο TCP θυρών: της TCP θύρας 445 και της 139 (η τελευταία είναι μία κληροδοτούμενη υπηρεσία βασισμένη στο netBIOS). Άλλες υπηρεσίες στις οποίες γίνεται συνήθως επίθεση μέσω μαντέματος κωδικού πρόσβασης είναι η Microsoft Remote Procedure (MSRPC) στην TCP θύρα 135, η υπηρεσία Terminal Services (TS) στην TCP θύρα 3389 (αν και μπορεί εύκολα να διαμορφωθεί για να ακροάζεται αλλού), η υπηρεσία SQL στην TCP θύρα 1433 και UDP

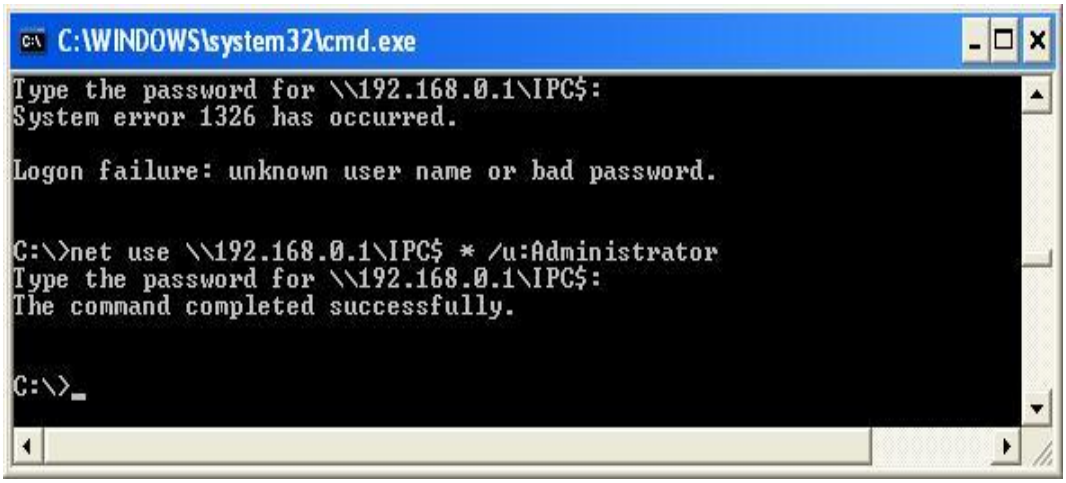
1434 και προϊόντα βασισμένα στο Web που χρησιμοποιούν πιστοποίηση των Windows όπως το SharePoint (SP) μέσω HTTP και HTTPS (TCP 80 και 44 ports) και ενδεχομένως προσαρμοσμένες θύρες. Στην συνέχεια θα μελετήσουμε εν συντομία τα εργαλεία και τις τεχνικές για κάθε μία από αυτές τις επιθέσεις.

Το SMB δεν είναι προσπελάσιμο εξ αποστάσεως στη προεπιλεγμένη διαμόρφωση των Windows Vista και Server 2008 επειδή μπλοκάρεται από την προεπιλεγμένη διαμόρφωση του Windows Firewall. Μια εξαίρεση σε αυτήν την κατάσταση είναι οι ελεγκτές τομέων του Windows Server, οι οποίοι αναδιαμορφώνονται αυτόματα κατά την αναβάθμιση για να κάνουν προσπελάσιμο το SMB στο δίκτυο. Υποθέτοντας ότι το SMB είναι προσπελάσιμο, η πιο αποτελεσματική μέθοδος ώστε να εισβάλετε σε ένα σύστημα των Windows είναι το καλό παλιό μοντάρισμα κοινόχρηστου πόρου εξ αποστάσεως: προσπαθούμε να συνδεθούμε σ' ένα κοινόχρηστο πόρο όπως το IPC$[1] ή C$ που έχουμε βρει με απαρίθμηση και δοκιμάζοντας διάφορους συνδυασμούς ονομάτων χρήστη/κωδικού πρόσβασης έως ότου βρούμε κάποιον που να δουλεύει.

Εξακολουθούν ωστόσο να υπάρχουν ακόμα υψηλά ποσοστά διάρρηξης με χειροκίνητες τεχνικές μαντέματος κωδικών πρόσβασης ,είτε από την γραμμή εντολών, όπως παρουσιάζεται παρακάτω χρησιμοποιώντας την εντολή **net use**. Βάζουμε την IP του στόχου μας και μετά το IPC$ βάζοντας έναν αστερίσκο (*) αντί για έναν κωδικό πρόσβασης αναγκάζετε το απομακρυσμένο σύστημα να σας ζητήσει ένα κωδικό πρόσβασης, όπως βλέπουμε εδώ:

```
C:\> net use \\192.168.0.1\IPC$ * /u:Administrator
Type the password for \\192.168.10.1\IPC$:
The command completed successfully.
```

Στην πιο κάτω εικόνα έχουμε εκτελέσει επίθεση σε ένα Server 2003 ο οποίος έχει εγκατασταθεί εικονικά στο VMware System του υπολογιστή μας. Όπως βλέπουμε η πρώτη προσπάθεια μας είναι ανεπιτυχής για τον λόγο ότι το user name ή το password είναι λάθος. Η δεύτερη προσπάθεια ολοκληρώθηκε επιτυχώς.



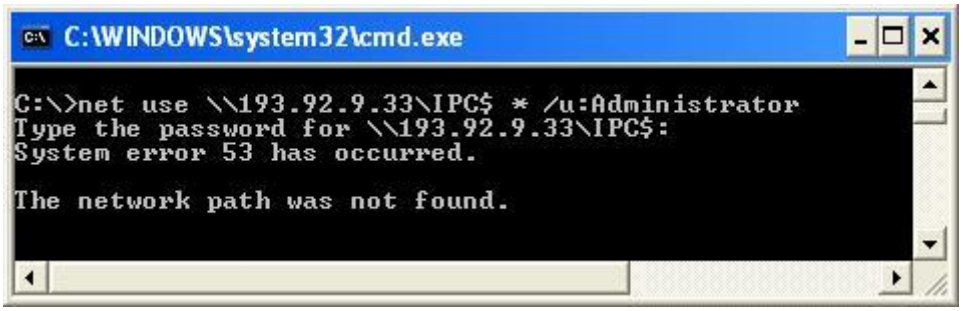
Εικόνα 1:Χειροκίνητη εισαγωγή κωδικού πρόσβασης.

[1] http://smallvoid.com/article/winnt-ipc-share.html
Περισσότερες Επεξηγήσεις στο Παράρτημα Β.1

Προσπάθεια παραβίασης κωδικού πρόσβασης www.epp.teiher.gr

Με την εντολή nslookup μετατρέψαμε την σελίδα www.epp.teiher.gr σε ip διεύθυνση. Με την ip διεύθυνση του στόχου προσπαθήσαμε να παραβιάσουμε τον κωδικό πρόσβασης του Ε.Π.Π.

Εικόνα 2:Μετατροπή url σε ip address.



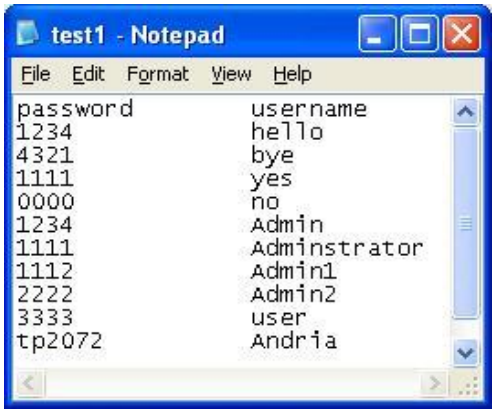
Εικόνα 3:Αποτυχημένη προσπάθεια παραβίασης www.epp.teiher.gr

Στην προσπάθεια μας εμφανίστηκε ένα σφάλμα συστήματος (error 53).

Το πιο κοινό σύμπτωμα ενός προβλήματος στην επίλυση NetBIOS είναι όταν με το ping επιστρέφει το μήνυμα λάθους 53. Αυτό το μήνυμα λάθους μας το εμφανίζει γενικά όταν αποτυγχάνει να δώσει ένα συγκεκριμένο όνομα υπολογιστή. Το σφάλμα 53 μπορεί επίσης να εμφανιστεί όταν υπάρχει ένα πρόβλημα για τη θέσπιση μιας περιόδου λειτουργίας του NetBIOS. Εάν ο υπολογιστής βρίσκεται στο τοπικό υποδίκτυο, επιβεβαιώνουμε ότι το όνομα είναι γραμμένο σωστά και ότι ο υπολογιστής προορισμού εκτελεί το πρωτόκολλο TCP / IP . Εάν ο υπολογιστής δεν είναι στο τοπικό υποδίκτυο, είμαστε βέβαιοι ότι το όνομα και η IP διεύθυνση χαρτογράφησης είναι διαθέσιμες στη βάση δεδομένων του DNS, του Hosts ή LMHOSTS, ή η βάση δεδομένων WINS.

Το μάντεμα ενός κωδικού πρόσβασης γίνεται επίσης εύκολα με script μέσω της γραμμής εντολών γράφοντας ένα απλό βρόγχο που να χρησιμοποιεί την εντολή FOR του κελύφους των Windows και την προηγούμενη σύνταξη του net use. Κατ' αρχάς, δημιουργούμε ένα απλό αρχείο με κοινούς συνδυασμούς ονομάτων χρηστών και κωδικών πρόσβασης (δείτε, για παράδειγμα, το http://www.virus.org/default-password/). Ένα τέτοιο αρχείο θα μπορούσε να μοιάζει με το πιο κάτω.

[file: test1.txt]



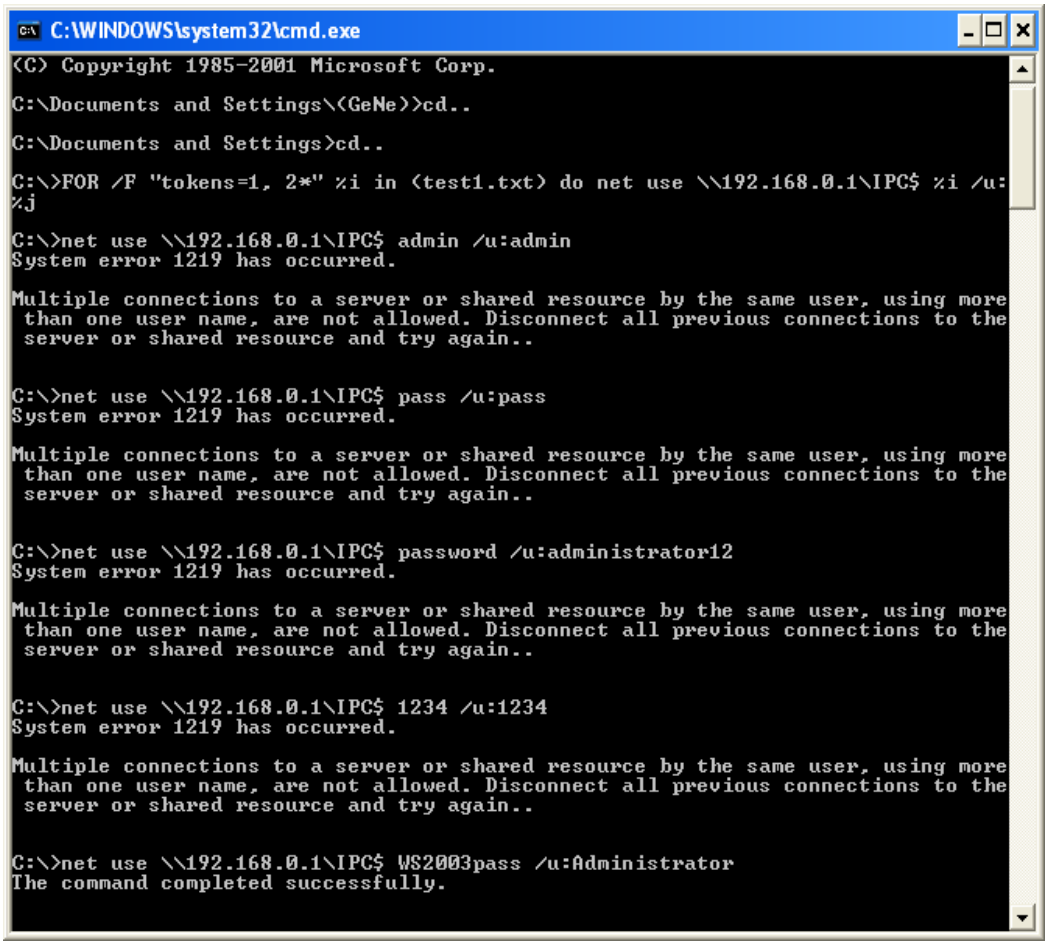
Εικόνα 4:Αρχείο με κοινούς συνδυασμούς ονομάτων χρηστών και κωδικών πρόσβασης

Σημειώστε ότι μπορεί να χρησιμοποιηθεί οποιοσδήποτε διαχωριστικό για να χωρίσετε τις τιμές – εμείς εδώ χρησιμοποιήσαμε tab. Επίσης παρατηρήσαμε ότι οι κενοί κωδικοί πρόσβασης θα πρέπει να υποδηλώνονται σαν εισαγωγικά («») στην αριστερή στήλη.

Τώρα μπορούμε να εισάγουμε αυτό το αρχείο στην εντολή FOR, όπως φαίνετε παρακάτω:

```
C:\>FOR /F "tokens=1, 2*" %i in (test1.txt) do net use \\target\IPC$
%i /u:%j
```

Αυτή η εντολή αναλύει το test1.txt, παίρνοντας τα δυο πρώτα στοιχεία από κάθε γραμμή και εισάγοντας μετά το πρώτο στοιχείο ως μεταβλητή %i (κωδικός πρόσβασης) και το δεύτερο ως %j (το όνομα χρήστη) σε μια τυπική προσπάθεια σύνδεσης με τη χρήση της εντολής net use στον κοινόχρηστο πόρο IPC$ του διακομιστή-στόχου. Πληκτρολογώντας FOR /? στη γραμμή εντολών μπορούμε να βρούμε περισσότερες πληροφορίες για την εντολή FOR –είναι μια από τις πιο χρήσιμες για τους hacker των Windows.



Εικόνα 5:Εκτέλεση script με την εντολή FOR για αυτοματοποίηση της διαδικασίας.

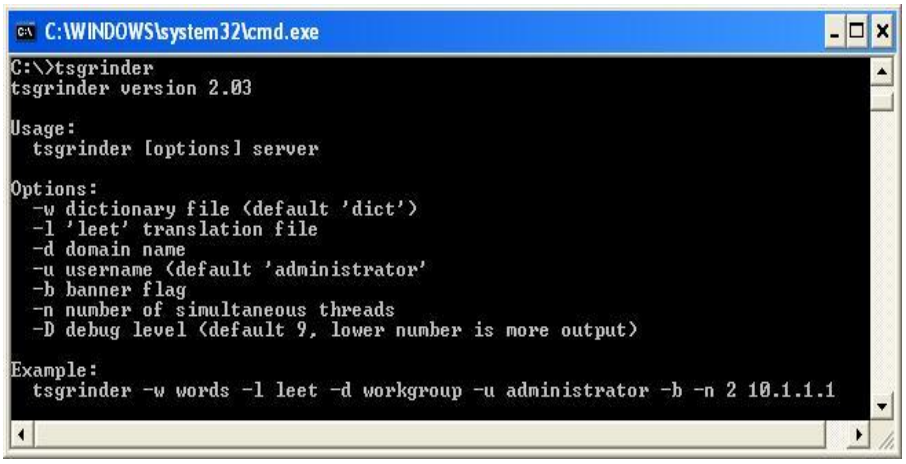
System error 1219 has occurred

Οι πολλαπλές συνδέσεις σε ένα διακομιστή ή κοινόχρηστο πόρο από τον ίδιο χρήστη, χρησιμοποιώντας περισσότερα username, δεν επιτρέπονται. Γίνεται αποσύνδεση όλων των προηγούμενων συνδέσεων με το διακομιστή ή κοινόχρηστο πόρο και προσπαθούμε ξανά μέχρι να βρεθεί ο σωστός συνδυασμός για να ολοκληρωθεί.

Φυσικά, πολλά ειδικά προγράμματα αυτοματοποιούν το μάντεμα ενός κωδικού πρόσβασης (ένας περιεκτικός κατάλογος βρίσκεται στο http://www.tenebril.com/src/spyware/password-guess-software.php). Μερικά από τα πιο δημοφιλή δωρεάν εργαλεία περιλαμβάνουν το enum, Brutus, THC Hydra, Medusa (www.foofus.net) και Venom (www.cqure.net - Το Venom μέσω του Windows Management Instrumentation ή WMI, εκτός από το SMB).

Το μάντεμα κωδικών πρόσβασης του Terminal Server είναι πιο περίπλοκο, αφού η εισαγωγή του κωδικού πρόσβασης γίνεται μέσω γραφικού περιβάλλοντος. (Bitmapped Graphical Interface). Το TSGrinder αυτοματοποιεί το μάντεμα κωδικού πρόσβασης στο Terminal Server από μακριά και είναι διαθέσιμο από την διεύθυνση http://www.hammerofgod.com/download.html.

Πιο κάτω φαίνονται οι διάφορες επιλογές που μπορούμε να χρησιμοποιήσουμε στο TSGrinder.



Εικόνα 6:Εντολή Tsgrinder

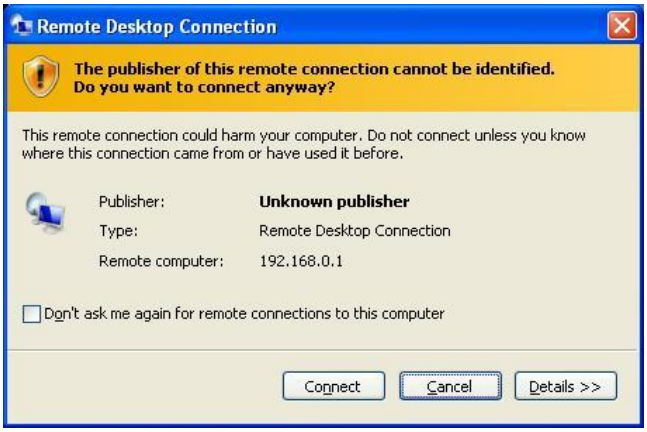
Παρακάτω δείχνουμε μια προσπάθεια σύνδεσης TSGrinder[2] που μαντεύει επιτυχώς έναν κωδικό πρόσβασης σε ένα σύστημα Windows Server 2003.

Βλέπουμε την αυτοματοποιημένη προσπάθεια που γίνεται μέχρι να βρεθεί ο αντίστοιχος κωδικό πρόσβασης.

```
C:\>tsgrinder 192.168.0.54
password hansel - failed
password gretel - failed
password witch - failed
password gingerbread - failed
password snow - failed
password white - failed
password apple - failed
password WS2003pass - success!
```

Το γραφικό παράθυρο σύνδεσης εμφανίζεται παράλληλα με αυτήν την σύνοδο μέσω γραμμής εντολών.

Αφού η προσπάθεια είναι επιτυχής τότε μας εμφανίζεται το παράθυρο Remote Desktop Connection για να ζητήσει άδεια ώστε να γίνει η σύνδεση.



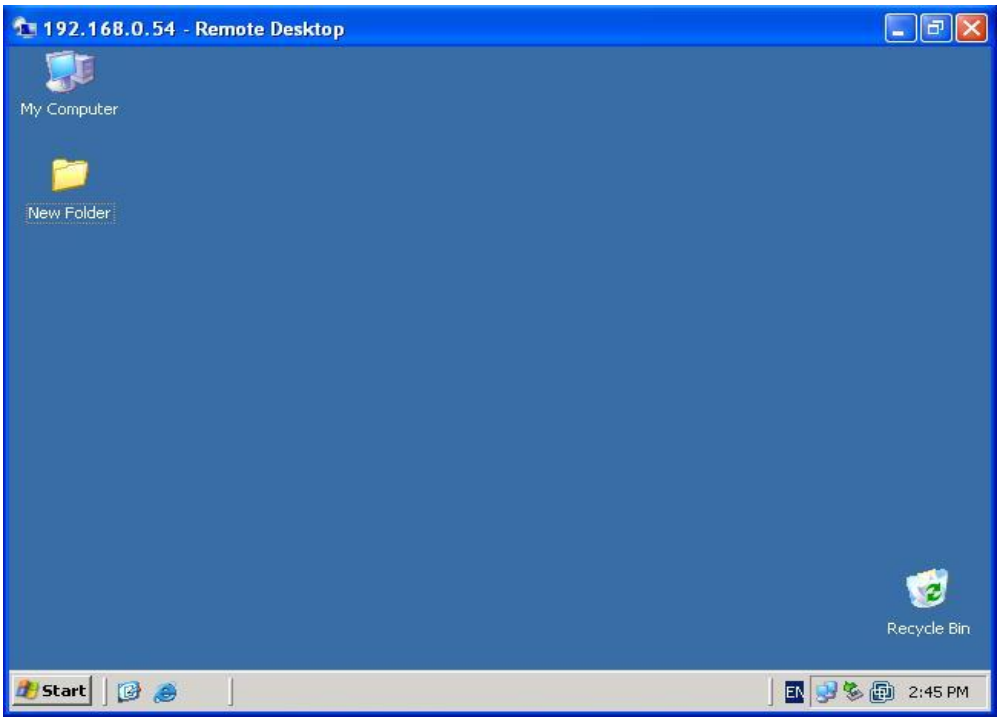
Εικόνα 7:Παράθυρο του Remote connection.

[2] Video: *http://www.youtube.com/watch?v=W8RnZfqDiQo*

Εφόσον επιλέξουμε την επιλογή Connect τότε συνδέεται αυτόματα στον Server 2003.

Εικόνα 8:Γραφικό Παράθυρο Σύνδεσης.

Εδώ ολοκληρώνεται με επιτυχία η διαδικασία απομακρυσμένης σύνδεσης με τη χρήση του TSGrinder.



Εικόνα 9:Σύνδεση στον Windows Server 2003.

Για μάντεμα άλλων υπηρεσιών όπως Sharepoint ,συστήνουμε πάλι το Hydra της THC ή το Brutus, αφού είναι συμβατά με πολλαπλά πρωτοκολλά, όπως το HTTP και το HTTPS. Το μάντεμα κωδικών πρόσβασης του SQL Server μπορεί να εκτελεσθεί με το sqlbf, που είναι διαθέσιμο για κατέβασμα από την διεύθυνση sqlsecurity.com.

2.1.1a Αντίμετρα στην Εύρεση Κωδικών Πρόσβασης

Μπορούμε να λάβουμε διάφορα αμυντικά μέτρα για να απαλείψουμε ή τουλάχιστον να αποτρέψουμε, μια τέτοια εύρεση κωδικών πρόσβασης, συμπεριλαμβανομένων των εξής:

• Χρησιμοποιούμε το Firewall στο δικτύου για να περιορίσουμε την πρόσβαση σε ενδεχομένως τρωτές υπηρεσίες (όπως στο SMB στην TCP 139 και 445,το MSRPC στην TCP 135 και το TS στην TCP 3389).

• Χρησιμοποιούμε το Windows Firewall (στα Windows XP και νεότερα) για να περιορίσουμε την πρόσβαση σε υπηρεσίες.

• Απενεργοποιούμε περιττές υπηρεσίες (να είστε ιδιαίτερα προσεκτικοί για το SMB στην TCP 139 και 445).

• Επιβάλλετε η χρήση δυνατών κωδικών πρόσβασης χρησιμοποιώντας πολιτικές.

• Ορίζουμε ένα κατώτατο όριο προσπαθειών σύνδεσης σε ένα λογαριασμό και εξασφαλίζουμε ότι ισχύει για τον ενσωματωμένο λογαριασμό του διαχειριστή.

•Καταγράφουμε τις αποτυχίες σύνδεσης σε λογαριασμούς και να επιθεωρούμε τακτικά το Event Logs.

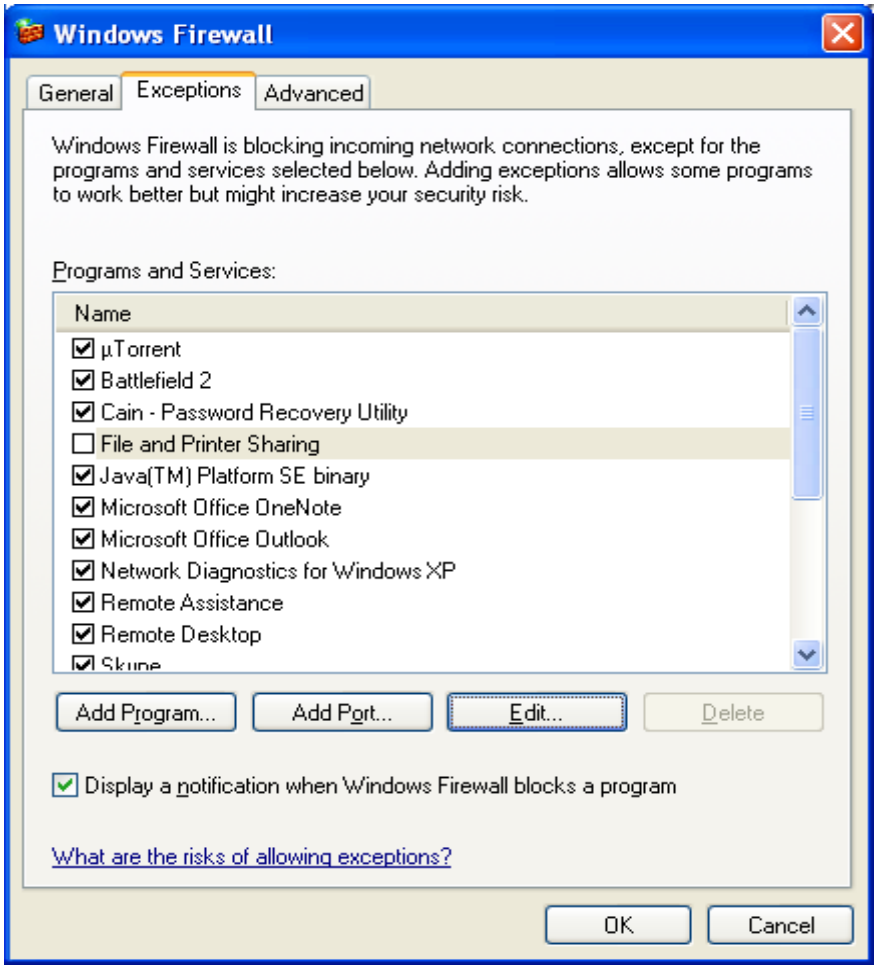
Ειλικρινά, υποστηρίζουμε ότι πρέπει να χρησιμοποιούμε όλους αυτούς τους μηχανισμούς παράλληλα για να επιτύχουμε μία εις βάθος άμυνα, αν είναι δυνατόν. Ας συζητήσουμε κάθε ένα από αυτά εν συντομία.

Περιορίζοντας την πρόσβαση σε υπηρεσίες χρησιμοποιώντας ένα Firewall Δικτύου

Αυτό είναι ενδεδειγμένο εάν το σύστημα των Windows δεν θα πρέπει να απαντά σε αιτήματα για κοινόχρηστους πόρους των Windows ή για απομακρυσμένη πρόσβαση τερματικών. Μπλοκάρετε την πρόσβαση σε όλες τις περιττές θύρες TCP και UDP στην περίμετρο του firewall ή του δρομολογητή του δικτύου, ειδικά τις TCP 139 και 445. Σπάνια να υπάρχει εξαίρεση για το SMB έξω από το firewall παρέχει απλώς πάρα πολλούς κίνδυνους και μπορεί να δεχτεί έτσι ένα ευρύ φάσμα επιθέσεων.

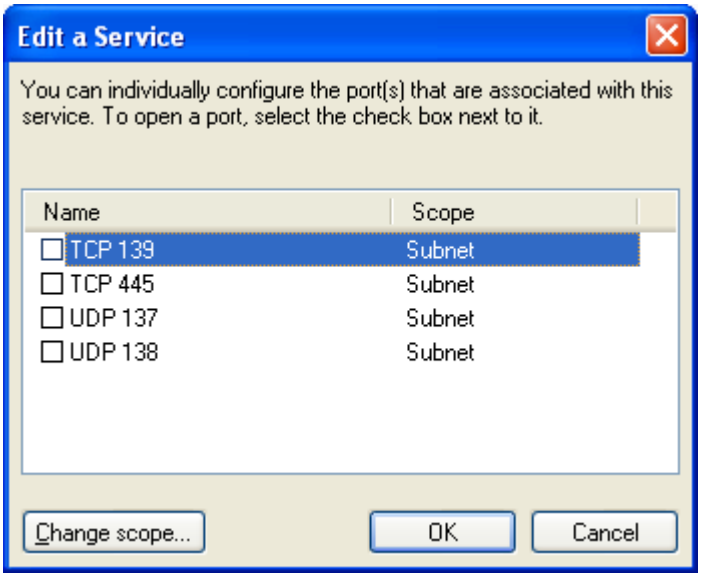
Για να μπλοκάρουμε την πρόσβαση σε όλες τις περιττές θύρες ακολουθούμε τα εξής βήματα:

Από το Start επιλέγουμε το Control panel και στην συνέχεια του Windows firewall την καρτέλα Exceptions.



Εικόνα 10:Εξαίρεση της υπηρεσίας File and Printer Sharing.

Για να απενεργοποιήσουμε τις συγκεκριμένες θύρες TCP και UDP αποεπιλέγουμε το File and Printer Sharing και στην συνέχεια πατάμε Edit.



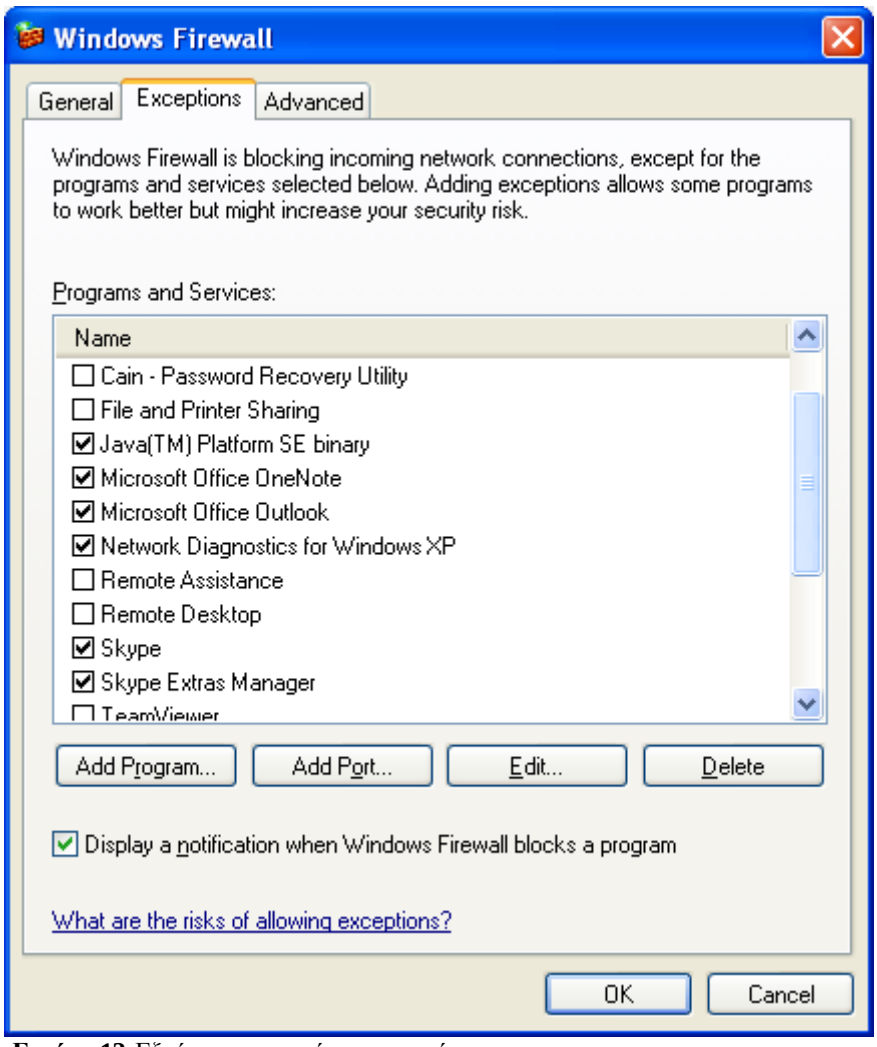
Εικόνα 11:Απενεργοποίηση περιττών θυρών TCP και UDP.

Απενεργοποιούμε τις θύρες των υπηρεσιών. Επίσης αυτό μπορεί να γίνει και μέσω άλλων Firewall.

Χρήση του Windows Firewall για να περιοριστεί η πρόσβαση στις υπηρεσίες

Το Internet Connection Firewall (ICF) εμφανίστηκε στα Windows XP και μετονομάστηκε σε επόμενες αναβαθμίσεις του λειτουργικού συστήματος σαν Windows Firewall. Μην ξεχνάμε ότι ένα Firewall είναι απλώς ένα εργαλείο-είναι οι κανόνες του Firewall που ορίζουν στην πραγματικότητα επίπεδο προστασίας, γι' αυτό πρέπει να είμαστε προσεκτικοί ποιες εφαρμογές επιτρέπουμε.

Για να απενεργοποιήσουμε την πρόσβαση σε όλες τις περιττές υπηρεσίες ακολουθούμε τα εξής βήματα: *Start →Control panel →Windows firewall →Tab exceptions.*



Εικόνα 12:Εξαίρεση περιττών υπηρεσιών.

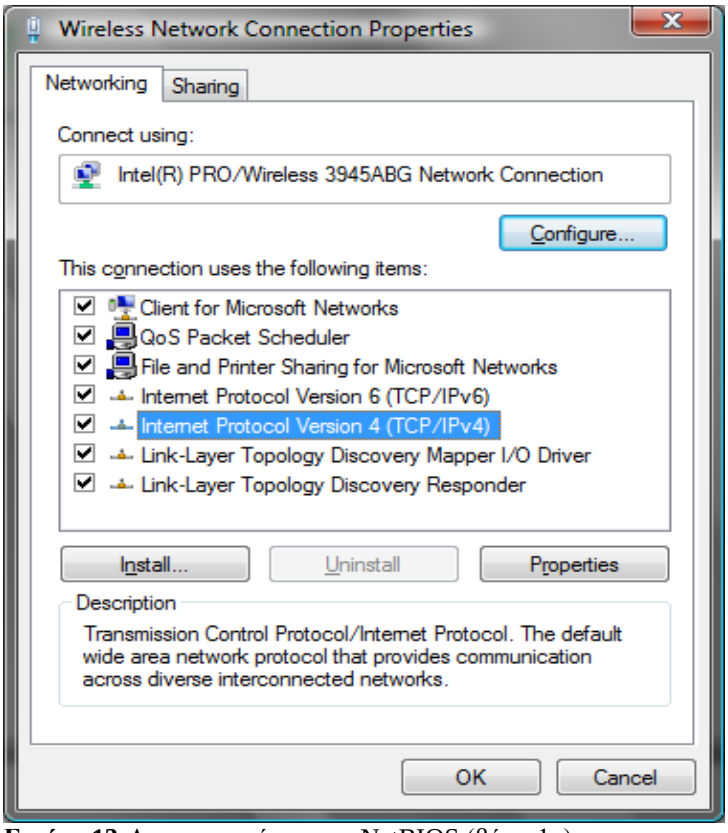
Δεν είναι απαραίτητο να έχουμε ενεργοποιημένες όλες τις υπηρεσίες όταν δεν τις χρησιμοποιούμε ούτως ώστε να έχουμε περισσότερη ασφάλεια στο λειτουργικό μας.

Απενεργοποίηση μη απαραίτητων υπηρεσιών

Η ελαχιστοποίηση του αριθμού των υπηρεσιών που εκτίθενται στο δίκτυο είναι ένα από τα σημαντικότερα μέτρα που λαμβάνουν τη βελτίωση ασφαλείας συστημάτων. Ειδικότερα, είναι σημαντικό να απενεργοποιήσουμε το NetBIOS[3] και SMB ώστε να μετριαστούν οι επιθέσεις που αναφέραμε νωρίτερα.

Η απενεργοποίηση του NetBIOS και SMB αποτελούσε ένα εφιάλτη για τις παλαιότερες εκδόσεις των Windows. Στα Vista και στον Windows 2008, μπορούν να απενεργοποιηθούν πρωτόκολλα δικτύων ή/και να αφαιρεθούν χρησιμοποιώντας το φάκελο Network Connections (αναζήτηση στο technet.microsoft.com για το "Enable or Disable a Network Protocol or Component" [ενεργοποίηση ή απενεργοποίηση ενός πρωτοκόλλου ή στατικού δικτύου] ή για το "Remove a Network Protocol or Component" [κατάργηση ενός πρωτοκόλλου ή συστατικού δικτύου]). Μπορούμε επίσης να χρησιμοποιήσουμε το Network and Sharing Center ώστε να ελέγχουμε την ανακάλυψη δικτύων και κοινή χρήση πόρων (αναζήτηση στο TechNet για "Enable or Disable Sharing and Discovery").

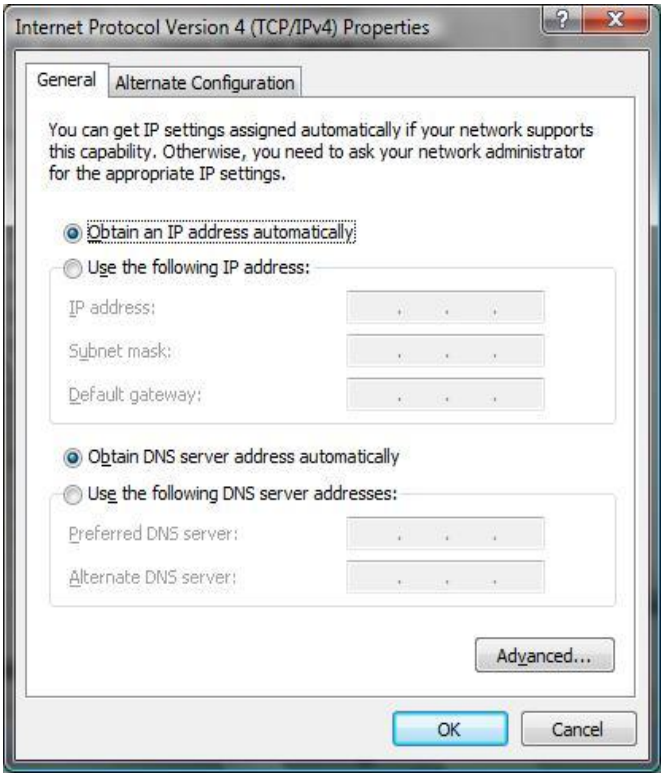
Για να απενεργοποιήσουμε το Netbios πηγαίνουμε στο Control Panel στο φάκελο Network Connections επιλέγουμε το Internel Protocol (IPv4).



Εικόνα 13: Απενεργοποίηση του NetBIOS (βήμα 1ο)

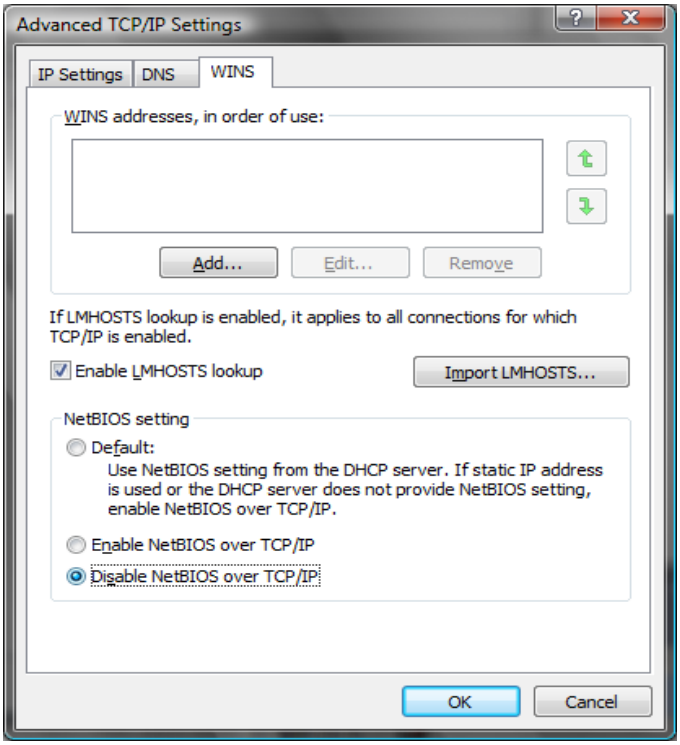
Εφόσον έχουμε επιλεγμένο το Internel Protocol (IPv4) πατάμε στην επιλογή Properties και έτσι μας εμφανίζεται το παράθυρο που βλέπουμε πιο κάτω.

[3] http://articles.techrepublic.com.com/5100-10878_11-6065923.html



Εικόνα 14:Απενεργοποίηση του Netbios (βήμα 2ο)

Επιλέγουμε την καρτέλα Advanced και στην συνέχεια από την καρτέλα WINS απενεργοποιούμε το NetBIOS.



Εικόνα 15:Απενεργοποίηση του Netbios (βήμα 3ο)

Στην πιο πάνω εικόνα έχει ολοκληρωθεί η διαδικασία της απενεργοποίησης του NetBIOS. Εάν θέλουμε όμως να έχουμε μεγαλύτερη ασφάλεια μπορούμε να το κάνουμε uninstall ώστε να μην υπάρχει τρόπος ενεργοποίησης του.

Για να το κάνουμε uninstall πηγαίνουμε στο Control Panel και ακολούθως στο φάκελο Network Connections και εκεί επιλέγουμε από το Local Area Connection το Properties. Στην συνέχεια επιλέγουμε Client For Microsoft Networks και πατάμε το κουμπί Uninstall. Αφού τελειώσει η διαδικασία του Uninstall , επιλέγουμε File And Printer Sharing For Microsoft Network και πατάμε το κουμπί Uninstall.

Το Group Policy μπορεί να χρησιμοποιηθεί για απενεργοποίηση της εύρεσης και κοινής χρήσης για συγκεκριμένους χρήστες και ομάδες μέσω ενός περιβάλλοντος Windows/domain. Ξεκινώντας το Group Policy Management Console (GPMC) κάνουμε κλικ στο Start, και μετά στο πλαίσιο Start Search πληκτρολογούμε **gpmc.msc**. Στο πλαίσιο πλοήγησης, ανοίγουμε τους παρακάτω φακέλους: Local Computer Policy,User Configuration, Administrative Templates, Windows Components, and Network Sharing. Επιλέγουμε την πολιτική που θέλουμε να επιβάλουμε από το πλαίσιο λεπτομερών, το ανοίγουμε και κάνουμε κλικ στο Enable ή Disable και μετά το OK.

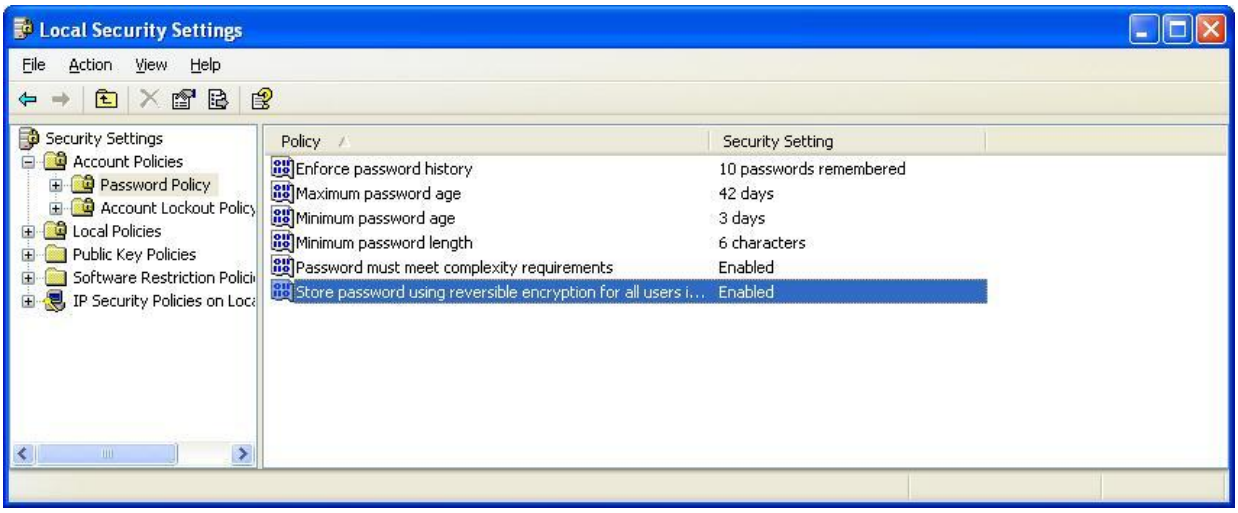
Επιβολή δυνατών κωδικών πρόσβασης χρησιμοποιώντας πολιτικές

Η Microsoft παρέχει διάφορους τρόπους να απαιτείται αυτόματα από τους χρήστες να χρησιμοποιούν δυνατούς κωδικούς πρόσβασης. Όλα έχουν εδραιωθεί στην λειτουργία πολιτικής λογαριασμών που βρίσκεται στο Security Policy| Account Policies|Password Policy στα Windows 2000 και νεότερα (το Security Policy μπορούμε να το βρούμε μέσω Control Panel | Administrative Tools, ή απλώς τρέχοντας το secpol.msc). Χρησιμοποιώντας αυτή τη λειτουργία, μπορούν να επιβληθούν ορισμένες πολιτικές κωδικών πρόσβασης λογαριασμών, όπως ελάχιστο μήκος και πολυπλοκότητα. Μπορούν επίσης να κλειδωθούν λογαριασμοί μετά από έναν καθορισμένο αριθμό αποτυχημένων προσπαθειών σύνδεσης. Η λειτουργία του Account Policy επιτρέπει σε διαχειριστές να αποσυνδέουν χρήστες όταν λήξη η ώρα σύνδεσης. Οι ρυθμίσεις στο Windows Account Policy παρουσιάζονται παρακάτω.[4]

Start → Control panel → Administrative tools → Local Security Policy → Account policy → Password policy

[4] Επεξήγηση στο Παράρτημα Γ.1

Στην πιο κάτω εικόνα έχουμε τροποποιήσει τις ρυθμίσεις του Password Policy.



Εικόνα 16:Διαμόρφωση του Windows Password policy.

- Στο Enforce password history ορίζουμε τον ελάχιστο αριθμό αποθήκευσης κωδικών πρόσβασης.

- Στο Maximum password age ορίζουμε τον μέγιστο αριθμό ημερών που διαρκεί ο κάθε κωδικός πρόσβασης.

- Στο Minimum password age ορίζουμε τον ελάχιστο αριθμό ημερών που διαρκεί ο κάθε κωδικός πρόσβασης.

- Στο Minimum password length ορίζουμε το ελάχιστο μήκος του κωδικού πρόσβασης.

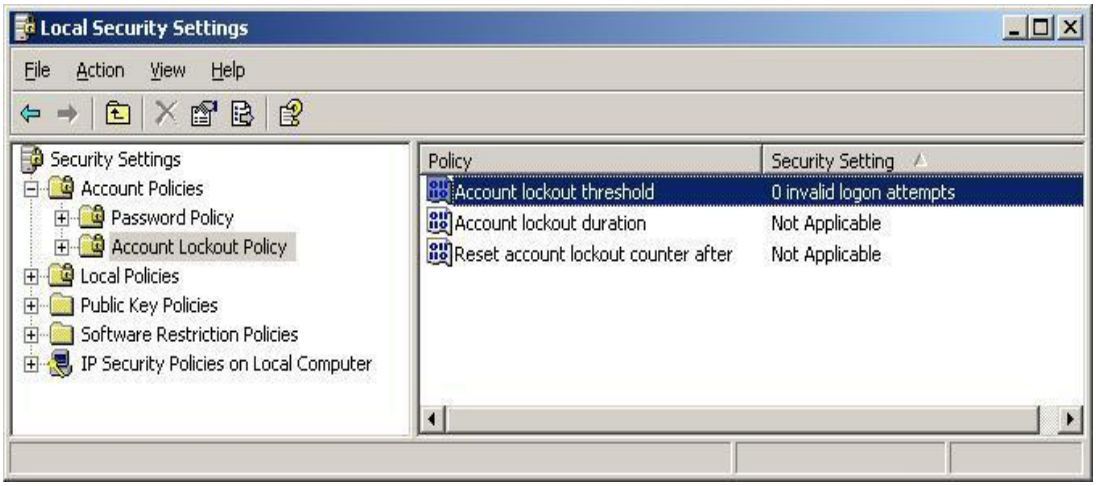
- Στο Password must meet complexity requirements κάνουμε ενεργοποίηση έτσι ώστε ο κωδικός πρόσβασης να πληροί την απαραίτητη πολυπλοκότητα.

- Στο Store password using reversible encryption for all users in the domain αποθηκεύονται οι κωδικοί πρόσβασης με την χρήση αναστρέψιμης κρυπτογράφησης για όλους τους χρήστες στον τομέα.

Όρια Κλειδώματος

Ίσως ένα από τα σημαντικότερα μέτρα όπου πρέπει να λάβουμε για να μετριάσουμε τις επιθέσεις μαντέματος κωδικών πρόσβασης SMB είναι να τεθεί ένα κατώτατο όριο κλειδώματος λογαριασμών. Μόλις ένας χρήστης φθάσει σ' αυτόν τον αριθμό αποτυχημένων προσπαθειών σύνδεσης, ο λογαριασμός κλειδώνεται έως ότου ο διαχειριστής τον επαναφέρει ή μέχρι να περάσει ένα χρονικό διάστημα καθορισμένο από τον διαχειριστή. Τα κατώτατα όρια κλειδώματος μπορούν να ορισθούν μέσω του Security Policy| Account Policies|Account Lockout Policy στα Windows 2000 και νεότερα.

Start → Control panel → Administrative tools → Local Security Policy → Account policy → Account Lockout Policy



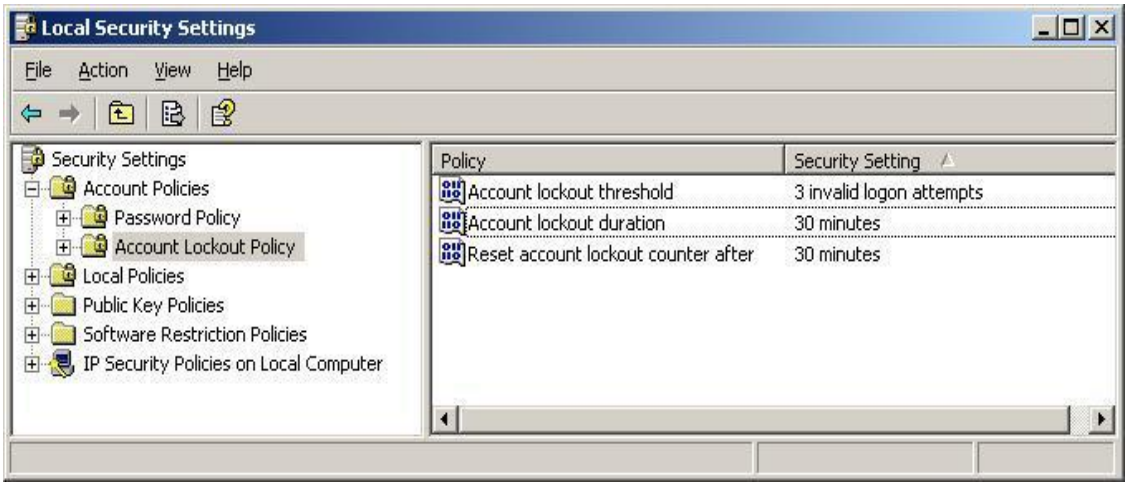
Εικόνα 17:Προκαθορισμένες ρυθμίσεις του Account Lockout Policy

Στην πιο κάτω εικόνα έχουμε τροποποιήσει τις ρυθμίσεις του Account Lockout Policy για καλύτερη ασφάλεια.

- Στο Account lockout threshold ορίζουμε τον αριθμό των προσπαθειών που μπορεί να κάνει ένας χρήστης για να ενωθεί σε ένα λογαριασμό, αυτό ονομάζεται όριο κλειδώματος.

- Στο Account lockout duration ορίζουμε το χρόνο που θα αναμένει ο χρήστης ώστε να μπορεί να ξανακάνει login στο σύστημα στην περίπτωση που έχει κλειδωθεί ο λογαριασμός του .

- Στο Reset account lockout counter ορίζουμε τον χρόνο που χρειάζεται για να μηδενιστεί ο μετρητής για να ξανακάνουμε login στον λογαριασμό.



Εικόνα 18:Ρύθμιση κλειδώματος Account Lockout Policy

Προσαρμοσμένα μηνύματα κατά τη σύνδεση TS

Για να εμποδίσουμε απλές επιθέσεις κωδικών πρόσβασης με το Terminal Service (TS), εφαρμόζουμε μια προσαρμοσμένη νομική ειδοποίηση στην σύνδεση στα Windows. Αυτό μπορεί να γίνει προσθέτοντας ή τροποποιώντας τις τιμές του Registry που βλέπετε εδώ:

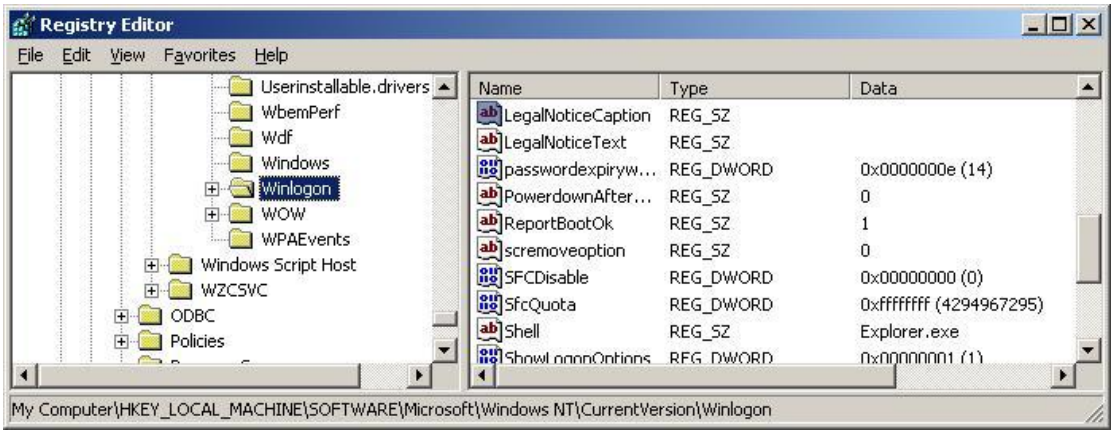
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

Για να μπούμε στο registry του υπολογιστή μας πάμε *start→run→regedit*

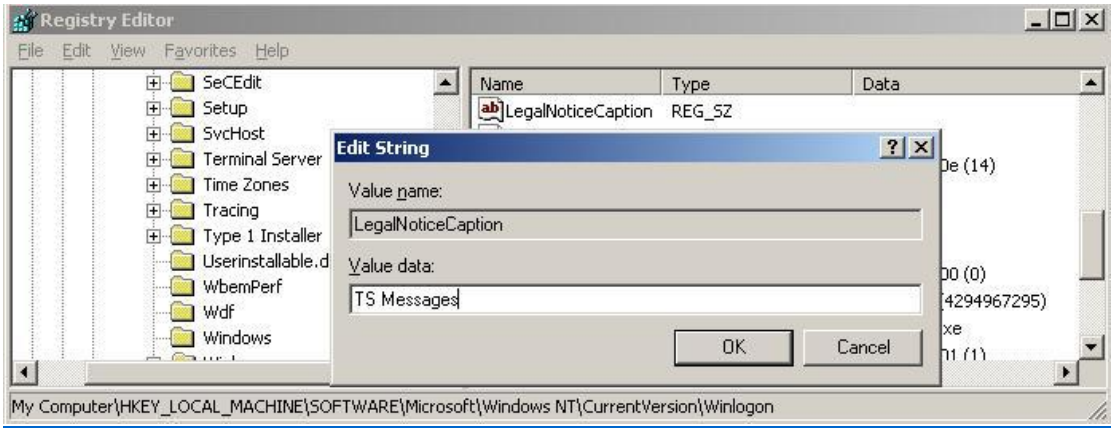
Όνομα	Τύπος δεδομένων	Τιμή
LegalNoticeCaption	REG_SZ	[προσαρμοσμένη λεζάντα]
LegalNoticeText	REG_SZ	[προσαρμοσμένο μήνυμα]

Πίνακας 1:Προσαρμογή μηνυμάτων κατά τη σύνδεση TS

Πιο κάτω φαίνονται οι τιμές LegalNoticeCaption και LegalNoticeText του Registry.

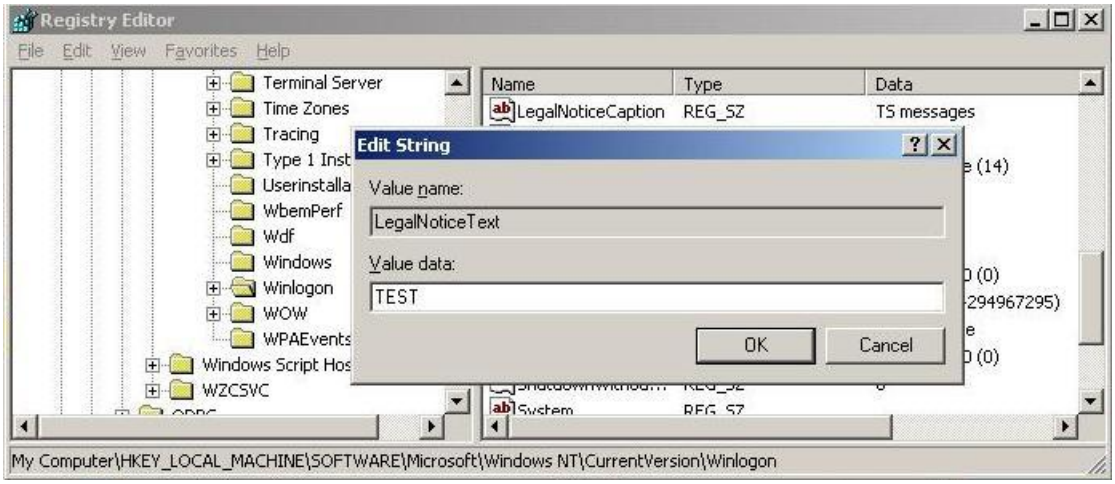


Εικόνα 19:Τροποποίηση των τιμών Registry για σύνδεση TS.



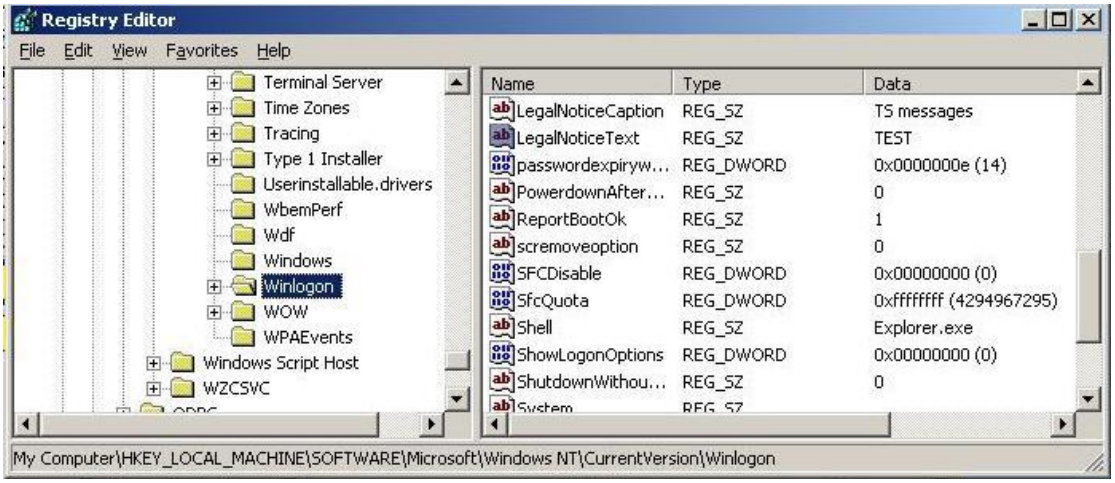
Εικόνα 20:Αλλαγή της τιμής Value Data του LegalNoticeCaption

Στο Value Data ορίζουμε την τιμή της προσαρμοσμένης λεζάντας σε TS Messages.



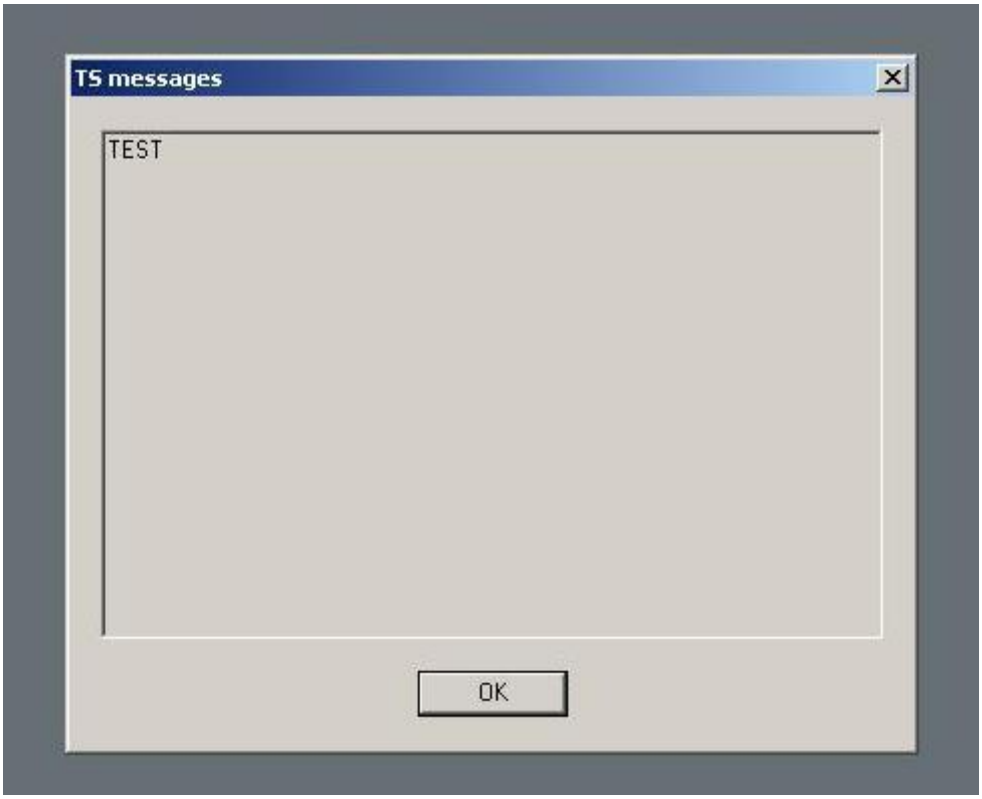
Εικόνα 21:Αλλαγή της τιμής Value Data του LegalNoticeText

Στο Value Data ορίζουμε την τιμή του προσαρμοσμένου μηνύματος σε TEST.



Εικόνα 22:Εμφάνιση τροποποίησης LegalNoticeCaption -LegalNoticeText

Τα Windows θα εμφανίσουν την προσαρμοσμένη λεζάντα και το μήνυμα που παρέχονται από αυτές τις τιμές αφού οι χρήστες πληκτρολογήσουν CTRL-ALT-DEL και πριν παρουσιασθεί το παράθυρο διαλόγου σύνδεσης, ακόμα και πριν γίνει σύνδεση μέσω Terminal Services.



Εικόνα 23:Εμφάνιση μηνύματος αναγνώρισης

Το TSGinder μπορεί εύκολα να παρακάμψει αυτό το αντίμετρο χρησιμοποιώντας την επιλογή –b, η οποία αναγνωρίζει οποιοδήποτε μήνυμα σύνδεσης πριν μαντέψει κωδικούς πρόσβασης.

Ακόμα κι αν δεν κάνει τίποτα για να εκτρέψει τις επιθέσεις με μάντεμα κωδικών πρόσβασης, ο καθορισμός προσαρμοσμένων μηνυμάτων θεωρείται μια αναγνωρισμένη ορθή πρακτική και μπορεί να παρέχει την δυνατότητα προσφυγής στην δικαιοσύνη, έτσι γενικά την συστήνουμε.

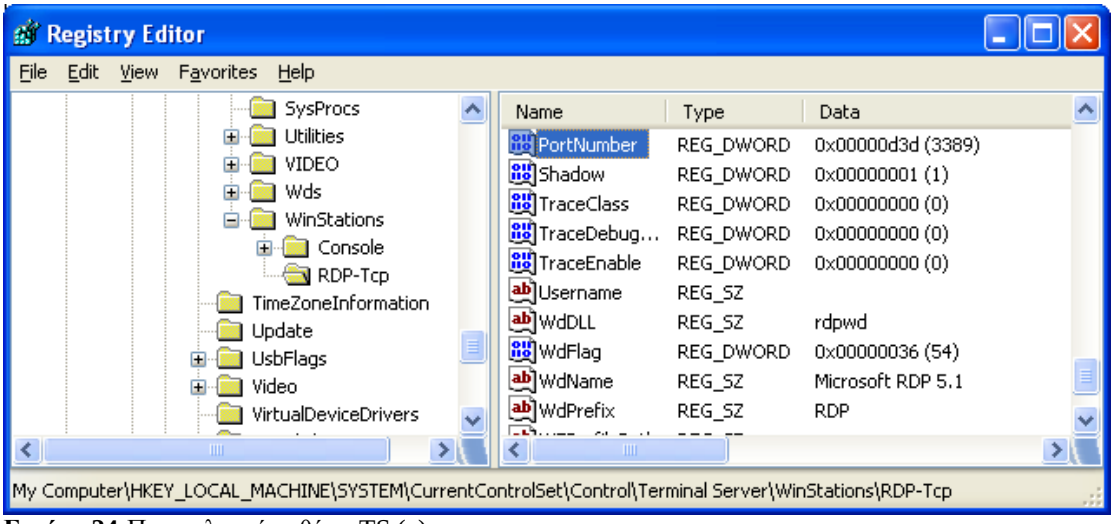
Αλλαγή προεπιλεγμένων θυρών TS

Ένα άλλο αντίμετρο για το μάντεμα κωδικού πρόσβασης είναι να αλλάξουμε την προεπιλεγμένη θύρα του Terminal Server. Φυσικά, αυτό δεν κάνει κάτι ώστε να δυσκολέψει την υπηρεσία να επιτεθεί, αλλά μπορεί να αποφύγει τους επιτιθέμενους που βιάζονται πολύ να διερευνήσουν πέρα από την προεπιλεγμένη σάρωση θυρών. Η αλλαγή της προεπιλεγμένης θύρας TS[5] μπορεί να γίνει τροποποιώντας το ακόλουθο στοιχείο του Registry.

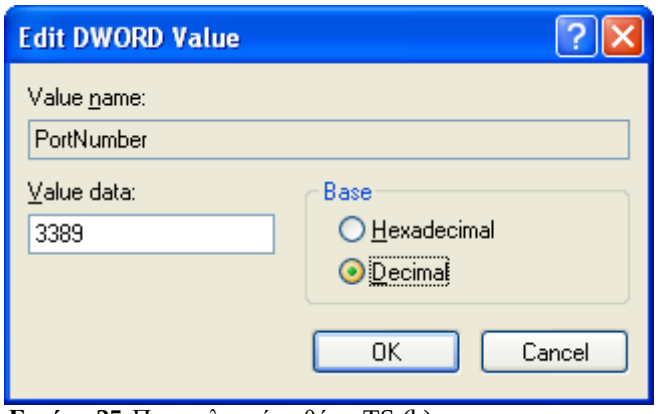
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\
WinStations\RDP-Tcp

[5] http://www.petri.co.il/use_rdp_client_to_connect_to_a_different_port.htm

Όταν βρούμε το υποκλειδί Port Number παρατηρούμε την αξία του 00000D3D, δεκαεξαδικού αντίστοιχο για το (3389).



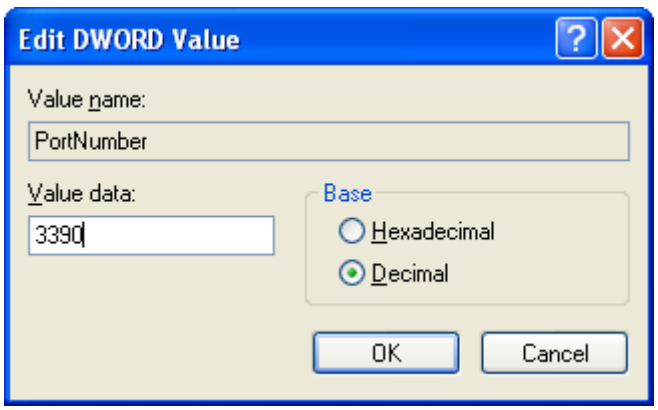
Εικόνα 24:Προεπιλεγμένη θύρα TS (a)



Εικόνα 25:Προεπιλεγμένη θύρα TS (b)

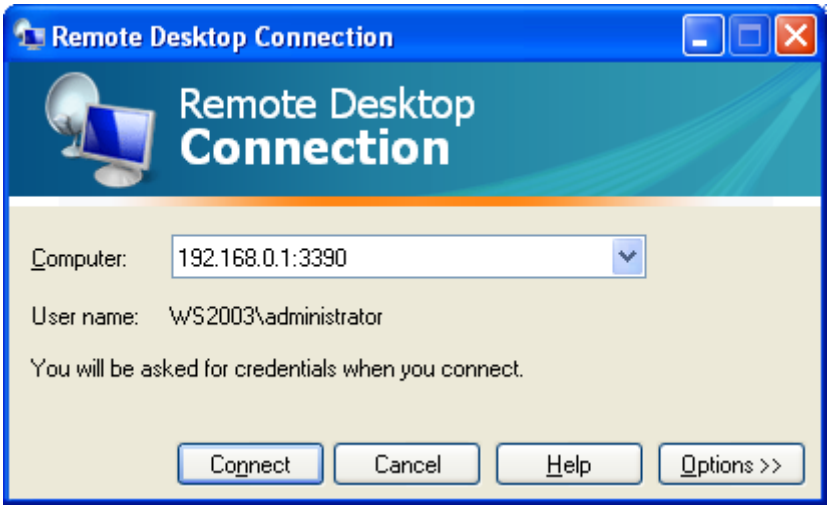
Στην συνέχεια, τροποποιούμε τον αριθμό θύρας σε δεκαεξαδική μορφή και αποθηκεύουμε τη νέα τιμή.

Στο Value data αλλάζουμε την θύρα Terminal Services.



Εικόνα 26:Αλλαγή προεπιλεγμένης θύρας TS σε 3390

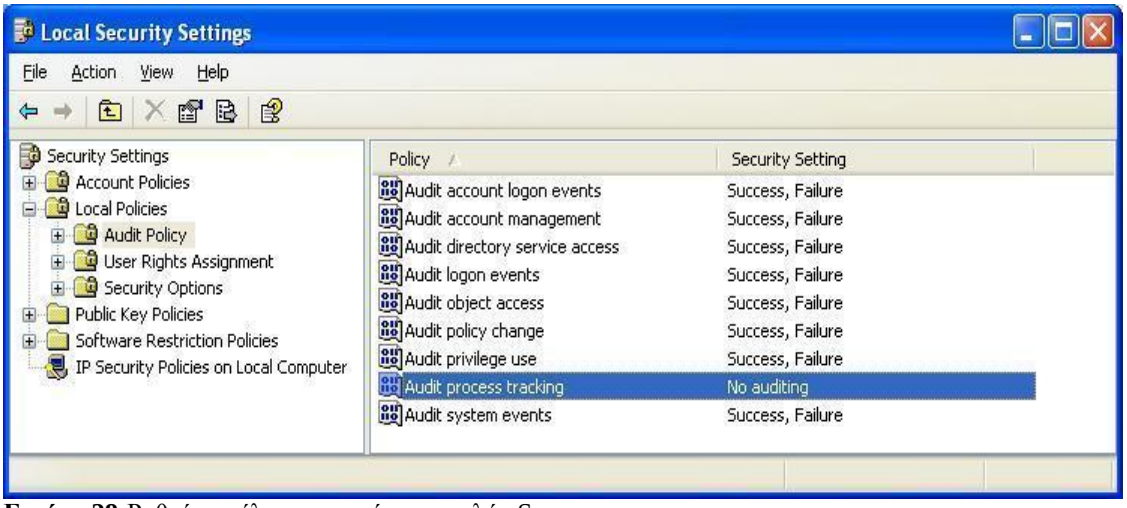
Φυσικά, οι πελάτες TS θα πρέπει τώρα να διαμορφωθούν για να φθάσουν στον server με την νέα θύρα, το οποίο γίνεται εύκολα με την προσθήκη «:[αριθμός_θύρας]» στο όνομα του server στο γραφικό πλαίσιο computer του πελάτη TS ή τροποποιώντας το αρχείο σύνδεσης πελάτη (*.rdp) για να συμπεριλαμβάνει τη γραμμή "Server Port = [αριθμός_θύρας]."



Εικόνα 27:Προσθήκη της νέας θύρας TS.

Έλεγχος και Σύνδεση

Ακόμα και αν κάποιος δεν μπορεί να μπει στο σύστημά μας μέσω εύρεσης κωδικών πρόσβασης επειδή έχουμε εφαρμόσει πολιτική πολυπλοκότητας και κλειδώματος κωδικών πρόσβασης, είναι ωστόσο καλύτερα να καταγράφουμε τις αποτυχημένες προσπάθειες σύνδεσης χρησιμοποιώντας Security Policy | Local Policies | Audit Policy. Στην πιο κάτω εικόνα παρουσιάζουμε την προτεινόμενη ρύθμιση για Windows XP στο Security Policy tool. Αν και αυτές οι ρυθμίσεις θα παράγουν τις πιο πληροφοριακές καταγραφές με σχετικά μικρές επιδράσεις στην απόδοση, προτείνουμε ότι θα πρέπει να δοκιμαστούν πριν εγκατασταθούν σε πραγματικά περιβάλλοντα.



Εικόνα 28:Ρυθμίσεις έλεγχου για ένα ασφαλής Server.

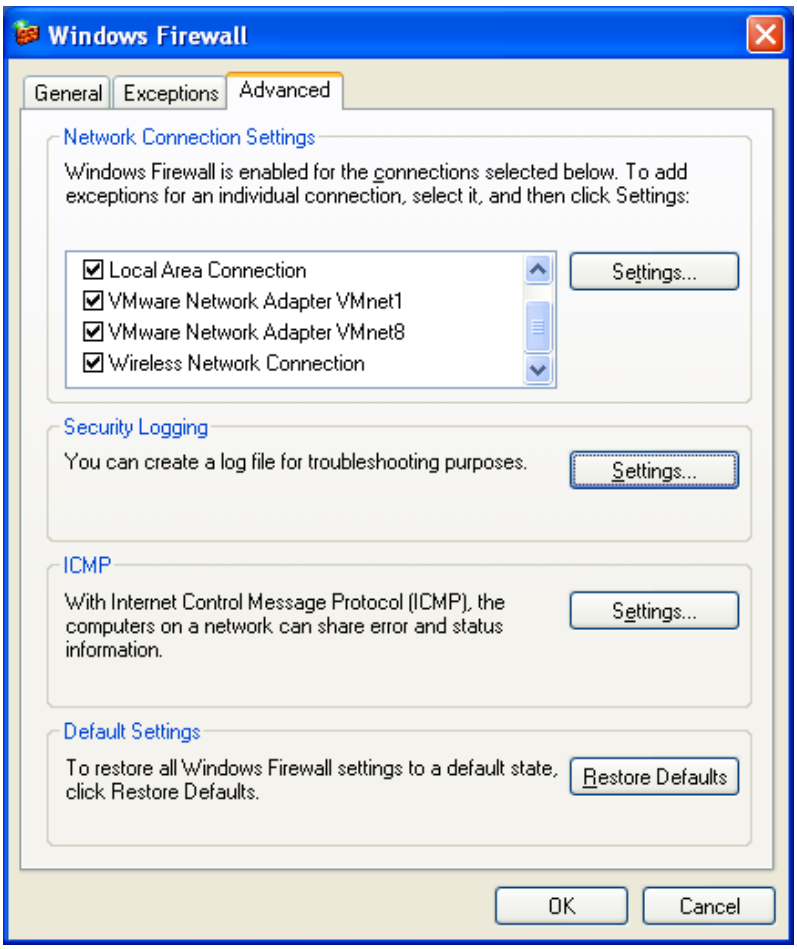
Για να ενεργοποιήσουμε το Security Log file πηγαίνουμε στο Control Panel στο φάκελο Network Connections επιλέγουμε το Local Area Connection.

Εφόσον έχουμε επιλεγμένο το Local Area Connection. πατάμε στην επιλογή Properties και έτσι μας εμφανίζεται το παράθυρο που βλέπουμε πιο κάτω.

Στην συνέχεια επιλέγουμε την καρτέλα Advanced και από το Windows Firewall πατάμε στο Settings.

Εικόνα 29: Local Area Connection Properties

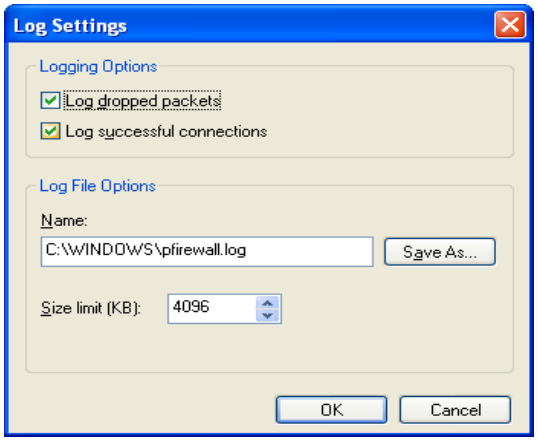
Ακολούθως από το παράθυρο που εμφανίζεται ξαναεπιλέγουμε την καρτέλα Advanced και από το Security Logging πατάμε στο Settings.



Εικόνα 30: Windows Firewall- Advanced

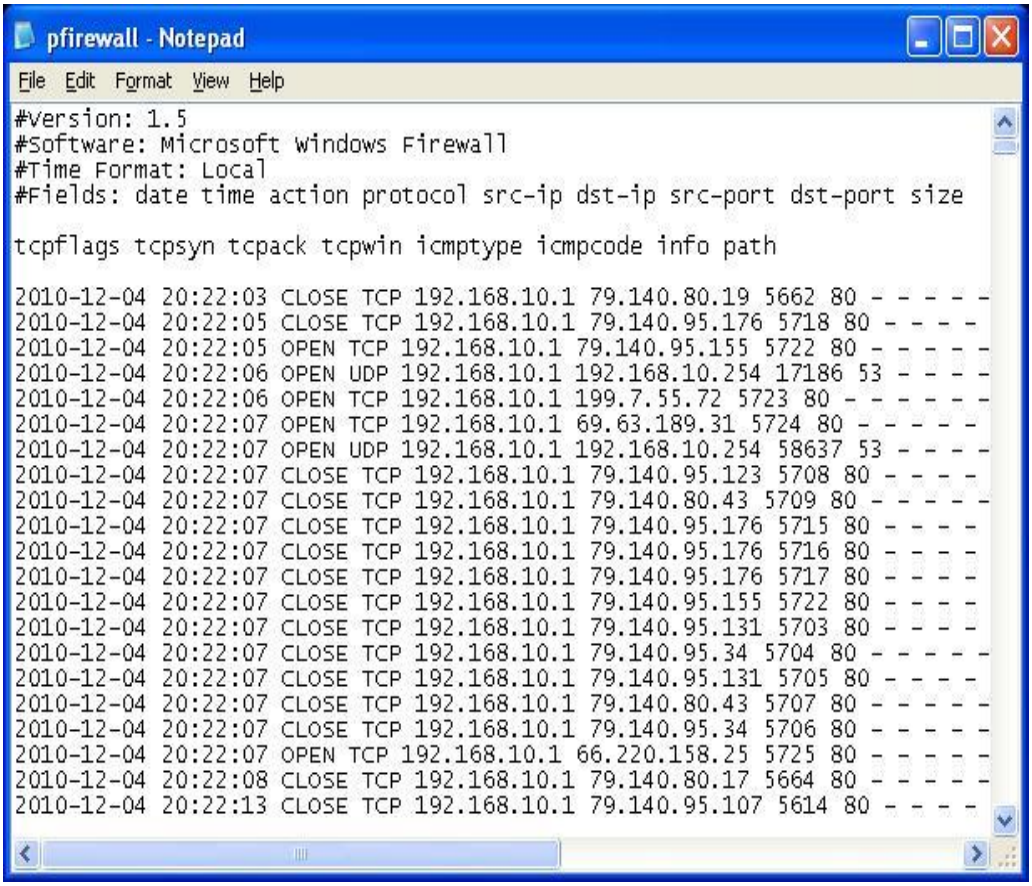
Πιο κάτω βλέπουμε τις ρυθμίσεις του Log Settings. Επιλέγουμε το Log dropped packets και Log Successful Connections.

Στο Log File Options επιλέγουμε το path που θέλουμε να αποθηκεύουμε τα Log Files και στο Size limit ορίζουμε το μέγεθος του αρχείου.



Εικόνα 31:Ρυθμίσεις Log File

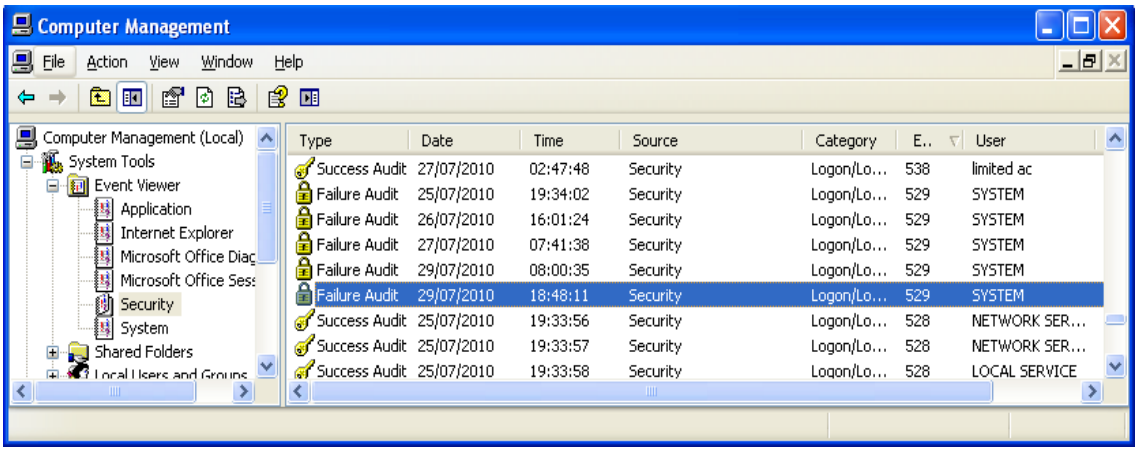
Πιο κάτω φαίνεται η δομή του Log File.



Εικόνα 32: Log File

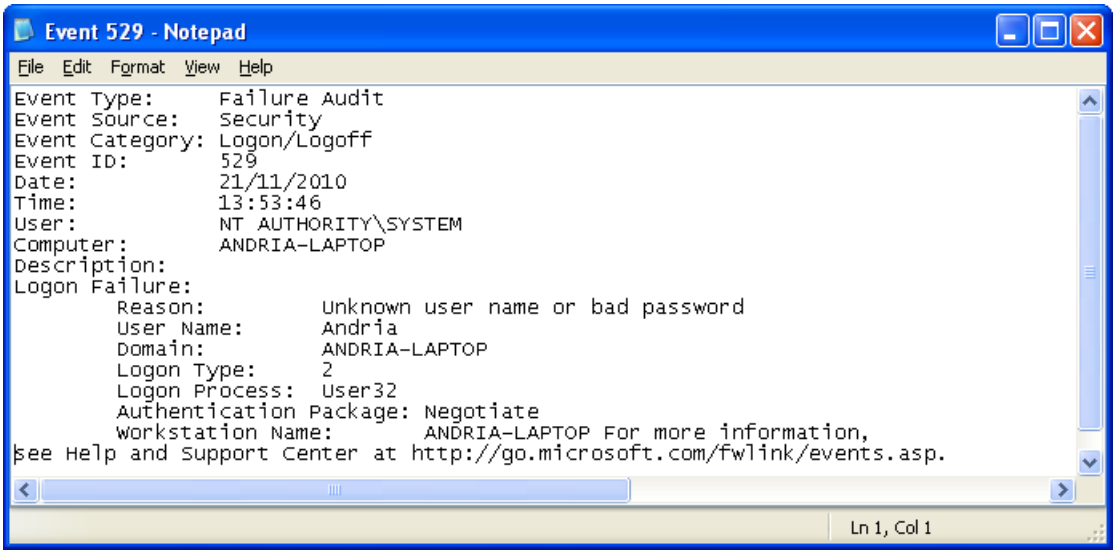
Φυσικά, δεν είναι αρκετό να ενεργοποιήσουμε απλώς τον έλεγχο. Θα πρέπει εξετάζουμε τακτικά τα logs για ενδείξεις εισβολής. Για παράδειγμα, ένα security log γεμάτο με συμβάντα 529 ή 539 αποτυχίες σύνδεσης / αποσύνδεσης και κλειδώματα λογαριασμών, αντίστοιχα-είναι μια πιθανή ένδειξη ότι είμαστε υπό μια αυτοματοποιημένη επίθεση (εναλλακτικά, μπορεί απλώς να σημαίνει ότι ένας κωδικός πρόσβασης υπηρεσίας κάποιου λογαριασμού έχει λήξει). Το αρχείο log θα προσδιορίσει ακόμη και το εμπλεκόμενο συστήματος στις περισσότερες περιπτώσεις. Δυστυχώς, η σύνδεση στα Windows δεν αναφέρει την IP διεύθυνση του συστήματος επίθεσης, μόνο το όνομα του NetBIOS. Φυσικά το ονόματα των NetBIOS μπορούν εύκολα να πλαστογραφηθούν(trivially spoofed), οπότε ο επιτιθέμενος μπορεί εύκολα να αλλάξει το όνομα του NetBIOS, και οι καταγραφές θα ήταν παραπλανητικές εάν το όνομα που επιλέχτηκε είναι συμβατό με κάποιου αλλού συστήματος ή αν το όνομα του NetBIOS επιλέγετε τυχαία με κάθε αίτηση.

Η <<χειροκίνητη>> εξέταση του Event Log είναι κουραστική, αλλά ευτυχώς ο Event Viewer έχει την δυνατότητα να φιλτράρει την ημερομηνία γεγονότος, τον τύπο, την πηγή, την κατηγορία, το χρήστη, τον υπολογιστή και το ID ενός συμβάντος .



Εικόνα 33: Event Veiwer

Περιεχόμενα του 529 Event Log

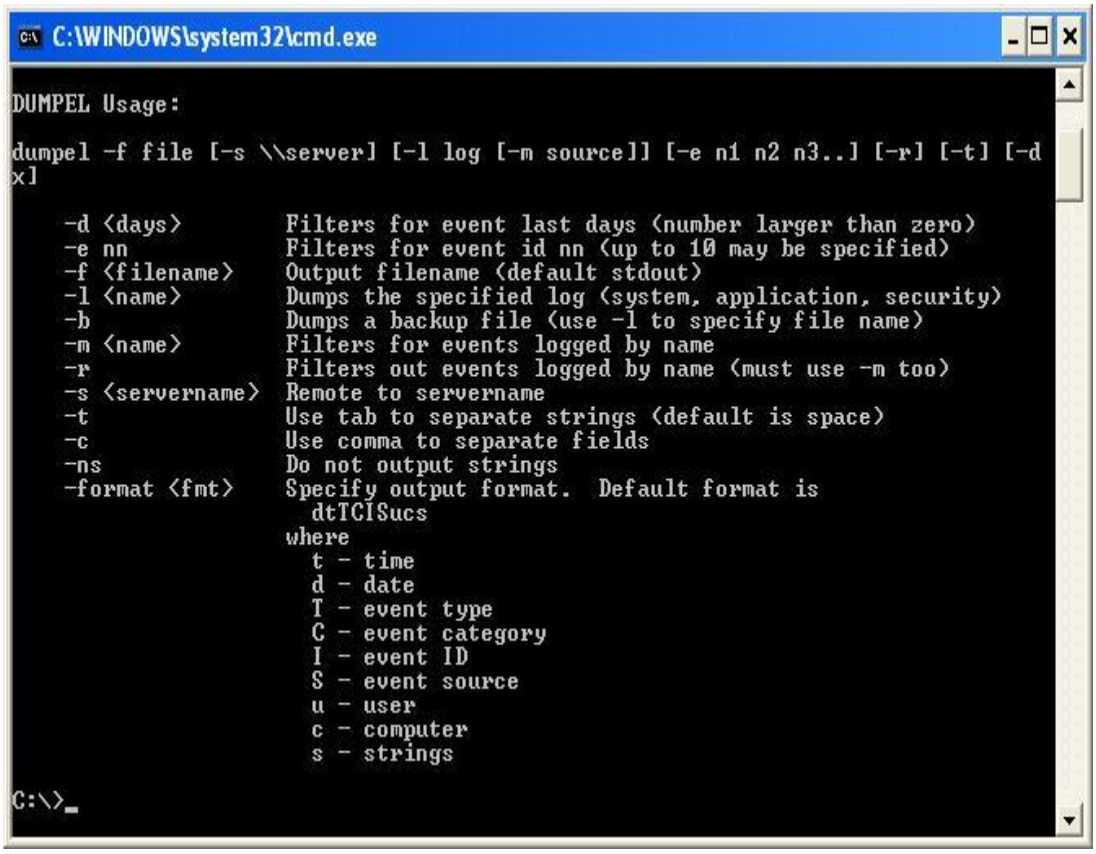


Εικόνα 34:Περιεχόμενα του 529 Event Log (Failure Logon/Logoff).

Γι' αυτούς που ψάχνουν για δυνατά, με δυνατότητα σύνταξης script, γραμμής εντολών, εργαλεία χειρισμού και ανάλυσης καταγραφών , ας δούμε το Dumpel[6], από το RK. Το Dumpel λειτουργεί στους απομακρυσμένους servers (απαιτούνται κατάλληλα δικαιώματα) και μπορεί να φιλτράρει μέχρι δέκα event IDs ταυτόχρονα.

[6] http://support.microsoft.com/kb/129266

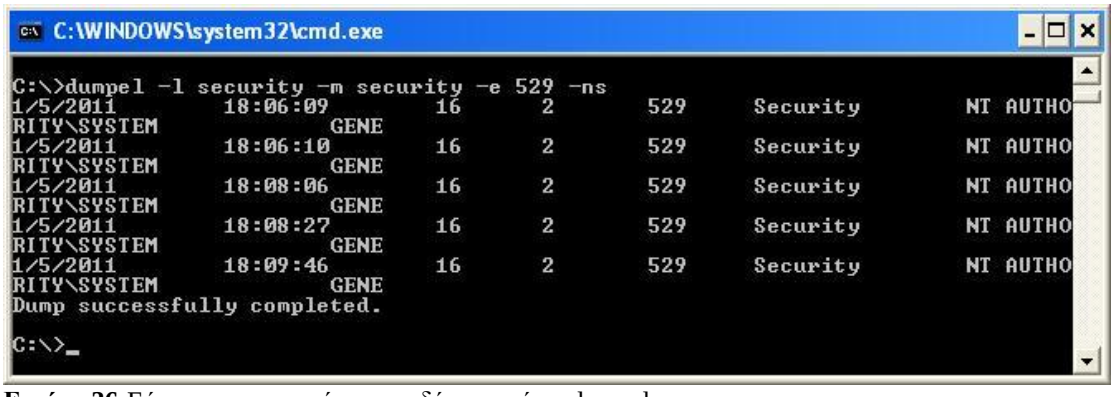
Πιο κάτω βλέπουμε όλες τις επιλογές που έχει το dumpel[7].



Εικόνα 35: Dumpel command

Για παράδειγμα, χρησιμοποιώντας το Dumpel μπορούμε να εξάγουμε αποτυχημένες προσπάθειες σύνδεσης (event ID 529) στο τοπικό σύστημα χρησιμοποιώντας την ακόλουθη σύνταξη:

```
C:\> dumpel -l security -m security -e 529 -ns
```



Εικόνα 36:Εύρεση αποτυχημένων συνδέσεων μέσω dumpel

[7] http://support.microsoft.com/kb/129266

Χρησιμοποιώντας τα κατάλληλα φίλτρα, φαίνεται ότι βρήκαμε πέντε προσπάθειες αποτυχημένης σύνδεσης στο σύστημα μας κάτι που πρέπει να μας ανησυχήσει.

Άλλο ένα καλό εργαλείο είναι το DumpEvt από τη Somarsoft (http://www.somarsoft.com).Το DumpEvt εμφανίζει ολόκληρο το Event Log ασφαλείας σε μια μορφή όπου είναι κατάλληλη για την εισαγωγή του σε μια βάση δεδομένων Access ή SQL. Παρόλα αυτά, αυτό το εργαλείο δεν είναι σε θέση να φιλτράρει σε συγκεκριμένα γεγονότα (events). Ένα άλλο ικανό δωρεάν εργαλείο είναι το Event Comb της Microsoft (http://support.microsoft .com /kb/308471). Το Event Comb είναι ένα πολύπλοκο(multithreaded) εργαλείο που θα αναλύει τα Event Logs από πολλούς servers συγχρόνως για συγκεκριμένα event IDs, τύπους event, πηγές event κ.λπ. Όλοι οι servers θα πρέπει να είναι μέλη σε κάποιο domain, επειδή το EventCombWindows λειτουργεί μόνο αν συνδεθούμε σε ένα domain.

Το ELM Log Manager από την TWindows (http://www.tntsoftware.com) είναι επίσης ένα καλό εργαλείο. Το ELM παρέχει κεντρική παρακολούθηση σε πραγματικό χρόνο και ειδοποιήσεις καταγραφής σε όλες τις εκδόσεις των Windows, καθώς επίσης και συμβατότητα με το Syslog και SNMP για συστήματα που δεν είναι Windows.

Συναγερμοί σε πραγματικό χρόνο

Το επόμενο βήμα μετά από τα εργαλεία καταγραφής είναι μία δυνατότητα ειδοποίησης σε πραγματικό χρόνο. Τα προϊόντα εντοπισμού εισβολής/ πρόληψη των Windows (IDS/IPS) και τα εργαλεία παρακολούθηση συμβάντων ασφαλείας και πληροφοριών (SEIM) παραμένουν δημοφιλής επιλογές για οργανισμούς, οι οποίοι θέλουν να αυτοματοποιήσουν το καθεστώς ελέγχου της ασφάλειας τους.

2.1.2 Υποκλοπή κωδικών πρόσβασης που διακονούνται μέσω του δικτύου

Το μάντεμα κωδικών πρόσβασης υποθετικά είναι δύσκολη δουλειά. Καθώς οι χρήστες συνδέονται σ' έναν διακομιστή μπορούμε να υποκλέψουμε τα πιστοποιητικά και στην συνέχεια να τα χρησιμοποιήσουμε για να αποκτήσουμε πρόσβαση στο σύστημα. Εάν ένας εισβολέας είναι σε θέση να «κρυφακούσει» την ανταλλαγή πληροφοριών που γίνεται κατά την σύνδεση στα Windows, αυτή η προσέγγιση μπορεί να μας γλυτώσει από πολλές τυχαίες εικασίες. Υπάρχουν τρία είδη κρυφακούσματος στις επιθέσεις εναντίον των Windows: LM, NTLM, και Kerberos.

Οι επιθέσεις εναντίον του κληροδοτούμενου πρωτόκολλου πιστοποίησης LanManager (LM) εκμεταλλεύονται μια αδυναμία των Windows στην υλοποίηση πρόκλησης/απόκρισης. Αυτό μας διευκολύνει να μαντέψουμε το αρχικό LM hash πιστοποιητικό (που είναι το αντίστοιχο ενός κωδικού πρόσβασης που μπορεί είτε να επαναληφθεί όπως είναι, είτε να σπάσει για να αποκαλύψει τον κωδικό πρόσβασης σε απλό κείμενο). Η Microsoft αντιμετώπισε αυτήν την αδυναμία στα Windows 2000 και διάφορα εργαλεία που αυτοματοποιούν αυτήν την επίθεση θα λειτουργήσουν μόνο εάν τουλάχιστον μια πλευρά που λαμβάνει μέρος στην πιστοποίηση έχει NT 4 ή προηγούμενο λειτουργικό σύστημα. Μερικά εργαλεία για επιθέσεις κατά την πιστοποίηση LM είναι το Cain από τον Massimiliano Montoro http://www.oxid .it, το LCP (διαθέσιμο από το http://www.lcpsoft.com) και L0pthcrack με το SMB Packet Capture (που δεν διατηρείται πλέον). Αν και η υποκλοπή κωδικών πρόσβασης είναι ενσωματωμένη στο L0phtcrack και το Cain μέσω του προγράμματος οδήγησης

πακέτων WinPcap, θα πρέπει να εισάγουμε με το χέρι τα αρχεία υποκλοπής στο LCP προκειμένου να εκμεταλλευτούμε την αδυναμία στην απόκριση του LM.

Το πιο ικανό από αυτά τα προγράμματα είναι το Cain το οποίο ενσωματώνει ομαλά την υποκλοπή και την διάρρηξη κωδικών πρόσβασης όλων των διαθέσιμων διαλέκτων των Windows (συμπεριλαμβανομένου LM, NTLM, και Kerberos) μέσω μεθόδων διάρρηξης brute force, λεξικού και Rainbow. Παρουσιάζει ένα υποκλοπέα πακέτων του Cain σε δράση, ενώ υποκλέπτει συνόδους σύνδεσης NTLM. Αυτές εισάγονται εύκολα στο ενσωματωμένο πρόγραμμα διάρρηξης κάνοντας δεξί κλικ στη λίστα με τους κωδικούς πρόσβασης που έχουν υποκλαπεί και επιλέγοντας Send All to Cracker.

Παράλληλα δεν πρέπει να είμαστε πολύ σίγουροι ότι μία αρχιτεκτονική δικτύου θα απαλείψει την δυνατότητα υποκλοπής κωδικών πρόσβασης. Οι επιτιθέμενοι μπορούν να εκτελέσουν διάφορες τεχνικές υποκλοπής ARP για να ανακατευθύνουν όλη την κίνηση μας στους επιτιθέμενους και με αυτόν τον τρόπο να υποκλέψουν την κίνηση μας. (Το Cain έχει επίσης μια ενσωματωμένη ARP λειτουργία δηλητηρίασης για υποκλοπή). Εναλλακτικά, ένας επιτιθέμενος θα μπορούσε «να προσελκύσει» τις προσπάθειες επικύρωσης των Windows με την αποστολή ενός ηλεκτρονικού ταχυδρομείου με URL της μορφής file://attackerscomputer/sharename/message.html. Αφού κάνουμε click στο URL θα προσπαθήσει να κάνει πιστοποίηση των Windows στον διακομιστή του επιτιθέμενου (το «attackerscomputer» σ' αυτό το παράδειγμα).

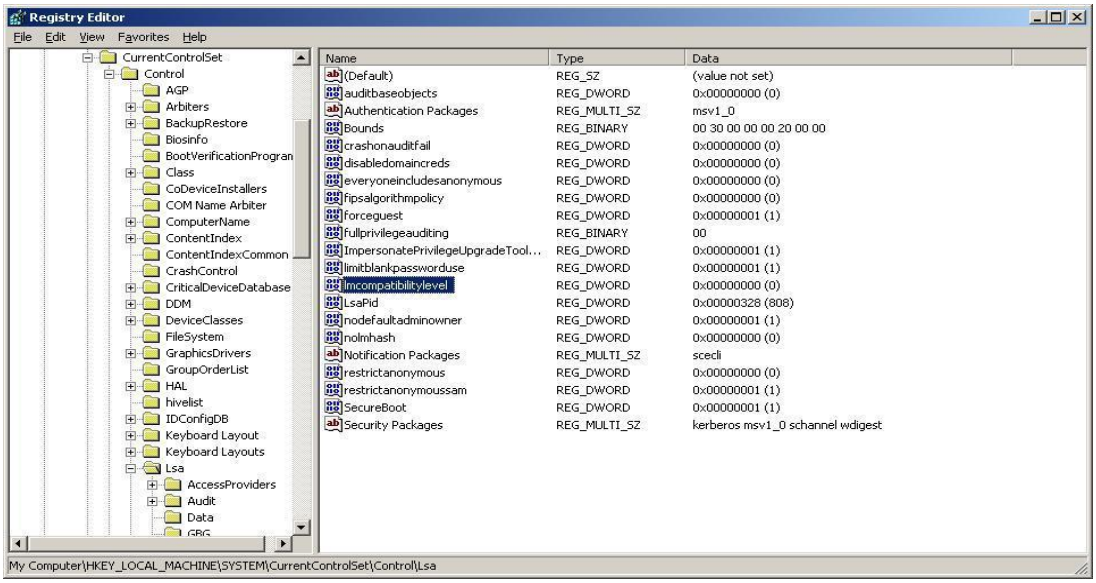
Το πιο ισχυρό πρωτόκολλο πιστοποίησης Kerberos είναι διαθέσιμο από τα Windows 2000, αλλά και αυτό έπεσε θύμα στις επιθέσεις υποκλοπής. Η βάση για αυτήν την επίθεση εξηγείται σε ένα έγγραφο του 2002 από το Frank O'Dwyer. Ουσιαστικά, η υλοποίηση των Windows Kerberos στέλνει ένα πακέτο με πρώιμη πιστοποίηση (preauthentication) που περιέχει ένα γνωστό plaintext (μια σφραγίδα χρόνου) κρυπτογραφημένο μ' ένα κλειδί που προέρχεται από τον κωδικό πρόσβασης του χρήστη. Κατά συνέπεια, μια επίθεση brute force ή μια επίθεση με λεξικό που αποκρυπτογραφεί το πακέτο πρώιμης πιστοποίησης και αποκαλύπτει μια δομή παρόμοια με μία τυπική σφραγίδα χρόνου (timestamp) που προδίνει τον κωδικό πρόσβασης του χρήστη. Όπως έχουμε δει ,το Cain έχει ένα ενσωματωμένο πακέτο υποκλοπής MSKerb5-PreAuth .Άλλα εργαλεία υποκλοπής πιστοποιήσεων και διάρρηξης κωδικών του Windows Kerberos περιλαμβάνουν τα KerbSniff και KerbCrack από την Arne Vidstrom. (www.ntsecurity.nu/toolbox/kerbcrack/). (δεν λειτουργούν τα KerbSniff και KerbCrack)

2.1.2.a Αντίμετρα έναντι της υποκλοπής της πιστοποίησης στα Windows

Το κλειδί για να απενεργοποιήσουμε τις επιθέσεις απόκρισης LM είναι να απενεργοποιήσουμε την πιστοποίηση LM. Η απόκριση LM χρησιμοποιείται από διάφορα εργαλεία. Ένα από αυτά είναι και το Cain το οποίο παράγει κωδικούς πρόσβασης. Εάν εμποδίσουμε την απόκριση LM να περάσει από το δίκτυο, θα μπλοκάρουμε τελείως αυτή την επίθεση. Η διάλεκτος NTLM δεν επηρεάζεται από τις αδυναμίες του LM και έτσι δεν απαιτεί πολύ περισσότερο χρόνο προκειμένου να σπάσει.

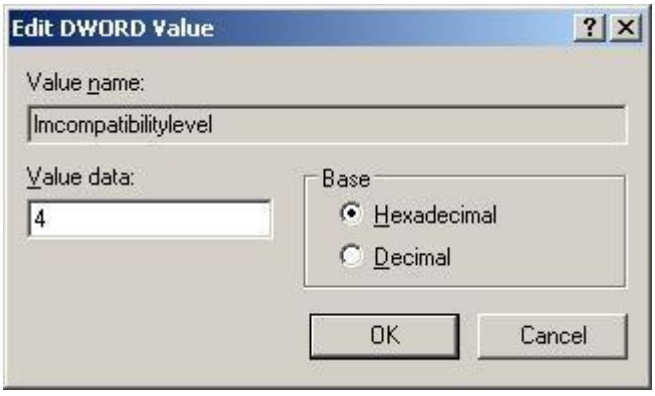
Μετά από το Windows NT 4.0 Service Pack 4, η Microsoft πρόσθεσε μία τιμή στο Registry που ελέγχει τη χρήση της πιστοποίησης LM την τιμή:

HKLM\System\Current\ControlSet\Control\LSARegistry\LMCompatibilityLevel.



Εικόνα 37:Τιμή για έλεγχος χρήσης της πιστοποίησης LM.

Οι τιμές από 4 και πάνω θα εμποδίσουν έναν domain controller να αποδεχτεί αιτήματα πιστοποίησης LM.



Εικόνα 38:Ρύθμιση της τιμής Imcompabilitylevel.

Στα Windows xp και σε νεότερα συστήματα, αυτή η ρύθμιση διαμορφώνεται πιο εύκολα χρησιμοποιώντας το Security Policy. Επίσης μας επιτρέπει να διαμορφώσουμε τα Windows να εκτελούν πιστοποίηση SMB με ένα από τους έξι τρόπους (από τον πιο ελάχιστα ασφαλή έως τον πιο ασφαλή).

- **Send LM & NTLM responses:** Το Level 0 είναι το χαμηλότερο επίπεδο ασφάλειας διότι το LM και NTLM θεωρούνται πλέον ξεπερασμένες. Οι clients σε αυτή τη ρύθμιση δεν χρησιμοποιούν ποτέ το NTLMv2 ενώ οι servers δέχονται οποιοδήποτε από τα τρία πρωτόκολλα.

- **Send LM & NLTM – χρησιμοποίηση NTLMv2 session security εάν διαπραγματεύεται:** Το Level 1 επιτρέπει τη χρήση των LM και NTLMv1, γι 'αυτό δεν εξαλείφει τις αδυναμίες που παρουσιάζουν τα συγκεκριμένα πρωτόκολλα. Οι servers σε αυτή τη ρύθμιση, θα συνεχίσουν να αποδέχονται οποιοδήποτε από τα τρία πρωτόκολλα, αν και οι πελάτες θα έχουν πλέον τη δυνατότητα να επιταχύνουν με το NTLMv2 εάν ο server το υποστηρίζει.

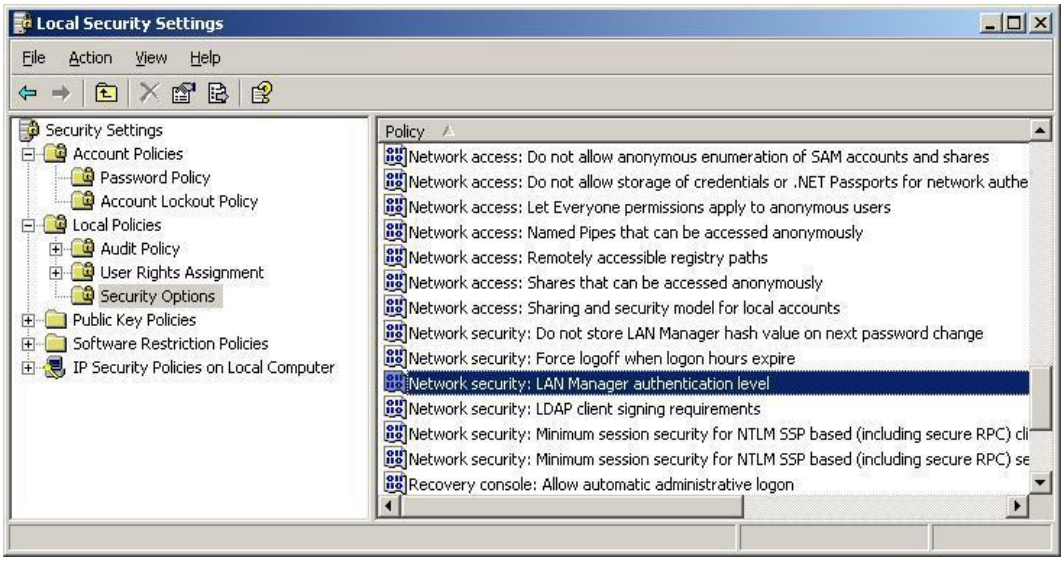
- **Send NTLM response only:** Όταν το Level 2 εφαρμόζεται σε έναν domain οι clients αρχίζουν να χρησιμοποιούν NTLMv1 και NTLMv2 αν οι servers υποστηρίζουν στο δίκτυο τους. Οι domain controllers θα συνεχίσουν πάλι να αποδέχονται οποιοδήποτε από τα τρία πρωτόκολλα.

- **Send NTLMv2 response only:** Στο Level 3, οι domain controllers αποδέχονται ακόμη τα τρία πρωτόκολλα, αλλά και οι clients χρησιμοποιήσουν μόνο NTLMv2, αγνοώντας την κίνηση του LM και του NTLMv1. Αυτό είναι το ελάχιστο αποδεκτό επίπεδο ασφαλείας με το συνδυασμό όλων των προηγούμενων τρόπων ασφαλείας τα οποία ορισμένοι πελάτες πρέπει οπωσδήποτε να συνεχίσουν να πιστοποιούν αν και δεν μπορούν να χρησιμοποιήσουν NTLMv2 (για παράδειγμα, παλαιότερα λειτουργικά συστήματα, όπως τα Windows 95/98, παλιές εκδόσεις Unix, Mac OS X 10.3 και νωρίτερα). Η επικοινωνία μεταξύ των servers και των παλαιότερων clients θα εξακολουθήσουν να είναι επισφαλής, αλλά η επικοινωνία μεταξύ servers και νεότερων clients (π.χ., Windows 2000 ή XP, Mac OS X 10.4, νέες διανομές Unix) θα είναι ασφαλής.

- **Send NTLMv2 response only\refuse LM:** Στο Level 4 οι clients και οι domain controllers αγνοούν την κίνηση του LM.Οι clients δέχονται NTLMv2 και οι domain controllers δέχονται NTLMv1.

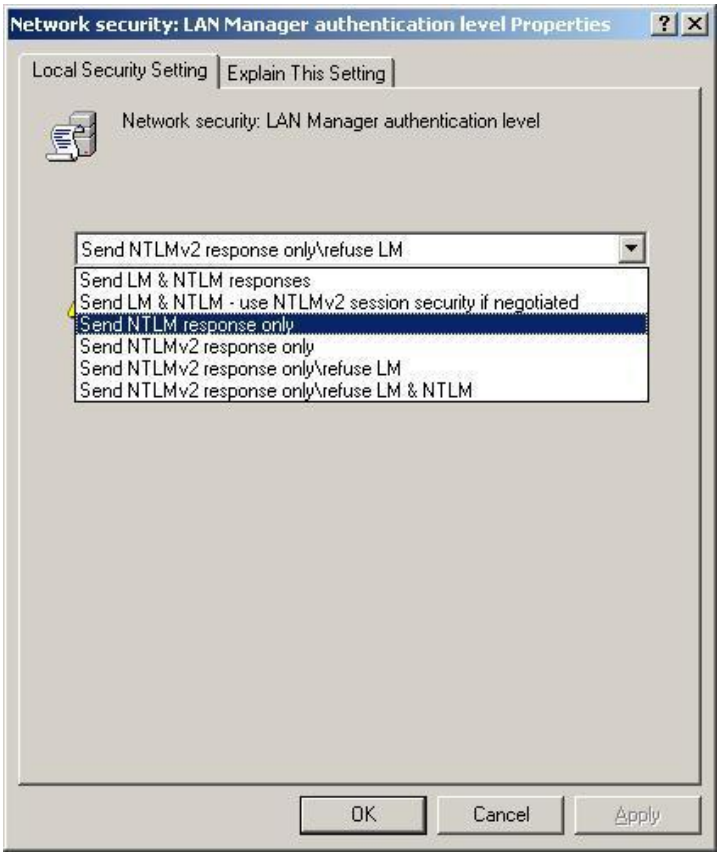
- **Send NTLMv2 response only\refuse LM & NTLM:** Το Level 5 είναι η υψηλότερη βαθμίδα ασφάλειας. Οι clients και οι servers απορρίπτουν την κίνηση LM και NTLMv1, χρησιμοποιώντας μόνο NTLMv2.

Κοιτάζοντας την ρύθμιση «LAN Manager Authentication Level» κάτω από τον κόμβο Security Options (αυτή η ρύθμιση βρίσκεται στο «Network Security: LAN Manager Authentication Level» στα Windows XP 2000 και νεότερα).



Εικόνα 39: Network Security: LAN Manager Authentication Level

Συστήνουμε να οριστεί αυτή η ρύθμιση τουλάχιστον στο Level 2, «Send NTLM Response Only» όπως φαίνεται και παρακάτω.



Εικόνα 40:Επιλογή ασφαλής τρόπου πιστοποίησης SMB.

Δυστυχώς, οι clients χαμηλότερου επιπέδου θα αποτύχουν που θα προσπαθήσουν να επικυρωθούν σ' έναν domain controller που έχει διαμορφωθεί κατ' αυτόν τον τρόπο, επειδή το DC θα δεχτεί μόνο Windows hash για πιστοποίηση (Το χαμηλότερο

επίπεδο αναφέρεται στα Windows 9 x, Windows for workgroups και προηγούμενες εκδόσεις.) Ακόμα χειρότερα, επειδή οι clients που δεν είναι Windows δεν μπορούν να εφαρμόσουν Windows hash, θα στείλουν μάταια αποκρίσεις LM μέσω του δικτύου, ακυρώνοντας κατά συνέπεια την ασφάλεια ως προς τις συλλήψεις SMB. Αυτή η διόρθωση είναι επομένως περιορισμένης πρακτικής χρήσης στους περισσότερους οργανισμούς που χρησιμοποιούν μία ποικιλία από προγράμματα –clients των Windows. Αν και η Microsoft αντιμετώπισε αυτό το πρόβλημα που ονομάζεται Dsclient.exe για clients χαμηλότερου επιπέδου (δείτε το άρθρο KB Article Q239869), αυτοί οι clients είναι τόσο ξεπερασμένοι που τώρα συστήνετε απλά να τους αναβαθμίσουμε.

Για να μετριάσουμε τις επιθέσεις υποκλοπής στο Kerberos, δεν υπάρχει μία τιμή στο Registry που να μπορούμε να ορίσουμε όπως στο LM. Στη δοκιμή μας, ο ορισμός της κρυπτογράφησης στο ασφαλές κανάλι δεν απέτρεψε αυτήν την επίθεση και η Microsoft δεν έχει εκδώσει καμιά οδηγία για να αντιμετωπίσει αυτό το θέμα. Κατά συνέπεια, μας μένει η κλασική άμυνα : καλή επιλογή κωδικών πρόσβασης. Το άρθρο του Frank O'Dwyer σημειώνει ότι οι κωδικοί πρόσβασης με μήκος οκτώ χαρακτήρων που περιέχουν κεφαλαία-πεζά και αριθμούς θα χρειαστούν κατ' εκτίμηση 67 χρόνια για να σπάσουν χρησιμοποιώντας αυτή την προσέγγιση σ' ένα μόνο υπολογιστή Pentium 1.5GHz. Γι' αυτό, χρησιμοποιούμε τη λειτουργία πολυπλοκότητας κωδικών πρόσβασης των Windows για να κερδίσουμε χρόνο. Επίσης πρέπει να θυμόμαστε ότι εάν ένας κωδικός πρόσβασης βρίσκεται σε ένα λεξικό, θα σπάσει αμέσως.

Οι Kasslin kai Tikkanen πρότειναν τις παρακάτω πρόσθετες ιδέες μετριασμού στο άρθρο τους για τις επιθέσεις στο Kerbero (http://users.tkk.fi/autikkan/kerberos/docs/phase1/pdf/LATEST_hijacking_attack.pdf)

- Χρησιμοποιήστε την μέθοδο preauthentication PKINIT, η οποία χρησιμοποιεί δημόσια κλειδιά αντί για κωδικούς πρόσβασης, έτσι δεν υποκύπτει σε επιθέσεις υποκλοπής μέσω παρακολούθησης.

- Χρησιμοποιήστε ενσωματωμένη υλοποίηση του Windows IPSec που πιστοποιεί και κρυπτογραφεί την κίνηση.

Για να προστατέψουμε το δίκτυό μας από επαναλαμβανόμενες επιθέσεις, μια αποτελεσματική λύση είναι η ανάπτυξη κρυπτογράφησης στο layer IP. Η χρήση του IPSec θα ήταν μια κατάλληλη προστατευτική δράση. Εάν το σύνολο της κίνησης IP είναι κρυπτογραφημένη ο εισβολέας δεν θα έχει κανένα τρόπο της σύλληψης των απαιτούμενων δεδομένων. Σε πολλά περιβάλλοντα που χρησιμοποιούν το IPSec για την ασφαλή κυκλοφορία όλων των client-server είναι ένα δύσκολο έργο το οποίο συχνά απαιτεί τη λειτουργία μιας PKI (Public Key Infrastructure). Θα πρέπει να σημειωθεί ότι όλοι οι κόμβοι του δικτύου πρέπει να ρυθμιστεί ώστε να απαιτήσουν IPSec σε όλες τις σχετικές συνδέσεις.

2.1.3 Επιθέσεις ενδιάμεσου

Οι επιθέσεις ενδιάμεσου (Man-in-the-middle-MITM) είναι καταστροφικές, καθώς μειώνουν την ακεραιότητα του καναλιού μεταξύ του νόμιμου πελάτη και του διακομιστή, αποτρέποντας οποιαδήποτε αξιόπιστη ανταλλαγή των πληροφοριών. Σε αυτή την ενότητα, θα ερευνήσουμε μερικές υλοποιήσεις των επιθέσεων MITM ενάντια στα πρωτόκολλα των Windows που έχουν εμφανιστεί τα τελευταία χρόνια.

Τον Μαΐο του 2001, ο Sir Dystic της Cult of the Dead Cow έγραψε και κυκλοφόρησε ένα εργαλείο αποκαλούμενο SMBRelay που ήταν ουσιαστικά ένας διακομιστής SMB που μπορούσε να μαζέψει κρυπτογραφημένα ονόματα χρηστών και τους κωδικούς πρόσβασης hashes από την εισερχόμενη κίνηση SMB. Όπως υποδηλώνει το όνομα, το SMBRelay μπορεί να ενεργήσει ως ένα κακόβουλο τελικό σημείο SMB -μπορεί επίσης να εκτελέσει τις επιθέσεις MITM σε ορισμένες περιστάσεις.

Ενεργώντας ως ένας πλαστός διακομιστής το SMBRelay είναι σε θέση να συλλάβει τους κωδικούς πρόσβασης δικτύων hashes που μπορούν να εισαχθούν σε εργαλεία διάρρηξης. Μπορεί επίσης να δημιουργήσει αντίστροφες συνδέσεις πίσω σε οποιοδήποτε πελάτη μέσω μιας εσωτερικής IP διεύθυνσης αναμετάδοσης, που επιτρέπει σε έναν επιτιθέμενο να αποκτήσει πρόσβαση σε ανυποψίαστους πελάτες μέσω SMB χρησιμοποιώντας τα προνόμια της αρχικής σύνδεσης.

Σε πλήρη κατάσταση MITM, το SMBRelay παρεμβάλλεται μεταξύ του πελάτη και του διακομιστή, αναμεταδίδει τη νόμιμη ανταλλαγή πιστοποίησης του πελάτη και αποκτά πρόσβαση στον διακομιστή χρησιμοποιώντας τα ίδια προνόμια με τον πελάτη. Το SMBRelay μπορεί να αποβεί ενοχλητικό, αλλά όταν εφαρμόζεται επιτυχώς, είναι σαφώς μια καταστροφική επίθεση: το MITM αποκτά πλήρη πρόσβαση σε πόρους του στόχου.

Ένα άλλο εργαλείο αποκαλούμενο SMBProxy (http://www.cqure.net/wp/11/) εφαρμόζει μία επίθεση «πέρασμα hash». Όπως σημειώσαμε νωρίτερα, οι κρυπτογραφημένοι κωδικοί πρόσβασης των Windows είναι ισοδύναμοι με τους κωδικούς πρόσβασης, έτσι αντί να προσπαθούν να τους σπάσουν εκτός σύνδεση, οι πιο προχωρημένοι επιτιθέμενοι μπορούν απλά να τους επαναλάβουν ώστε να αποκτήσουν μη πιστοποιημένη πρόσβαση (αυτή η τεχνική διαδόθηκε αρχικά από τον Hernan Ochoa).

Το SMBProxy λειτουργεί σε Windows NT 4 και Windows 2000, αλλά δεν γνωρίζουμε την αναφερόμενη δυνατότητα να θέσει σε κίνδυνο νεότερες εκδόσεις των Windows, όπως ξέρουμε με το SMBRelay. Θεωρητικά, οι ίδιες αυτές τεχνικές είναι εφαρμόσιμες και στις νεότερες εκδόσεις, αλλά δεν έχουν εφαρμοστεί επιτυχώς σε ένα εργαλείο.

Το Cain είναι το εργαλείο του Montoro Massimiliano, που προσφέρει τις χρήσιμες δυνατότητες SMB MITM, συνδυάζοντας μια ενσωματωμένη λειτουργία ARP Poison Routing(ARP) με υποκλοπή NTLM και υποβιβάζει τις λειτουργίες επίθεσης. Χρησιμοποιώντας το Cain, ένας επιτιθέμενος μπορεί να ανακατευθύνει την τοπική κίνηση του δικτύου στον εαυτό του χρησιμοποιώντας ARP και υποβαθμίζοντας τους clients στις πιο επιτεθειμένες διαλέκτους πιστοποίησης των Windows. Το Cain δεν εφαρμόζει έναν πλήρη διακομιστή MITM SMB σε αντίθεση με το SMBRelay.

Το Terminal server υπόκειται επίσης σε επίθεση MITM μέσο του APR του Cain για υλοποίηση της επίθεση που περιγράφηκε τον Απρίλιο του 2003 από τον Erik Forsberg (δείτε το http://www.securityfocus.com/ archive/1/317244) και ενημερώθηκε το 2005 από το συντάκτη του Cain, τον Massimiliano Montoro (δείτε το http://www.oxid.it/downloads/rdp-gbu.pdf).Επειδή η Microsoft επαναχρησιμοποιεί το ίδιο κλειδί για να αρχίσει την πιστοποίηση, το Cain χρησιμοποιεί το γνωστό κλειδί για να υπογράψει ένα νέο κλειδί MITM που ο τυπικός client Terminal server απλώς επαληθεύει καθώς έχει σχεδιαστεί να δέχεται τυφλά το υλικό που υπογράφεται από το γνωστό κλειδί της Microsoft. Το APR διασπά την αρχική επικοινωνία πελάτη-διακομιστή , έτσι ώστε κανείς τους να μην ξέρει ότι μιλά στην πραγματικότητα στο MITM. Το τελικό αποτέλεσμα είναι ότι η κίνηση Terminal server μπορεί να υποκλαπεί, να αποκρυπτογραφηθεί και να καταγράφει από το Cain, εφαρμόζοντας τα πιστοποιητικά διαχειριστή που θα μπορούσαν να χρησιμοποιηθούν για εισβολή στον διακομιστή.

Αν και παρουσιάζει μικρότερο κίνδυνο από το αναμφισβήτητο MITM, για περιβάλλοντα που εξακολουθούν να βασίζονται σε πρωτόκολλα NetBIOS (NBNS, UDP θύρα 137), μπορεί να χρησιμοποιηθεί υποκλοπή ονομάτων για να διευκολύνει τις επιθέσεις MITM. Για παράδειγμα, το team της Toolcrypt.org δημιούργησε ένα εργαλείο που ακροάζεται αναμεταδόσεις NetBIOS σε ερωτήματα ονομάτων στην UDP 137 και απαντά θετικά με ένα όνομα που είναι συνδεδεμένο σε μια διεύθυνση IP της επιλογής του επιτιθεμένου (δείτε το http://www.toolcrypt.org/index.html?hew).

Ο επιτιθέμενος είναι έπειτα ελεύθερος να υποκριθεί ότι είναι ο νόμιμος διακομιστής εφ' όσον μπορεί να ανταποκριθεί γρηγορότερα στα αιτήματα ονομάτων NBNS.

2.1.3α Αντίμετρα στο MITM

Οι επιθέσεις MITM απαιτούν γενικά να είναι κόντρα στα συστήματα των θυμάτων για να εφαρμοστούν με επιτυχία, όπως η τοπική παρουσία τμήματος στο τοπικό LAN. Εάν ένας επιτιθέμενος έχει ήδη αποκτήσει μια τέτοια θέση στο δίκτυό σας, είναι δύσκολο να μετριαστούν πλήρως οι πολλές πιθανές μεθοδολογίες επιθέσεων MITM που θα μπορούσαν να χρησιμοποιηθούν.

Οι βασικές αρχές ασφάλειας στην επικοινωνία των δικτύων μπορούν να βοηθήσουν για να προστατευθούμε από επιθέσεις MITM. Η χρήση επικυρωμένων και κρυπτογραφημένων επικοινωνιών μπορεί να περιορίσει την εισβολή πλαστών πελατών ή διακομιστών σε μία νόμιμη ροη επικοινωνίας. Οι κανόνες του Windows Firewall στα Vista και σε νεότερα συστήματα μπορούν να παρέχουν πιστοποιημένες και κρυπτογραφημένες συνδέσεις, εφόσον και τα δύο σημεία είναι μέλη του ιδίου τομέα Active Directory (AD) και εφαρμόζεται μιας πολιτική IPSec για να δημιουργηθεί μια εξασφαλισμένη σύνδεση μεταξύ των endpoints.

Από τα Windows NT, είναι διαθέσιμη μία λειτουργία που ονομάζεται υπογραφή SMB για να επικυρώνει συνδέσεις SMB. Ωστόσο, δεν έχουμε δει ποτέ να εφαρμόζεται ευρέως, και επιπλέον δεν είμαστε βέβαιοι ως προς τη δυνατότητά του να εκτρέψει επιθέσεις MITM σε ορισμένα σενάρια. Διάφορα εργαλεία όπως το SMBRelay προσπαθούν να απενεργοποιήσουν της SMB υπογραφές. Παραδείγματος

χάριν το Windows Firewall με IPSec/Connection Security Rules είναι πιθανώς καλύτερο.

Τελευταίο αλλά όχι και το πιο ασήμαντο, για να αντιμετωπίσουμε επιθέσεις υποκλοπής ονόματος NetBIOS, συστήνουμε την απλή απενεργοποίηση του NetBIOS Name Service ,αν δεν είναι χρήσιμο. Το NBNS είναι πολύ εύκολο να υποκλαπεί (επειδή είναι βασισμένο στο UDP), και οι περισσότερες πρόσφατες εκδόσεις των Windows μπορούν να επιζήσουν χωρίς αυτό αν έχουν μιας κατάλληλα διαμορφωμένη υποδομή DNS. Εάν πρέπει να εφαρμόσουμε NBNS, η διαμόρφωση ενός πρωτεύοντος και ενός δευτερεύοντος διακομιστή Windows Internet Naming Service (WINS) στην υποδομή μπορεί να βοηθήσει να μετριάσουμε την ασυγκράτητη υποκλοπή NBNS (http://support.microsoft.com/kb/150737/ για περισσότερες πληροφορίες).

2.2 Επιθέσεις με μη εξουσιοδοτημένη πρόσβαση εξ αποστάσεως

Σε αντίθεση με τη συζήτηση μέχρι τώρα για τις επιθέσεις σε πρωτόκολλα πιστοποίησης των Windows, οι εξ αποστάσεως επιθέσεις με μη εξουσιοδοτημένη πρόσβαση στοχεύει σε ρωγμές ή σε άσχημες διαμορφώσεις του ίδιου του λογισμικού των Windows. Οι απομακρυσμένες τεχνικές εκμετάλλευσης, που στο παρελθόν εστιάζονταν κυρίως σε TCP/IP υπηρεσίες δικτύων, έχουν επεκταθεί σε επιθέσεις τα τελευταία χρόνια σε περιοχές των Windows που προηγούμενος δεν ήταν στόχος, συμπεριλαμβανομένων των προγραμμάτων οδήγησης για συσκευές και μέσα, καθώς επίσης και σε κοινές εφαρμογές χρηστών των Windows, όπως το Microsoft Office . Σε αυτή την ενότητα θα εξετάσουμε ορισμένες αξιοσημείωτες επιθέσεις αυτής της μορφής.

2.2.1 Εκμετάλλευση υπηρεσιών δικτύων

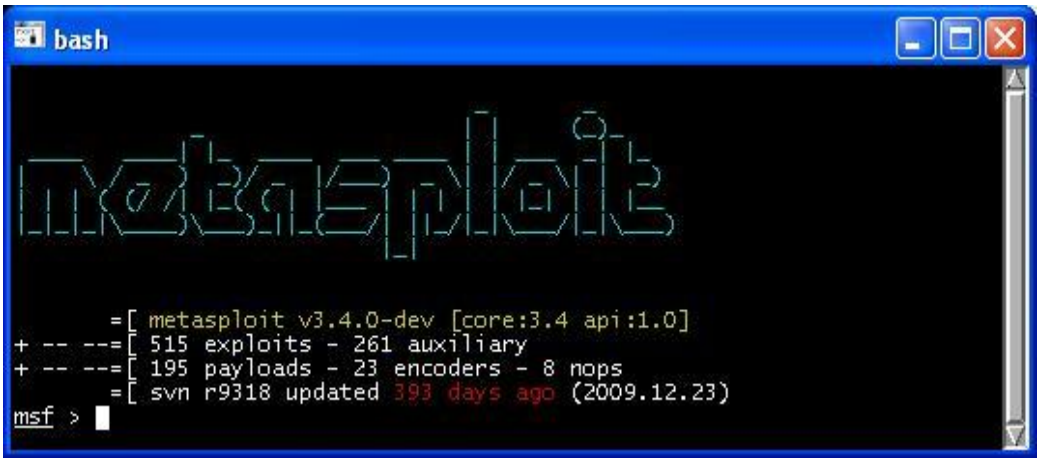
Τώρα πλέον θεωρείται της παλιάς σχολής από μερικούς , η εξ αποστάσεως εκμετάλλευση των υπηρεσιών δικτύων παραμένει η βασική εισβολή στα Windows. Υπήρχε εποχή όπου οι επίδοξοι hacker έπρεπε να ψάχνουν στο internet για προσαρμοσμένα προγράμματα εκμετάλλευσης που είχαν γραφτεί από ερευνητές, περνώντας πολλές ώρες βελτιώνοντας περίεργο κώδικα και προσδιορίζοντας διάφορες παραμέτρους που ήταν απαραίτητες να κάνουν το πρόγραμμα να λειτουργεί αξιόπιστα.

Σήμερα, αυτά τα προγράμματα εκμετάλλευσης πωλούνται έτοιμα και κάνουν όλη αυτή τη διαδικασία πολύ εύκολα. Ένα από τα πιο δημοφιλή προγράμματα είναι το Metasploit (http://framework.metasploit.com), το όποιο δημιουργήθηκε για να παρέχει πληροφορίες στις τεχνικές εκμεταλλεύσεις (exploit) και να δημιουργεί ένα χρήσιμο πόρο για εκμετάλλευση από προγραμματιστές και ειδικούς ασφαλείας.

Η δημοσιευμένη λειτουργική μονάδα της Metasploit είναι γενικά αρκετούς μήνες πίσω από τις τελευταίες αδυναμίες της Microsoft. Δεν περιέχει όλες τις σημαντικές αδυναμίες τις Microsoft παρόλα αυτά είναι ένα ισχυρό εργαλείο για δοκιμή της ασφάλειας των Windows.

Στο σημείο αυτό να αναφέρουμε ότι αυτή τη στιγμή η έκδοση 3.4 του Metasploit περιλαμβάνει:

- 515 exploits
- 195 payloads



Εικόνα 41: Metasploit 3.4

Όσον αφορά το χειρισμό του, το Metasploit παρέχει τρία διαφορετικά interface: command line, console και web interface. Παρόλα αυτά η κονσόλα εντολών (console interface) θεωρείται πιο ισχυρό και πλήρες.

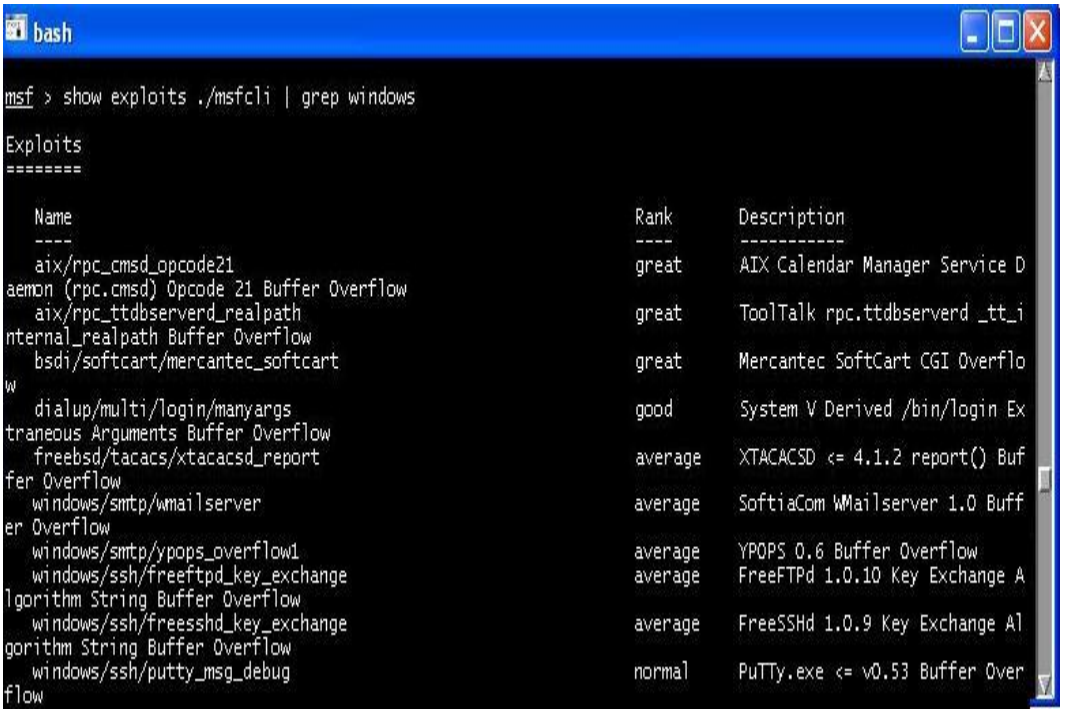
Το πιο σημαντικό και κρίσιμο σημείο στη χρήση του Metasploit είναι η επιλογή του κατάλληλου exploit. Η σωστή επιλογή του εξαρτάται από τις υπηρεσίες που τρέχουν σε κάποιο σύστημα και τις αδυναμίες που αυτές εμφανίζουν.

Τα διαθέσιμα exploits μπορούμε να τα δούμε εκτελώντας:

```
show exploits
```

Παρατηρούμε ότι είναι ταξινομημένα κατά λειτουργικό σύστημα και πρωτόκολλο. Αν θέλουμε να επικεντρωθούμε στην αναζήτηση exploit συγκεκριμένου λειτουργικού ή πρωτοκόλλου τότε μπορούμε να χρησιμοποιήσουμε το command line interface και κάποιο φίλτρο όπως το grep. Για παράδειγμα με τον παρακάτω τρόπο θα εμφανιστούν μόνο όσα είναι διαθέσιμα για Windows:

```
./msfcli | grep windows
```



Εικόνα 42:Εντολή στο Metasploit- show exploits των Windows

Αν θέλουμε να δούμε περισσότερες πληροφορίες για κάποια απ' αυτά αρκεί να εφαρμόσουμε το συντακτικό:

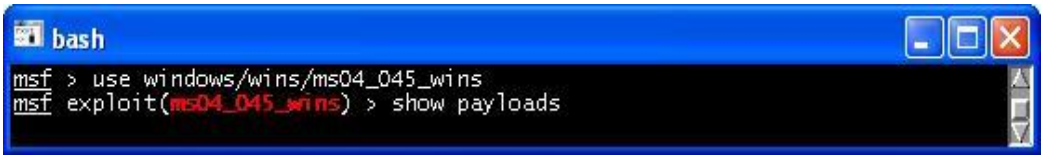
```
info name_exploit
```

Για να χρησιμοποιήσουμε το exploit που θέλουμε γράφουμε:

```
Use exploit
```

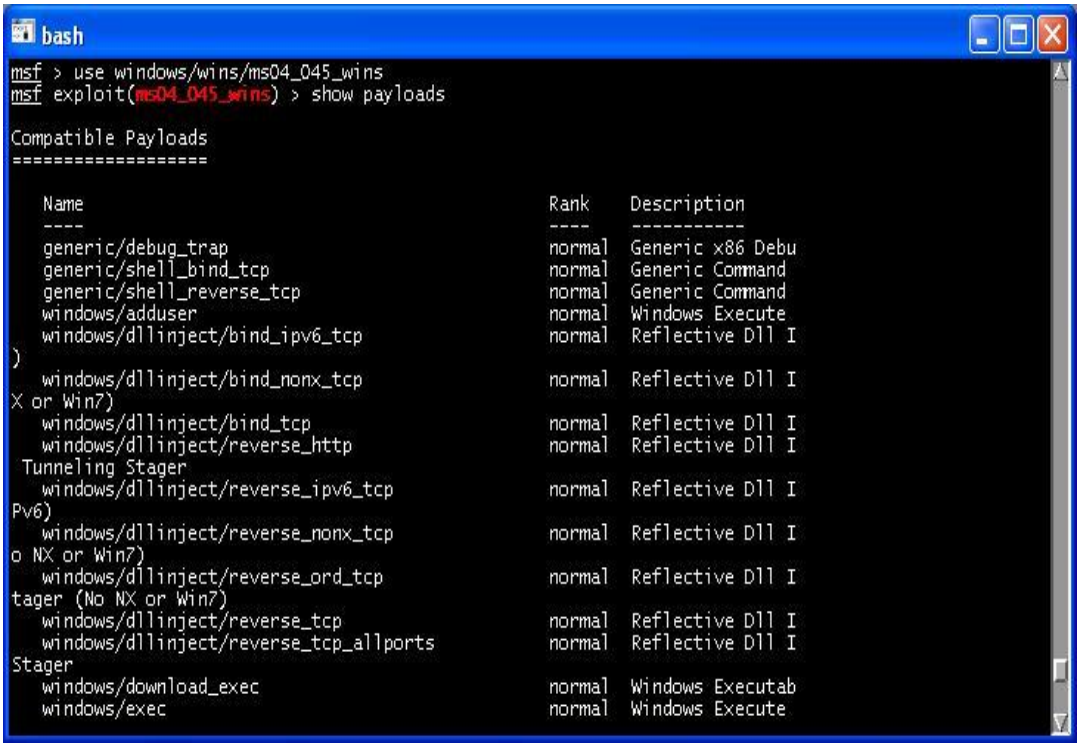
Στη συνέχεια πρέπει να επιλέξουμε το payload που θα χρησιμοποιηθεί. Εδώ αξίζει να σημειωθεί ότι ενώ η επιλογή του exploit εξαρτάται από τις αδυναμίες που υπάρχουν στο απομακρυσμένο σύστημα, η επιλογή του payload εξαρτάται αποκλειστικά από τι θέλουμε να κάνουμε μετά την επιτυχή σύνδεση στο σε αυτό. Για να δούμε όλα τα payloads, εκτελούμε:

```
show payloads
```



Εικόνα 43:Εντολές στο Metasploit- use exploits & show payloads

Πιο κάτω βλέπουμε τα συμβατά Payloads για το συγκεκριμένο exploit.



Εικόνα 44: Metasploit-Compatible Payloads

Αν επιλέξουμε την εμφάνιση τους αφού πρώτα έχουμε επιλέξει το exploit που θα χρησιμοποιηθεί, θα εμφανιστούν μόνο τα payloads που μπορούν να χρησιμοποιηθούν με αυτό. Για να δούμε περισσότερες πληροφορίες σχετικά με κάποιο payload απλά εκτελούμε:

```
info payload_name
```

Τα payloads, αυτά μπορούν να διαχωριστούν σε επτά (7) κατηγορίες

- VNC injection (windows/vncinject)

Όταν εκτελεστεί αυτό το payload δημιουργεί στο απομακρυσμένο σύστημα - στόχο έναν VNC server. Παράλληλα αποδίδει πλήρη πρόσβαση σε αυτό και επιτρέπει το χειρισμό του μέσω γραφικού περιβάλλοντος. Παρόλα αυτά θεωρείται «επικίνδυνη» η χρήση του γιατί οποιαδήποτε ενέργεια είναι ορατή στο στόχο. Επιπλέον για την αποτελεσματική χρήση του απαιτείται σύνδεση με υψηλό Bandwidth.

- File execution (windows/upexec)

Επιτρέπει τι μεταφορά και εκτέλεση αρχείων στον στόχο. Μπορεί να χρησιμοποιηθεί για την δημιουργία και backdoor και rootkit σε αυτόν.

- Interactive shell (shell)

Παρέχει ένα shell όπου μπορούμε να αλληλεπιδρούμε με το απομακρυσμένο σύστημα εκτελώντας εντολές για τον έλεγχο του.

- Command execution

Μοιάζει με το Interactive shell μόνο που εκτελεί μια μόνο εντολή στο απομακρυσμένο σύστημα χωρίς να επιτρέπει αλληλεπίδραση με αυτό.

- DLL injection

Χρησιμοποιείται για να προσθέσουμε κώδικα και να αλλάξουμε την «συμπεριφορά» κάποιων αρχείων ddl. Αυτό το payload χρησιμοποιείται αυτόματα για την εκτέλεση VNC injection και meterpreter payloads

- Add user

Προσθέτει ένα νέο χρήστη στο σύστημα με όνομα και κωδικό που ορίζονται ως παράμετροι σ' αυτό. Όταν χρησιμοποιείται ενάντια σε Windows, προσθέτει τον χρήστη στην ομάδα administrators ενώ όταν εκτελείται σε Linux ο χρήστης έχει UID 0, δηλαδή δικαιώματα superuser.

- Meterpreter

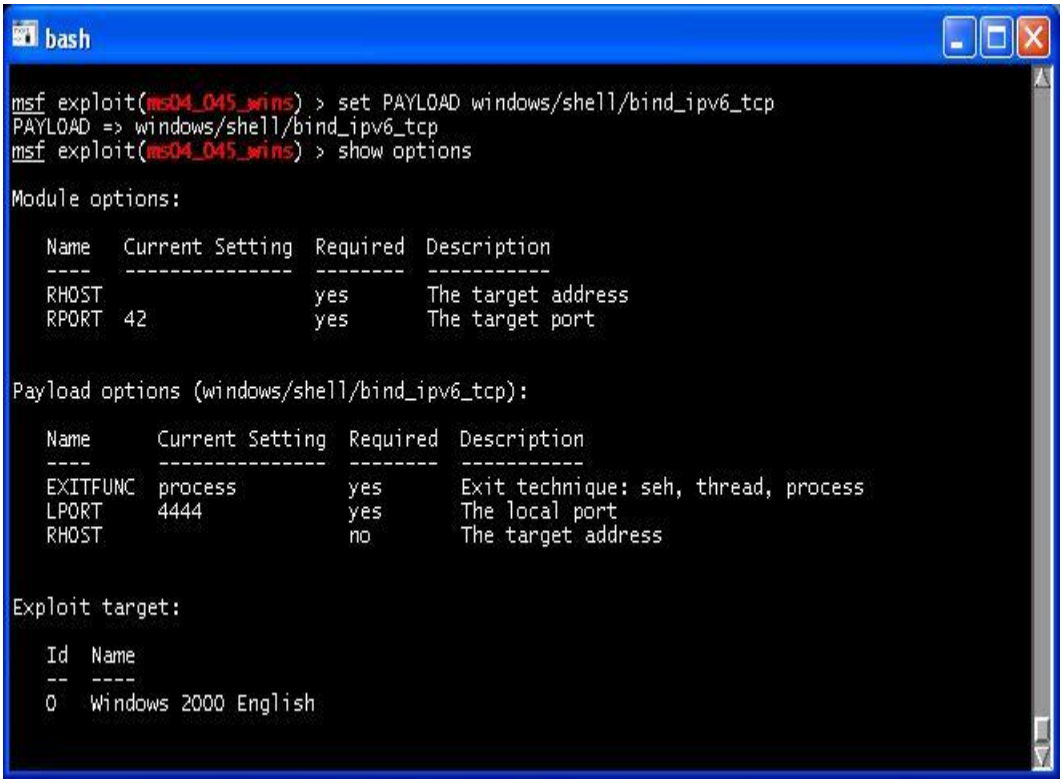
Είναι ένα διαδεδομένο payload μόνο για Windows προσφέροντας ένα ισχυρό περιβάλλον command line για αλληλεπίδραση με το σύστημα - στόχο. Έχει ξεχωριστή σημασία αν αναλογιστεί κανείς ότι το command shell των windows έχει περιορισμένη λειτουργικότητα. Παράλληλα επιτρέπει τη μεταφορά αρχείων από και προς το απομακρυσμένο σύστημα.

Για να χρησιμοποιήσουμε ένα payload αφού έχουμε επιλέξει κάποιο exploit, ακολουθούμε το συντακτικό:

```
set PAYLOAD payload_name
```

Τέλος πρέπει να ελέγξουμε ποίες παράμετροι πρέπει να οριστούν ώστε να εκτελεστεί σωστά το exploit. Για να δούμε ποίες είναι αυτές αρκεί να εκτελέσουμε:

```
show options
```



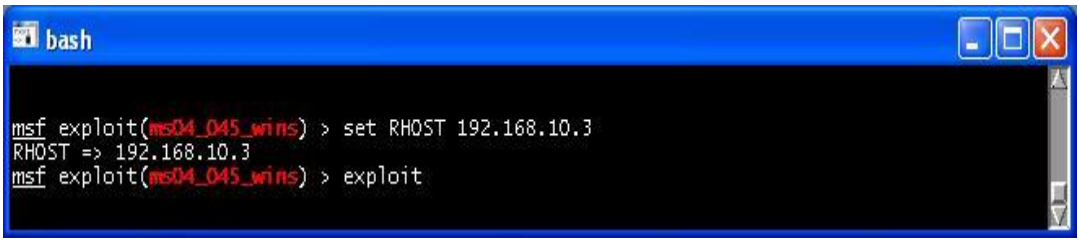
Εικόνα 45:Εντολές στο Metasploit- set PAYLOAD payload_name & show options

Για να θέσουμε τιμή σε κάποια μεταβλητή χρησιμοποιούμε την εντολή set. Για παράδειγμα για την IP διεύθυνση του στόχου:

```
set RHOST 192.168.10.3
```

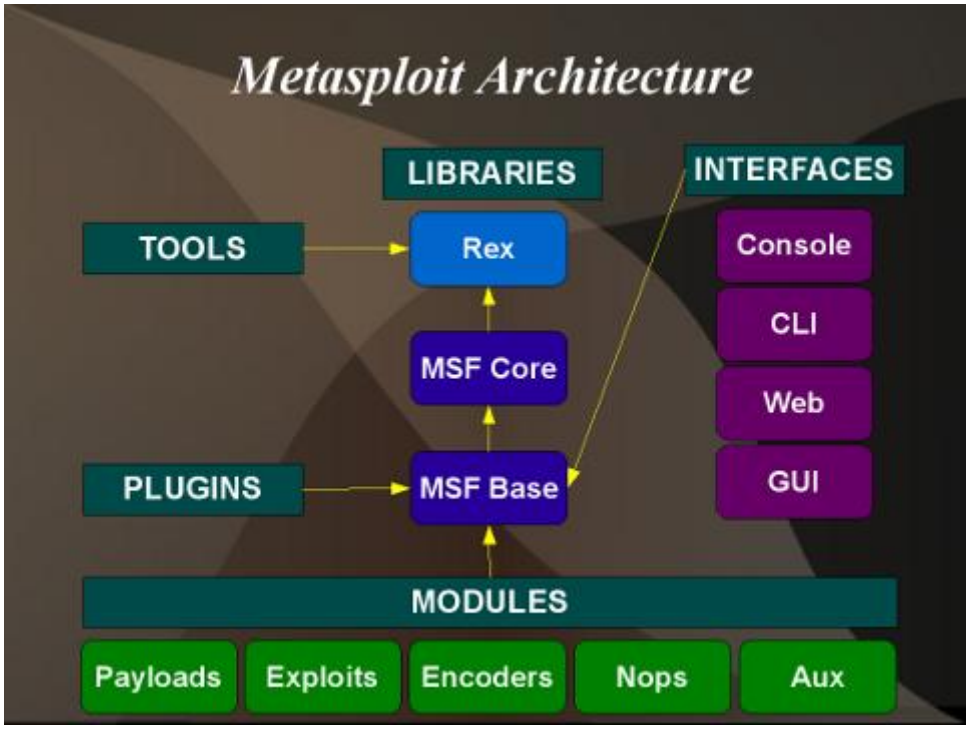
Έχοντας ορίσει όλες τις επιλογές μπορεί να ξεκινήσει η επίθεση με την εντολή:

```
Exploit
```



Εικόνα 46:Εντολές στο Metasploit- set RHOST & exploit

Γενική αρχιτεκτονική του Metasploit[8]



Εικόνα 47: Metasploit 3.4 Architecture

2.2.1.a Αντίμετρα στην Εκμετάλλευση Υπηρεσιών Δικτύων

Οι τυπικές συμβουλές για μετριασμό των τρωτών σημείων της Microsoft σε επίπεδο κώδικα είναι

- Δοκιμή και εφαρμογή των διορθώσεων (patch).
- Στο μεταξύ, δοκιμάζουμε και εφαρμόζουμε οποιοδήποτε διαθέσιμο αντίμετρο, όπως μπλοκάρισμα της πρόσβασης ή/και απενεργοποίηση της τρωτής απομακρυσμένης υπηρεσίας .
- Ενεργοποίηση logging και παρακολούθηση για να προσδιορίσουμε τα τρωτά συστήματα και τις πιθανές επιθέσεις έτσι ώστε να δημιουργηθεί ένα σχέδιο αντιμετώπισης.

Η γρήγορη εγκατάσταση των διορθώσεων είναι η καλύτερη επιλογή , καθώς απαλείφει το τρωτό σημείο. Και παρά αυτούς που φοβούνται αρχικά τις διορθώσεις , διαφορές ενδείξεις για πραγματικές εισβολές υποδεικνύουν ότι υπάρχει ένας συγκεκριμένος χρόνος καθυστέρησης μεταξύ της διαθεσιμότητας μιας διόρθωσης και

[8] http://www.metasploit.com/redmine/projects/framework/wiki/DeveloperGuide

την εκμετάλλευσης του τρωτού (δείτε για παράδειγμα την διεύθυνση http://www.verizonbusiness.com/resources/security/databreachreport.pdf).
Επίσης συνιστάτε να χρησιμοποιούμε αυτοματοποιημένα εργαλεία διαχείρισης των διορθώσεων όπως το Systems Management Server (SMS) έτσι ώστε να εγκαθιστάτε γρήγορα και να ελέγχουμε της διορθώσεις. Υπάρχουν πολλά σχετικά άρθρα στο διαδίκτυο όπου δίνουν περισσότερες λεπτομέρειες για τη δημιουργία ενός αποτελεσματικού προγράμματος για διορθώσεις σφαλμάτων και γενικότερα για τη διαχείριση των τρωτών σημείων.

Φυσικά υπάρχει κίνδυνος όσο χρόνο περιμένουμε να εμφανιστεί η διόρθωση από τη Microsoft.Τότε είναι βολικό να αντιμετωπίσετε το πρόβλημα με άλλο τρόπο. Η αντιμετώπιση είναι γενικά κάποιες επιλογές διαμόρφωσης είτε στο τρωτό σύστημα είτε στο γύρο περιβάλλον που μπορούν να μετριάσουν το αντίκτυπο της επίθεσης στην περίπτωση όπου δεν μπορεί να εφαρμοστεί μία διόρθωση. Για παράδειγμα, στην περίπτωση του MS07-029 , η Microsoft εξέδωσε μία συμβουλή ασφαλείας πριν από την διόρθωση (δείτε την διεύθυνση http://www.microsoft.com/technet/security/advisory/ για τις τρέχουσες συμβουλές).

Στην περίπτωση της εκμετάλλευσης του DNS, η Microsoft σύστησε την απενεργοποίηση της απομακρυσμένης διαχείρισης του DNS service μέσω RPC ορίζοντας μία συγκεκριμένη τιμή του Registry (HKLM\SYSTEM\CurrentControlSet\Services\DNS\Parameters\RpcProtocol, REG_DWORD= 4), εξαλείφοντας το τρωτό σημείο. Ο γκουρού της ασφαλείας Jesper Johansson σύστησε την εφαρμογή αυτού του αντίμετρου χρησιμοποιώντας αυτοματοποιημένα script(δείτε τη σελίδα http://msinfluentials.com/blogs/jesper/archive/2007/04/13/turn-off-rpc-management-of-dns-on-all-dcs.aspx).

Πολλά τρωτά σημεία μετριάζονται συνήθως εύκολα μπλοκάροντας την πρόσβαση στην τρωτή TCP/IP θύρα .Στην περίπτωση του τρέχοντος τρωτού DNS , θα ήταν πιθανός καλή ιδέα να περιορίσουμε/να πιστοποιήσουμε την πρόσβαση στην TCP 1025 και 1026 χρησιμοποιώντας firewall επιπέδου δικτύου και κύριου υπολογιστή, αλλά αυτό δεν είναι πρακτικό λόγω της πιθανής μεταβολής της θύρας που εκτίθεται από το RPC και ο πιθανός αρνητικός αντίκτυπος σε άλλες RPC εφαρμογές . Τουλάχιστον θα πρέπει να προοριστεί η εξωτερική πρόσβαση σε αυτές τις θύρες .

Τελευταίο αλλά όχι και το πιο ασήμαντο , είναι κρίσιμης σημασίας να παρακολουθούμε και να σχεδιάσουμε πως θα ανταποκρινόμασταν σε ενδεχόμενες εισβολές γνωστών τρωτών σημείων ενός συστήματος. Ιδανικά, θα πρέπει να υπάρχουν ήδη προγράμματα παρακολούθησης της ασφάλειας και απόκρισης σε συμβάντα τα όποια να επιτρέπουν γρήγορη διαμόρφωση μιας προσαρμοσμένης σάρωσης και πλάνα απόκρισης για πιθανά νέα τρωτά σημεία εάν αυτά πέρασαν ένα συγκεκριμένο όριο.

Για πλήρεις πληροφόρηση για μετριασμό του συγκεκριμένου τρωτού σημείου , δείτε το άρθρο ασφαλείας της Microsoft στο http://www.microsoft.com/technet/security/bulletin/MS07-029.mspx.

2.2.2 Εκμετάλλευση Τρωτών Εφαρμογών Χρηστών

Οι επιτιθέμενοι έχουν ανακαλύψει ότι η πιο αδύνατη σύνδεση σε οποιοδήποτε περιβάλλον είναι συνήθως οι τελικοί χρήστες και οι εφαρμογές που τρέχουν. Το γενικά κακώς διαχειριζόμενο και πλούσιο λογισμικό στην πλευρά του πελάτη παρέχει μεγάλες δυνατότητες επίθεσης για τους κακόβουλους εισβολείς. Επίσης, οι επιτιθέμενοι έρχονται συνήθως σε άμεση επαφή με τα δεδομένα και τα πιστοποιητικά των τελικών χρηστών με ελάχιστη αναζήτηση και χωρίς να ανησυχούν ότι μπορεί να τους καταλάβει ένας επαγγελματίας του τμήματος ασφάλειας. Μέχρι σήμερα, έχει δοθεί πολύ λιγότερη προσοχή στο λογισμικό των τελικών χρηστών σε σχέση με την ασφάλεια κατά τη διάρκεια της ανάπτυξης, αφού η επικρατούσα νοοτροπία ήταν να διορθωθούν αρχικά τα καταστρεπτικά τρωτά σημεία από την πλευρά των διακομιστών.

Όλοι αυτοί οι παράγοντες απεικονίζονται σε μια διαφοροποίηση στα άρθρα για την ασφάλεια της Microsoft που εμφανίστηκαν κατά την διάρκεια των ετών, καθώς η τάση είναι περισσότερο προς τις εφαρμογές των τελικών χρηστών, όπως τον Internet Explorer και το Office και λιγότερο συχνά εμφανίζονται για προϊόντα διακομιστών, όπως τα Windows και το Exchange.

Μία από τις πιο πρόσφατες καταστρεπτικές επιθέσεις από την πλευρά του πελάτη είναι το Windows Animated Cursor Remote Code Execution Vulnerability (που συνήθως αναφέρεται απλώς ως ANI, την επέκταση του αρχείου του τρωτού). Το ANI, που αρχικά ανακαλύφθηκε από τον Alexander Sotirov, περιλαμβάνει ένα τρωτό σημείο υπερχείλισης buffer στη συνάρτηση LoadAnilcon() στο USER32.dll και μπορεί να γίνει εκμετάλλευση του χρησιμοποιώντας την οδηγία CURSOR ενός φύλλου στυλ μέσα σε μία ιστοσελίδα για να φορτωθεί ένα κακόβουλο αρχείο ANI. Η εκμετάλλευση του τρωτού καταλήγει στη δυνατότητα να εκτελεσθούν αυθαίρετες εντολές με τα προνόμια του συνδεδεμένου χρήστη.

Το Metasploit μπορεί να χρησιμοποιηθεί για να εκμεταλλευτεί αυτό το τρωτό αρκετά εύκολα. Το Windows ANI LoadAnilcon() Chunk Size Stack Overflow (HTTP) δημιουργεί ένα κακόβουλο αρχείο ANI έτοιμο να εκμεταλλευτεί ένα συγκεκριμένο σύνολο από πλατφόρμες (π.χ., τα Vista), διαμορφώνει έναν τοπικό διακομιστή HTTP στον υπολογιστή του επιτιθέμενου και εξυπηρετεί το κακόβουλο αρχείο. Τα αθώα θύματα που συνδέονται στον HTTP διακομιστή μολύνονται και εκτελείται οποιαδήποτε αυθαίρετη ενέργεια έχει διαμορφωθεί μέσω του Metasploit (π.χ., εμείς χρησιμοποιήσαμε την επιλογή διοχέτευσης του κελύφους των Windows).

2.2.2.aΑντίμετρα Έναντι της Εκμετάλλευσης Εφαρμογών των Τελικών Χρηστών

Για πλήρεις πληροφορίες για το μετριασμό του τρωτού ANI, δείτε το άρθρο ασφάλειας της Microsoft στο http://www.microsoft.com/technet/security/Bulletin/MS07-017.mspx.

Γενικά, τα αντίμετρα για τις εφαρμογές των τελικών χρηστών είναι ένα μεγάλο και σύνθετο θέμα. Έχουμε συγκεντρώσει τα παρακάτω «Δέκα Βήματα για μία πιο Ασφαλή Εμπειρία στο Διαδίκτυο».

1. Αναπτύσσουμε ένα προσωπικό firewall, ιδανικά ένα firewall που μπορεί επίσης να διαχειριστεί εξερχόμενες προσπάθειες σύνδεσης. Το ενημερωμένο Windows firewall στο XP SP2 και νεότερο είναι μία καλή επιλογή.

Το Windows Firewall είναι ένα προστατευτικό όριο του υπολογιστή που παρακολουθεί και περιορίζει τις πληροφορίες που ταξιδεύουν μεταξύ του υπολογιστή μας και ενός δικτύου ή του Internet. Παρέχει μια γραμμή άμυνας ενάντια σε κάποιον που θα προσπαθήσει να έχει πρόσβαση στον υπολογιστή «έξω» από το τείχος προστασίας των Windows χωρίς την άδειά μας.

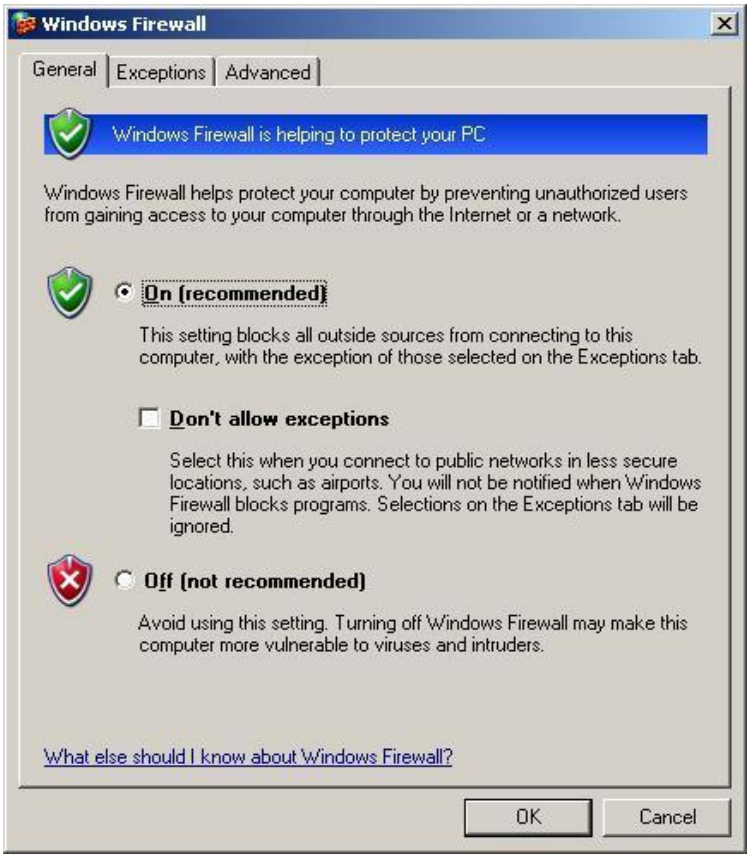
Εάν τρέχουμε το Windows XP Service Pack 2 (SP2), το Windows Firewall είναι ενεργοποιημένο από προεπιλογή. Ωστόσο, ορισμένοι κατασκευαστές υπολογιστών και διαχειριστές δικτύων το απενεργοποιούν.

Για να ανοίξουμε το Τείχος προστασίας των Windows

- Κάνουμε κλικ στο κουμπί Start και στη συνέχεια κάντε κλικ στην επιλογή Control Panel.
- Στον πίνακα ελέγχου, κάνουμε κλικ στο Windows Security Center.
- Κάνουμε κλικ στο Firewall των Windows.

Εικόνα 48:Τείχος προστασίας των Windows

Για ενεργοποίηση του Windows Firewall επιλέγουμε ON.

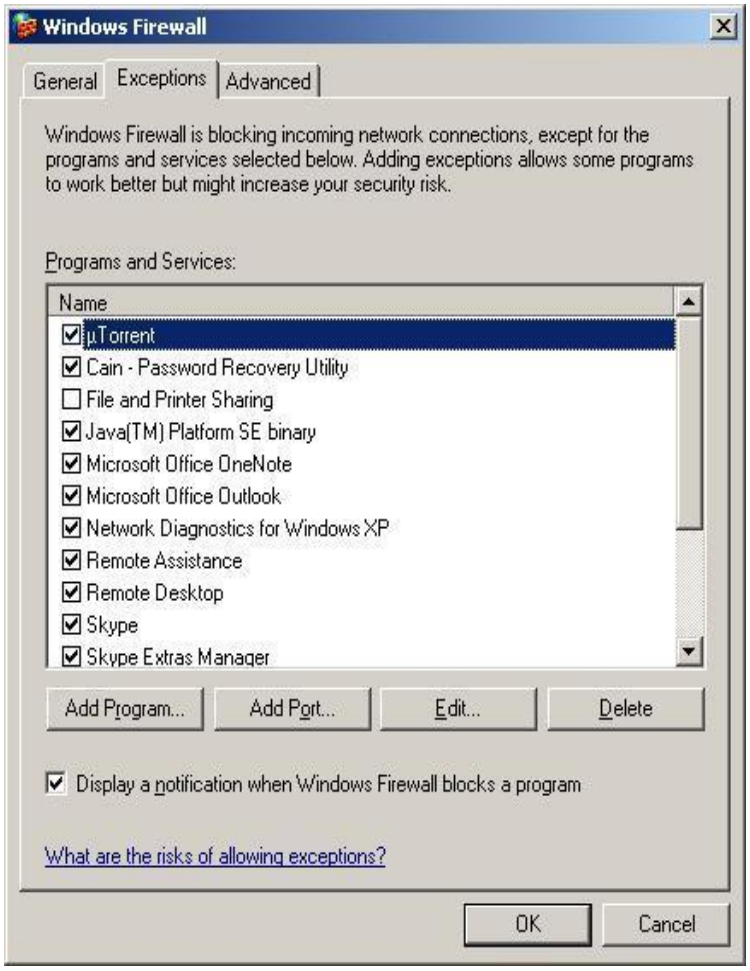


Εικόνα 49:Ενεργοποίηση Windows Firewall.

Ορισμένες φορές ίσως να θέλουμε να κάνουμε μια εξαίρεση και να επιτρέψουμε σε κάποιο πρόσωπο να συνδεθεί με τον υπολογιστή σας. Για παράδειγμα , τα παρακάτω σενάρια περιγράφουν περιπτώσεις κατά τις οποίες ίσως θέλουμε να δώσουμε σε κάποιο πρόσωπο/πρόγραμμα τη δυνατότητα σύνδεσης με τον υπολογιστή μας:

- Παίζουμε ένα παιχνίδι για/με πολλούς παίκτες στο Internet.
- Περιμένουμε να λάβουμε ένα αρχείο το οποίο αποστέλλεται μέσω ενός προγράμματος ανταλλαγής άμεσων μηνυμάτων
- Επιτρεπόμενη λήψη αρχείων από Utorrent

Στην καρτέλα **Exceptions** κάνουμε κλικ στην επιλογή **Add Program** για να προσθέσουμε τα προγράμματα τα οποία θα έχουμε πρόσβαση και δεν θα εμποδίζονται από το Windows Firewall**.**



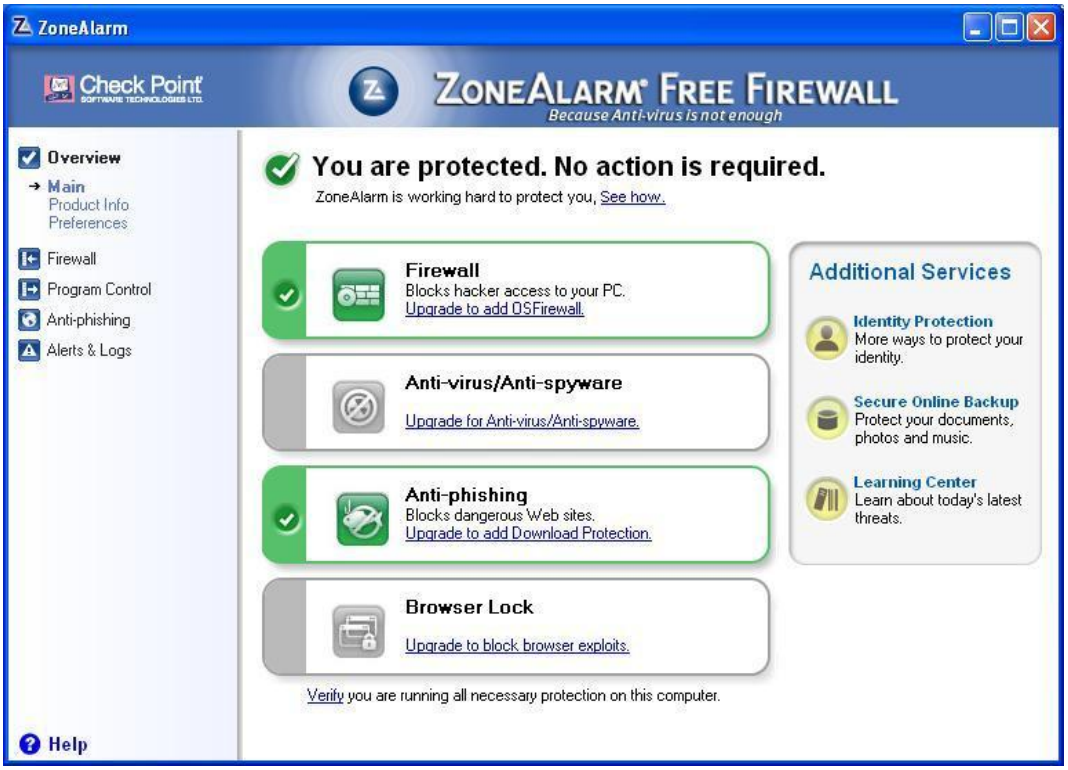
Εικόνα 50: Exceptions programs and services

Δεν είναι απαραίτητο να χρησιμοποιούμε το Windows Firewall ως προστατευτικό τοίχος. Μπορούμε να εγκαταστήσουμε και να τρέξουμε οποιοδήποτε άλλο τοίχος προστασίας ανάλογα με τις απαιτήσεις και τις ανάγκες μας. Εάν επιλέξουμε ένα άλλο τοίχος προστασίας πρέπει να απενεργοποιήσουμε το Windows Firewall.

Επιλογή τοίχου προστασίας Zone Alarm

Το ZoneAlarm μπλοκάρει τους hacker's από την διείσδυση στον υπολογιστή μας κρύβοντας την κίνηση του δικτύου. Με την ανίχνευση και την πρόληψη παρεμβολών, το ZoneAlarm Free Firewall κρατά τον υπολογιστή σας απαλλαγμένο από ιούς που επιβραδύνουν τις επιδόσεις και τα spyware που κλέβει προσωπικά στοιχεία, κωδικούς πρόσβασης και οικονομικά στοιχεία.

Παρακάτω βλέπουμε την αρχική σελίδα του ZoneAlarm .Παρατηρούμε ότι είναι ενεργοποιημένα το Firewall και το Anti-phishing στην έκδοση που κατεβάσαμε. Υπάρχουν δωρεάν εκδόσεις και για Anti-virus και για Browser Lock εμείς όμως δεν θα ασχοληθούμε με αυτά εδώ.

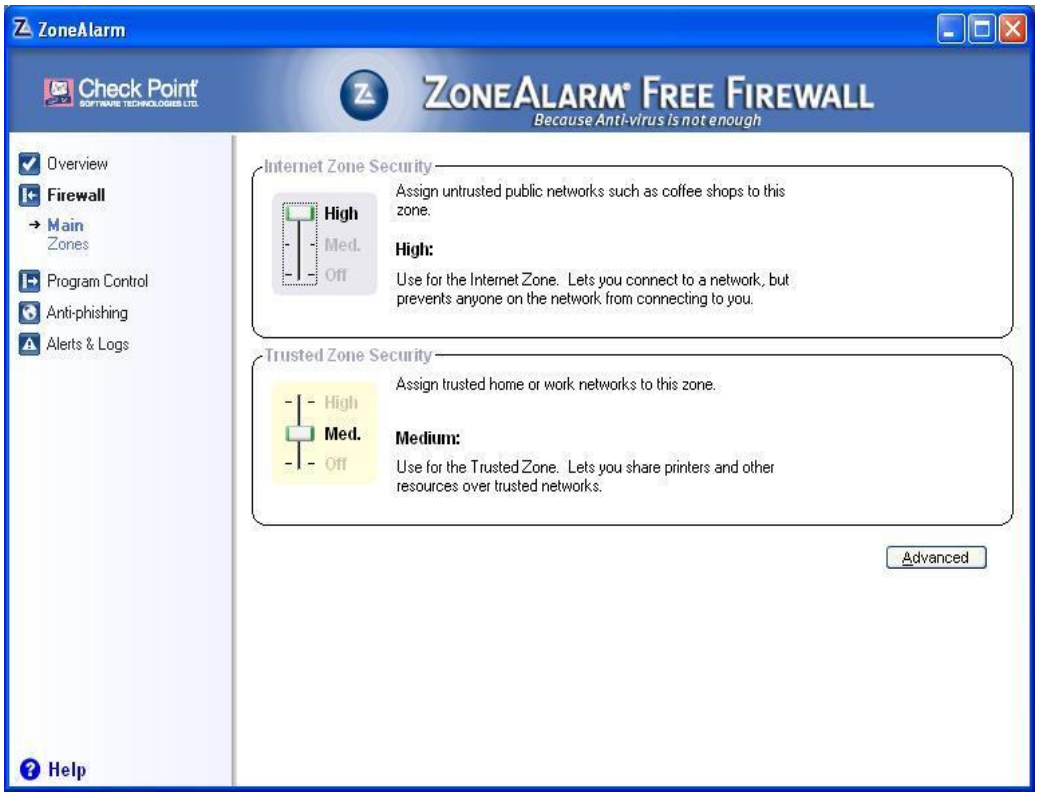


Εικόνα 51: ZoneAlarm firewall.

Στην καρτέλα του Firewall έχουμε τρείς επιλογές για το internet zone security (high, medium,off). Εμείς ανάλογα με τις ανάγκες μας θα πρέπει να τα ρυθμίσουμε συμφώνα με τα επίπεδα ασφάλειας που θέλουμε. Εισήγηση μας είναι η επιλογή High.

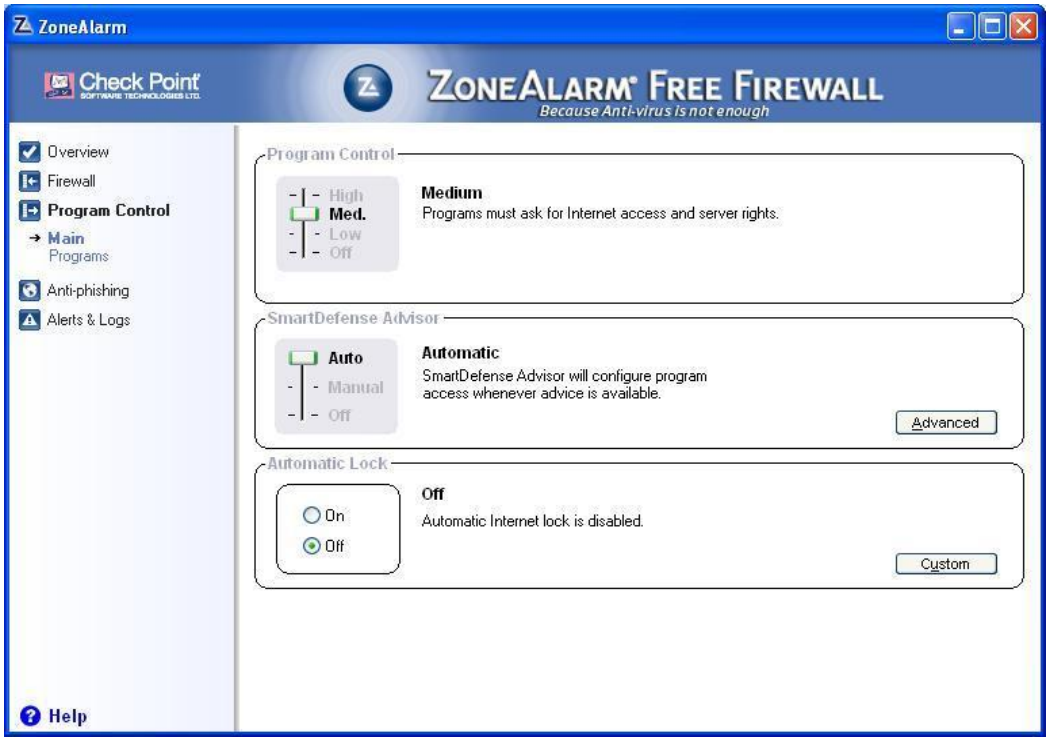
Στην ίδια καρτέλα είναι και το Trusted zone security όπου έχει να κάνει με το δίκτυο μας στο σπίτι και τη δουλεία όπου είναι πιο ασφαλής η σύνδεση. Η εισήγηση μας εδώ είναι να επιλέξουμε το Medium.

Στο κουμπί Advance έχουμε περισσότερες επιλογές και είναι για πιο ειδικευόμενη χρήση.



Εικόνα 52:Ζώνες ασφαλείας - ZoneAlarm.

Στην καρτέλα του Program Control ρυθμίζουμε πως θα λειτούργει το πρόγραμμα και κατά πόσο θα θέλαμε να μας εμφανίζει μηνύματα με συμβουλές για να μας προτείνει μια βελτίωση .

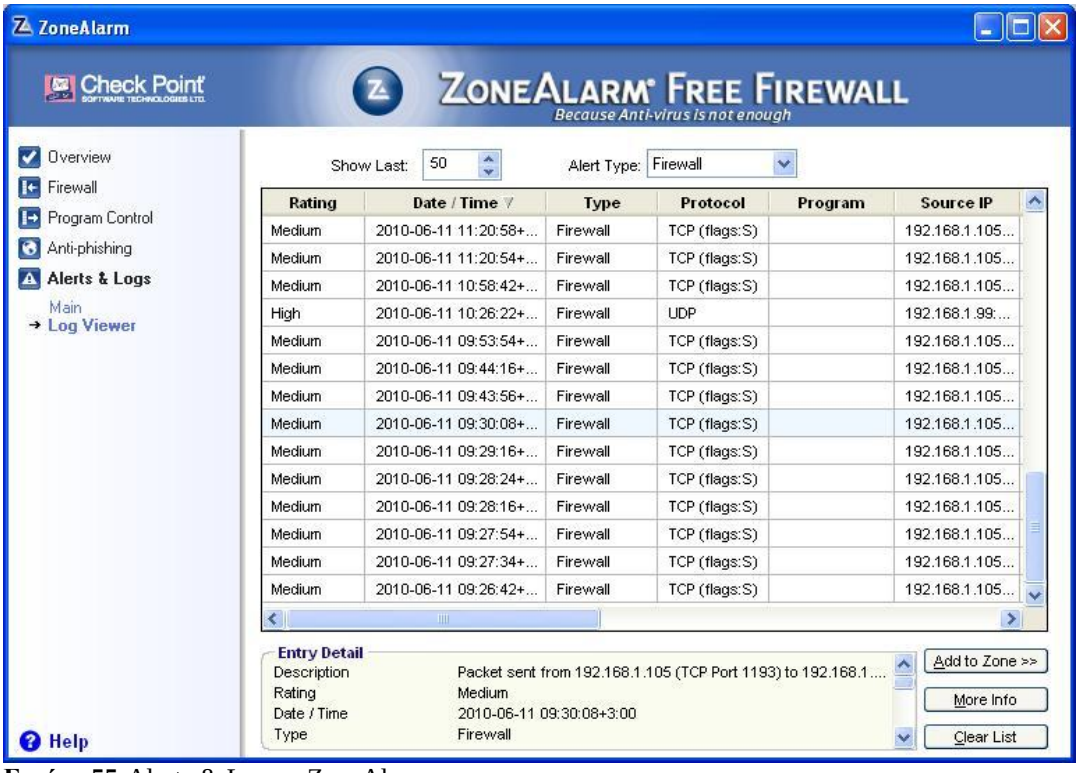


Εικόνα 53: Program Control - ZoneAlarm .

Εδώ βλέπουμε το Anti-phishing να είναι ενεργοποιημένο για περισσότερη ασφάλεια.

Εικόνα 54: Anti-phishing – ZoneAlarm.

Το Alerts & Logs όπου κρατάει ένα αρχείο με τις ειδοποιήσεις του Firewall.

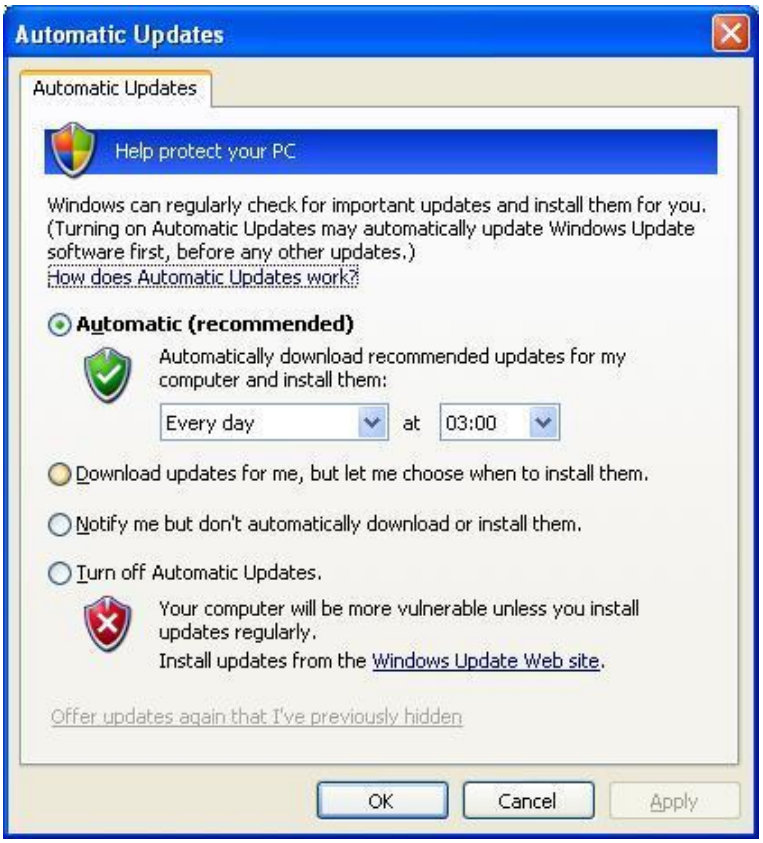


Εικόνα 55: Alerts & Logs – ZoneAlarm.

2. Διατηρούμε ενημερωμένες όλες τις σχετικές διορθώσεις ασφάλειας λογισμικού. Οι χρήστες των Windows θα πρέπει να διαμορφώσουν το Microsoft Automatic Updates ώστε να επιτυγχάνεται ευκολότερα αυτός ο στόχος.

Για να ενημερώσουμε τις διορθώσεις ασφάλειας ακολουθούμε τα εξής βήματα:

Από το menu **Start** επιλέγουμε **Control Panel** και στην συνέχεια **Automatic Updates** .



Εικόνα 56: Microsoft Automatic Updates.

Ορίζουμε στο Automatic Updates κάθε πόσο θα ελέγχει για να κατεβάζει νέες διορθώσεις ασφάλειας και αναβαθμίσεις του συστήματος.

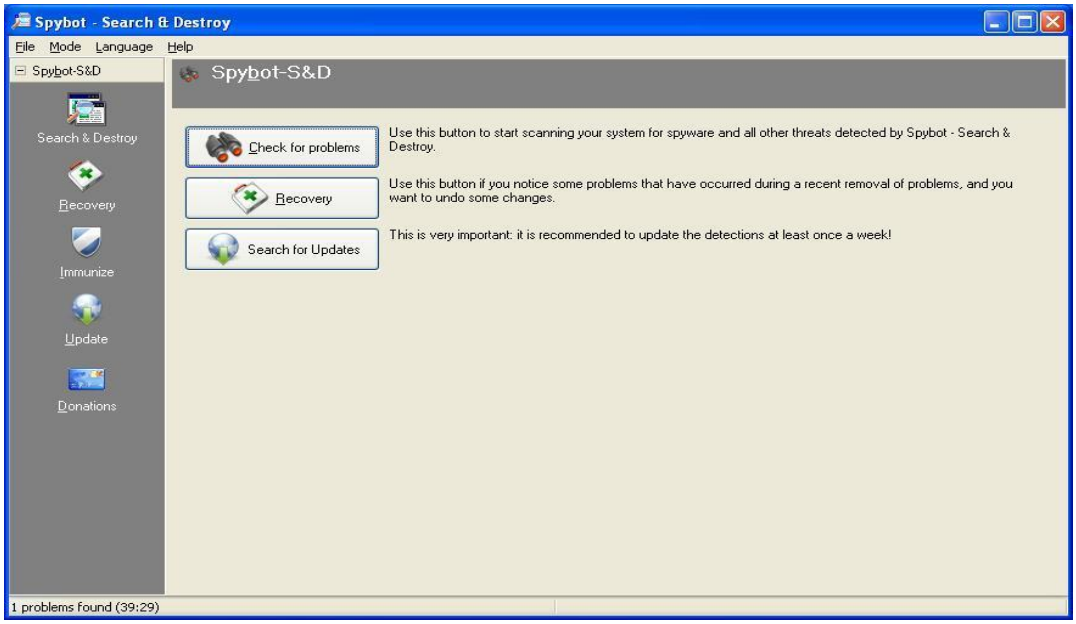
3. Τρέχοντας αντιβιοτικό λογισμικό που να σαρώνει αυτόματα το σύστημα μας (ιδιαίτερα τα εισερχόμενα συνημμένα ηλεκτρονικού ταχυδρομείου) και ενημερώνεται μόνο του. Συστήνετε επίσης να έχουμε βοηθητικά προγράμματα antiadware/spyware και για ηλεκτρονικό ψάρεμα (antiphishing).

Επιλογή προγράμματος spyware Spybot

Το Spybot - Search & Destroy ανιχνεύει και διαγράφει τα spyware. Είναι σχετικά ένα νέο είδος απειλής που δεν καλύπτετε ακόμη από κοινές εφαρμογές anti-virus. Τα Spyware αθόρυβα ανιχνεύουν την συμπεριφορά πλοήγησης μας ώστε να δημιουργήσουν ένα προφίλ προώθησης αγαθών για μας το οποίο μεταδίδετε εν αγνοία μας στους compilers και πωλείτε σε διαφημιστικές εταιρίες. Αν δούμε νέα toolbars μέσα στον Internet Explorer όπου δεν έχουμε εγκαταστήσει εκ προθέσεως ή αν ο browser μας ανεξήγητα "κολλάει" ή αν η αρχική μας σελίδα είναι σε "ομηρία-hijacked" (ή αν αλλάξει χωρίς να το γνωρίζουμε), ο υπολογιστής μας είναι πιθανότατα μολυσμένος με spyware. Ακόμη και αν δεν μπορούμε να δούμε τα συμπτώματα, ο υπολογιστής μας μπορεί να είναι μολυσμένος, διότι όλο και περισσότερα spyware αναδύονται.

Επιλέξαμε το Spybot - Search & Destroy για τη δουλειά αυτή επειδή είναι ένα καλό πρόγραμμα και οι κυροί λόγοι είναι ότι έχει παρά πολλές δυνατότητες, η συνεχής ενημέρωση που έχει με αναβαθμίσεις και παρέχεται δωρεάν.

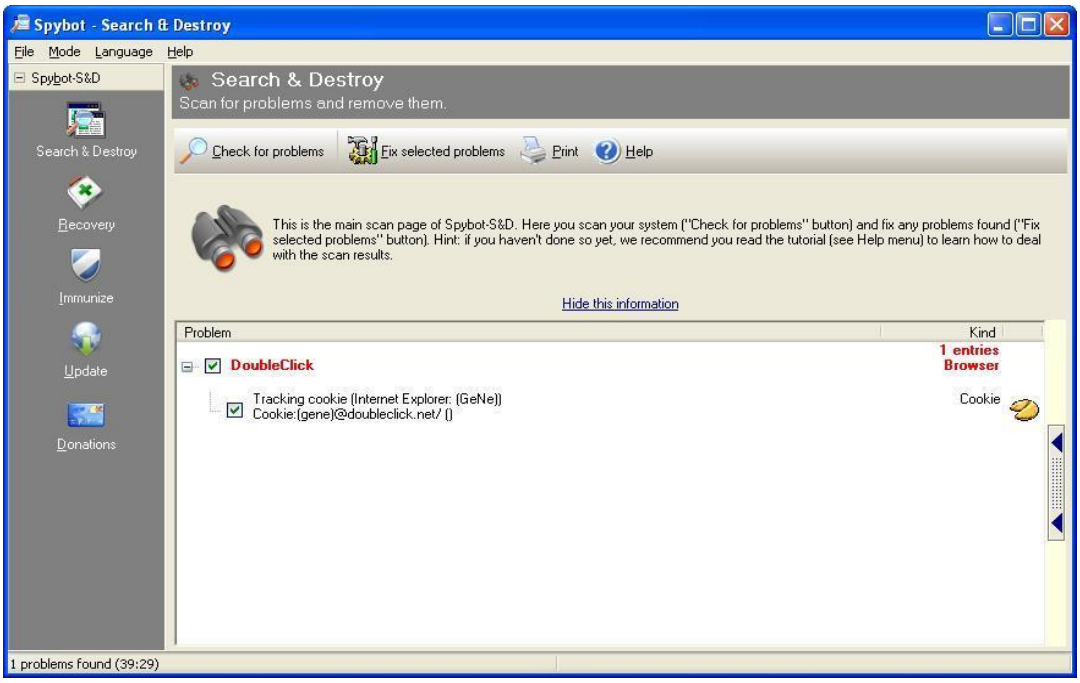
Από την γραμμή εργαλείων του Spybot-S & D επιλέγουμε "*Check for problems*" για να ξεκινήσει το scanning για ανίχνευση spyware.



Εικόνα 57: Spyware Spybot-S & D.

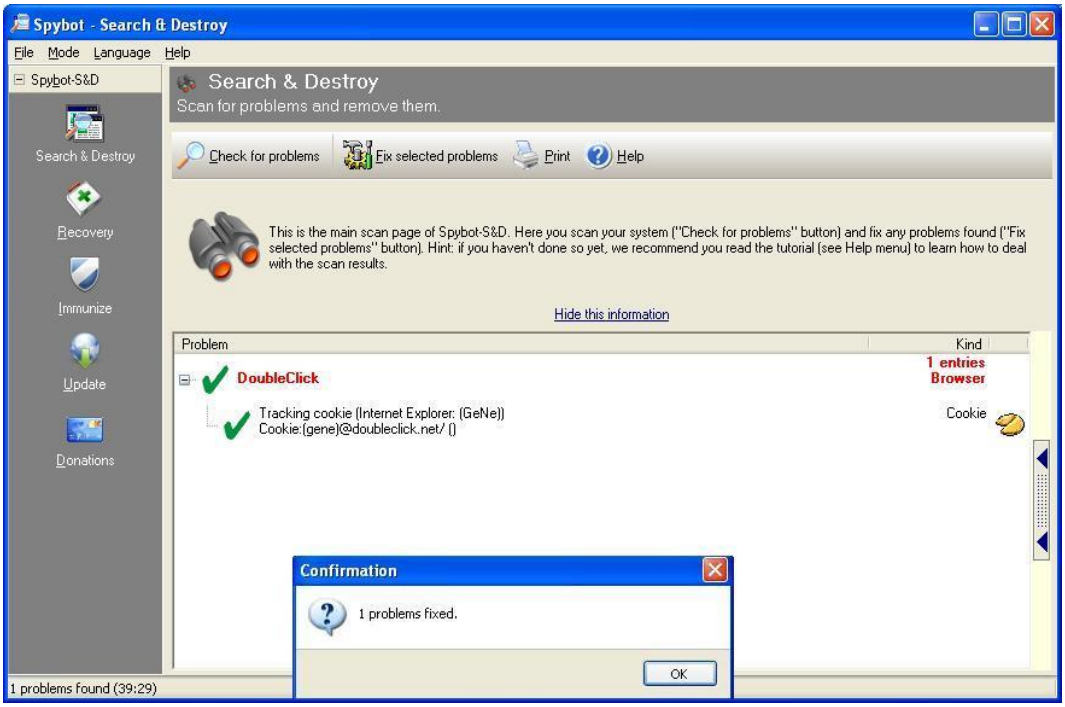
Κατά την διάρκεια του scanning εντοπίσαμε ένα πρόβλημα.

- DoubleClick



Εικόνα 58: Check for problems - Spybot-S & D.

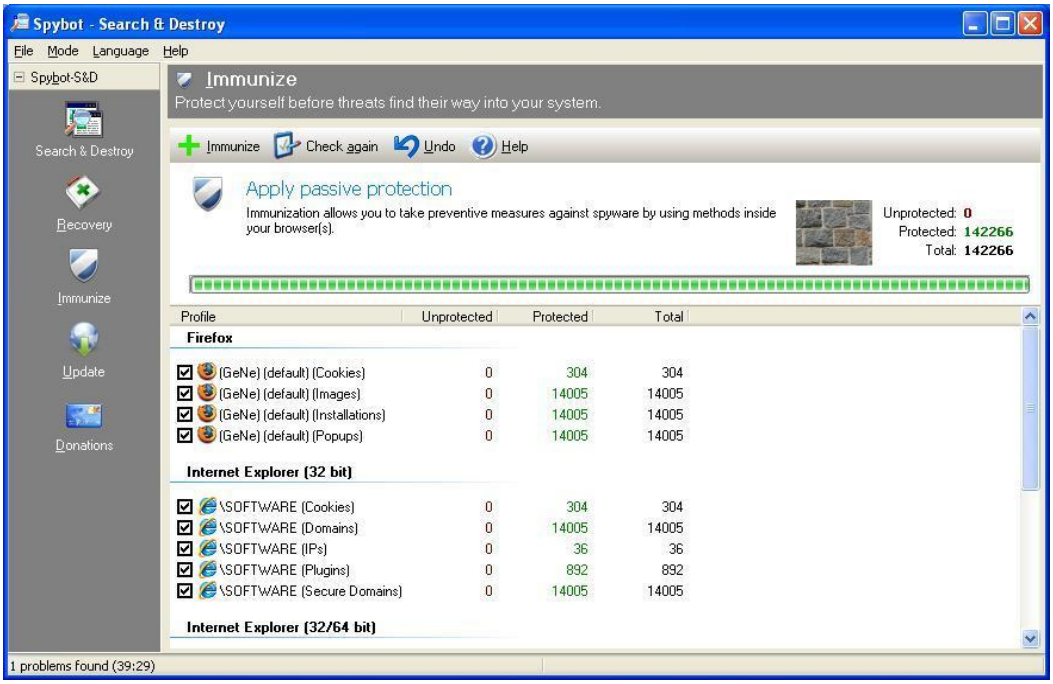
Στην συνέχεια για να το επιλύσουμε επιλέγουμε το κουμπί *Fix selected problems.*



Εικόνα 59: Fix selected problems -Spybot-S & D.

Η λειτουργία Immunize εμποδίζει π.χ. Tracking Cookies από την είσοδο του συστήματός μας. Το Immunize λειτουργεί με τον Mozilla Firefox, Internet Explorer

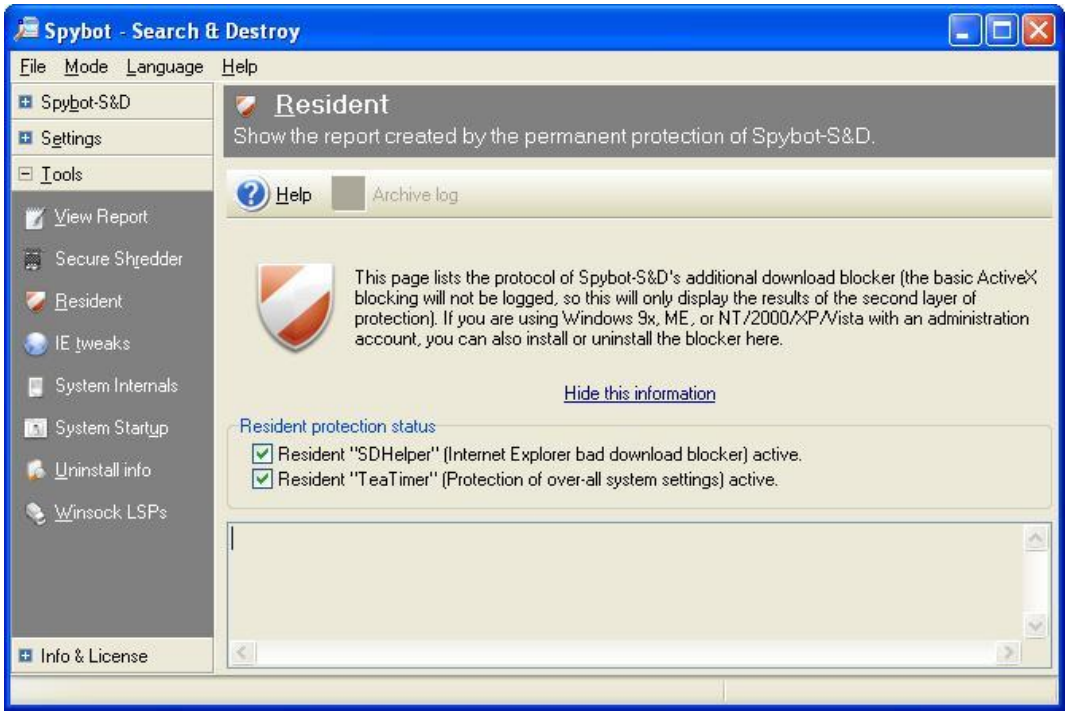
και Opera, επιτρέποντάς μας να προσαρμόσουμε ειδικές ρυθμίσεις του browser για να εμποδίσει γνωστούς spyware installers, που περιλαμβάνονται ήδη στη βάση δεδομένων του Spybot-S & D .



Εικόνα 60:Λειτουργία Immunize - Spybot-S & D .

Από το Mode επιλέγουμε το Advance.

Η υπηρεσία **Resident TeaTimer** αποτρέπει την εγκατάσταση των ανεπιθύμητων αρχείων.



Εικόνα 61:Υπηρεσία Resident TeaTimer

Εάν γνωρίζουμε κάποιες κακόβουλες διαδικασίες που θέλουν να ξεκινήσουν, το TeaTimer τις τερματίζει αμέσως δίνοντας μας τρεις επιλογές πώς να αντιμετωπίσουμε αυτή την διαδικασία.

- Να μας ενημερώσει όταν η διαδικασία προσπαθήσει να ξεκινήσει ξανά.
- Αυτόματος τερματισμός της διαδικασίας.
- Επιτρέπουν την διαδικασία να τρέξει.

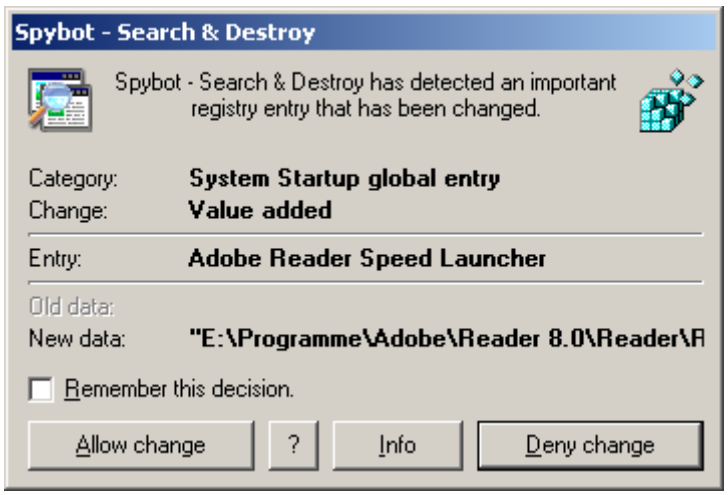
Υπάρχει επίσης μία επιλογή για να διαγράψουμε το αρχείο που συνδέεται με αυτή την διαδικασία.

Αν κάποιος προσπαθεί να αλλάξει κρίσιμα κλειδιά μητρώου (registry keys), το TeaTimer θα τον εντοπίσει.

Το TeaTimer μπορεί να μας προστατεύσει από τις μεταβολές αυτές δίνοντας μας μία εντολή :Μπορούμε να επιτρέψουμε ή να αρνηθούμε την αλλαγή. Το TeaTimer λειτουργεί πάντα στο παρασκήνιο.

Ξεκινάμε το Resident TeaTimer πατώντας Tools στην συνέχεια επιλέγουμε Resident στην αριστερή γραμμή προήγησης. Εκεί μπορούμε να τσεκάρουμε τα κουτάκια δίπλα από το Resident TeaTimer (προστασία όλων των ρυθμίσεων του συστήματος) που δραστηριοποιούνται για την ενεργοποίηση του TeaTimer.

Από το Spybot-S & D 1.6 και μετά το TeaTimer χρησιμοποιεί τη βάση δεδομένων της εταιρίας, όπου είναι γνωστά αρχεία βαθμολογημένα ως καλά ή επικίνδυνα. Αυτή η βάση δεδομένων περιέχει εκατοντάδες χιλιάδες εγγραφές που διευρύνονται συνεχώς. Παρ' όλα αυτά υπάρχουν και αρχεία τα οποία δεν καλύπτονται ακόμη. Σε αυτές τις περιπτώσεις θα ζητηθεί η άδεια για κάθε αλλαγή που θα γίνει.



Εικόνα 62: Άδεια αλλαγής registry.

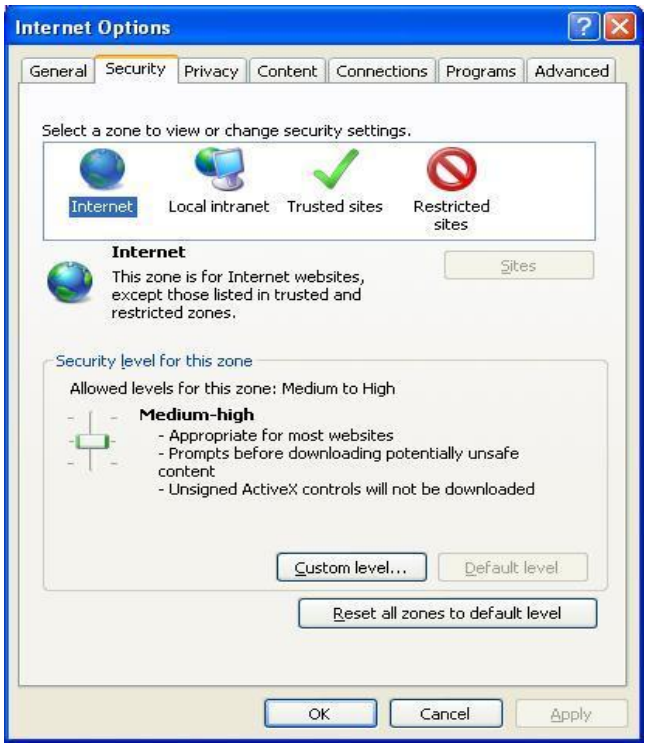
4. Διαμορφώνουμε το Windows Internet Options στο Control Panel που είναι προσπελάσιμο μέσω του Internet Explorer.

Ο Internet Explorer περιλαμβάνει τέσσερις προκαθορισμένες ζώνες: Internet, Τοπικό intranet (Local intranet), Αξιόπιστες τοποθεσίες (Trusted Sites) και Ελεγχόμενες τοποθεσίες (Restricted Sites).

Ζώνη Internet

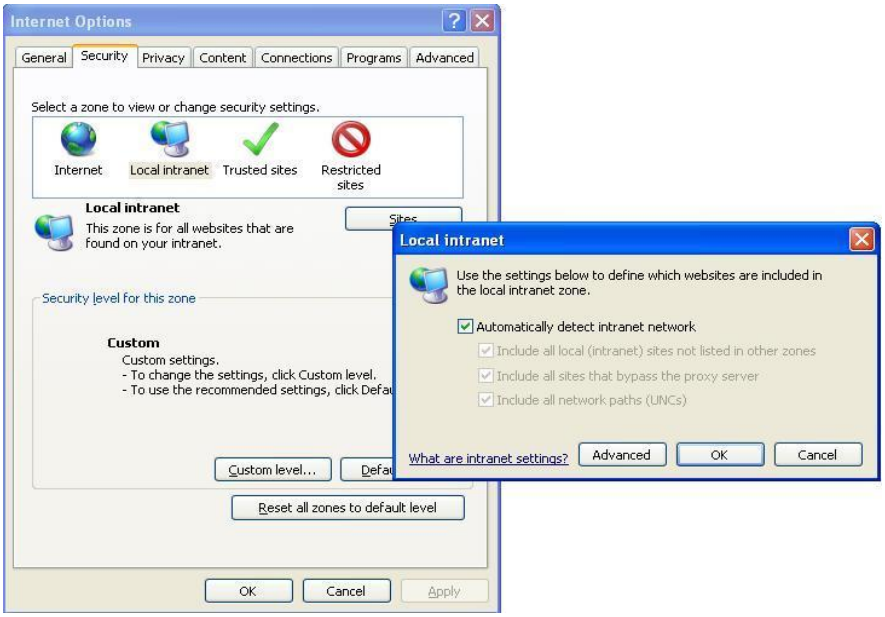
Αυτή η ζώνη περιέχει τοποθεσίες Web οι οποίες δεν βρίσκονται στον υπολογιστή ή το τοπικό μας Intranet ή δεν έχουν ήδη αντιστοιχιστεί σε κάποια άλλη ζώνη.

Το προεπιλεγμένο επίπεδο ασφαλείας είναι "Μεσαίο" (Medium).



Εικόνα 63:Επίπεδο ζώνης ασφαλείας Internet – Medium.

Από προεπιλογή, η ζώνη "Τοπικό intranet" (Local intranet) περιέχει όλες τις συνδέσεις δικτύου που έχουν εγκατασταθεί με χρήση μιας διαδρομής η οποία βασίζεται στη Διεθνή Σύμβαση Ονομάτων (Universal Naming Convention-UNC) καθώς και τις τοποθεσίες Web που παρακάμπτουν το διακομιστή μεσολάβησης ή φέρουν ονόματα τα οποία δεν περιλαμβάνουν τελείες (για παράδειγμα, http://local), με την προϋπόθεση ότι δεν έχουν αντιστοιχιστεί στις ζώνες "Ελεγχόμενες τοποθεσίες" (Restricted Sites) ή "Αξιόπιστες τοποθεσίες" (Trusted Sites). Το προεπιλεγμένο επίπεδο ασφαλείας για τη ζώνη "Τοπικό Intranet" (Local Intranet) είναι "Μεσαίο" (Medium). Όταν έχουμε πρόσβαση σε ένα τοπικό δίκτυο (LAN) ή σε ένα κοινόχρηστο στοιχείο του Intranet ή σε μια τοποθεσία Intranet στο Web, χρησιμοποιώντας μια διεύθυνση IP (Internet Protocol) ή χρησιμοποιώντας ένα πλήρως αναγνωρισμένο όνομα τομέα (FQDN), το κοινόχρηστο στοιχείο ή η τοποθεσία Web προσδιορίζεται ότι βρίσκεται στη ζώνη Internet αντί για τη ζώνη τοπικού Intranet.

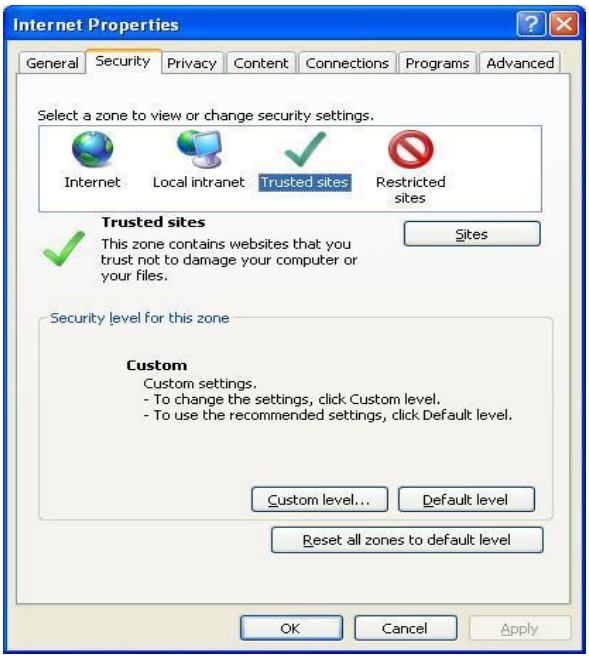


Εικόνα 64:Επίπεδο ζώνης ασφαλείας Local Intranet - Medium.

Ζώνη αξιόπιστων τοποθεσιών (Trusted Sites)

Αυτή η ζώνη περιέχει τοποθεσίες Web τις οποίες εμπιστευόμαστε ως ασφαλείς (όπως τοποθεσίες Web οι οποίες βρίσκονται στο τοπικό intranet της εταιρείας μας ή προέρχονται από εταιρείες που εμπιστευόμαστε). Όταν προσθέσουμε μια τοποθεσία Web στη ζώνη "Αξιόπιστες τοποθεσίες" (Trusted Sites), θεωρείται δεδομένο ότι τα αρχεία των οποίων κάναμε λήψη ή τα οποία εκτελούνται από αυτήν την τοποθεσία Web δεν θα προκαλέσουν ζημιές στον υπολογιστή ή τα δεδομένα μας.

Το επίπεδο ασφαλείας είναι ορισμένο σε "Χαμηλό" (Low).

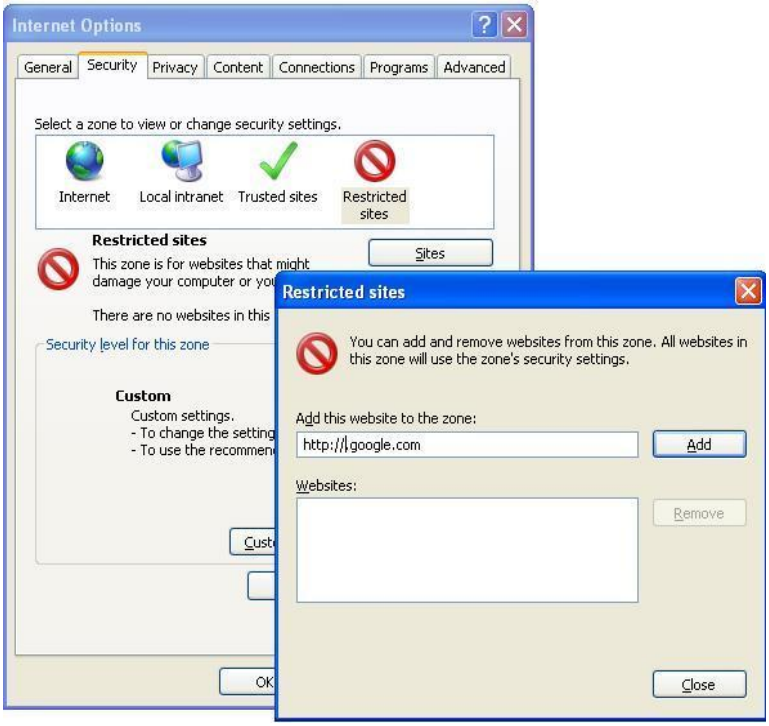


Εικόνα 65:Επίπεδο ζώνης ασφαλείας Trusted Sites - Low.

Ζώνη ελεγχόμενων τοποθεσιών (Restricted Sites)

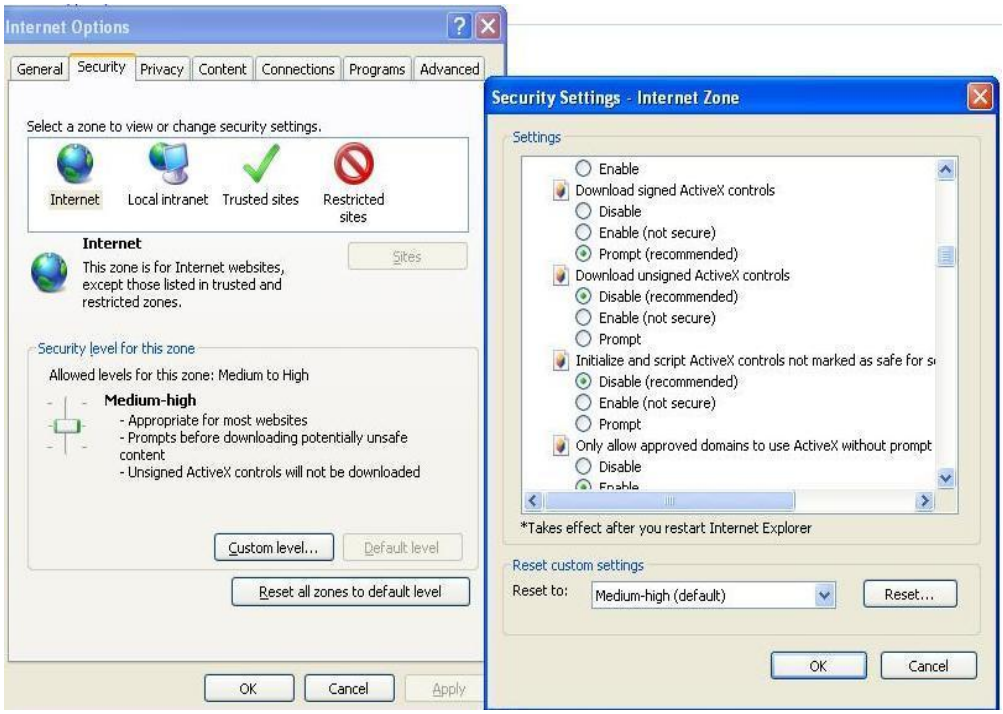
Αυτή η ζώνη περιέχει τοποθεσίες Web τις οποίες δεν θεωρούμε αξιόπιστες. Όταν προσθέσουμε μια τοποθεσία Web στη ζώνη "Ελεγχόμενες τοποθεσίες" (Restricted Sites), ενδέχεται τα αρχεία που κάνουμε λήψη ή τα οποία εκτελούμε από αυτήν την τοποθεσία Web να προκαλέσουν ζημιές στον υπολογιστή ή τα δεδομένα μας. Το επίπεδο ασφαλείας είναι ορισμένο σε "Υψηλό" (High).

Οι ρυθμίσεις ασφαλείας εφαρμόζονται μόνο σε αρχεία του υπολογιστή μας τα οποία βρίσκονται στο φάκελο "Προσωρινά αρχεία Internet" (Temporary Internet Files). Οι ρυθμίσεις αυτές χρησιμοποιούν το επίπεδο ασφαλείας της τοποθεσίας Web από την οποία προέρχονται τα αρχεία. Όλα τα άλλα αρχεία θεωρούνται ασφαλή.



Εικόνα 66:Επίπεδο ζώνης ασφαλείας Restricted Sites- High.

Πιο κάτω παρατηρούμε ότι σε κάθε μία από τις τέσσερις προκαθορισμένες ζώνες υπάρχει η επιλογή Custom Level που μπορούμε πέραν από το να αλλάξουμε το επίπεδο ασφαλείας να διαφοροποιήσουμε και τις παραμέτρους που υφίστανται με τις ανάγκες ασφάλειας που εμείς θέλουμε να έχουμε.



Εικόνα 67:Ρύθμιση Custom Level.

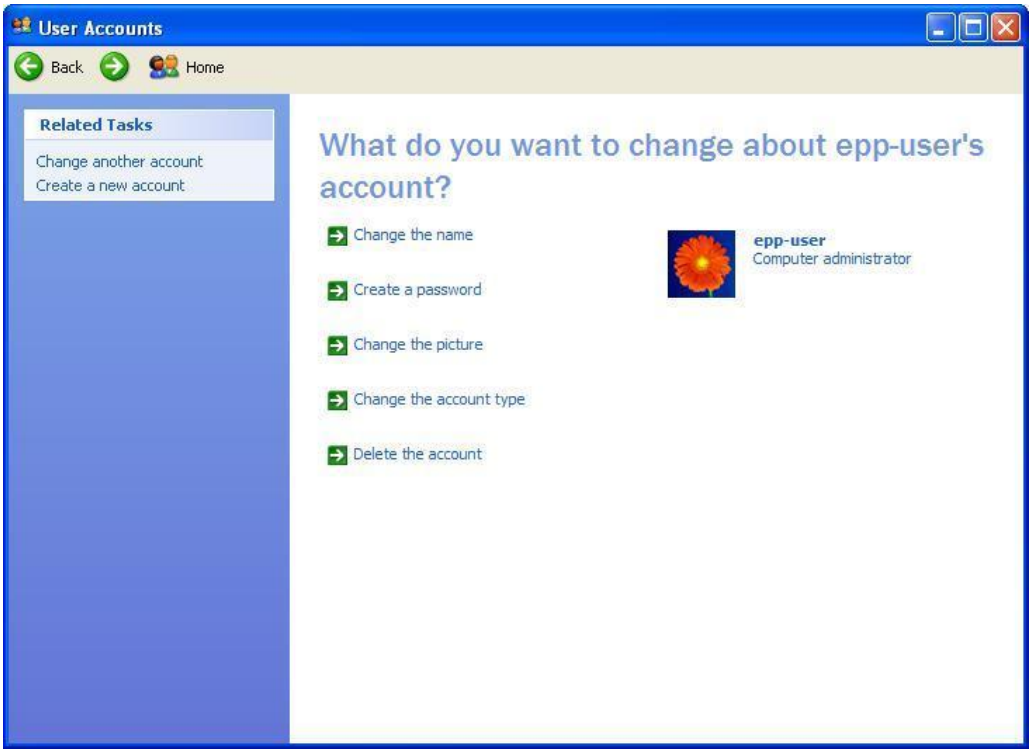
5. Σύνδεση με λιγότερα προνόμια. Να μην συνδεόμαστε ποτέ ως Administrator (ή με ένα αντίστοιχο προνομιούχο λογαριασμό) σ' ένα σύστημα που θα χρησιμοποιήσουμε ώστε να περιηγηθούμε στο Διαδίκτυο ή για να διαβάσουμε το ηλεκτρονικό ταχυδρομείο. Χρησιμοποιούμε λειτουργίες με περιορισμένα προνόμια, όπως το Windows UAC και Low Rights IE (LoRIE), όπου είναι δυνατόν.

Ο έλεγχος λογαριασμού χρήστη (UAC) μάς ειδοποιεί πριν πραγματοποιηθούν αλλαγές στον υπολογιστή σας, για τις οποίες απαιτούνται δικαιώματα επιπέδου διαχειριστή. Η προεπιλεγμένη ρύθμιση UAC μάς ειδοποιεί όταν κάποια προγράμματα επιχειρούν να πραγματοποιήσουν αλλαγές στον υπολογιστή μας αλλά μπορούμε να αλλάζουμε πόσο συχνά θα λαμβάνουμε ειδοποιήσεις UAC.

Προκειμένου να προστατευθούν τα Windows από κακόβουλο λογισμικό και ακούσια καταστροφικά λάθη, η Microsoft διαθέτει το λειτουργικό σύστημα με το User Account Control (UAC) του συστήματος. Το σύστημα αυτό απαιτεί όλοι οι χρήστες να χρησιμοποιούν το πρότυπο λειτουργίας χρήστη και στη συνέχεια να ζητά από αυτούς επιβεβαίωση πιστοποίησης διαχειριστή πριν από την εκτέλεση μιας λειτουργίας.

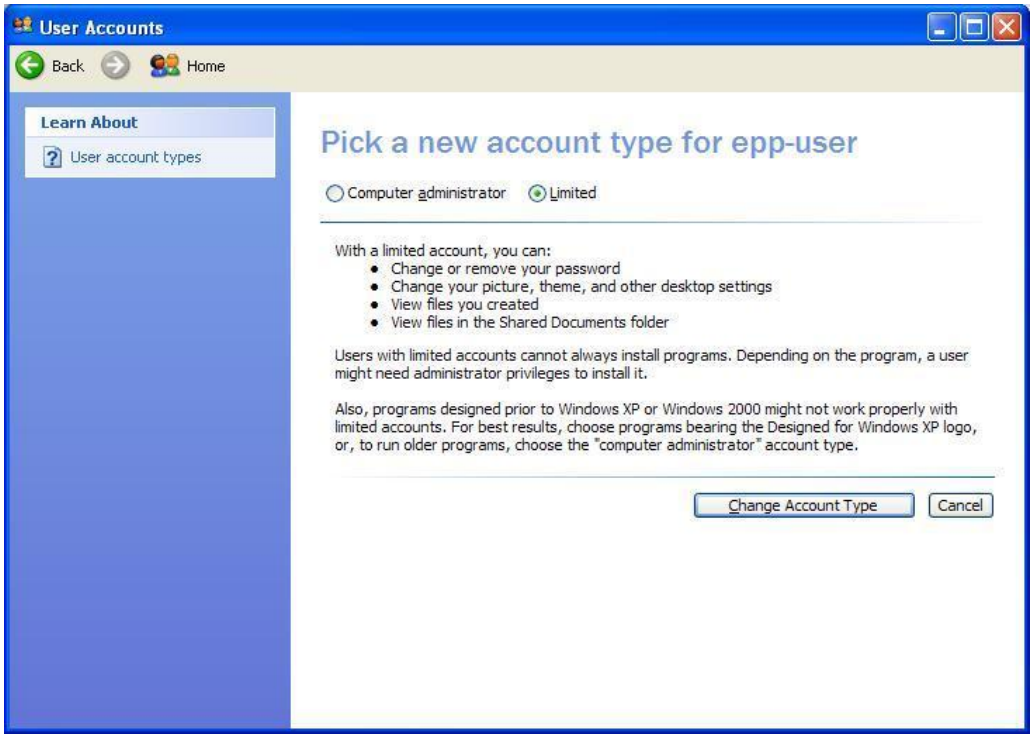
Μπορούμε να χρησιμοποιήσουμε τον προκάτοχό UAC στα Windows XP με την εντολή RunAs.

Εδώ φαίνεται πώς να χρησιμοποιούμε την έκδοση Windows XP της UAC:



Εικόνα 68:Σύνδεση στον υπολογιστή ως διαχειριστής Administrator-βήμα 1ο.

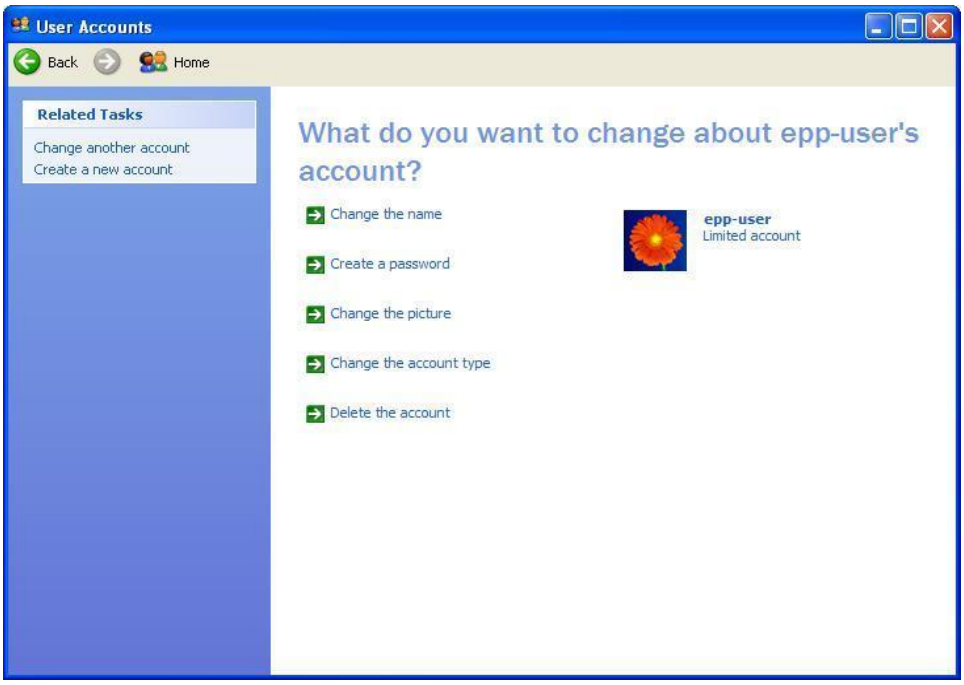
Εντόπιση του λογαριασμού χρήστη που έχουμε για να αλλάξουμε τον τύπο του λογαριασμού μας από διαχειριστή του υπολογιστή σε ένα Limited λογαριασμό ή να δημιουργήσουμε ένα καινούργιο λογαριασμό.



Εικόνα 69:Αλλαγή λογαριασμού από Administrator σε Limited–βήμα 2ο.

Αποσύνδεση από το λογαριασμό διαχειριστή και επανασύνδεση με το νέο Limited λογαριασμό μας.

Εικόνα 70:Σύνδεση στον λογαριασμό Limited-βήμα 3ο.



Εικόνα 71: Login στο epp-user–βήμα 4ο.

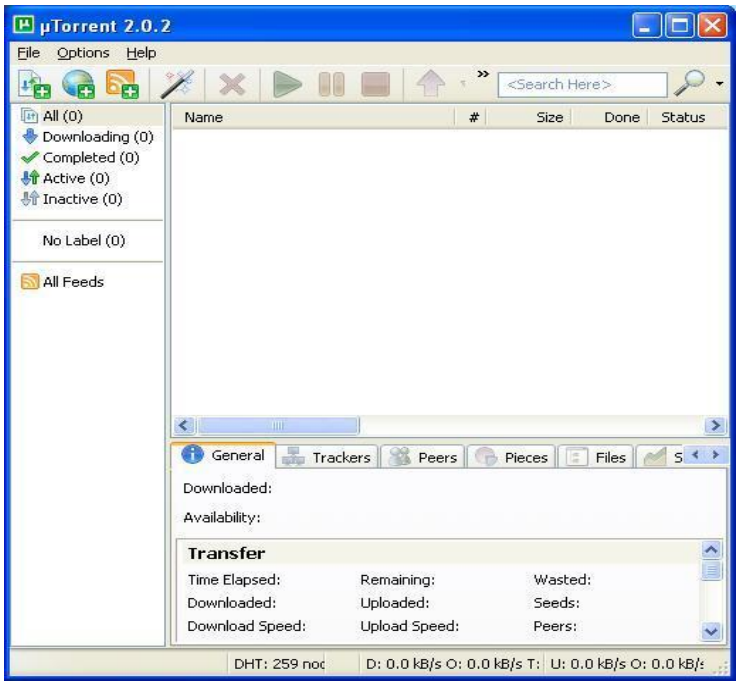
Αν προκύψει μια κατάσταση κατά την οποία θα πρέπει να έχουμε πιστοποιήσεις/επιβεβαιώσεις διαχειριστή, πιέζουμε το πλήκτρο [Shift], όπως κάνουμε δεξί κλικ στο εκτελέσιμο αρχείο της εφαρμογής ή στο εικονίδιό και επιλέγουμε την εντολή RunAs.

Εικόνα 72:Εκτέλεση εντολής RunAs –βήμα 5ο.

Όταν εμφανιστεί το παράθυρο διαλόγου RunAs, επιλέγουμε το κουμπί επιλογής "the following user" για να επιλέξουμε το λογαριασμό Administrator και στη συνέχεια να πληκτρολογήσουμε τον κωδικό πρόσβασης.

Εικόνα 73:Εισαγωγή user name και password – βήμα 6ο.

Στην συνέχεια κάνουμε κλικ στο OK για να ολοκληρωθεί η διαδικασία. Τώρα μπορούμε να εκτελέσουμε οποιαδήποτε εργασία που απαιτεί πιστοποιήσεις διαχειριστή όπως φαίνεται για παράδειγμα πιο κάτω το utorrent.

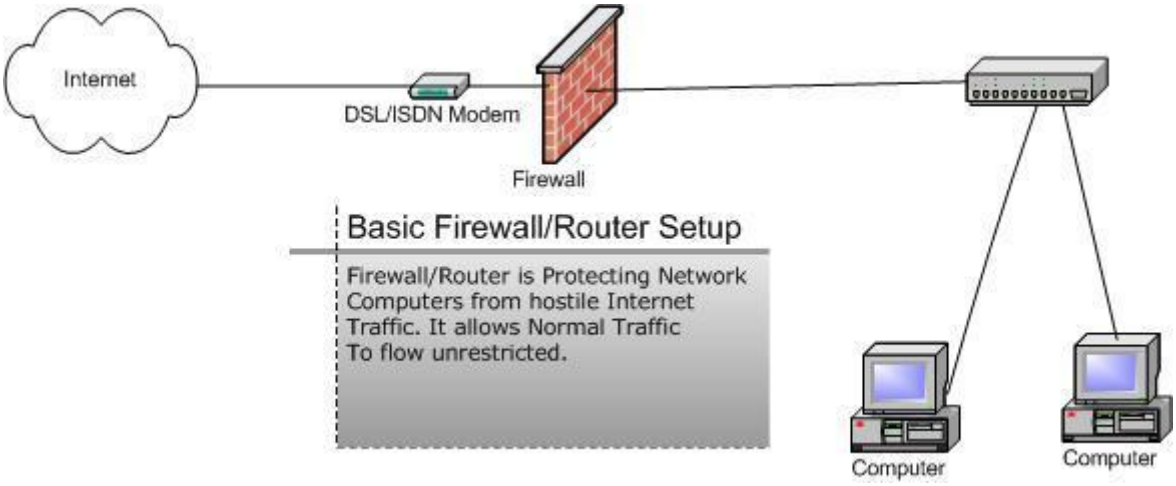


Εικόνα 74:Πιστοποίηση διαχειριστή – παράδειγμα πρόγραμμα utorrent.

Low Rights IE (LoRIE)

Σε αυτό το αντίμετρο θα δούμε πως μπορούμε να τρέχουμε σαν administrator και να έχουμε ασφαλές πρόσβαση στο internet ρίχνοντας τα περιττά διοικητικά προνόμια όταν χρησιμοποιούμε οποιοδήποτε εργαλείο για να έχουμε πρόσβαση στο internet.
http://cybercoyote.org/security/drop.shtml

6. Οι διαχειριστές μεγάλων δικτύων σε συστήματα των Windows θα πρέπει να εφαρμόσουν τις προηγούμενες τεχνολογίες σε σημεία-κλειδιά του δικτύου με σημάδια μπλοκαρίσματος (δηλ., σε firewall βασισμένα στο δίκτυο εκτός από το να βασίζονται σε ένα κύριο υπολογιστή, αντιβιοτικά σε διακομιστές αλληλογραφίας κ.λπ.) ώστε να προστατεύσουν μεγάλο αριθμό χρηστών πιο αποτελεσματικά.

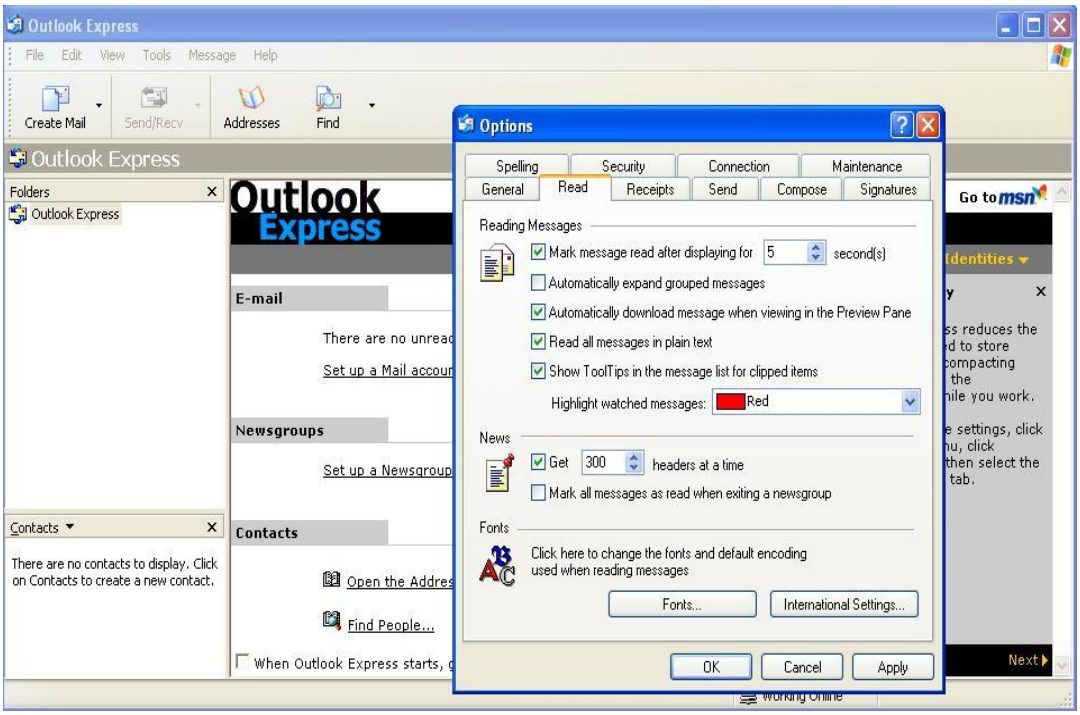


Εικόνα 75: Firewall Δικτύου.

7. Να διαβάζουμε το ηλεκτρονικό ταχυδρομείο σε απλό κείμενο.

Από την άποψη της ασφάλειας το απλό ηλεκτρονικό κείμενο είναι καλύτερη λύση. Το Plain text e-mail δεν υποστηρίζει ενσωματωμένες εικόνες, χρησιμοποιεί μόνο HTML. Η ανάγνωση e-mail σε μορφή απλού κειμένου προσφέρει σημαντικά πλεονεκτήματα ασφάλειας που υπεραντιστάθμισαν την απώλεια σε αρκετά έγχρωμες γραμματοσειρές.

Από το Tools επιλέγουμε Options,μετά από την καρτέλα Read επιλέγουμε Read all messages in plain text.



Εικόνα 76: Plaintext email-Outlook Express.

8. Να διαμορφώσουμε τα παραγωγικά προγράμματα ενός γραφείου όσο το δυνατόν με μεγαλύτερη ασφάλεια. Για παράδειγμα, να ορίσουμε τα προγράμματα του Microsoft Office να έχουν ασφάλεια μακροεντολών Very High στο |Tools |Macro|Security. Μπορούμε να χρησιμοποιήσουμε MOICE (Microsoft Office Isolated Conversion Environment – απομονωμένο περιβάλλον μετατροπής του Microsoft Office) όταν ανοίγουμε δυαδικά αρχεία προ του Office 2007 Word, Excel ή PowerPoint.

Η δυνατότητα " Περιβάλλον μεμονωμένης μετατροπής του Microsoft Office " (MOICE) που προστίθεται στο πακέτο συμβατότητας Microsoft Office για τις μορφές αρχείων Word, Excel και PowerPoint 2007 χρησιμοποιείται για να ανοίγονται με πιο ασφαλή τρόπο αρχεία δυαδικής μορφής των Word, Excel και PowerPoint.

Για να προστατεύσουμε τον υπολογιστή μας από τον κίνδυνο, γενικά να μην ανοίγουμε αρχεία που λαμβάνουμε ως συνημμένα σε μηνύματα ηλεκτρονικού ταχυδρομείου, αν τα μηνύματα αυτά φτάνουν απροσδόκητα. Επίσης, να μην ανοίγουμε αρχεία που λαμβάνουμε ως συνημμένα σε περίπτωση που τα αρχεία προέρχονται από πρόσωπο που δεν γνωρίζουμε.

Αν πρέπει να ανοίξουμε τα συνημμένα, χρησιμοποιούμε τη δυνατότητα MOICE για να μειωθεί ο κίνδυνος για την ασφάλειας. Η δυνατότητα MOICE μπορεί να βοηθήσει να μειωθεί η επίδραση των επιθέσεων που προέρχονται μέσων αρχείων δυαδική μορφής των Word, Excel, PowerPoint. Χρησιμοποιούμε τη δυνατότητα MOICE όταν υποπτευόμαστε ότι βρισκόμαστε υπό άμεση επίθεση και δεν έχουμε μια ενημέρωση λογισμικού που μπορεί να χρησιμοποιηθεί για την επίλυση της ευπάθειας.

Η δυνατότητα MOICE χρησιμοποιεί τους μετατροπής του συστήματος του Microsoft Office 2007 για να μετατρέψει τα αρχεία δυαδικής μορφής του Office σε αρχεία μορφής Open XML του Office. Αυτή η διαδικασία βοηθά στην απομάκρυνση της πιθανής απειλής που μπορεί να υπάρξει αν τα έγγραφα ανοιχτούν στη δυαδική μορφή. Επιπλέον, η δυνατότητα MOICE μετατρέπει τα εισερχόμενα αρχεία σε μεμονωμένο περιβάλλον. Αυτό βοηθά στην προστασία του υπολογιστή από πιθανή απειλή.

Σημείωση Η δυνατότητα MOICE υποστηρίζεται μόνο όταν χρησιμοποιείται μαζί με το Microsoft Office 2003 ή μαζί με την οικογένεια προγραμμάτων του Office 2007. Η δυνατότητα MOICE δεν υποστηρίζεται για καμία άλλη έκδοση του Microsoft Office.

Η δυνατότητα MOICE υποστηρίζει τις ακόλουθες μορφές εγγράφων:

- .doc
- .ppt
- .pot
- .pps
- .xls
- .xlt
- .xla

Εγκατάσταση του MOICE

Προϋποθέσεις

- Για να εγκαταστήσετε τη δυνατότητα MOICE, πρέπει να έχετε εγκατεστημένο το Office 2003 ή μια οικογένεια προγραμμάτων του Office 2007.

Για να εγκαταστήσετε τη δυνατότητα MOICE, πρέπει να έχετε το πακέτο συμβατότητας για μορφές αρχείων του Word, Excel, και του PowerPoint 2007.

9. Προσεγγίζουμε τις προκλήσεις και συναλλαγές του Internet με πολύ σκεπτικισμό. Δεν πρέπει να κάνουμε κλικ σε συνδέσεις, σε μηνύματα ηλεκτρονικού ταχυδρομείου από μη αξιόπιστες πηγές.

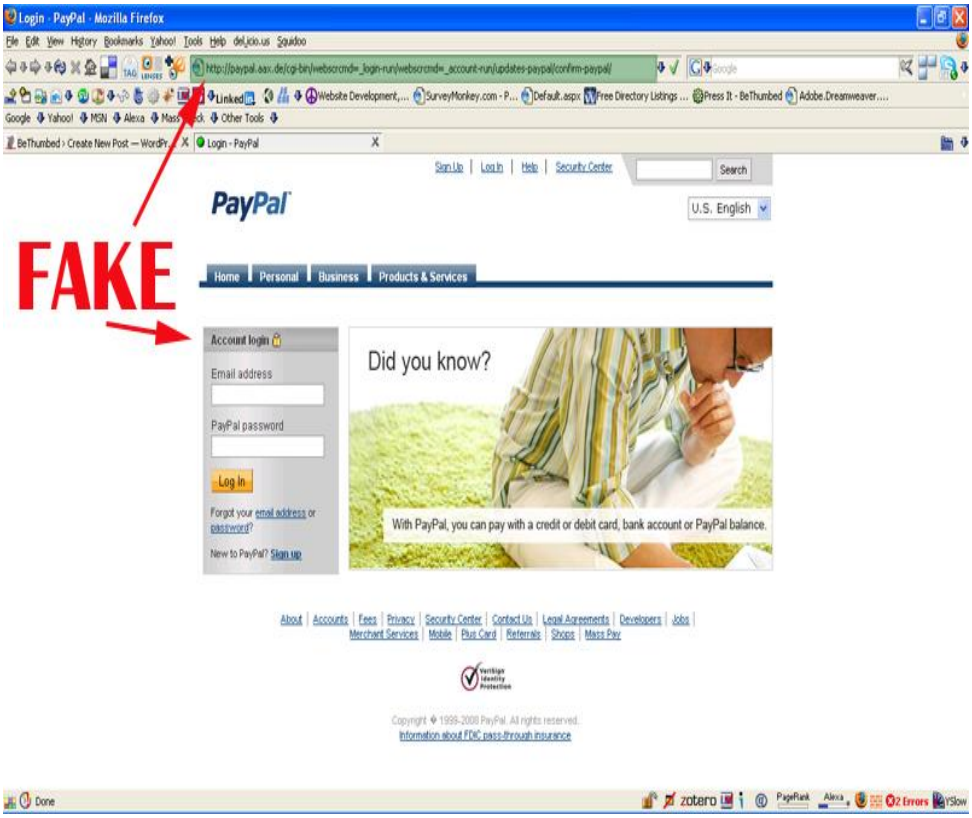
Paypal

Ένα παράδειγμα εξαπάτησης που έχει εντοπιστεί είναι η ψεύτικη χρήση της υπηρεσίας Paypal όπου κάνει online πληρωμές. Κάποιοι επιτιθέμενοι άλλαξαν το url της σελίδας σε www.paypa1.com αντί σε www.paypal.com που είναι η πραγματική σελίδα (δηλαδή αντικατέστησαν το l (L) σε 1). Οπότε αυτό δεν ήταν αντιληπτό και έτσι παραπλανούσε τον κόσμο.

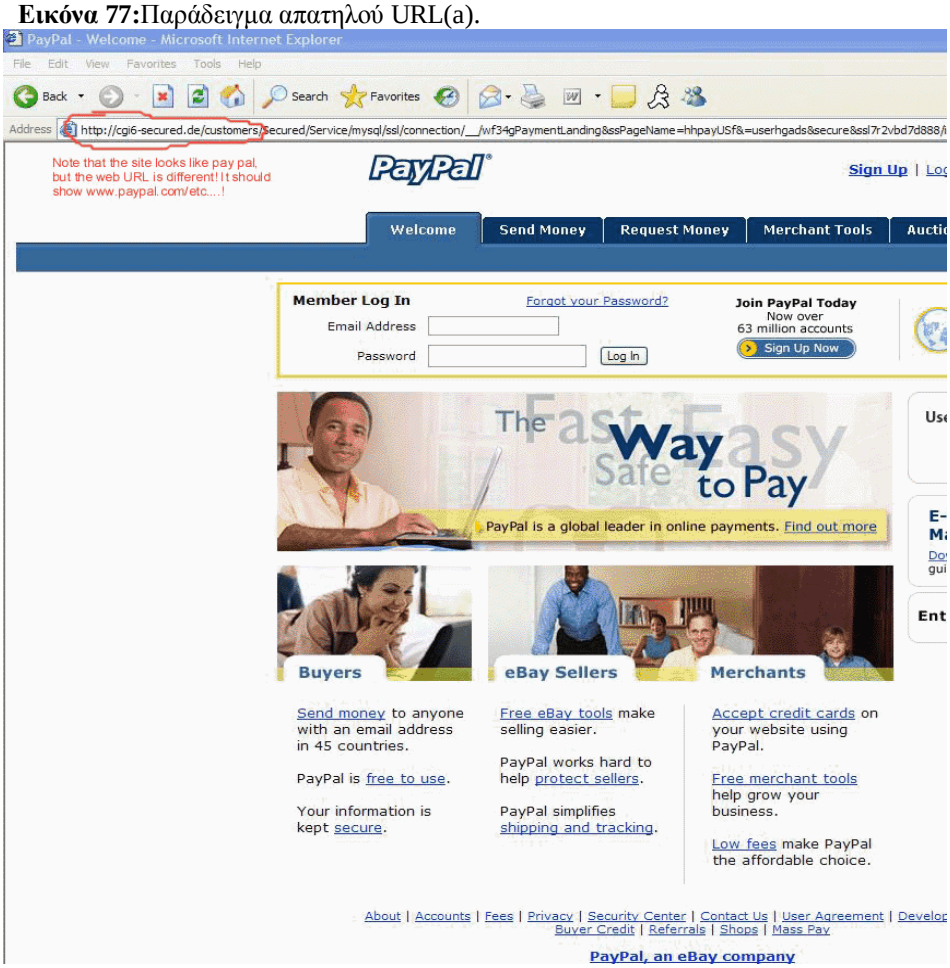
Ακόμη και αν μια διεύθυνση URL περιέχει τη λέξη "PayPal", ίσως να μην είναι το PayPal site. Άλλα παραδείγματα του απατηλού URL περιλαμβάνουν: www.paypalsecure.com , www.paypa1.com , www.secure-paypal.com , και www.paypalnet.com.

Θα πρέπει πάντα να συνδεόμαστε με το PayPal, ανοίγοντας ένα νέο web browser και πληκτρολογώντας την ακόλουθη διεύθυνση: https: / / www.paypal.com/

Δεν πρέπει ποτέ να συνδεόμαστε με το PayPal από μια σύνδεση σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου.



Εικόνα 77:Παράδειγμα απατηλού URL(a).



Εικόνα 78:Παράδειγμα απατηλού URL(b).

Εάν δούμε ένα σύμβολο @ στη μέση ενός URL, υπάρχει μια πιθανότητα αυτό να είναι απάτη. Γι αυτό και οι εταιρείες χρησιμοποιούν ένα όνομα τομέα (π.χ. https: / / www.company.com).

Έτσι θα πρέπει να είμαστε πιο προσεκτικοί όταν έχουμε να κάνουμε συναλλαγές και όταν ανταλλάζουμε σημαντικές πληροφορίες στο διαδίκτυο.

10. Να διατηρούνται οι συσκευές μας ασφαλείς με φυσικό τρόπο.

2.2.3 Εκμετάλλευση τρωτών σε προγράμματα οδήγησης συσκευών

Αν και δεν εξετάζονται συχνά με την ίδια βαρύτητα όπως η εκμετάλλευση τρωτών σημείων σε απομακρυσμένες υπηρεσίες του δικτύου , τα τρωτά σημεία σε προγράμματα οδήγησης συσκευών είναι εκτεθειμένα σε εξωτερικούς επιτιθέμενους και σε μερικές περιπτώσεις, σε μεγάλο βαθμό. Ένα εντυπωσιακό παράδειγμα δημοσιεύτηκε από τους Johnny Cache, HD Moore και εμφανίστηκε στα τέλη του 2006(δείτε το http://www.uninformed.org/?v=all&a=29&t=sumry), το οποίο επισήμαινε έξυπνα πώς τα ασύρματα προγράμματα οδήγησης για την δικτύωση των Windows θα μπορούσαμε να χρησιμοποιηθούν περνώντας απλώς κοντά από ένα σημείο του δικτύου για να εισαχθούν κακόβουλα πακέτα.

Θα πρέπει να είμαστε σαφείς ότι τα τρωτά σημεία που αναφέρθηκαν από τον Cache και άλλους προέκυψαν από προγράμματα οδήγησης τα οποία γραφτήκαν από επιχειρήσεις έξω από την Microsoft .Ωστόσο , η ανεπάρκεια του λειτουργικού συστήματος να προστατευθεί από τέτοιες επιθέσεις είναι πολύ ενοχλητική- τελικά, η Microsoft έκανε δημοφιλή τη φράση <<σύνδεση και λειτουργικά >> (plug and play) ώστε να τονίσει την πολύ ανώτερη συμβατότητα της με το μεγάλο εύρος συσκευών που είναι διαθέσιμο στους τελικούς χρήστες σήμερα. Η έρευνα του Cache δείχνει ότι το μειονέκτημα αυτής της τεράστιας συμβατότητας αυξάνει εντυπωσιακά τις επιθέσεις στο λειτουργικό σύστημα με κάθε πρόγραμμα οδήγησης που εγκαθίσταται (όπως το Ethernet , Bluetooth , DVD και τις χιλιάδες άλλες εκθέσεις σε εξωτερικούς κινδύνους).

Ίσως το χειρότερο σχετικά μ'αυτές τις επιθέσεις είναι ότι γενικά καταλήγουν να εκτελούνται μέσα στην ιδιαίτερα προνομιούχο κατάσταση πυρήνα, καθώς τα προγράμματα οδήγησης συσκευών γενικά κάπου την διασύνδεση σ 'ένα τέτοιο χαμηλό επίπεδο προκειμένου να προσπελάσουν αποτελεσματικά τα βασικά επίπεδα υλικού. Έτσι , το μόνο που χρειάζεται είναι ένα τρωτό πρόγραμμα οδήγησης συσκευής για να γίνει συνολική εισβολή στο σύστημα σας.

Ο HD Moore κωδικοποίησε μία λειτουργική μονάδα επίθεσης για το Metasploit για ασύρματα προγράμματα οδήγησης καρτών δικτύου από τρεις δημοφιλής προμηθευτές: τους Broadcom , D-Link και Netgear. Κάθε επίθεση απαιτεί τη βιβλιοθήκη Lorcon και δουλεύει μόνο στο Linux με μία υποστηριζόμενη ασύρματη κάρτα . Η λειτουργική μονάδα επίθεσης του Netgear , για παράδειγμα, στέλνει ένα ασύρματο πλαίσιο μεγάλου μεγέθους που καταλήγει σε απομακρυσμένη εκτέλεση κώδικα σε κατάσταση πυρήνα σε συστήματα που τρέχουν τις τρωτές κάρτες του Netgear. Όλες οι τρωτές κάρτες της Netgear μέσα στο εύρος της επίθεσης θα επηρεαστούν από οποιαδήποτε λαμβανόμενα πλαίσια αναγνωριστικών σημάτων , αν

και οι κάρτες θα πρέπει να είναι σε ειδική κατάσταση ώστε να δουλέψει αυτή η επίθεση.

Σκεφτείτε αυτήν την επίθεση την επόμενη φορά που θα περάσετε σε μια ζώνη με πολλά ασύρματα σημεία πρόσβασης όπως σε μια πολυπληθή, μητροπολιτική περιοχή ή ένα σημαντικό αεροδρόμιο. Οποιοδήποτε από αυτά τα <<διαθέσιμα ασύρματα δίκτυα >> θα μπορούσε να έχει ήδη ριζώσει στον υπολογιστή σας.

2.2.3.a Αντίμετρα έναντι της εκμετάλλευσης προγραμμάτων οδήγησης

Ο πιο προφανής τρόπος να μειωθεί ο κίνδυνος για επιθέσεις σε προγράμματα οδήγησης συσκευών είναι να εφαρμοστούν, το συντομότερο δυνατόν, διορθώσεις από τους προμηθευτές.

Η άλλη επιλογή είναι να απενεργοποιηθεί η επηρεαζόμενη λειτουργικότητα (συσκευή) σε περιβάλλοντα υψηλού κινδύνου. Για παράδειγμα. Στην περίπτωση επιθέσεων σε προγράμματα οδήγησης ασύρματων δικτύων που περιγράφηκαν προηγουμένως, συστήνεται να απενεργοποιήσουμε το ασύρματο ραδιόφωνο μας, ενώ περνάμε από περιοχές με μεγάλη πυκνότητα σημείων πρόσβασης. Οι περισσότεροι προμηθευτές laptop παρέχουν έναν εξωτερικό διακόπτη υλικού γι αυτό.
Φυσικά, χάνετε μέρος της λειτουργικότητας της συσκευής μ' αυτό το αντίμετρο, έτσι δεν είναι πολύ χρήσιμο εάν πρέπει να χρησιμοποιήσετε την εν λόγω συσκευή (και στην περίπτωση ασύρματης συνδετικότητας , σχεδόν πάντα θα την χρειάζεστε).

Η Microsoft έχει αναγνωρίσει αυτό το θέμα και γι αυτό παρέχει υπογραφές στα προγράμματα οδήγησης στις πιο πρόσφατες εκδόσεις των Windows. Στην πραγματικότητα, οι εκδόσεις 64-bit των Vista και του Server 2008 απαιτούν αξιόπιστες υπογραφές στο λογισμικό πυρήνα (δείτε το http://www.microsoft.com/whdc/winlogo/drvsign/drvsign.mspx). Φυσικά η υπογραφή στα προγράμματα οδήγησης υποθέτει ότι ο υπογεγραμμένος κώδικας είναι ένας σωστά κατασκευασμένος κώδικας και δεν παρέχει καμία πραγματική διαβεβαίωση ότι δεν εξακολουθούν να υπάρχουν κενά στην ασφάλεια, όπως υπερχειλίσεις buffer στον κώδικα. Έτσι, ο αντίκτυπος της υπογραφής του κώδικα σε προγράμματα οδήγησης συσκευών δεν έχει γίνει ακόμα γνωστός.

Στο μέλλον, διάφορες προσεγγίσεις, όπως το User-Mode Driver Framework (UMDF) της Microsoft, μπορεί να παρέχουν καλύτερο μετριασμό γι αυτήν την κλάση των τρωτών σημείων (δείτε). Η ιδέα πίσω από το UMDF είναι να παρέχει ένα αποκλειστικό API μέσω, του οποίου τα προγράμματα οδήγησης λιγότερων προνομίων θα μπορούν να έχουν πρόσβαση στον πυρήνα με καλά ορισμένους τρόπους. Κατά συνέπεια, ακόμα κι αν το πρόγραμμα οδήγησης έχει ένα τρωτό σημείο ασφάλειας, του οποίου μπορεί να γίνει εκμετάλλευση, ο αντίκτυπος στο σύστημα θα είναι πολύ μικρότερος από ότι στην περίπτωση ενός παραδοσιακού προγράμματος οδήγησης σε κατάσταση πυρήνα.

Κεφάλαιο 3 Επιθέσεις με πιστοποίηση

Μέχρι τώρα έχουμε επεξηγήσει τα πιο συνηθισμένα εργαλεία και τεχνικές για να επιτευχθεί κάποιο επίπεδο πρόσβασης σ' ένα σύστημα των Windows. Αυτοί οι μηχανισμοί οδηγούν γενικά σε διάφορα επίπεδα προνομίων στο σύστημα-στόχο, από Guest έως System. Ανεξάρτητα από το βαθμό των προνομίων που επιτυγχάνονται, ωστόσο, η πρώτη κατάκτηση σε οποιοδήποτε περιβάλλον των Windows είναι γενικά μόνο η αρχή μιας πολύ πιο μακροχρόνιας εκστρατείας.

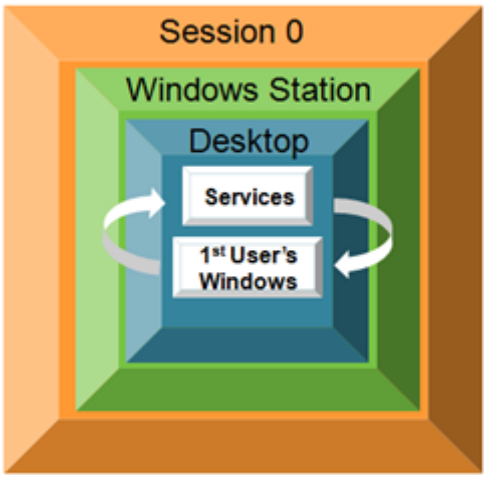
3.1 Κλιμάκωση δικαιωμάτων

Μόλις αποκτήσουν οι επιτιθέμενοι έναν λογαριασμό χρήστη σ' ένα σύστημα των Windows, θα προσπαθήσουν αμέσως να αποκτήσουν δικαιώματα Administrator ή System. Ένα από τα μεγαλύτερα κενά όλων των εποχών των Windows ήταν η οικογένεια τρωτών *getadmin*. Το getadmin ήταν η πρώτη σοβαρή επίθεση κλιμάκωσης δικαιωμάτων στα Windows NT4 και αν και αυτή η συγκεκριμένη επίθεση έχει διορθωθεί (μετά το NT4 SP3), η βασική τεχνική με την οποία δουλεύει , η εμφύτευση DLL, υπάρχει και εξακολουθεί να χρησιμοποιείται αποτελεσματικά ακόμα και σήμερα.

Η δύναμη του getadmin μετριάζεται κάπως από το γεγονός ότι πρέπει να τρέξει από έναν διαλογικό χρήστη στο σύστημα-στόχο, όπως πρέπει να γίνεται και στις περισσότερες επιθέσεις κλιμάκωσης δικαιωμάτων. Επειδή οι περισσότεροι χρήστες δεν μπορούν να συνδεθούν διαλογικά, εξ ορισμού, με έναν διακομιστή Windows, είναι χρήσιμο μόνο για να βρίσκονται μέλη των διαφόρων ενσωματωμένων ομάδων Operators (Account, Backup, Server κ.λπ) και του προεπιλεγμένου λογαριασμού του Internet Server, του IUSR_*machinename*, που έχει αυτά τα δικαιώματα. Εάν κάποια κακόβουλα άτομα έχουν ήδη διαλογικά δικαιώματα σύνδεσης στον Server σας, η κλιμάκωση της εκμετάλλευσης των δικαιωμάτων δεν πρόκειται να κάνει τα πράγματα πολύ χειρότερα. Έχουν ήδη πρόσβαση σχεδόν σε οτιδήποτε άλλο θέλουν.

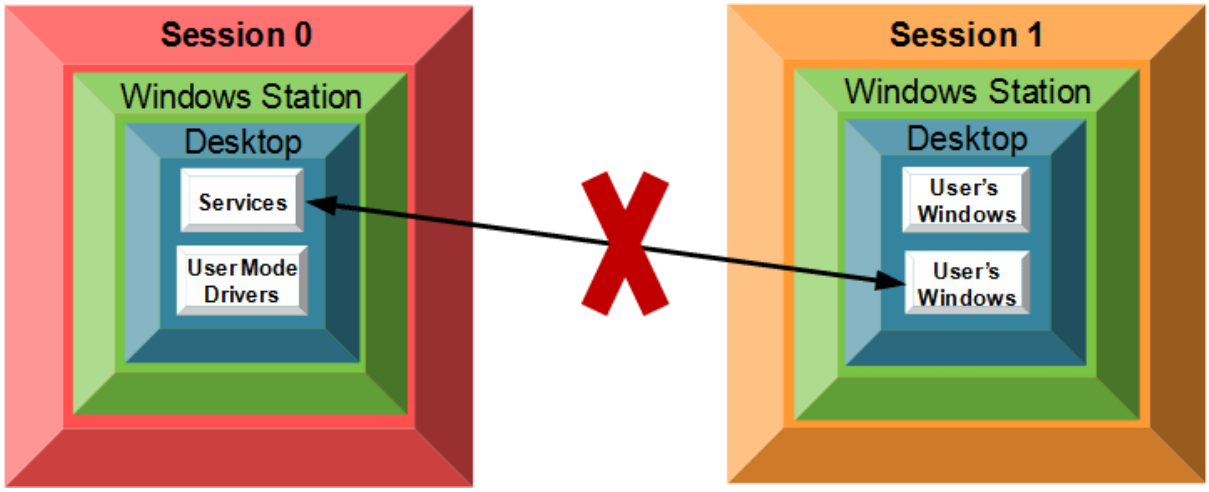
Η αρχιτεκτονική των Windows δυσκολεύεται ακόμα να αποτρέψει τους διαλογικά συνδεδεμένους λογαριασμούς από το να κάνουν κλιμάκωση των δικαιωμάτων τους, περισσότερο εξαιτίας της ποικιλομορφίας και της πολυπλοκότητας του διαλογικού περιβάλλοντος της σύνδεσης των Windows (δείτε, π.χ http://blogs.technet.com/ askperf/archive/2007/07/24/sessions-desktops-and-windows-stations.aspx).

Τα διαγράμματα που ακολουθούν παρουσιάζουν τις σχέσεις μεταξύ των sessions, των windows stations, των desktops και των υπηρεσιών των Windows Vista σε σύγκριση με τα παλαιότερα λειτουργικά συστήματα Windows XP / 2003. Στα Windows XP, Windows Server 2003, καθώς και σε παλαιότερες εκδόσεις του λειτουργικού συστήματος των Windows, όλες οι υπηρεσίες που τρέχουν στο ίδιο session όπως τον πρώτο χρήστη που συνδέεται πάνω στην κονσόλα το session αυτό ονομάζεται session 0. Τρέχει υπηρεσίες και εφαρμογές χρηστών με session 0 και ενέχουν κίνδυνο ασφαλείας, επειδή οι υπηρεσίες που λειτουργούν σε υψηλά προνόμια είναι συνεπώς οι στόχοι για τους κακόβουλους παράγοντες οι οποίοι αναζητούν ένα μέσο για να ανυψώσει το δικό τους επίπεδο προνομίου.



Εικόνα 79: Sessions in Windows XP / 2003

Το λειτουργικό σύστημα Microsoft Windows Vista μετριάζει αυτόν τον κίνδυνο ασφαλείας, απομονώνοντας τις υπηρεσίες στο session 0 και κάνοντας το session 0 μη διαδραστικό. Στα Windows Vista , μόνο διεργασίες του συστήματος και των υπηρεσιών τρέχουν σε session 0. Ο χρήστης συνδέεται στο session 1. Με το Windows Server, μετέπειτα οι χρήστες μπορούν να συνδεθούν στα επόμενα sessions (session 2,session 3 κλπ). Αυτό σημαίνει ότι οι υπηρεσίες που δεν λειτουργούν στο ίδιο session όπως χρήστες εφαρμογής προστατεύονται από επιθέσεις που προέρχονται από την εφαρμογή κώδικα.



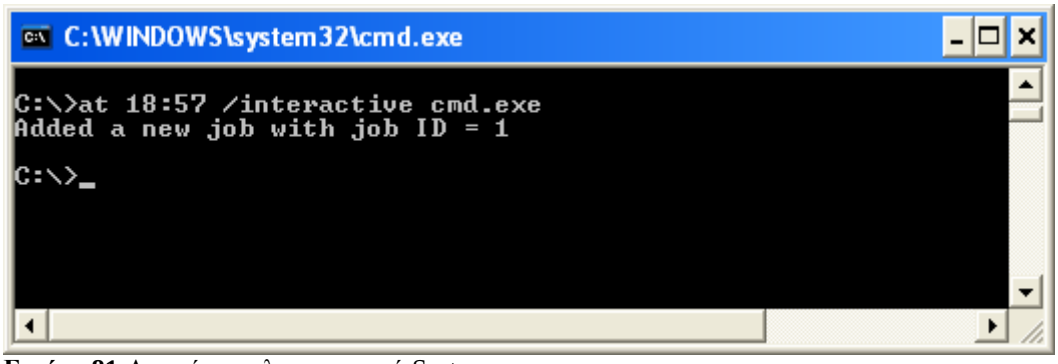
Εικόνα 80: Sessions in Windows Vista

Ακόμα χειρότερα, η διαλογική σύνδεση έχει διαδοθεί περισσότερο, καθώς το Windows Terminal Server παρέχει απομακρυσμένη διαχείριση και κάνει κατανεμημένη επεξεργασία. Τέλος, είναι σημαντικό να λάβουμε υπόψη ότι ο πιο σημαντικός παράγοντας για κλιμάκωση των δικαιωμάτων σε συστήματα πελάτη του Internet είναι η περιήγηση στο Web και η επεξεργασία ηλεκτρονικού ταχυδρομείου.

Τέλος, θα πρέπει να σημειώσουμε ότι η απόκτηση δικαιωμάτων Administrator δεν είναι τεχνικά τα υψηλοτέρα δικαιώματα που μπορεί να αποκτήσει κάποιος σε ένα υπολογιστή Windows. Ο λογαριασμός SYSTEM (επίσης γνωστός ως Local System,

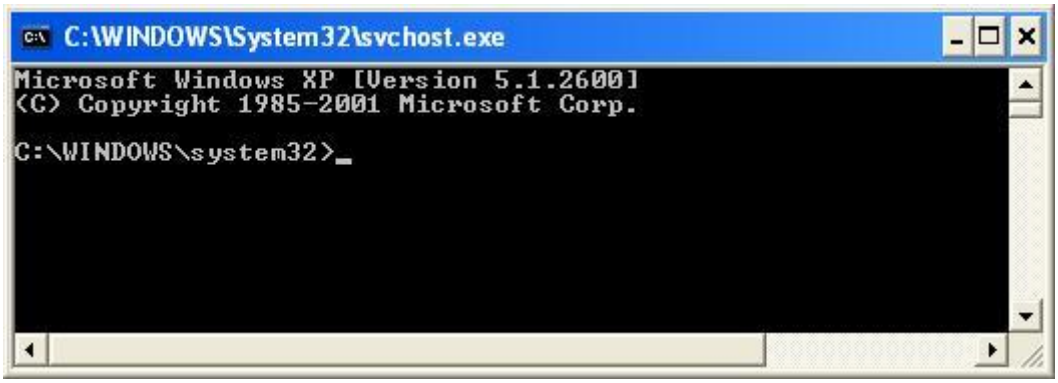
ή ως λογαριασμός NT/AUTHORITY/SYSTEM) στην πραγματικότητα έχει περισσότερα δικαιώματα από τον Administrator. Ωστόσο, υπάρχουν μερικά κοινά τεχνάσματα που επιτρέπουν σε διαχειριστές να αποκτήσουν αρκετά εύκολα δικαιώματα SYSTEM. Ο ένας τρόπος είναι να ανοίξετε ένα κέλυφος εντολών που να χρησιμοποιεί την υπηρεσία Windows Scheduler ως εξής :

```
C:\>at 18:57  /INTERACTIVE cmd.exe
```



Εικόνα 81:Δικαιώματα λογαριασμού System

Αφού ολοκληρωθεί η πιο πάνω διαδικασία τότε αποκτούμε δικαιώματα SYSTEM εξ αποστάσεως.



Εικόνα 82:Σύνδεση εξ αποστάσεως με δικαιώματα System

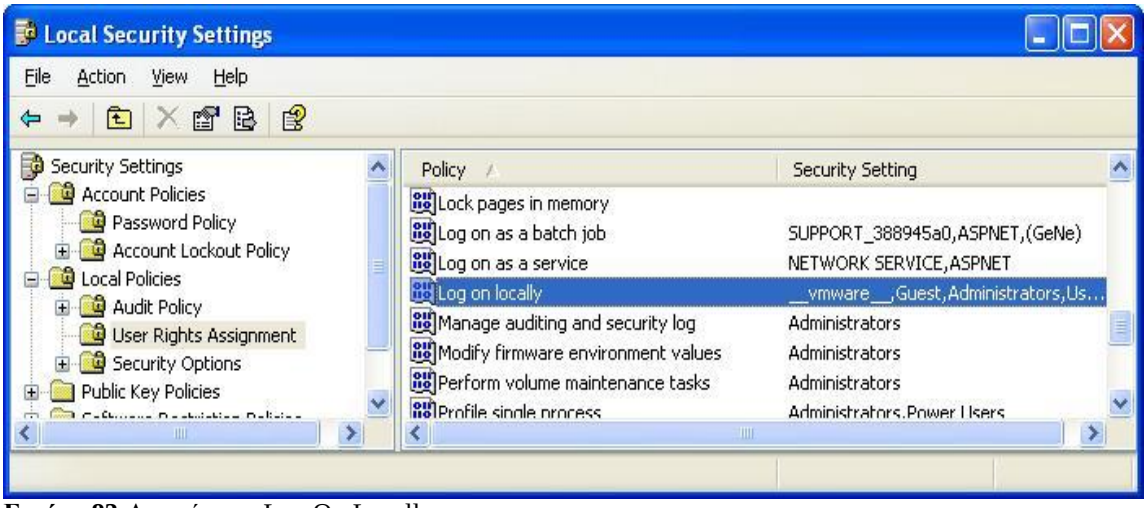
Ή θα μπορούσαμε να χρησιμοποιήσουμε το δωρεάν εργαλείο psexec από το Sysinternals.com, το οποίο θα επιτρέψει ακόμη και σε μας να συνδεθούμε με δικαιώματα SYSTEM εξ αποστάσεως.

3.1.1 Αποτροπή της κλιμάκωσης των δικαιωμάτων

Καταρχήν, εγκαθιστούμε τις διορθώσεις (patch) στα συστήματα των Windows. Οι διάφορες επιθέσεις με τρωτά, όπως το getadmin εκμεταλλεύονται κενά του πυρήνα του λειτουργικού συστήματος και δεν μπορούν να μετριαστούν εντελώς έως ότου διορθωθούν αυτά τα κενά σε επίπεδο κώδικα.

Φυσικά, τα διαλογικά προνόμια σύνδεσης θα πρέπει να περιοριστούν σοβαρά σε οποιοδήποτε σύστημα περιέχει εμπιστευτικά δεδομένα, επειδή η εκμετάλλευση διαφόρων τρωτών όπως αυτών γίνεται πολύ ευκολότερα μόλις γίνει αυτό το κρίσιμο βήμα. Για να ελέγχουμε τα διαλογικά δικαιώματα σύνδεσης στα Windows 2000 και νεότερα, τρέχουμε το βοηθητικό πρόγραμμα Security Policy (είτε το Local είτε το

Group), βρίσκουμε τον κόμβο Local Policies\User Rights Assignment και ελέγχουμε πως έχουν συμπληρωθεί τα δικαιώματα Log On Locally (τοπική σύνδεση).

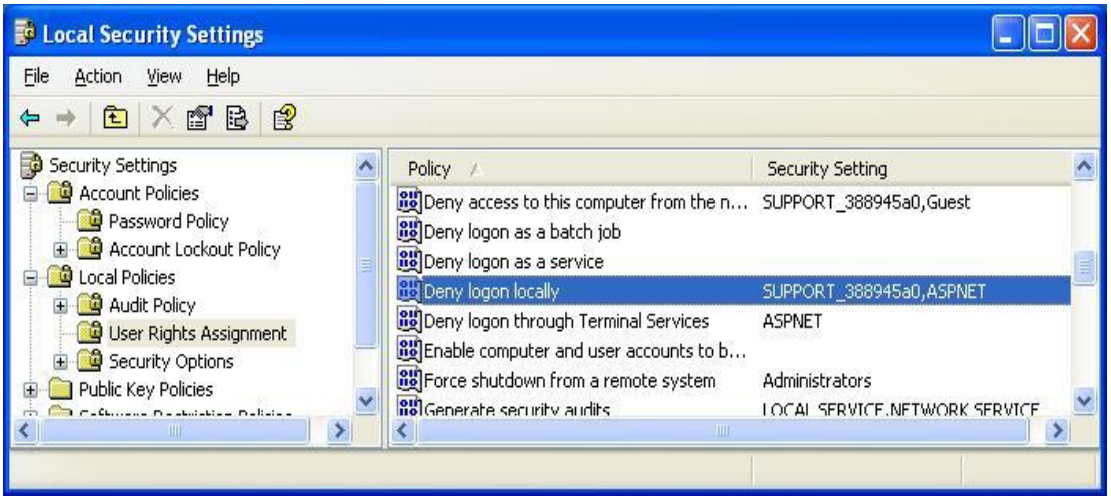


Εικόνα 83:Δικαιώματα Log On Locally.

Πιο κάτω βλέπουμε ποιοι μπορούν να έχουν δικαιώματα Log On Locally (τοπικής σύνδεσης).

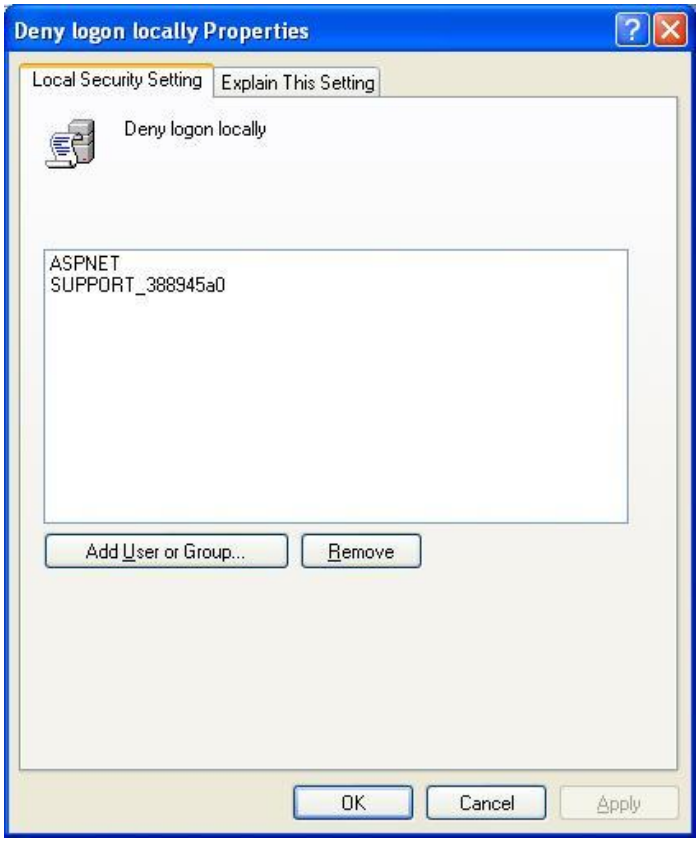
Εικόνα 84:Δικαιούχοι - Log On Locally.

Νέα λειτουργία στα Windows 2000 και νεότερα, είναι ότι πολλά τέτοια προνόμια έχουν τώρα αντίστοιχες ιδιότητες που επιτρέπουν σε συγκεκριμένες ομάδες ή χρήστες να αποκλείονται από δικαιώματα. Σ' αυτό το παράδειγμα θα μπορούσαμε να χρησιμοποιήσουμε το δικαίωμα Deny Logon Locally (αποκλεισμός τοπικής σύνδεσης), όπως βλέπουμε εδώ :



Εικόνα 85: Deny Logon Locally.

Εδώ βλέπουμε ομάδες ή χρήστες που αποκλείονται από τα δικαιώματα τοπικής σύνδεσης.



Εικόνα 86:Δεν έχουν πρόσβαση σε δικαιώματα.

3.2 Εξαγωγή και διάρρηξη κωδικών πρόσβασης

Μόλις αποκτηθούν δικαιώματα ισοδύναμα μ' αυτά του διαχειριστή, οι επιτιθέμενοι αρχίζουν γενικά να ενδιαφέρονται πώς να αποκτήσουν όσο το δυνατόν περισσότερες πληροφορίες τις οποίες θα μπορούν να χρησιμοποιηθούν για ακόμα περισσότερες εισβολές σε συστήματα. Επιπλέον, οι επιτιθέμενοι με δικαιώματα ισοδύναμα μ' αυτά του διαχειριστή μπορούν να παίξουν ένα δευτερεύοντα μόνο ρόλο στην δομή του δικτύου σας και ίσως να θελήσουν να εγκαταστήσουν πρόσθετα εργαλεία για να κατοχυρώσουν την επιρροή τους. Κατά συνέπεια, μία από τις πρώτες δραστηριότητες μετά την εισβολή των επιτιθέμενων είναι να μαζέψουν όσο γίνεται περισσότεροι ονόματα χρηστών και κωδικούς πρόσβασης, καθώς αυτά τα πιστοποιητικά είναι γενικά το κλειδί στην επέκταση της εισβολής σε ολόκληρο το περιβάλλον και πιθανώς και σε άλλα περιβάλλοντα που είναι συνδεδεμένα μέσω αντίστοιχων σχέσεων.

3.2.1 Διάρρηξη Κρυπτογραφημένων Κωδικών Πρόσβασης

Αφού αποκτήσουμε δικαιώματα Administrator , η επόμενη μας κίνηση είναι να κάνουμε άμεση επίθεση στους κρυπτογραφημένους κωδικούς πρόσβασης του συστήματος. Αυτοί είναι αποθηκευμένοι στο Windows Security Account Manager (SAM) στα NT4 και προγενέστερα και στους ελεγκτές τομέων (domain controllers-DC) του Active Directory των Windows 2000 και νεότερων. Τα windows αποθηκεύουν τους κωδικούς των χρηστών (πχ administrator , userX , guest) σε ένα αρχείο που καλείται sam file (Security Accounts Manager). Το εν λόγω αρχείο βρίσκεται στους φακέλους του συστήματος των windows και δεν μπορεί να διαβαστεί παρά μόνο με την χρήση κάποιων cracking tools. Επίσης δεν μπορεί να αντιγραφεί ή να αποκοπεί όση ώρα λειτουργούν τα Windows, ούτε από τον Adminstrator. Το SAM περιέχει τα ονόματα χρηστών και τους κρυπτογραφημένους κωδικούς πρόσβασης όλων των χρηστών στο τοπικό σύστημα , ή στον τομέα , εάν ό εν λόγω υπολογιστής είναι ελεγκτής τομέα .

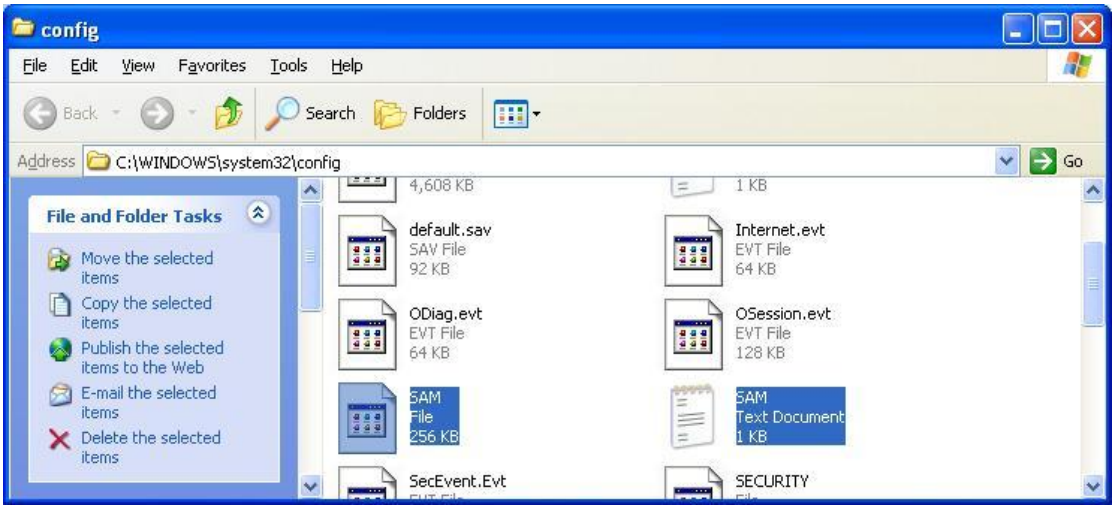
Για να διαβάσει κάποιος τα παραπάνω αρχείο, πρέπει με κάποιο τρόπο να αποκτήσει πρόσβαση στον δίσκο. Ο καλύτερος τρόπος για να γίνει αυτό είναι πχ να χρησιμοποιηθεί κάποια δισκέτα η CD που κάνει απευθείας εκκίνηση τον Η/Υ (bootable) παρακάμπτοντας τελείως το φάκελο εκκίνησης των Windows.

Αυτή είναι η απόλυτη εισβολή σε συστήματα των Windows , το αντίστοιχο του αρχείου /etc/passwd για τα UNIX. Ακόμα κι αν το εν λόγω SAM προέρχεται από ένα αυτόνομο σύστημα των Windows , οι πιθανότητες είναι ότι ή διάρρηξη θα αποκαλύψει πιστοποιητικά που παρέχουν πρόσβαση σένα ελεγκτή τομέα , χάρις την ευρεία επαναχρησιμοποίηση κωδικών πρόσβασης από τους τυπικούς χρήστες. Κατά συνέπεια , η διάρρηξη του SAM αποτελεί επίσης ένα από τα πιο δυνατά εργαλεία για κλιμάκωση των προνομίων και εκμετάλλευση του.

Απόκτηση των Κρυπτογραφημάτων

Το πρώτο βήμα σε οποιαδήποτε διάρρηξη κωδικών πρόσβασης είναι να πάρει κάποιος τα κρυπτογραφήματα(hash) των κωδικών πρόσβασης. Ανάλογα με την έκδοση των Windows , αυτό μπορεί να επιτευχθεί με διάφορους τρόπους.

Σε αυτόνομα συστήματα των Windows ,οι κρυπτογραφημένοι κωδικοί πρόσβασης αποθηκεύονται στο %systemroot%\system32\config\SAM .



Εικόνα 87:Κρυπτογραφημένοι κωδικοί πρόσβασης – SAM

Το SAM είναι κλειδωμένο εφόσον τρέχει το λειτουργικό σύστημα.

Εικόνα 88:Αδύνατη πρόσβαση στο αρχείο SAM.

Το αρχείο SAM αντιπροσωπεύω επίσης σε μία από τις πέντε σημαντικές κυψέλες του Windows Registry κάτω από το κλειδί HKEY_LOCAL_MACHINE\SAM. Αυτό το κλειδί δεν είναι διαθέσιμο για περιστασιακή εξέταση ,ακόμη και από τον λογαριασμό του Administrator (ωστόσο, με λίγη πονηρία και την υπηρεσία Scheduler , μπορεί να γίνει αυτό). Σε ελεγκτές τομέων , οι κρυπτογραφημένοι κωδικοί πρόσβασης διατηρούνται στο Active Directory(%windir%WindowsDS\ntds.dit). Τώρα που ξέρουμε που αποθηκεύονται τα χρήσιμα πράγματα, πως θα αποκτήσουμε; Υπάρχει διάφοροι τρόποι, αλλά ο ευκολότερος είναι να εξάγουμε τους κρυπτογραφημένους κωδικούς πρόσβασης προγραμματιστικά από το SAM ή το Active Directory χρησιμοποιώντας διάφορα διαθέσιμα εργαλεία.

Εξαγωγή των κρυπτογραφημάτων με το pwdump

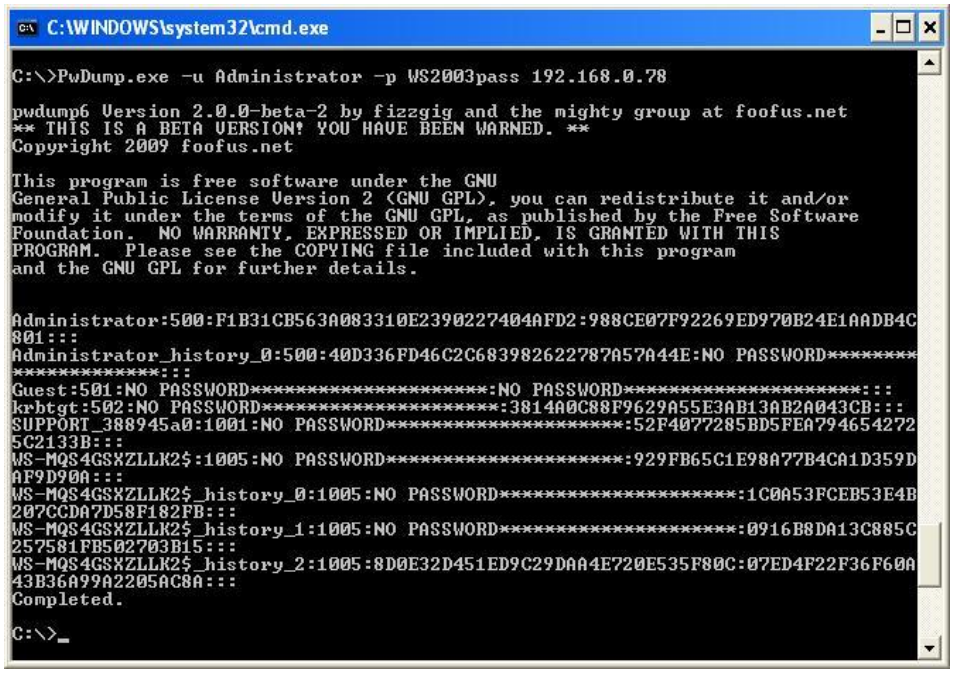
Με πρόσβαση επιπέδου Administrator, οι κρυπτογραφημένοι κωδικοί πρόσβασης μπορούν εύκολα να εμφανιστούν κατευθείαν από το Registry σε μία δομημένη μορφή που είναι κατάλληλη για ανάλυση εκτός σύνδεσης. Το πρωτότυπο βοηθητικό πρόγραμμα για να επιτευχθεί αυτό ονομάζεται pwdump από τον Jeremy Allison και έχουν κυκλοφορήσει πολλές βελτιωμένες εκδόσεις του , συμπεριλαμβανόμενου του pedump2 από τον Todd Sabin ,το pwdump3 από την e-business technology και το pedump6 από την foofus.net Team (www.foofus.net).

Η foofus.net εμφάνισε επίσης το fgdump , το οποίο περιλαμβάνει το pwdump6 όπως και άλλα εργαλεία που αυτοματοποιούν την αποκρυπτογραφημένη εξαγωγή hash την εμφάνιση της LSA cache και την απαρίθμηση προστατεμένων δεδομένων (θα συζητήσουμε τις τελευταίες δυο τεχνικές σύντομα). Η οικογένεια των εργαλείων pwdump χρησιμοποιεί την τεχνική της <<εμφύτευσης>> στο DLL ώστε να μπει στο σύστημα σαν μία προνομιούχος διαδικασία (γενικά lsass.exe) προκειμένου να εξάγει κρυπτογραφημένους κωδικούς πρόσβασης.

Το pwdump6 εργάζεται από μακριά μέσο SMB (TCP 139 ή 445) αλλά δεν θα δουλέψει μέσα σε μια διαλογική σύνοδο σύνδεσης (μπορείτε ακόμα να χρησιμοποιήσετε το fgdump για διαλογική εμφάνιση κωδικών πρόσβασης). Στο παρακάτω παράδειγμα παρουσιάζουμε το pwdump6 ενώ χρησιμοποιείτε ένα σύστημα Server 2003 με απενεργοποιημένο το Windows Firewall:

```
D:\Toolbox>PwDump.exe -u Administrator -p password IP
```

Τα περιεχόμενα του sam, σε περίπτωση που μπορεί να έχει κάποιος πρόσβαση σε αυτά θα είναι κάπως έτσι.



Εικόνα 89:Εξαγωγή κρυπτογραφημένων κωδικων πρόσβασης με την χρήση Pwdump.

Αυτό μας δείχνει ότι το αρχείο μπορεί να περιέχει τους κωδικούς των accounts αλλά να είναι όλοι κωδικοποιημένοι και έτσι ακόμα και σε περίπτωση που ανοιχτεί δεν μπορεί να γίνει κατανοητό το περιεχόμενό του χωρίς την χρήση κάποιου cracking tool.

Παρατηρούμε στην έξοδο NO PASSWORD στο τρίτο πεδίο που υποδεικνύει ότι αυτός ο διακομιστής δεν αποθηκεύει κρυπτογραφήματα στην πιο αδύνατη μορφή LM.

3.2.1.a Αντίμετρα για το pwdump

Εφόσον εξακολουθεί να δουλεύει ακόμα η <<εμφύτευση>> DLL στα Windows , δεν υπάρχει καμία άμυνα σε παράγωγα του pwdump. Παρηγορηθείτε ωστόσο γιατί το pwdump απαιτεί προνόμια ισοδύναμα με του διαχειριστή. Εάν οι επιτιθέμενοι έχουν ήδη αυτό το πλεονέκτημα , πιθανών να υπάρχουν ελάχιστα προγράμματα που να μπορούν να επιτύχουν στο τοπικό σύστημα που δεν έχουν ήδη (ωστόσο όπως θα δούμε σύντομα αποτελεί άλλο θέμα η χρησιμοποίηση κρυπτογραφημένων κωδικών πρόσβασης για επίθεση σε αξιόπιστα συστήματα.

3.2.2 Διάρρηξη κωδικών πρόσβασης

Η διαδικασία παραγωγής κωδικών πρόσβασης σε καθαρό κείμενο από κρυπτογραφημένους κωδικούς πρόσβασης αναφέρεται γενικά ως διάρρηξη κωδικών πρόσβασης ή απλός διάρρηξη (cracking). Η διάρρηξη κωδικών πρόσβασης είναι ένα γρήγορο , περίπλοκο μάντεμα κωδικών πρόσβασης εκτός σύνδεσης . Μόλις γίνει γνωστός ο αλγόριθμος κρυπτογράφησης (hashing) ,μπορεί να χρησιμοποιηθεί για να υπολογισθεί το hash για μία λίστα από πιθανές τιμές κωδικών πρόσβασης (ας πούμε , οι λέξεις του αγγλικού λεξικού) και να συγκριθούν τα αποτελέσματα με έναν κρυπτογραφημένο κωδικό πρόσβασης που έχει ανακτηθεί χρησιμοποιώντας ένα εργαλείο όπως το pwdump. Εάν βρεθεί αντιστοιχία, ο κωδικός πρόσβασης έχει μαντευθεί σωστά ή << έχει γίνει διάρρηξη του>>. Αυτή η διαδικασία εκτελείται συνήθως εκτός σύνδεσης σε κλεμμένους κρυπτογραφημένους κωδικούς πρόσβασης έτσι ώστε να μην γίνει κλείδωμα ενός λογαριασμού και το μάντεμα να μπορεί να συνεχιστεί επ' αόριστο.

Από πρακτική σκοπιά , η διάρρηξη κωδικών πρόσβασης γίνεται με βάσει ότι έχουν χρησιμοποιηθεί αδύνατοι αλγόριθμοι κρυπτογράφησης (εάν υπάρχουν διαθέσιμοι) , έξυπνες εικασίες , εργαλεία και φυσικά , χρόνος επεξεργασίας, Ας συζητήσουμε καθένα από αυτά με την σειρά.

Αδύνατοι Αλγόριθμοι Κρυπτογράφησης

Όπως έχουμε συζητήσει , ο αλγόριθμος κρυπτογράφησης του LanManager (ή LM) έχει γνωστά τρωτά σημεία που επιτρέπουν να γίνει διάρρηξη πολύ πιο γρήγορα ο κωδικός πρόσβασης χωρίζεται σε δυο μέρη των 7 χαρακτήρων και όλα τα γράμματα αλλάζουν σε κεφαλαία ,μειώνοντας αποτελεσματικά τους 2^{84} πιθανούς αλφαριθμητικούς κωδικούς πρόσβασης που υπάρχουν με τους κωδικούς πρόσβασης , τα περισσότερα κρυπτογραφημένα LM μπορούν να διαρρηχτούν σε δευτερόλεπτα ,ανεξάρτητα από τν πολυπλοκότητα των κωδικών πρόσβασης. Η Microsoft άρχισε να

απαλείφει τη χρήση κρυπτογραφημένων αλγορίθμων LM σε πρόσφατες εκδόσεις των Windows ώστε να μετριάσει αυτές τις αδυναμίες.

Το νεότερο NTLM hash δεν έχει αυτές τις αδυναμίες και έτσι απαιτεί πολύ μεγαλύτερη προσπάθεια για να σπάσει . Εάν ακολουθηθούν καλές πρακτικές επιλογής κωδικών πρόσβασης (δηλ. να υπάρχει ένα κατάλληλο ελάχιστο μήκος στους κωδικούς πρόσβασης και να επιβληθεί η προεπιλεγμένη πολιτική πολυπλοκότητας κωδικών πρόσβασης που υπάρχει εξ ορισμού στα Windows Vista και νεότερα), οι κρυπτογραφημένοι κωδικοί πρόσβασης NTML θα είναι αδύνατον να σπάσουν με τεχνικές brute force που χρησιμοποιούν τις τρέχουσες δυνατότητες επεξεργασίας.

Όλα τα hash των Windows πάσχουν από μία πρόσθετη αδυναμία : δεν έχει 'salt'. Τα περσότερα άλλα λειτουργικά συστήματα προσθέτουν μία τυχαία τιμή που ονομάζεται salt (αλάτι) σε ένα κωδικό πρόσβασης πριν τον κατακερματίσουν και τον αποθηκεύσουν. Το salt αποθηκεύεται μαζί με το hash, έτσι ώστε να μπορεί αργότερα να ελεγχτεί ένας κωδικός πρόσβασης σε σχέση με το hash. Αυτό δεν μοιάζει να επηρεάζει έναν πολύ προικισμένο επειδή θα μπορούσε απλώς να εξάγει τα salt μαζί με τα hash,όπως δείξαμε νωρίτερα χρησιμοποιώντας εργαλεία όπως το pwdump. Ωστόσο, το salt μετριάζει έναν άλλο τύπο επίθεσης: επειδή κάθε σύστημα δημιουργεί ένα τυχαίο salt για κάθε κωδικό πρόσβασης, είναι αδύνατον να προϋπολογίσετε πίνακες κρυπτογράφησης που να επιταχύνουν την διάρρηξης. Θα συζητήσουμε τις επιθέσεις σε προϋπολογισμένους πίνακες κρυπτογράφησης όπως τους πίνακες Rainbow που θα δούμε αργότερα σ'αυτή την ενότητα. Η Microsoft έχει επιλέξει ιστορικά να αυξήσει τη δύναμη του αλγορίθμου κρυπτογράφησης των κωδικών πρόσβασης της αντί να χρησιμοποιήσει salt, πιθανόν με βάση την υπόθεση ότι δεν είναι πρακτική η δημιουργία προϋπολογισμένων πινάκων προκειμένου να παραχθεί ένα δυνατότερο αλγόριθμο.

Έξυπνες Εικασίες

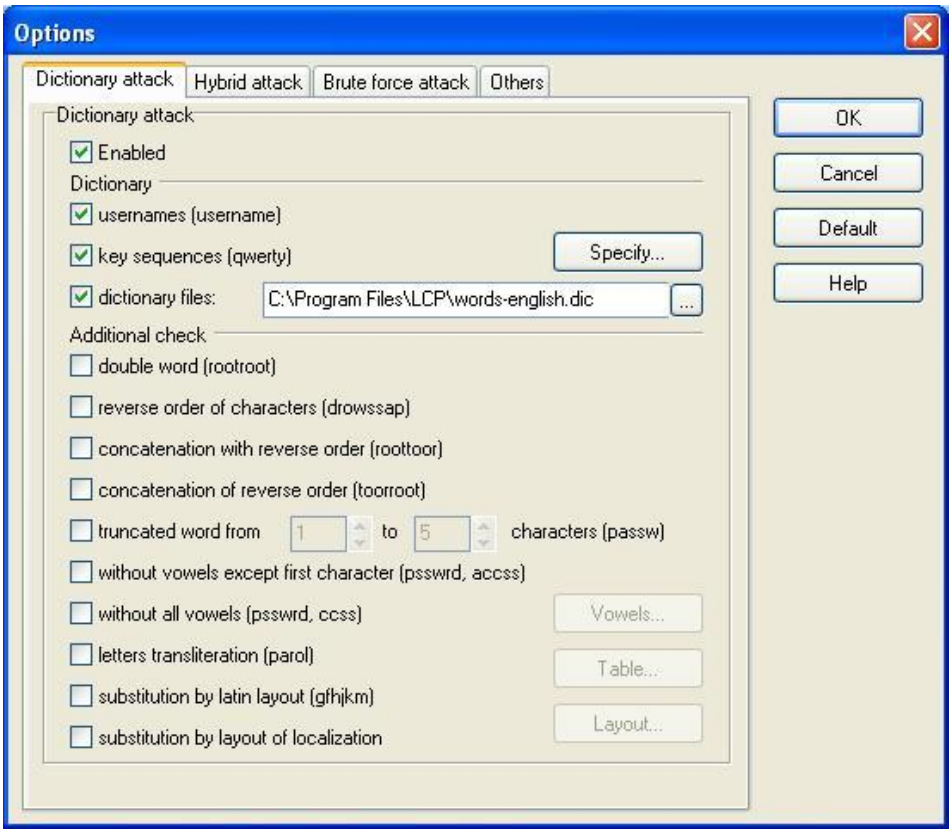
Παραδοσιακά υπάρχουν δύο τρόποι να παρέχετε στοιχεία στην διάρρηξη κωδικών πρόσβασης : με λεξικό ή με μέθοδο brute force. Πρόσφατα, οι προϋπολογισμένοι πίνακες διάρρηξης έχουν γίνει δημοφιλείς γιατί επιταχύνουν το ρυθμό την αποτελεσματικότητα της διάρρηξης.

Η διάρρηξη με λεξικό είναι η πιο απλή προσέγγιση διάρρηξης. Παίρνει μία λίστα με όρους και τους κατακερματίζει ένα-ένα, συγκρίνοντας τους με την λίστα των κλεμμένων κρυπτογραφημάτων καθώς προχωρά. Προφανώς αυτή η προσέγγιση περιορίζεται στο να βρίσκει μόνο αυτούς τους κωδικούς πρόσβασης που περιλαμβάνονται στο λεξικό που παρέχεται από τον επιτιθέμενο. Αντίστροφα θα προσδιορίσει γρήγορα οποιονδήποτε κωδικό πρόσβασης του λεξικού ανεξάρτητα από το πόσο δυνατός είναι ο αλγόριθμος κρυπτογράφησης (ναι, ακόμα και τα NTLM hash).

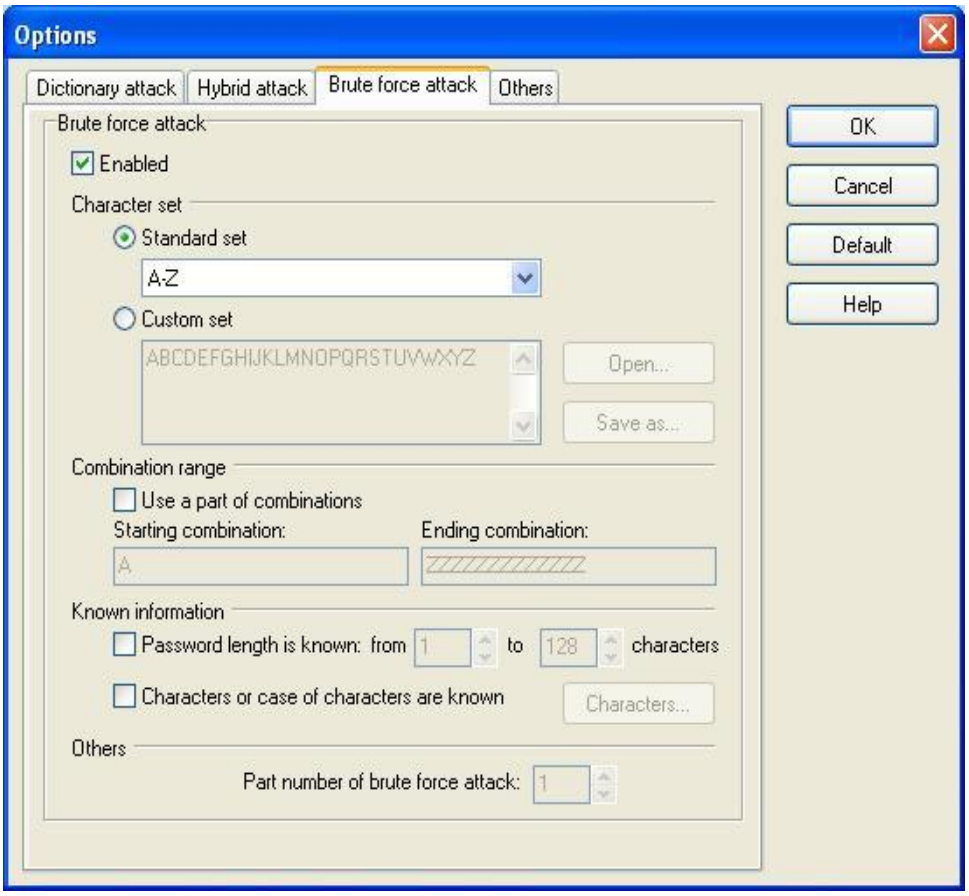
Η διάρρηξη brute force υποθέτει ότι παράγονται τυχαίες συμβολοσειρές από το επιθυμητό σύνολο χαρακτήρων και μπορεί να πρόσθεση πολύ χρόνο στην προσπάθεια διάρρηξης λόγω της μεγάλης προσπάθειας που απαιτείται για να κατακερματιστούν όλες οι πιθανές τυχαίες τιμές μέσα στον συγκεκριμένο χώρο χαρακτήρων(π.χ υπάρχουν 26 πιθανές αγγλικές αλφαβητικές συμβολοσειρές σε

κεφαλαίο των 7 ή λιγότερων χαρακτήρων, δηλ. θα πρέπει να δημιουργηθούν πάνω από 8 δισεκατομμύρια hash) .

Μία καλή μέση κατάσταση μεταξύ της διάρρηξης με brute force και με λεξικό είναι αν προσαρτηθούν γράμματα και αριθμοί σε λέξεις του λεξικού, μία συνηθισμένη τεχνική επιλογής κωδικών πρόσβασης από τους οκνηρούς χρήστες που επιλέγουν κωδικούς πρόσβασης όπως το 'password123' ελλείψει ενός πιο καλού συνδυασμού. Το δημοφιλές αλλά μη υποστηριζόμενο πλέον εργαλείο διάρρηξης L0phtcrack πρόσφερε μία υβριδική επιλογή διάρρηξης με λεξικό/brute force όπως αυτό. Τα νεότερα εργαλεία διάρρηξης κωδικών πρόσβασης εφαρμόζουν βελτιωμένες 'έξυπνες' τεχνικές μαντέματος, όπως αυτές παρουσιάζονται στην εικόνα πιο κάτω του εργαλείου διάρρηξης LCP.



Εικόνα 90:LCP Options – Dictionary Attack



Εικόνα 91:LCP Options – Brute Force Attack

Πρόσφατα, η διάρρηξη έχει εξελιχθεί και χρησιμοποιεί προϋπολογισμένους πίνακες κρυπτογράφησης ώστε να μειωθεί κατά πολύ ο χρόνος που είναι απαραίτητος για να παραχθούν hash για λόγους σύγκρισης . Το 2003 ο Philippe Oechslin δημοσίευσε ένα έγγραφο(μια βελτιωμένη εργασία από το 1980 από τον Hellman και βελτιώθηκε από τον θρυλικό κρυπτογράφο Rivest 1982) που περιέγραφε μία κρυπταναλυτική τεχνική ανταλλαγής χρόνου/μνήμη που του επέτρεπε να σπάσει 99,9% από τους αλφαριθμητικούς κρυπτογραφημένους κωδικούς πρόσβασης LanManager(2^{37}) σε 13,6 δευτερόλεπτα. Στην ουσία , το πρόβλημα είναι να γίνει εκ των προτέρων όλη η προσπάθεια της διάρρηξης σε προϋπολογισμένους πίνακες κρυπτογράφησης, επονομαζόμενους <<ουράνιο τόξο>>(rainbow) χρησιμοποιώντας μεθόδους λεξικού και brute force. Για μία πολύ καλύτερη εξήγηση από τον εφευρέτη του ίδιου του μηχανισμού πινάκων rainbow, δείτε την διεύθυνση www.isc2.org/cgi-bin/content.cgi?page=738).

Το ProjectRainbow Crack ήταν ένα από τα πρώτα εργαλεία μιας τέτοιας προσέγγισης (δείτε την διεύθυνση http://project-rainbowcrack.com/) και πολλά νεότερα εργαλεία διάρρηξης υποστηρίζουν προϋπολογισμένους πίνακες κρυπτογράφησης .

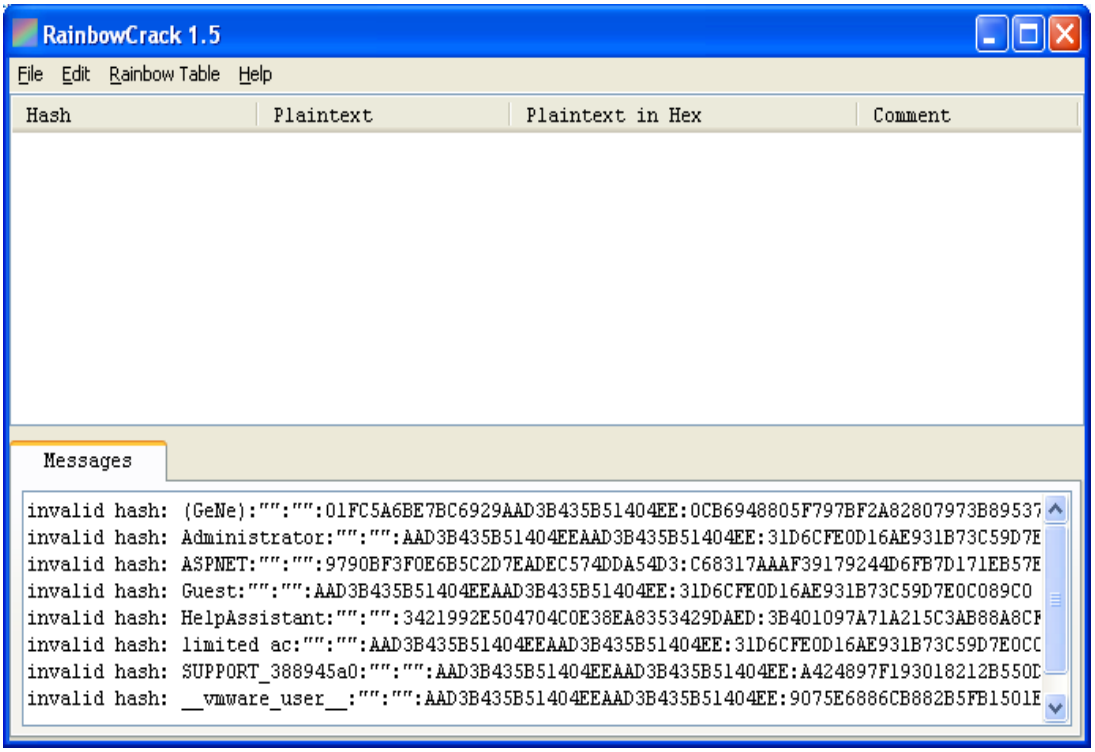
Η συγκεκριμένη τακτική είναι αρκετά γρήγορη παρόλα αυτά όμως είναι χρήσιμη στο να σπάει μόνο μερικά είδη κρυπτογραφημένων κωδικών. Χρησιμοποιεί ένα σέτ από μεγάλα tables από προ-υπολογισμένους κρυπτογραφημένους κωδικούς (Rainbow

Tables), ώστε να βελτιώσει τις μεθόδους ανταλλαγής οι οποίες είναι γνωστές σήμερα και για να ανακτήσει γρηγορότερα διάφορους κωδικούς.

Είναι συμβατό με το RainbowCrack, και υποστηρίζει Rainbow Tables για τους εξής αλγόριθμους:

LM
FastLM,
NTLM
CiscoPIX
MD2, MD4, MD5
SHA-1, SHA-2 (256), SHA-2 (384), SHA-2 (512),
MySQL (323), MySQL (SHA1),
RIPEMD160

Η Cryptanalysis Attack δεν είναι συμβατή με το να σπάει hashes κωδικών τα οποία αιχμαλωτίζονται σε ένα δίκτυο, αντιθέτως είναι αρκετά αποτελεσματική να σπάει hashes τα οποία συχνά χρησιμοποιούνται για να υποθηκεύσουν κρυπτογραφημένους κωδικούς τοπικά.



Εικόνα 92: Rainbow Crack

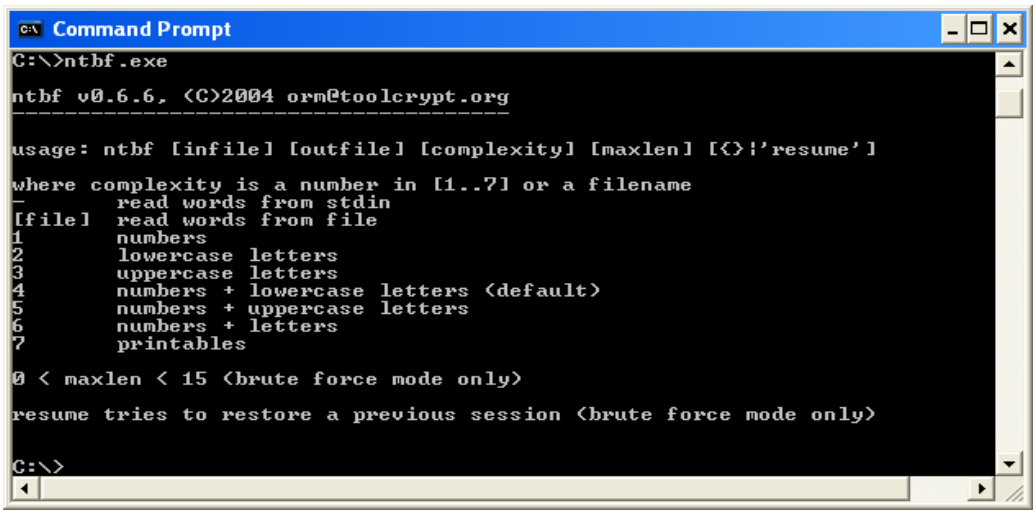
Γενικότερα, το Cain & Abel είναι ένα πανίσχυρο εργαλείο και οι δυνατότητες του δεν περιορίζονται μόνο στην εύρεση κωδικών λογαριασμών χρηστών. Δυστυχώς μπορεί να χρησιμοποιηθεί μόνο σε Windows και όχι σε Unix συστήματα ώστε να μπορέσει να διαβάσει το /etc/passwd file. Μπορεί να χρησιμοποιηθεί σε πάρα πολλές περιπτώσεις εύρεσης-ανάκτησης κωδικών γενικότερα, ασφάλειας ,ως διαγνωστικό σύστημα για τον εντοπισμό δικτυακών προβλημάτων, όπως, επίσης, ως σύστημα απομακρυσμένης διαχείρισης των Windows υπολογιστών τοπικών δικτύων. Για

περισσότερες πληροφορίες σχετικά με το ισχυρό αυτό cracking tool υπάρχουν στην διεύθυνση: http://www.oxid.it/

Εργαλεία

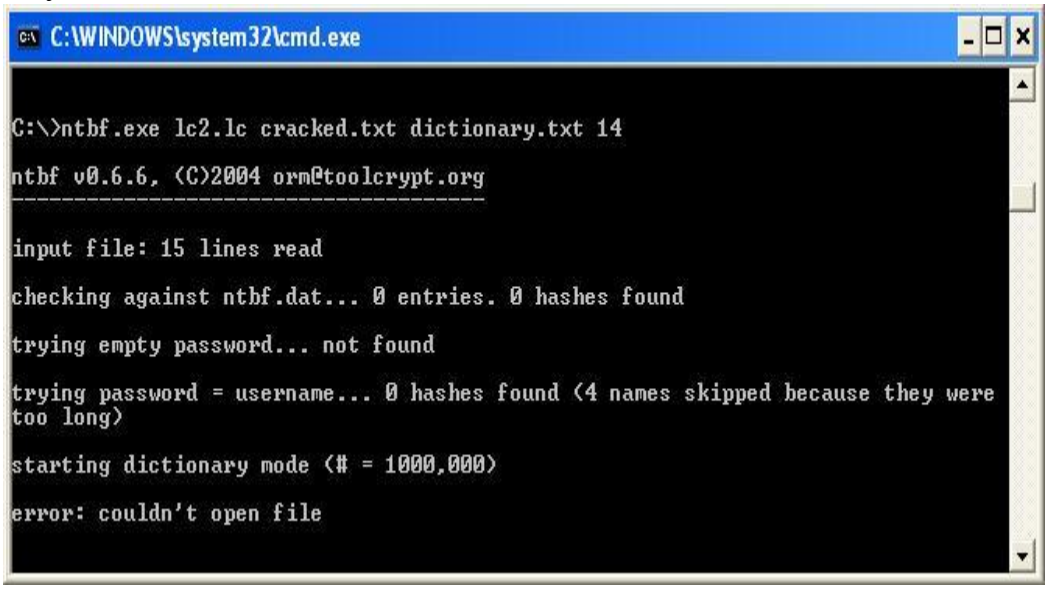
Τα εργαλεία διάρρηξης κωδικών πρόσβασης των windows έχουν μια μακροχρόνια και δυνατή ιστορία . Ένα από τα πιο διάσημα ήταν το L0phtcrack που είχε παραχθεί από την ερευνητική εταιρία ασφάλειας γνωστή ως L0pht. Το L0phtcrack δυστυχώς δεν υποστηρίζεται πλέον , αλλά υπάρχουν ακόμα διάφορα καλά εργαλεία διαθέσιμα για διάρρηξη κωδικών πρόσβασης.

Στο τμήμα γραμμής εντολών του εργαλείου , υπάρχει το lmbf και το ntbf (www.toolcrypt.org) το John the Ripper (www.openwall.com/john/) και το MDcrack (c3rb3r.openwall.net/mdcrack/).



Εικόνα 93: Εντολή ntbf.

Το παρακάτω είναι ένα παράδειγμα της διάρρηξης ntbf κωδικών πρόσβασης NTLM με λεξικό:

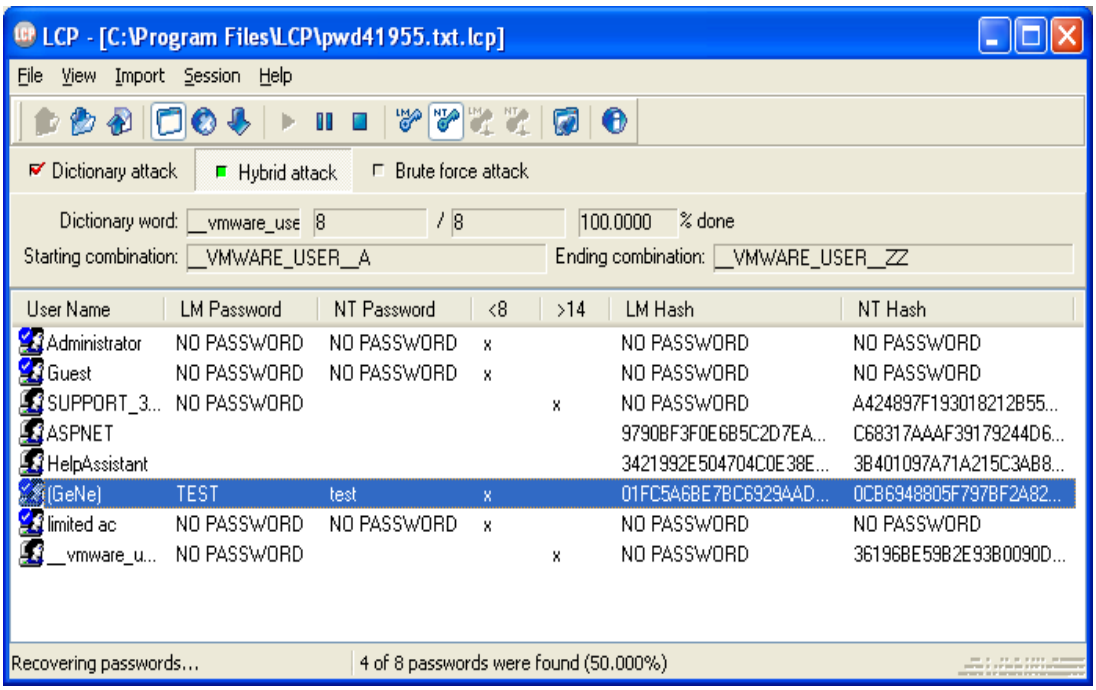


Εικόνα 94:Διάρρηξης κωδικών πρόσβασης με ntbf.

Το John the Ripper παραμένει επίσης μία καλή επιλογή, αλλά θα πρέπει να λάβουμε ξεχωριστά την διόρθωση εάν θέλουμε να προσπαθήσουμε κάνουμε διάρρηξη NTLM (www.openwall.com/john/contrib/john -1.7.2.-ntml-alainesp-6.1diff.gz).

Τα γραφικά προγράμματα διάρρηξης κωδικών πρόσβασης για τα Windows περιλαμβάνουν το LCP (www.lcpsoft.com), το Cain (www.oxid.it) και το Ophcrack που βασίζεται σε πίνακες ουράνιου τόξου (ophcrack.sourceforge.net). Η πιο κάτω εικόνα παρουσιάζει το LCP να εκτελεί διάρρηξη με βάση ένα λεξικό σε κρυπτογραφημένα NTLM σε ένα σύστημα Windows Server 2003.

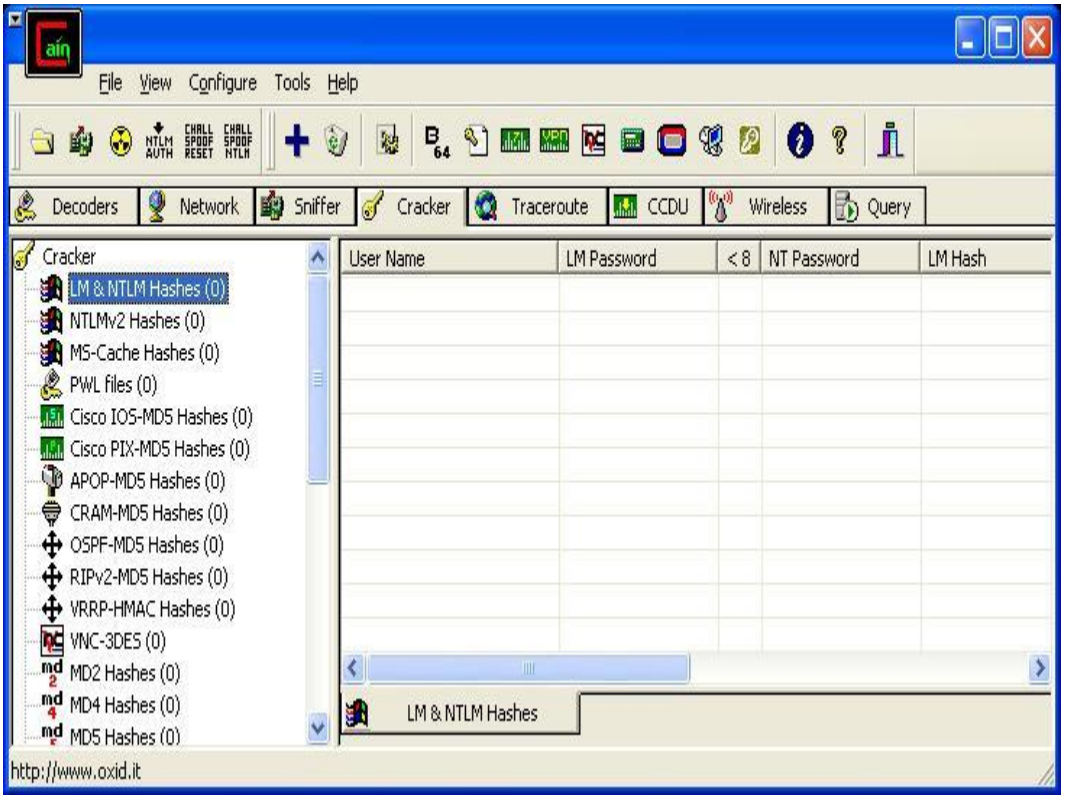
Αυτό το παράδειγμα χρησιμοποιεί ένα λεξικό προσαρμοσμένο για τους κρυπτογραφημένους στόχους που κατέληξαν σ' ένα υψηλό ποσοστό επιτυχίας, το οποίο (και πάλι) δεν είναι γενικά αντιπροσωπευτικό της διάρρηξης NTLM σε καλά επιλεγμένους κωδικούς πρόσβασης.



Εικόνα 95:Διάρρηξη κωδικών πρόσβασης με LCP.

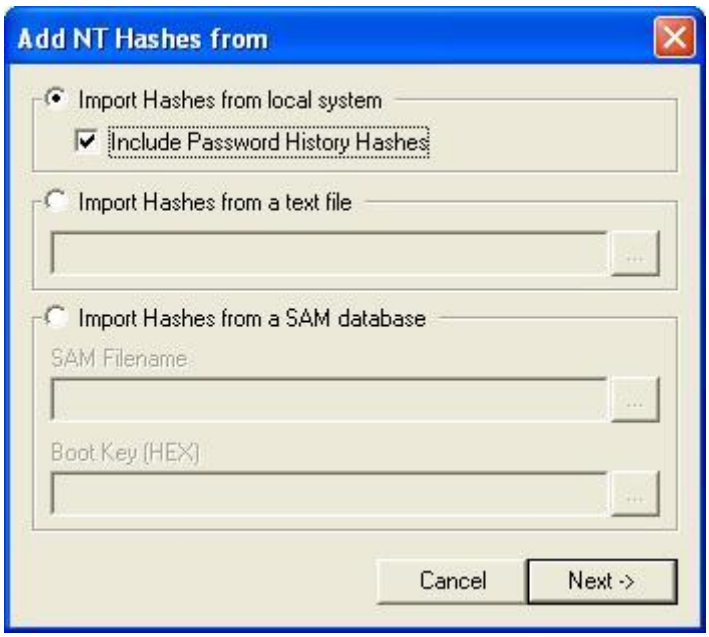
Πιθανώς το πρόβλημα με τις περισσότερες λειτουργίες διάρρηξης κωδικών πρόσβασης είναι το Cain (σίγουρα αυτό το εργαλείο εμφανίζεται πολύ συχνά στα πλαίσια της δοκιμής της ασφάλειας των Windows).

Παρακάτω θα επιχειρήσουμε να σπάσουμε τους κωδικούς των λογαριασμών χρηστών που βρίσκονται στο σύστημα. Έχοντας επιλέξει στην καρτέλα Cracker την κατηγορία LM & NTLM Hashes πατάμε το κουμπί + ώστε να εμφανίσουμε τα διαθέσιμα.



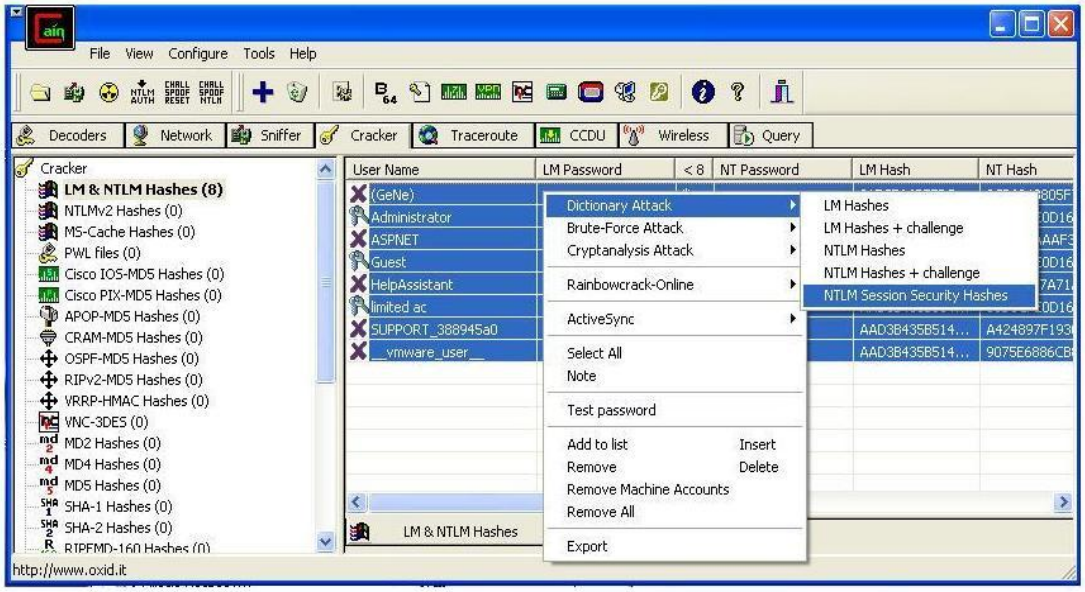
Εικόνα 96:LM & NTLM Hashes

Στην συνέχει μας εμφανίζει το πιο κάτω παράθυρο και επιλέγουμε το Include Password History Hashes και πατάμε Next για να μας εμφανίσει τα hashes.



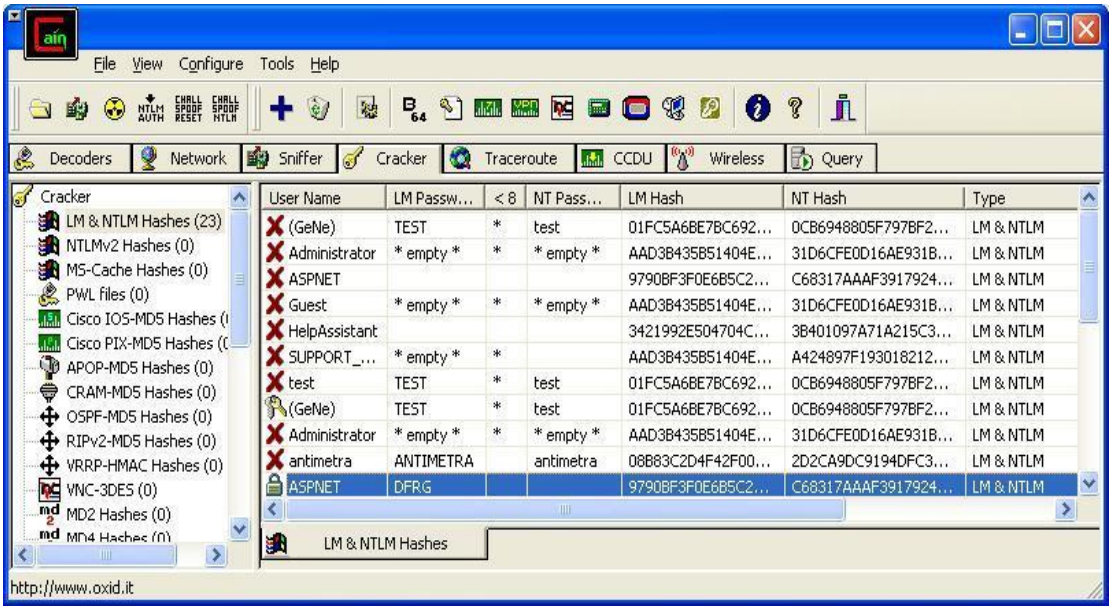
Εικόνα 97: Add NT Hashes

Το Cain σπάει NTLM Session Security hash που έχουν συγκεντρωθεί μέσω του ενσωματωμένου υποκλοπέα.



Εικόνα 98:NTLM Session Security hash –Cain.

Πιο κάτω παρατηρούμε τα LM & NTLM hashes μαζί με τα username και τα passwords.



Εικόνα 99:Αποκρυπτογράφηση LM & NTLM hashes

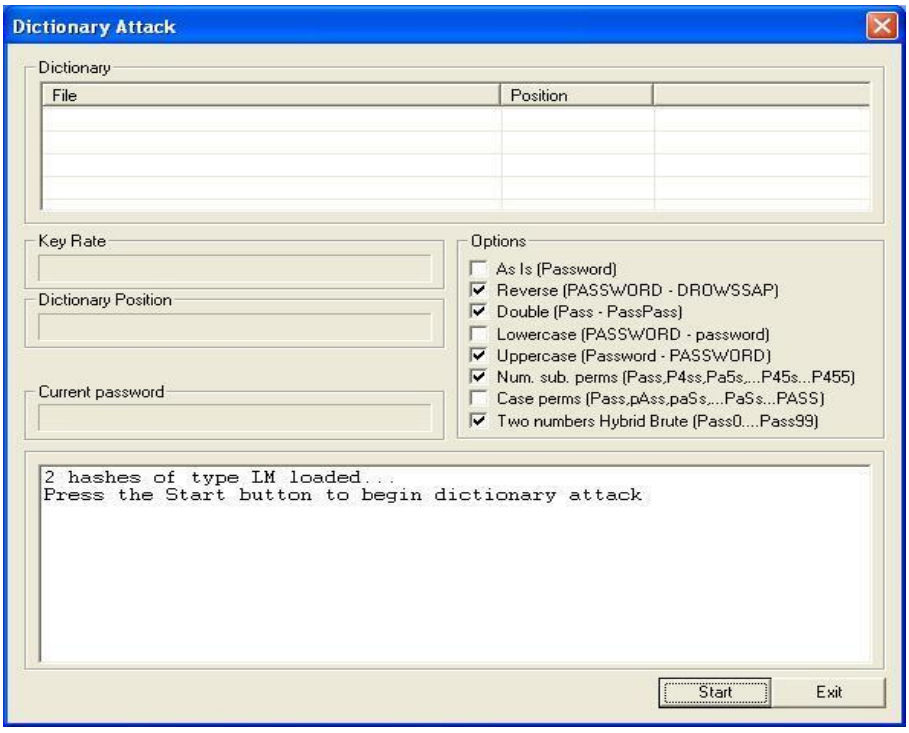
Το Cain μπορεί να εκτελέσει όλες τις τυπικές προσεγγίσεις διάρρηξης, οι οποίες περιλαμβάνουν :

- Με λεξικό και brute force
- LM hash
- NTLM hash
- Υποκλοπή πρόκλησης/αποκρίσεων (συμπεριλαμβανομένων των LM,NTLM και NTLM Session Security)
- Διάρρηξη Rainbow (μέσω Ophcrack , RainbowCrack ή winrtgen)

DICTIONARY ATTACK

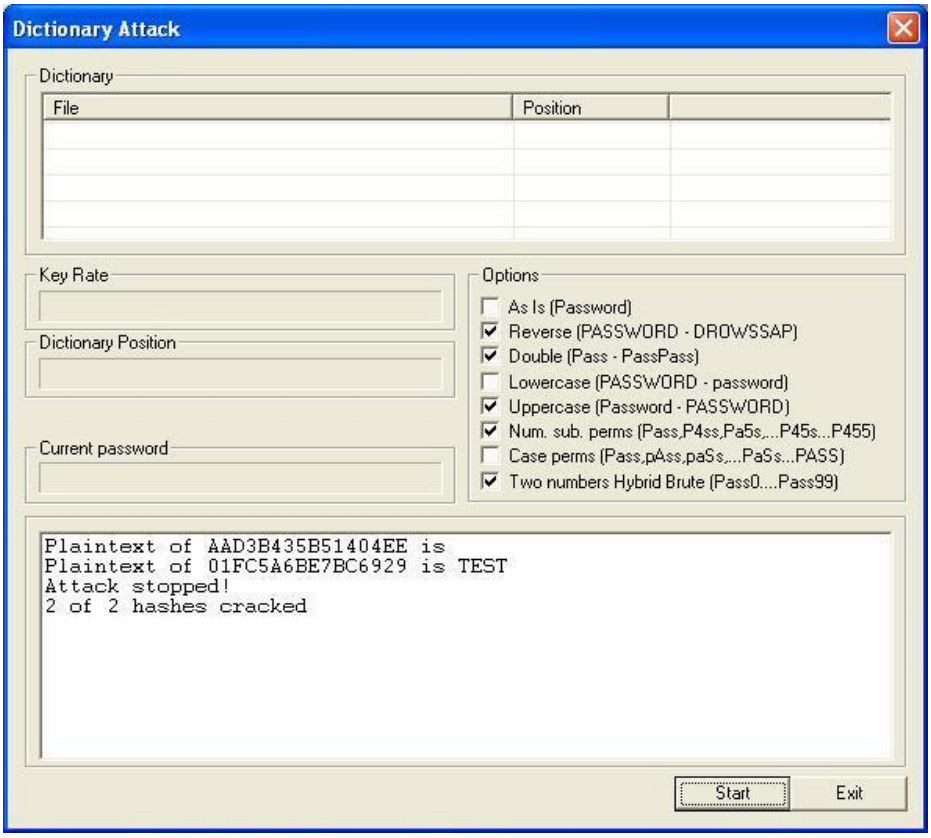
Η μέθοδος του λεξικού χρησιμοποιεί μια έτοιμη λίστα από λέξεις (ή γενικότερα συνδυασμούς χαρακτήρων) τις οποίες κρυπτογραφεί με τον ίδιο αλγόριθμο που έχει δημιουργήσει τον κωδικό, ελέγχοντας αν το κρυπτογραφημένο κείμενο που δημιουργείται, είναι ίδιο με την κρυπτογραφημένη μορφή κωδικού. Το Cain παρέχει από μόνο του ένα μέσου μεγέθους λεξικό της τάξης των 3,30MB το οποίο, όμως, μπορεί να αλλάξει με κάποιο λεξικό δικής μας προτίμησης το οποίο έχουμε φτιάξει εμείς ή έχουμε βρει έτοιμο από το Internet.

Προσέγγιση διάρρηξης LM hashes με την χρήση Dictionary.



Εικόνα 100:Διάρρηξη LM hashes με Dictionary Attack.

Εμφάνιση αποκρυπτογράφησης του κωδικού πρόσβασης TEST.



Εικόνα 101: Hashes cracked με Dictionary Attack – Cain.

BRUTE FORCE ATTACK

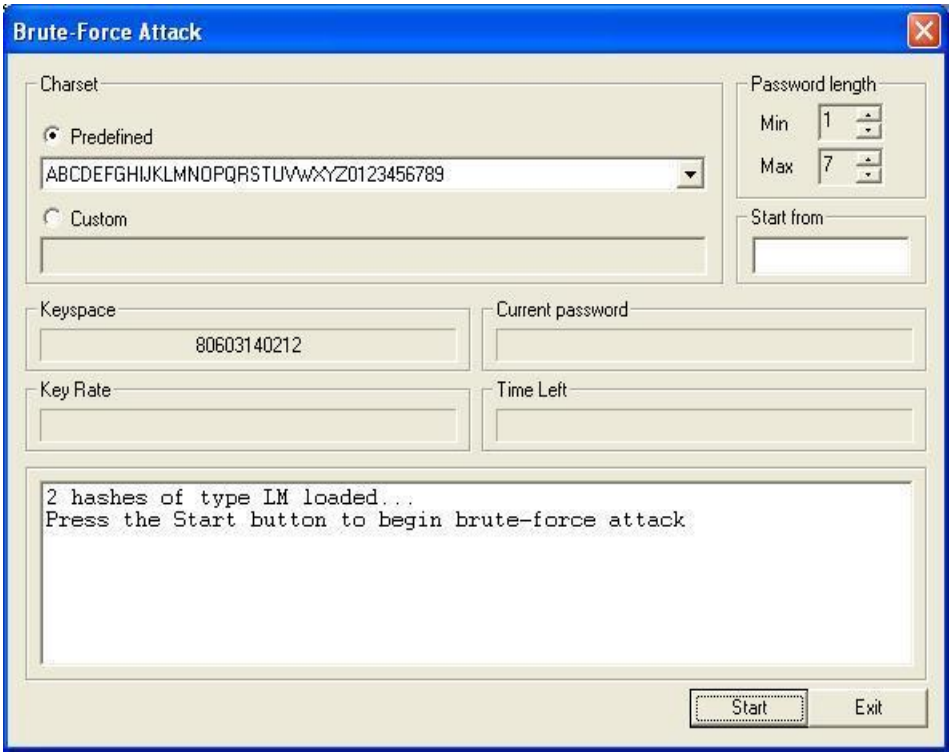
Η μέθοδος της Brute Force επίθεσης (κυριολεκτικά: επίθεση με την χρήση "ωμής βίας") είναι ο πιο γνωστός και διαδεδομένος τρόπος αποκρυπτογράφησης κωδικών, αφού για την χρήση τους δεν απαιτείται τίποτε περισσότερο από την κατοχή του κρυπτογραφημένου κειμένου και τη γνώση του αλγόριθμου με τον οποίο έχει κρυπτογραφηθεί. Το Cain υλοποιεί ένα εξελιγμένο υποσύστημα Brute Force αποκρυπτογράφησης, το οποίο είναι προσβάσιμο από την αντίστοιχη επιλογή, που εμφανίζεται κάνοντας δεξί κλικ πάνω σε ένα account.

Από το παράθυρο διαλόγου Brute Force Attack μπορούν να οριστούν κάποιοι παράμετροι προτού ξεκινήσει το σπάσιμο των κωδικών. Μπορούμε να επιλέξουμε (από το πεδίο Predefined) το σύνολο των χαρακτήρων (Charset) που περιέχει όλους τους χαρακτήρες που - πιθανώς - περιέχονται στην αρχική, μη κρυπτογραφημένη μορφή του κωδικού. Η πολυπλοκότητα της διαδικασίας αυξάνεται ανάλογα προς το μέγεθος του Character set που χρησιμοποιείται. Από την άλλη, ένα σύνολο χαρακτήρων που περιέχει, για παράδειγμα, μόνο τα πεζά γράμματα του λατινικού αλφαβήτου, πιθανώς να μην δημιουργήσει τον κατάλληλο συνδυασμό για την αποκρυπτογράφηση του κωδικού.

Από την περιοχή Password length μπορούμε να επιλέξουμε το ελάχιστο (πεδίο Min) και το μέγιστο (πεδίο Max) μήκος των κωδικών που θα δοκιμαστούν. Ομοίως προς το Character set, το μέγεθος του κωδικού είναι μια παράμετρος που καθορίζει την

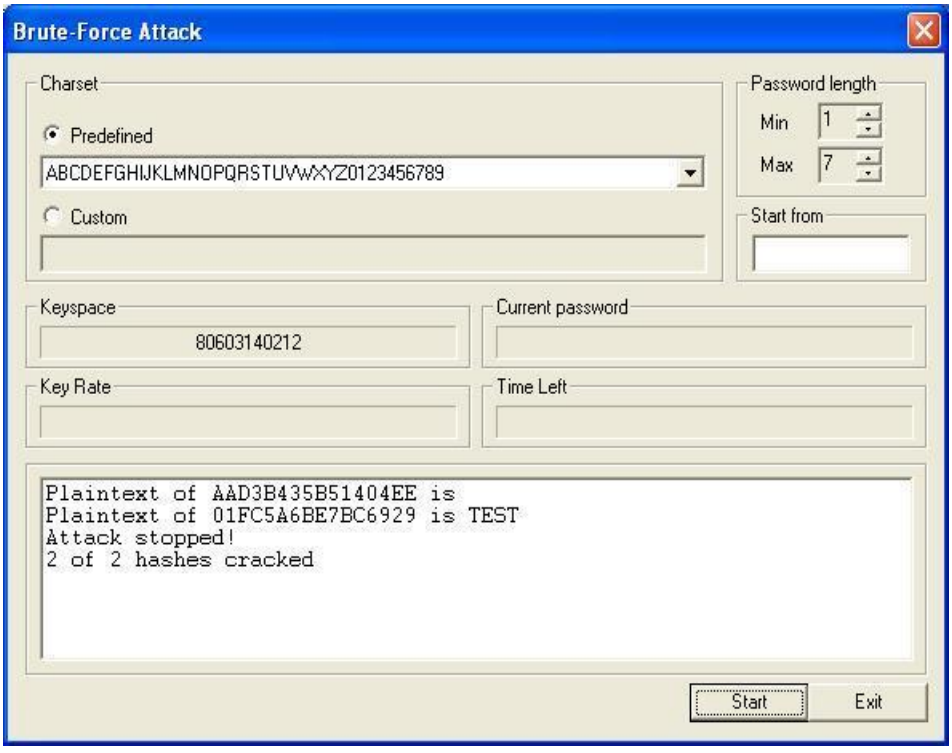
πολυπλοκότητα του εγχειρήματος, οπότε και την πιθανή μέγιστη διάρκεια τις επίθεσης.

Η πρώτη προσέγγιση διάρρηξης LM hashes με την χρήση Brute –Force.



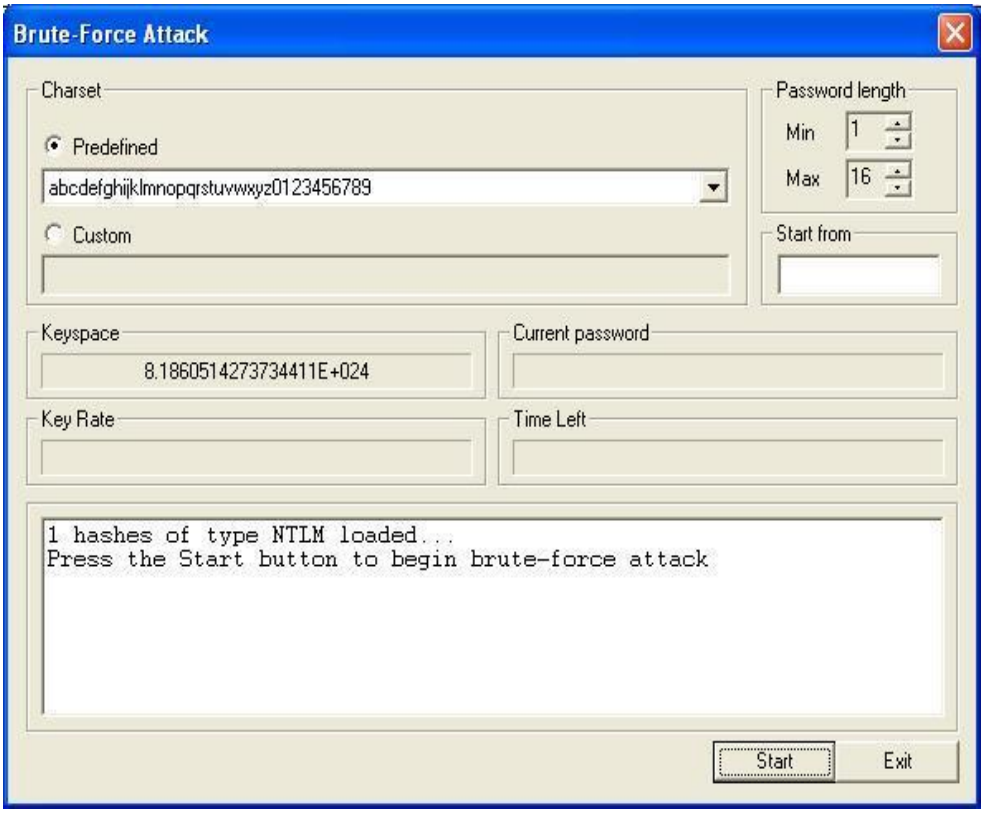
Εικόνα 102:Διάρρηξη LM hashes με Brute-Force Attack

Εμφάνιση αποκρυπτογράφησης του κωδικού πρόσβασης TEST.



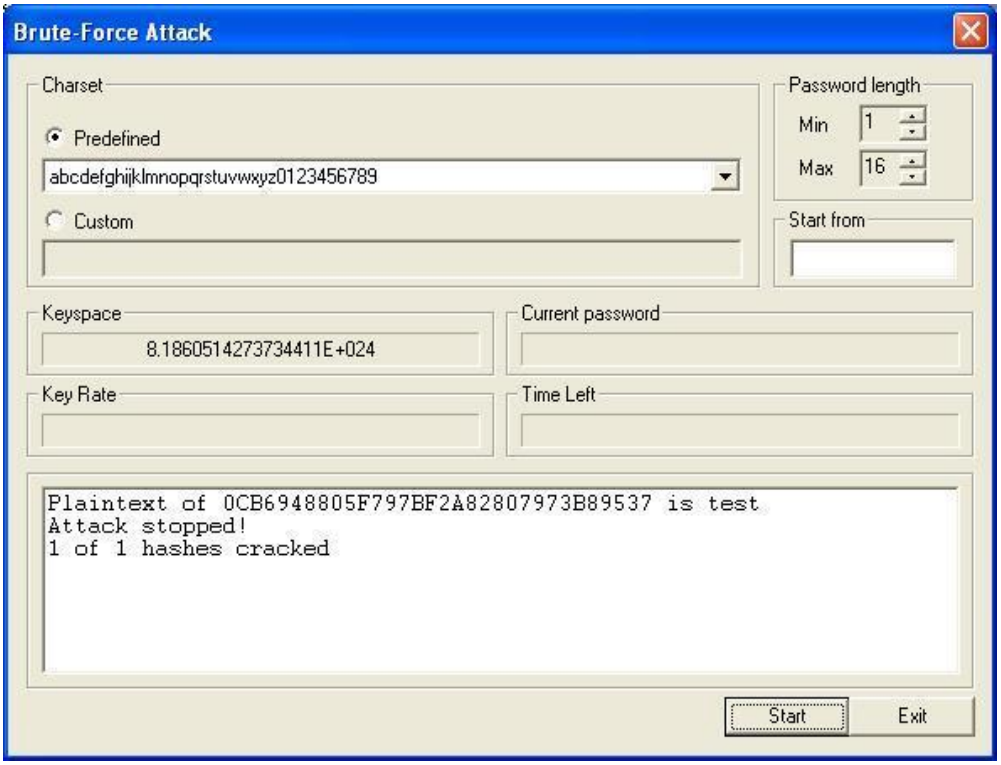
Εικόνα 103:LM Hashes cracked με Brute Force Attack – Cain.

Η δεύτερη προσέγγιση διάρρηξης NTLM hashes με την χρήση Brute –Force.



Εικόνα 104:Διάρρηξη NTLM hashes με Brute Force Attack.

Εμφάνιση αποκρυπτογράφησης του κωδικού πρόσβασης TEST.



Εικόνα 105:NTLM Hashes cracked με Brute Force Attack – Cain.

Τέλος , εάν ψάχνουμε για διάρρηξη επαγγελματικού επιπέδου, ελέγχουμε τον προμηθευτή λογισμικού ανάκτησης κωδικών πρόσβασης Elcomsoft με δυνατότητα ανάκτησης κωδικών πρόσβασης που εκμεταλλεύεται τον συνδυασμό των CPU μέχρι 10.000 τερματικών σταθμών, καθώς επίσης και το Graphics Processing Unit (GPU) που υπάρχει στην κάρτα οθόνης του κάθε συστήματος προκειμένου να αυξήσει την αποτελεσματικότητα διάρρηξης κατά έναν παράγοντα μέχρι 50 (elcomsoft.com/edpr.html).

Χρόνος επεξεργασίας

Οι αδύνατοι αλγόριθμοι όπως το LM hash με (σχετικά) μικρό χώρο χαρακτήρων καταλήγει σε εικασίες μέσω brute force και σε προϋπολογισμένους πίνακες Rainbow σε δευτερόλεπτα. Αλλά το LM hash γίνεται όλο και πιο σπάνιο, τώρα που το αφαίρεσε Microsoft από τις νεότερες εκδόσεις των Windows, βασιζόμενη αποκλειστικά στο NTLM hash εξ ορισμού στα Vista,Server 2008 και νεότερα. Η διάρρηξη του NTLM hash, με βάση τον 128-bit MD5 αλγόριθμο, απαιτεί πάρα πολύ μεγαλύτερη προσπάθεια για να σπάσει.

Κάποιος μπορεί να εκτιμήσει πόση περισσότερη προσπάθεια απαιτείται αν γίνει η απλή υπόθεση ότι κάθε πρόσθετος χαρακτήρας σε έναν κωδικό πρόσβασης αυξάνει τη μη προβλεπτικότητα του ή την εντροπία του ,κατά την ίδια τιμή. Το πληκτρολόγιο των 94-χαρακτήρων οδηγεί σε 94^7 πιθανά LM hash μήκους των 7 χαρακτήρων (το μέγιστο για το LM), ξεχνώντας για μια στιγμή ότι το LM hash χρησιμοποιεί μόνο κεφαλαία. Το NTLM hash, με ένα θεωρητικό μέγιστο 128 χαρακτήρων, θα είχε έτσι εντροπία 94^{128} bit. Υποθέτοντας ένα μέσο ρυθμό 5 εκατομμυρίων ελέγχων κρυπτογράφησης ανά δευτερόλεπτο σε έναν τυπικό υπολογιστή γραφείου (http://en.wikipedia.org/wiki/Password_strength) η διάρρηξη θα διαρκούσε κατά προσέγγιση $7{,}27^{245}$ δευτερόλεπτα ή 2,3 x 10^{238} χρόνια για εκτενή αναζήτηση στο χώρο των κωδικών πρόσβασης των 128-χαρακτήρων NTLM ή/και για να παραχθούν NTLN Rainbow πίνακες.

Ακόμα μία πιο πρακτική σκοπιά, οι περιορισμοί του ανθρώπινου εγκεφάλου θα εμποδίσουν την χρήση αληθινά τυχαίων κωδικών πρόσβασης 128-χαρακτήρων. Κατά συνέπεια, η προσπάθεια διάρρηξης εξαρτάται ρεαλιστικά από την τρέχουσα τιμή της εντροπίας στον κωδικό πρόσβασης που κρυπτογραφείται. Ακόμα χειρότερα, έχει γίνει ευρέως κατανοητό ότι οι ανθρώπινες συνήθειες επιλογής κωδικών πρόσβασης οδηγούν σε ουσιαστικά μειωμένη εντροπία σε σχέση με μία ψευδοτυχαία επιλογή, ανεξάρτητα από τον αλγόριθμο (δείτε ,για παράδειγμα το NIST Special Publication 800-63 at http://csrc.nist.gov/ publications/nistpubs/800-63/SP800-63V1_0_2.pdf, Appendix A) . Έτσι, η «δύναμη bit» του αλγόριθμου hash δεν έχει σημασία αφού διαψεύδεται από την εντροπία των πραγματικών κωδικών πρόσβασης. Η εταιρεία λογισμικού ανάκτησης κωδικών πρόσβασης AccessData υποστήριξε κάποτε ότι χρησιμοποιώντας ένα σχετικά απλό σύνολο ρουτινών βασισμένων σε λεξικό, το λογισμικό τους θα μπορούσε να σπάσει 55% έως 65% όλων των κωδικών πρόσβασης μέσα σ έναν μήνα (δείτε την διεύθυνση http://www.schneier .com/blog/archives/2007/01/choosing_secure.html). Όπως θα δείτε στην παρακάτω συζήτηση για τα αντίμετρα, αυτό τοποθετεί την ευθύνη της άμυνας στην επιλογή ενός δυνατού κωδικού πρόσβασης.

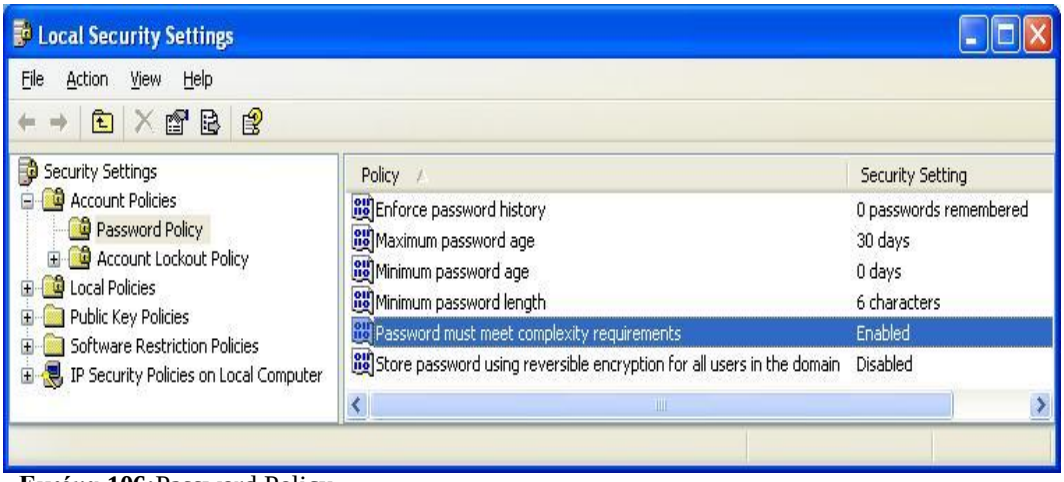
3.2.2.a Αντίμετρα στην Διάρρηξη Κωδικών Πρόσβασης

Όπως φάνηκε στην προηγούμενη συζήτηση για την δυναμική της διάρρηξης κωδικών πρόσβασης, η καλύτερη άμυνα στην διάρρηξη κωδικών πρόσβασης είναι σίγουρα μη τεχνική, αλλά ωστόσο είναι πιθανώς η πιο σημαντική, δηλαδή να επιλέγουμε δυνατούς κωδικούς πρόσβασης.

Οι πιο σύγχρονες εκδόσεις των Windows διαμορφώνονται εξ ορισμού με ενεργοποιημένη την ρύθμιση Security Policy «Passwords must meet complexity requirements» (οι κωδικοί πρόσβασης θα πρέπει να ανταποκρίνονται σε απαιτήσεις πολυπλοκότητας»).

Αυτό απαιτεί ότι οι κωδικοί πρόσβασης όλων των χρηστών, όταν δημιουργούνται ή αλλάζουν ,θα πρέπει να καλύπτουν τις παρακάτω απαιτήσεις (με μοντέλο των Windows Server 2003):

- Δεν μπορεί να περιέχει το όνομα λογαριασμού του χρήστη ή μέρη του πλήρους ονόματος του χρήστη σε παραπάνω από δύο διαδοχικούς χαρακτήρες.
- Πρέπει να είναι τουλάχιστον έξι χαρακτήρες σε μήκος.
- Πρέπει να περιέχει χαρακτήρες από τρείς από τις παρακάτω τέσσερεις κατηγορίες.
    - Αγγλικούς κεφαλαίους χαρακτήρες (A έως Z)
    - Αγγλικούς πεζούς χαρακτήρες (a έως z)
    - Τα βασικά 10 ψηφία (0 μέχρι 9)
    - Μη αλφαβητικούς χαρακτήρες (για παράδειγμα,!,$,#,%)



Εικόνα 106: Password Policy

Συστήνουμε να αυξηθεί το ελάχιστο μήκος των 6-χαρακτήρων που περιγράφηκε στην προηγούμενη διαμόρφωση σε 8 χαρακτήρες, με βάση τις εκτιμήσεις του NIST 800-63, που δείχνουν ότι η πρόσθετη εντροπία ανά χαρακτήρα μειώνεται κάπως μετά τον $8^{ο}$ χαρακτήρα (με άλλα λόγια, τα πλεονεκτήματα σας αρχίζουν να μειώνονται μετά από κάθε πρόσθετο χαρακτήρα μετά τον $8^{ο}$). Αυτή η σύσταση δεν υπονοεί ότι δεν θα πρέπει να επιλέγουμε μεγαλύτερους κωδικούς πρόσβασης όποτε είναι δυνατόν, αλλά μάλλον αναγνωρίζει το μειονεκτήματα ότι οι χρήστες δεν μπορούν να τους απομνημονεύουν. Έτσι, θα πρέπει επίσης να διαμορφώσουμε την ρύθμιση του Security Policy «Maximum password length» (μέγιστο μήκος κωδικού πρόσβασης) σε τουλάχιστον 8 χαρακτήρες. (Εξ ορισμού είναι μηδέν, που σημαίνει ότι η προεπιλεγμένη ρύθμιση των Windows είναι τρωτή σε επιθέσεις διάρρηξης ως προς τους κωδικούς πρόσβασης των 6-χαρακτήρων.)

Τα αντίμετρα έναντι της διάρρηξης περιλαμβάνουν επίσης ορισμό πολιτικών επαναχρησιμοποίησης και λήξης κωδικών πρόσβασης, οι οποίες διαμορφώνονται επίσης χρησιμοποιώντας το Security Policy των Windows. Η ιδέα πίσω από αυτές τις ρυθμίσεις είναι να μειωθεί το χρονικό πλαίσιο, μέσα στο οποίο θα είναι χρήσιμος ένας κωδικός πρόσβασης και έτσι να περιορίσουμε τις ευκαιρίες που έχει ένας επιτιθέμενος να τον σπάσει. Ο ορισμός της λήξης είναι κάπως αντιφατικός, καθώς αναγκάζει τους χρήστες να δημιουργούν δυνατούς κωδικούς πρόσβασης πιο συχνά και επιδεινώνει έτσι τις κακές συνήθειες επιλογής κωδικών πρόσβασης. Συστήνουμε, ωστόσο, να ορίζεται την λήξη επειδή, θεωρητικά, οι κωδικοί πρόσβασης που δεν λήγουν είναι πολύ επικίνδυνοι. Ωστόσο, συστήνουμε επίσης μεγάλο χρονικό διάστημα λήξης αρκετών μηνών ώστε να μην προσθέτετε φορτίο στους χρήστες (το NIST 800-63 είναι επίσης βοηθητικό εδώ).

Και, φυσικά, θα πρέπει να απενεργοποιήσουμε την αποθήκευση των εξαιρετικά αδύνατων, LM hash χρησιμοποιώντας την ρύθμιση Security Policy "Network Security: Do Not Store LAN Manager Hash Value On Next Passwords Chance" ("ασφάλεια δικτύου: να μην αποθηκεύουμε την κρυπτογραφημένη τιμή LAN Manager κατά την επόμενη αλλαγή κωδικού πρόσβασης"). Η προεπιλεγμένη ρύθμιση στον Server 2008 είναι "Enabled". Αν και αυτή η ρύθμιση μπορεί να προκαλέσει προβλήματα συμβατότητας προς τα πίσω σε μικτά περιβάλλοντα των Windows, την συστήνουμε έντονα λόγω της πολύ αυξημένης προστασίας που προσφέρει σε επιθέσεις διάρρηξης κωδικών πρόσβασης.

3.2.3 Εμφάνιση κωδικών πρόσβασης από την cache

Τα Windows έχουν ιστορικά αποκτήσει μία κακή συνήθεια να διατηρούν πληροφορίες κωδικών πρόσβασης εναποθηκευμένων σε διάφορα μέρη εκτός από την κύρια βάση δεδομένων κωδικών πρόσβασης των χρηστών. Ένας επιτιθέμενος σε μία εταιρεία, μόλις αποκτήσει αρκετά προνόμια, μπορεί εύκολα να εξάγει αυτά τα πιστοποιητικά.
Η λειτουργία LSA Secrets είναι ένα από τα πιο δόλια παραδείγματα του κινδύνου να είναι τα πιστοποιητικά σε μία κατάσταση προσπελάσιμη από λογαριασμούς με ειδικά δικαιώματα. Η Local Security Authority (LSA) Secrets cache, που είναι διαθέσιμη κάτω από το υποκλειδί του Registry HKLM\SECURITY\Policy\Secrets, περιέχει τα παρακάτω στοιχεία :

- Κωδικοί πρόσβασης λογαριασμών υπηρεσιών σε *απλό κείμενο*. Οι λογαριασμοί υπηρεσιών που απαιτούνται από λογισμικό που πρέπει να συνδέεται κάτω από το πλαίσιο ενός τοπικού χρήστη για να εκτελέσει διάφορες εργασίες, όπως αντίγραφα ασφάλειας. Είναι γενικά λογαριασμοί που υπάρχουν σε εξωτερικούς τομείς και όταν αποκαλύπτονται από ένα σύστημα, στο οποίο έχει γίνει εισβολή, παρέχει έναν τρόπο στον επιτιθέμενο να συνδεθεί κατευθείαν στον εξωτερικό τομέα.

- Εναποθηκευμένοι κρυπτογραφημένοι κωδικοί πρόσβασης των τελευταίων δέκα χρηστών που συνδέθηκαν σ' έναν υπολογιστή.

- Κωδικοί πρόσβασης FTP και Web χρηστών σε απλό κείμενο.

- Ονόματα και κωδικοί πρόσβασης λογαριασμών μέσω τηλεφώνου Remote Access Services (RAS).

- Κωδικοί πρόσβασης λογαριασμών υπολογιστών για πρόσβαση σε τομέα (domain).

Προφανώς, οι κωδικοί πρόσβασης λογαριασμών υπηρεσιών που τρέχουν με δικαιώματα χρηστών τομέα, οι πληροφορίες τελευταίας σύνδεσης των χρηστών, οι κωδικοί πρόσβασης τομέα σε τερματικούς σταθμούς κ.λπ., μπορούν όλα να δώσουν σε έναν επιτιθέμενο την δυνατότητα να δει την δομή του τομέα.

Για παράδειγμα, φανταστείτε έναν αυτόνομο διακομιστή που τρέχει τις υπηρεσίες Microsoft SMS ή SQL που τρέχουν στο πλαίσιο ενός χρήστη τομέα. Εάν αυτός ο διακομιστής έχει έναν κενό τοπικό κωδικό πρόσβασης Administrator, θα μπορούσε να χρησιμοποιηθεί το LSA Secrets για να αποκτηθεί ο λογαριασμός και ο κωδικός πρόσβασης του χρήστη επιπέδου τομέα. Αυτό το πρώτο σημείο θα μπορούσε επίσης να οδηγήσει σε παραβίαση μιας κύριας διαμόρφωσης τομέα χρηστών. Εάν ένας διακομιστής τομέα πόρων έχει μία υπηρεσία που εκτελείται στα πλαίσια ενός λογαριασμού χρήστη από τον κύριο τομέα χρήστη, μια παραβίαση του διακομιστή του τομέα πόρων θα μπορούσε να επιτρέψει στον κακόβουλο να αποκτήσει διαπιστευτήρια του κύριου τομέα.

Ο Paul Ashton έχει δημοσιεύσει κώδικα που εμφανίζει το LSA Secrets σε διαχειριστές που είναι συνδεδεμένοι τοπικά. Μια ενημερωμένη έκδοση αυτού του κώδικα, που ονομάζεται lsadump2, είναι διαθέσιμη στην διεύθυνση.

Το lsadump2 χρησιμοποιεί την ίδια τεχνική με το pwdump2 («εμφύτευση» DLL) για παράκαμψη όλης της ασφάλειας του λειτουργικού συστήματος. Το lsadump2 βρίσκει αυτόματα το PID του LSASS, εισάγεται μόνο του και αρπάζει το LSA Secrets, όπως βλέπετε εδώ :

```
C:\>lsadump2
$MACHINE.ACC


6E 00 76 00 76 00 68 00 68 00 5A 00 30 00 41 00 n.v.v.h.h.Z.0.A.
66 00 68 00 50 00 6C 00 41 00 73 00             f.h.P.l.A.s.
_SC_MSSQLServer
```

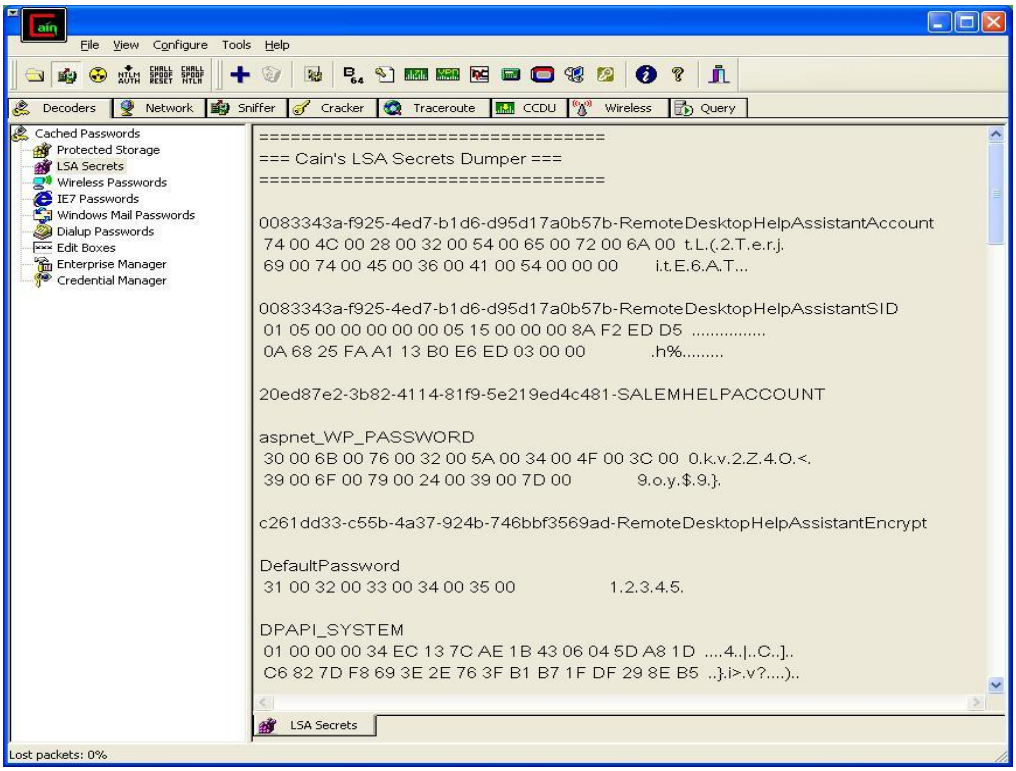
```
32 00 6D 00 71 00 30 00 71 00 71 00 31 00 61 00  p.a.s.s.w.o.r.d.
_SC_SQLServerAgent
32 00 6D 00 71 00 30 00 71 00 71 00 31 00 61 00 p.a.s.s.w.o.r.d.
```

Μπορούμε να δούμε τον κωδικό πρόσβασης του λογαριασμού του υπολογιστή για τον τομέα και δύο κωδικούς πρόσβασης σχετικούς με τον λογαριασμό υπηρεσίας SQL μεταξύ των LSA Secrets αυτού του συστήματος. Δεν απαιτείται πολλή φαντασία για να ανακαλύψετε ότι μεγάλα δίκτυα των Windows μπορούν να ανατραπούν γρήγορα μέσω αυτού του είδους απαρίθμησης των κωδικών πρόσβασης.

Ξεκινώντας από τα Windows XP, η Microsoft μετακίνησε μερικά πράγματα και έκανε το lsadump2 να μην λειτουργεί αν δεν τρέχει με το λογαριασμό SYSTEM. Έχουν δημοσιευτεί τροποποιήσεις στον πηγαίο κώδικα του lsadump2 που ξεπερνούν αυτό το πρόβλημα. Το γενικό εργαλείο εισβολής Cain για τα Windows έχει επίσης έναν ενσωματωμένο εξαγωγέα LSA Secrets που παρακάμπτει αυτά τα θέματα όταν τρέχει σαν ένας λογαριασμός διαχειριστή.

Το Cain έχει διαφόρους άλλους εναποθηκευμένους εξαγωγείς κωδικών πρόσβασης που εργάζονται σ' έναν τοπικό υπολογιστή ένα τρέχουν με προνόμια διαχειριστή. Στην επόμενη εικόνα μέσο του Cain εξάγουμε το LSA Secrets από ένα σύστημα με Windows XP Service Pack 2 επίσης εμφανίζει τις άλλες αποθήκες από τις οποίες μπορεί το Cain να εξάγει κωδικούς πρόσβασης, συμπεριλαμβανομένων των Protected Storage, Internet Explorer 7, ασύρματη δικτύωση, Windows Mail, συνδέσεις μέσω τηλεφώνου, πλαίσια επεξεργασίας, SQL Enterprise και Manger Credential Manager.

Τα Windows βάζουν επίσης στην cache τα πιστοποιητικά των χρηστών που έχουν συνδεθεί προηγουμένως σ' έναν τομέα. Εξ ορισμού, διατηρούνται οι τελευταίες δέκα συνδέσεις μ' αυτό τον τρόπο. Δεν είναι τόσο απλή η χρησιμοποίηση αυτών των πιστοποιητικών όσο η εξαγωγή απλού κειμένου που παρέχεται από το LSADump, ωστόσο, αφού οι κωδικοί πρόσβασης αποθηκεύονται σε κρυπτογραφημένη μορφή και κρυπτογραφούνται περαιτέρω με ένα κλειδί συγκεκριμένο για τον υπολογιστή. Τα κρυπτογραφημένα εναποθηκευμένα hash είναι αποθηκευμένα κάτω από το κλειδί HKLM\SECURITY\CACHE\NL$n του Registry, όπου το *n* αντιπροσωπεύει μία αριθμητική τιμή από 1 έως 10 που αντιστοιχεί στις τελευταίες δέκα συνδέσεις που είναι αποθηκευμένες στην cache.



Εικόνα 107:LSA Secrets- Password –Αποκωδικοποίηση κωδικού πρόσβαση από την Cache.

Φυσικά, κανένα μυστικό δεν είναι ασφαλές σε κάποιον που έχει δικαιώματα ισοδύναμα με του Administrator ή του SYSTEM. Το CacheDump του Arnaud Pilon (δείτε www.cr0.net:8040/misc/cachedump.html) αυτοματοποιεί την εξαγωγή των προηγούμενα κρυπτογραφημένων cache. Το Cain έχει επίσης μία ενσωματωμένη δυνατότητα εμφάνισης της cache στο εργαλείο Cracking, που ονομάζεται MS-Cache Hashes.

Τα κρυπτογραφήματα θα πρέπει, φυσικά, στην συνέχεια να σπάσουν ώστε να αποκαλύψουν τους κωδικούς πρόσβασης σε απλό κείμενο (δεν έχουν δημοσιευτεί για κάποιο χρόνο ενημερωμένα εργαλεία για εκτέλεση «περάσματος του hash», ή άμεση επαναχρησιμοποίηση κρυπτογραφημένων κωδικών πρόσβασης). Οποιοδήποτε από τα εργαλεία διάρρηξης κωδικών πρόσβασης στα Windows που έχουμε συζητήσει σ' αυτό το κεφάλαιο μπορούν να εκτελέσουν αυτήν την εργασία. Ένα άλλο εργαλείο που δεν έχουμε αναφέρει ακόμα, το cachebf, θα σπάσει κατευθείαν την έξοδο από το CacheDump. Μπορείτε να βρείτε το cachebf στην διεύθυνση http://www.toolcrypt.org/tools/cachebf/index.html .

Όπως μπορείτε να φανταστείτε, αυτά τα πιστοποιητικά μπορούν να είναι αρκετά χρήσιμα σε επιτιθέμενους – πρέπει να έχουμε ανοικτά τα μάτια μας γι αυτά που υπάρχουν στις cache συνδέσεις, ακόμη και στους πιο άχρηστους υπολογιστές μιας εταιρείας.

3.2.3.a Αντίμετρα στην εμφάνιση κωδικών πρόσβασης από την cache

Δυστυχώς, η Microsoft δεν βρίσκει την αποκάλυψη αυτών των δεδομένων τόσο σημαντική, δηλώνοντας ότι η πρόσβαση αυτών των πληροφοριών από τον Administrator είναι δυνατή «για λόγους σχεδίασης» στο άρθρο Microsoft KB Article ID Q184017, το οποίο περιγράφει τη διαθεσιμότητα μιας αρχικής διόρθωσης LSA. Αυτή η διόρθωση κρυπτογραφεί και άλλο την αποθήκευση κωδικών πρόσβασης τερματικών των λογαριασμών υπηρεσιών, των συνδέσεων τομέα της cache και των κωδικών πρόσβασης τερματικών σταθμών χρησιμοποιώντας κρυπτογράφηση στυλ SYSKEY. Φυσικά, το lsadump2 απλώς το παρακάμπτει αυτό χρησιμοποιώντας «εμφύτευση» DLL.

Επομένως, η καλύτερη άμυνα στο lsadump2 και σε παρόμοια εργαλεία εμφάνισης της cache είναι να αποφύγουμε να έχουμε δικαιώματα διαχειριστή. Επιβάλλοντας λογικές πολιτικές σχετικά με το ποιος αποκτά πρόσβαση ως διαχειριστής στα συστήματα της επιχείρηση σας. Είναι επίσης σοφό να είμαστε πολύ προσεκτικοί για την χρήση λογαριασμών υπηρεσιών και αξιόπιστων τομέων. Οπωσδήποτε αποφεύγουμε να χρησιμοποιούμε ιδιαίτερα προνομιούχους λογαριασμούς τομέα για να ξεκινήσουμε υπηρεσίες σε τοπικούς υπολογιστές.

Όταν συνδεθούμε στα Windows χρησιμοποιούμε συνδέσεις προσωρινής αποθήκευσης πληροφοριών, εάν ο domain controller δεν διατίθεται για να επικυρώσει το λογαριασμό μας. Ωστόσο, μπορούμε να αποκτήσουμε πρόσβαση σε πόρους δικτύου που δεν απαιτούν επικύρωση τομέα.

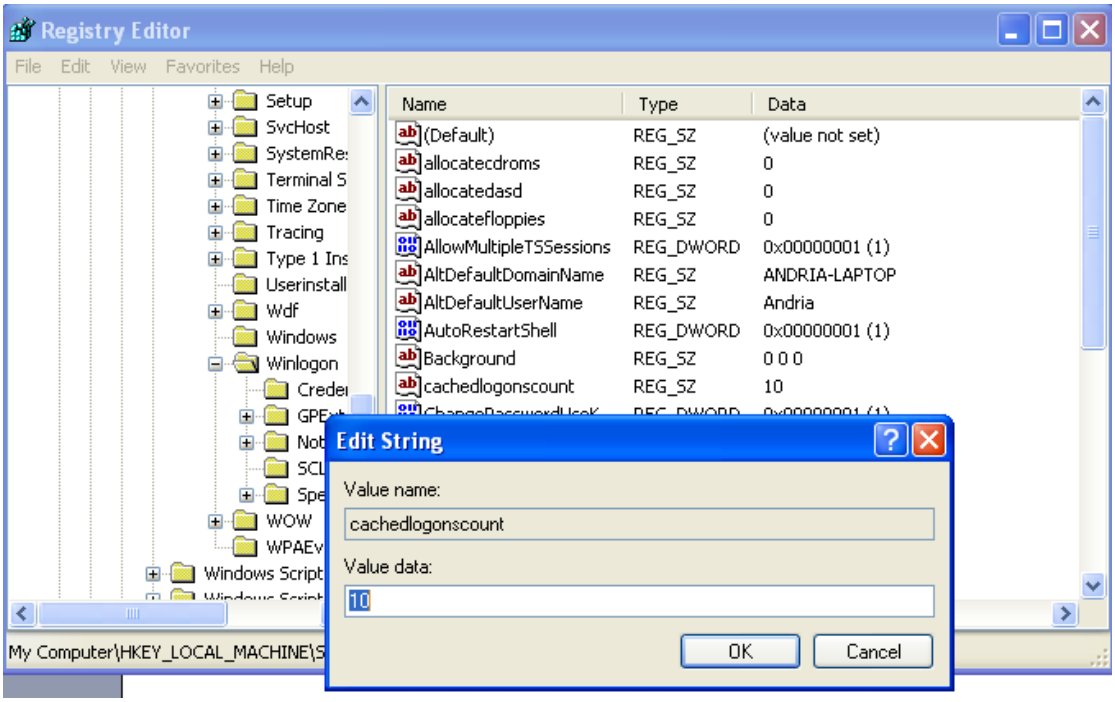
Υπάρχει μια συγκεκριμένη ρύθμιση της διαμόρφωσης που μπορεί να βοηθήσει να μετριασθούν οι επιθέσεις εμφάνισης της cache . Η λύση αυτή είναι να αλλάξουμε το κλειδί του Registry HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon σε μία κατάλληλη τιμή.

Μέσω του μητρώου και ενός βοηθητικού προγράμματος πόρων (Regkey.exe), μπορούμε να αλλάξουμε τον αριθμό των προηγούμενων προσπαθειών σύνδεσης που αποθηκεύει προσωρινά σ' ένα διακομιστή. Η έγκυρη περιοχή τιμών για αυτήν την παράμετρο είναι από 0 έως 50. Η τιμή 0 απενεργοποιεί την προσωρινή αποθήκευση σύνδεσης και οποιαδήποτε τιμή πάνω από 50 αποθηκεύει προσωρινά μόνο 50 προσπάθειες σύνδεσης. (η προεπιλογή είναι 10 – δείτε http://support.microsoft.com/?kbid=172931).

Προσωρινή αποθήκευση πληροφοριών σύνδεσης ελέγχεται από το ακόλουθο κλειδί:

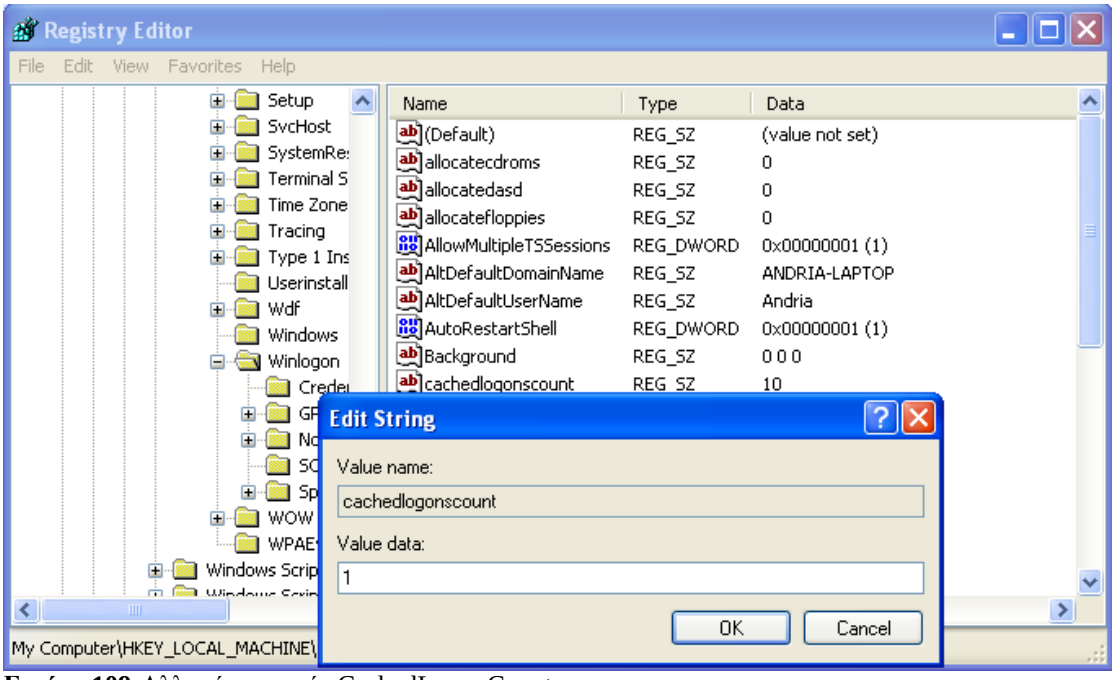
```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\Current Version\Winlogon\

ValueName: CachedLogonsCount
Data Type: REG_SZ
Values: 0 - 50
```

Από προεπιλογή, όλες οι εκδόσεις των Windows αποθηκεύουν 10 προσωρινές συνδέσεις εκτός από τον Windows Server 2008 και Vista.



Εικόνα 108:Προκαθορισμένη τιμή στο CachedLogonCount

Αυτή η ρύθμιση είναι επίσης προσπελάσιμη από το Security Policy κάτω από το "Interactive Logon: number of previous logons to cache (in case domain controller is not available-διαλογική σύνδεση: αριθμός προηγούμενων συνδέσεων στην cache-σε περίπτωση που ο ελεγκτής είναι διαθέσιμος)". Πρέπει να είμαστε προσεκτικοί, γιατί αν κάνουμε μηδέν την έξοδο αυτής της ρύθμισης (το πιο ασφαλές) θα εμποδίσουμε μετακινούμενους χρήστες να συνδεθούν όταν δεν είναι προσπελάσιμος ένας ελεγκτής τομέα. Μία πιο λογική τιμή μπορεί να είναι το 1, που μας αφήνει τρωτούς αλλά όχι στην ίδια έκταση με τις προκαθορισμένες τιμές των Windows.



Εικόνα 109:Αλλαγή της τιμής CachedLogonCount.

Οι αλλαγές που κάνουμε σε αυτό το κλειδί απαιτούν την επανεκκίνηση του υπολογιστή για να εφαρμοστούν.

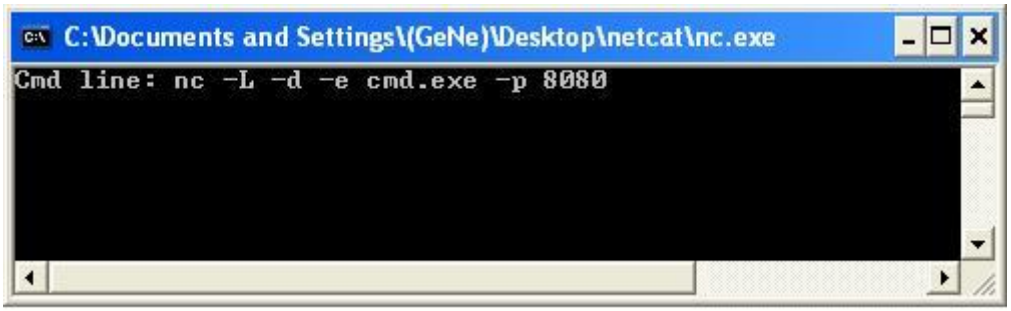
3.3 Έλεγχος από απόσταση και πίσω πόρτες

Αφού αποκτηθεί πρόσβαση Administrator και εξαχθούν οι κωδικοί πρόσβασης , οι εισβολής επιδιώκουν γενικά να παγιώσουν τον έλεγχο τους σε ένα σύστημα μέσω διαφόρων υπηρεσιών που επιτρέπουν τον απομακρυσμένο έλεγχο. Τέτοιες υπηρεσίες ονομάζονται μερικές φορές *πίσω πόρτες (back doors)* και γενικά κρύβονται χρησιμοποιώντας τεχνικές.

3.3.1 Εργαλεία ελέγχου από απόσταση της γραμμής εντολών

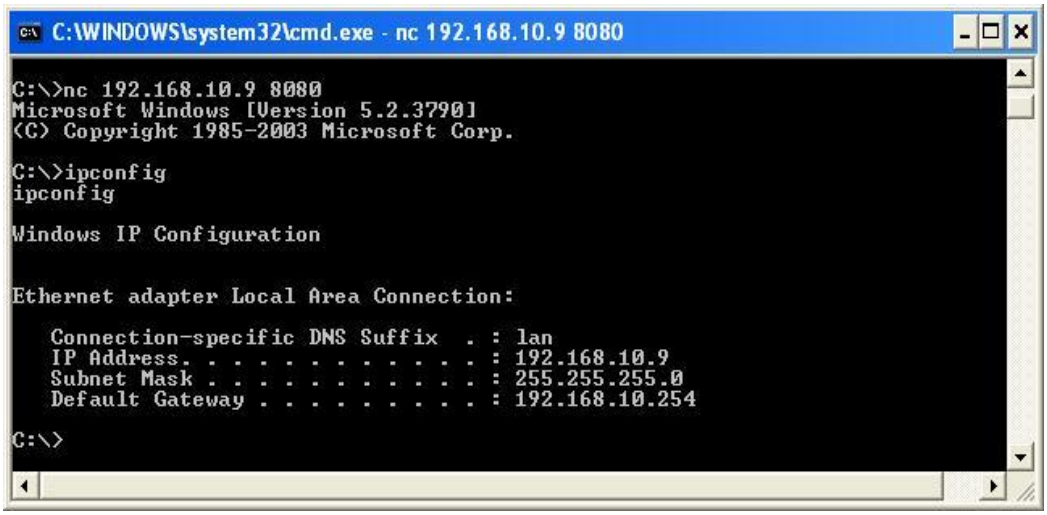
Μία από τις ευκολότερες στην διαμόρφωση πίσω πόρτες ελέγχου από απόσταση χρησιμοποιεί το netcat, το «το πολύ-εργαλείο μαχαίρι του TCP/IP»(δείτε http://en.wikipedia.org/wiki/Netcat). Το netcat μπορεί να διαμορφωθεί ώστε να ακροάζεται μια συγκεκριμένη θύρα και να ξεκινά ένα εκτελέσιμο αρχείο όταν ένα απομακρυσμένο σύστημα συνδέεται μ' αυτήν την θύρα. Ξεκινώντας έναν ακροατή netcat για να χρησιμοποιήσετε ένα κέλυφος εντολών των Windows, αυτό το κέλυφος μπορεί να ανοίξει σε ένα απομακρυσμένο σύστημα. Η σύνταξη για την εκκίνηση του netcat σε μυστική κατάσταση ακρόασης βλέπετε εδώ:

```
C:\TEMP\NC11Windows>nc -L -d -e cmd.exe -p 8080
```



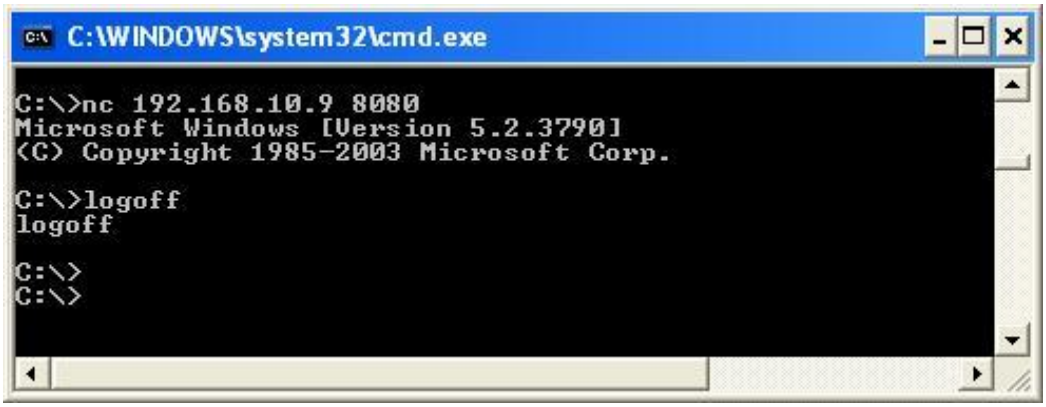
Εικόνα 110:Σύνταξη για την εκκίνηση του netcat.

Το –L κάνει τον ακροατή μόνιμο στην διάρκεια πολλαπλών συνδέσεων, το –d τρέχει το netcat σε κατάσταση μυστικότητας (χωρίς διαλογική κονσόλα) και το –e καθορίζει το πρόγραμμα που θα ξεκινήσει (σ' αυτή την περίπτωση, το cmd.exe, τον διερμηνέα εντολών των Windows). Τέλος, το –p καθορίζει την θύρα ακρόασης. Αυτό θα επιστρέψει ένα απομακρυσμένο κέλυφος εντολών σε οποιονδήποτε εισβολέα συνδεθεί με την θύρα 8080.
Στην επόμενη ακολουθία, χρησιμοποιούμε το netcat σ' ένα απομακρυσμένο σύστημα ώστε να συνδεθούμε με την θύρα ακρόασης του υπολογιστή που είδαμε νωρίτερα (διεύθυνση IP 192.168.10.9) και λαμβάνει ένα απομακρυσμένο κέλυφος εντολών. Για να μειωθεί η σύγχυση, θα πρέπει να ορίσουμε πάλι την προτροπή εντολών στο τοπικό σύστημα C:\> ενώ ή απομακρυσμένη προτροπή είναι C:\TEMP\NC11Windows>.



Εικόνα 111:Σύνδεση σε απομακρυσμένο σύστημα με την θύρα ακρόασης.

Εφόσον το σύστημα μας είναι συνδεδεμένο εκτελούμε την πιο κάτω εντολή Logoff.

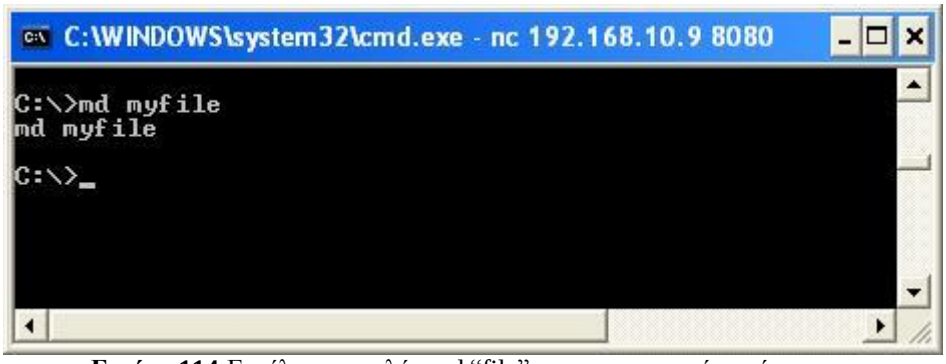


Εικόνα 112:Εκτέλεση εντολής logoff σε απομακρυσμένο σύστημα.

Εμφανίζεται το παράθυρο σύνδεσης για να κάνει ξανά Log in ο χρήστης.

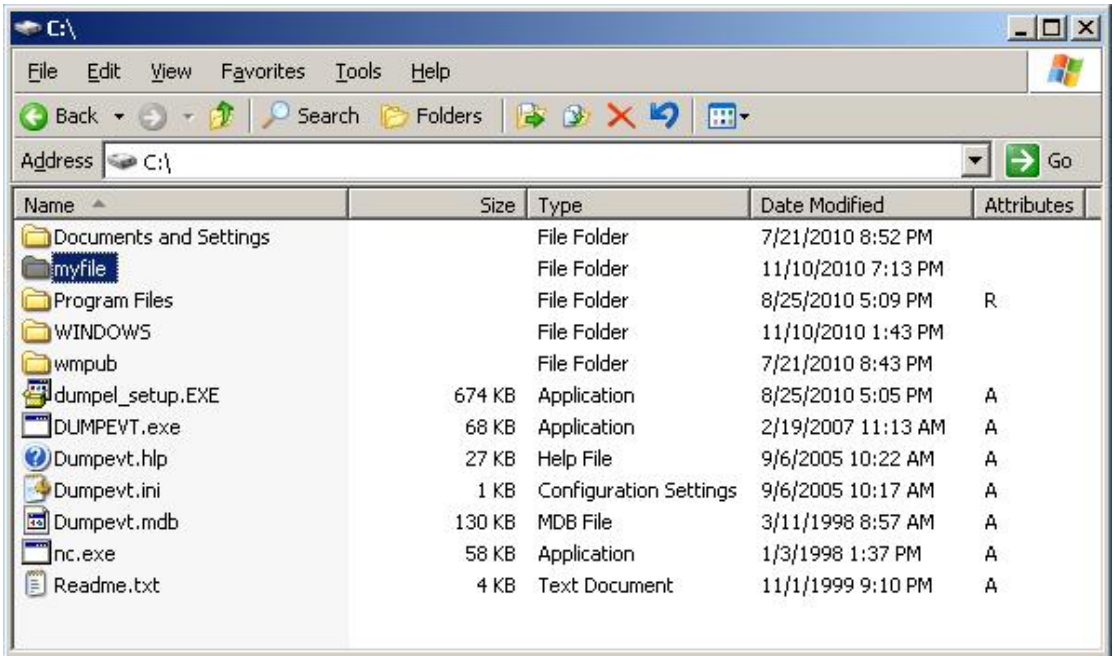
Εικόνα 113:Εμφάνιση της λειτουργίας της εντολής logoff σε απομακρυσμένο σύστημα

Χρήση της εντολής "md[9]" για δημιουργία ενός φακέλου σε ένα απομακρυσμένο σύστημα (myfile).



Εικόνα 114:Εκτέλεση εντολής md "file"σε απομακρυσμένο σύστημα.

Σε αυτό το σημείο βλέπουμε το φάκελο που έχει δημιουργηθεί.

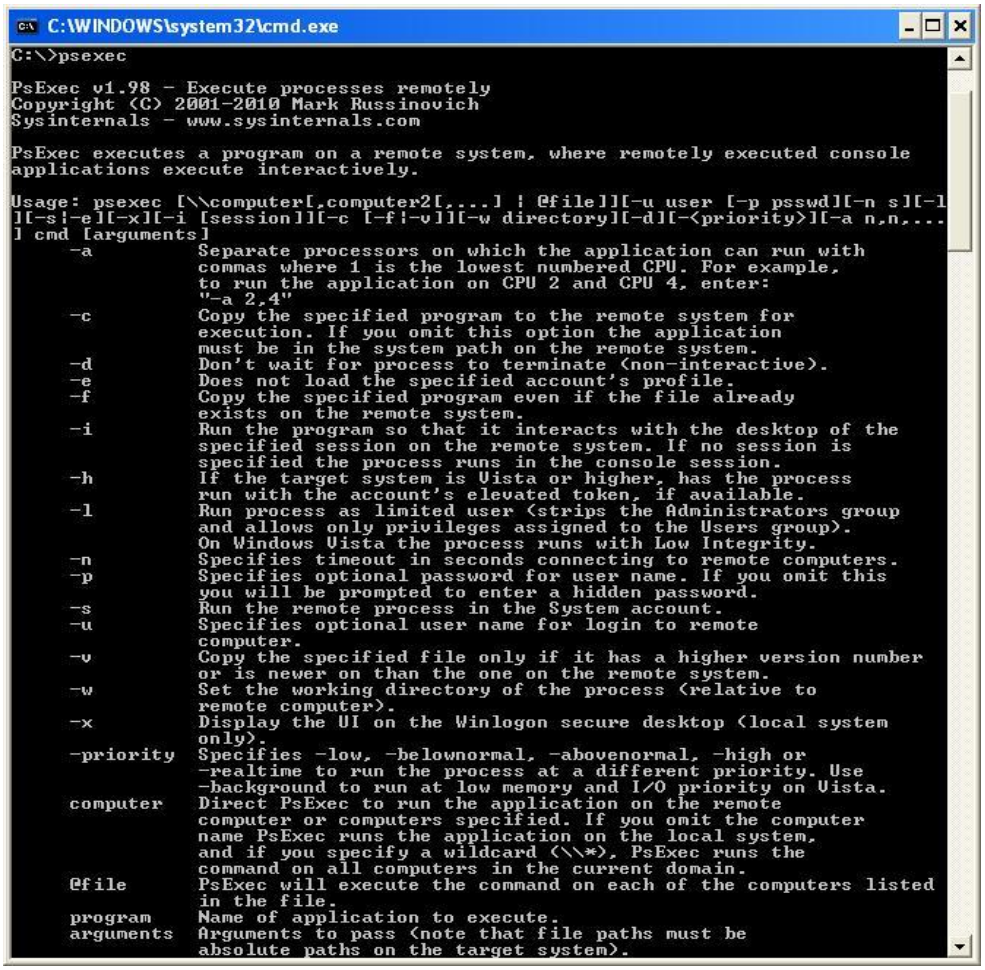


Εικόνα 115:Έλεγχος λειτουργίας της εντολής md.

Όπως μπορούμε να δούμε, οι απομακρυσμένοι χρήστες μπορούν τώρα να εκτελέσουν εντολές και να ξεκινήσουν αρχεία. Είναι περιορισμένοι μόνο από το πόσο δημιουργικοί μπορούν να γίνουν με την κονσόλα των Windows.

Το netcat δουλεύει καλά όταν χρειάζεται μία προσαρμοσμένη θύρα, με τη οποία να μπορείτε να δουλέψετε, αλλά εάν έχετε πρόσβαση στο SMB (TCP θύρα 139 ή 145), το καλύτερο εργαλείο είναι το psexec, από την διεύθυνση http://www.sysinternals.com.

[9] Windows CMD command line http://ss64.com/nt/



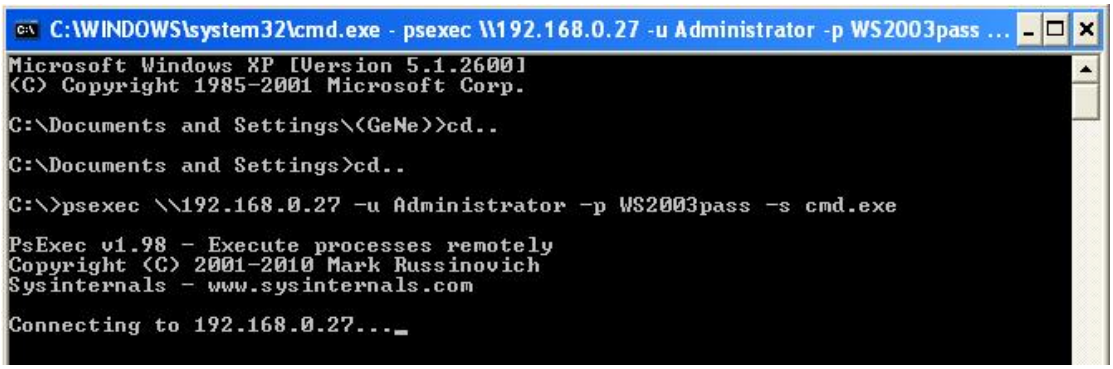
Εικόνα 116:Εντολή psexec.

Το psexec εκτελεί απλώς μία εντολή στον απομακρυσμένο υπολογιστή χρησιμοποιώντας την παρακάτω σύνταξη:

```
C:\>psexec \\server-name-or-ip -u admin_username -p admin_password command
```

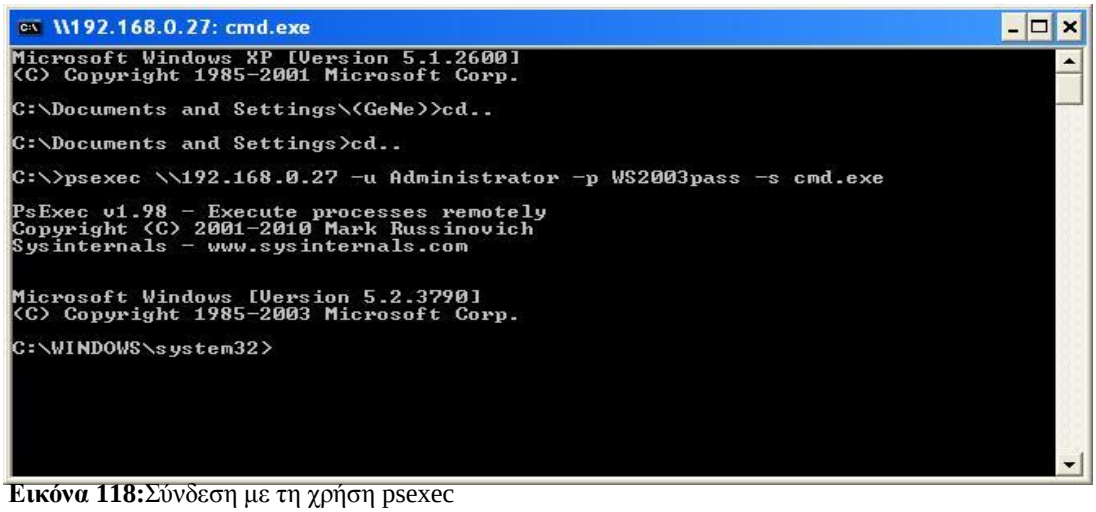
Εδώ βλέπουμε ένα παράδειγμα μιας τυπικής εντολής:

```
C:\>psexec \\192.168.0.27 -u Administrator -p WS2003pass-s cmd.exe
```



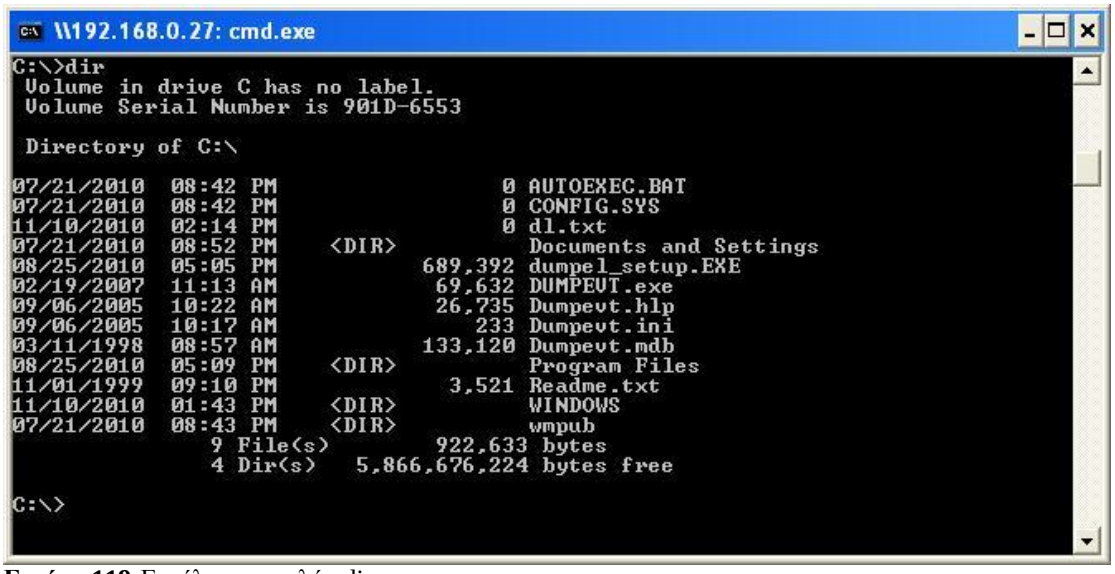
Εικόνα 117:Σύνδεση σε απομακρυσμένο υπολογιστή με τη χρήση του psexec.

Εφόσον συνδεθούμε με το απομακρυσμένο σύστημα μπορούμε να εκτελέσουμε διάφορες εντολές.



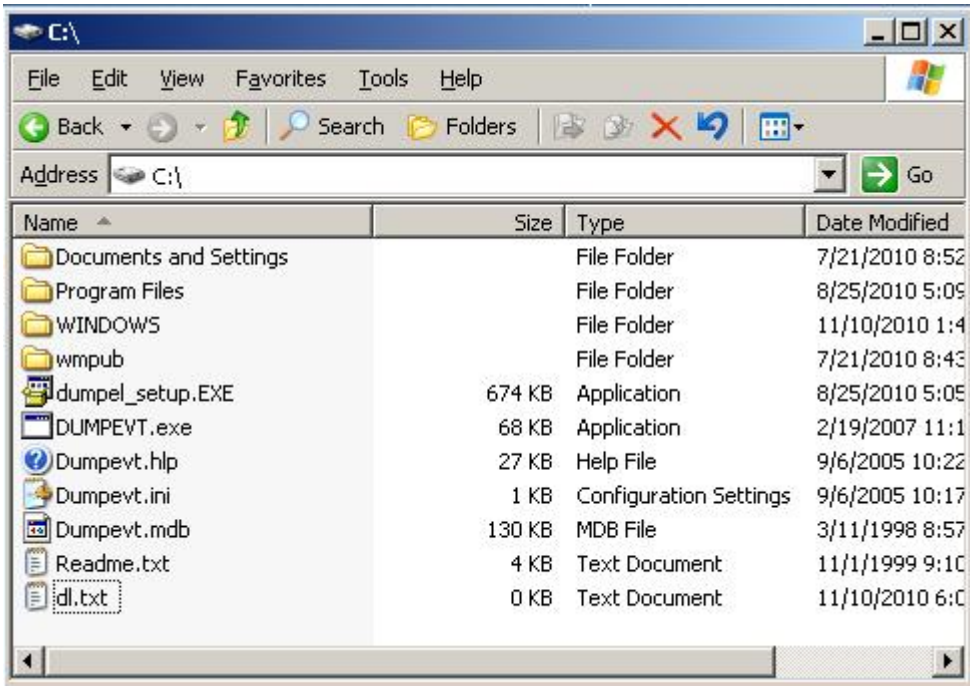
Εικόνα 118:Σύνδεση με τη χρήση psexec

Με την εντολή dir εμφανίζονται τα αρχεία στο Directory C του απομακρυσμένου υπολογιστή μέσω της γραμμής εντολών.



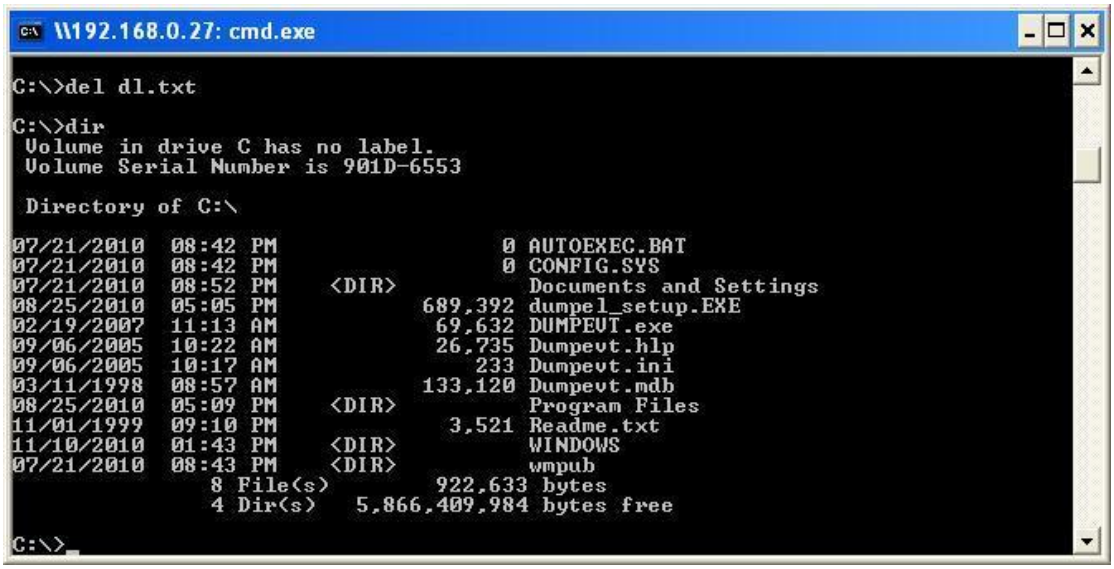
Εικόνα 119:Εκτέλεση εντολής dir

Εμφάνιση αρχείων στο Directory C του απομακρυσμένου υπολογιστή.



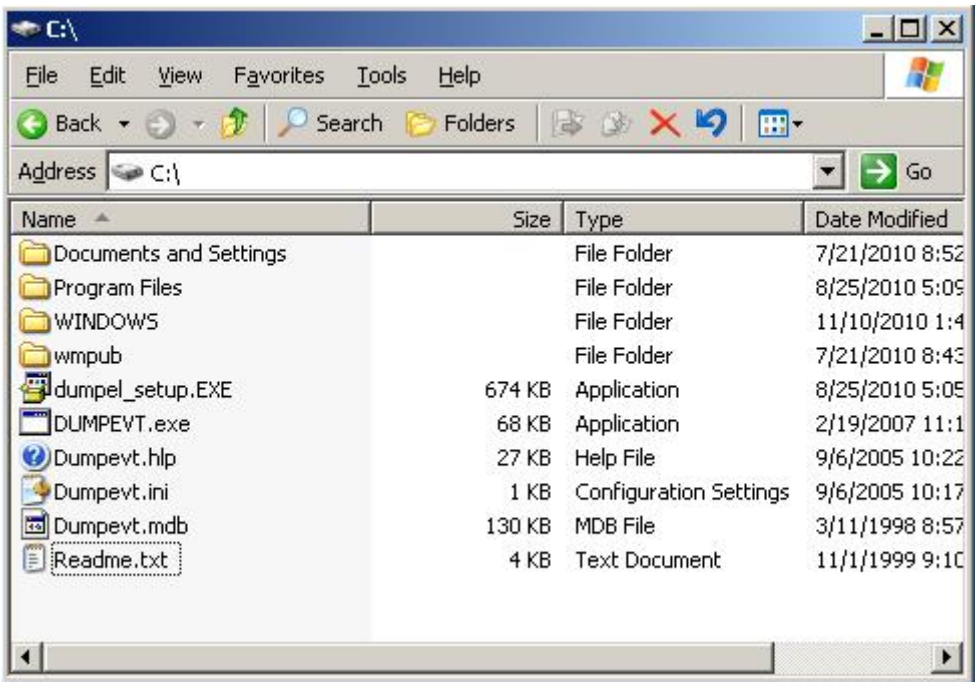
Εικόνα 120:Εμφάνιση αρχείων στο δίσκο C:\.

Εκτέλεση της εντολής del για την διαγραφή του αρχείου dl.txt.



Εικόνα 121:Εκτέλεση της εντολής del.

Παρατηρούμε στο directory ότι το αρχείο έχει διαγραφεί.



Εικόνα 122:Διαγραφή του αρχείου με χρήση της εντολής del.

Δεν γίνεται να είναι τα πράγματα πιο εύκολα από αυτό. Συνηθίσαμε να χρησιμοποιούμε την εντολή AT για να σχεδιάσουμε την εκτέλεση εντολών σε απομακρυσμένα συστήματα, αλλά το psexec κάνει αυτήν την διαδικασία πολύ εύκολη εφόσον έχουμε πρόσβαση στο SMB (το οποίο απαιτεί οπωσδήποτε την εντολή AT).

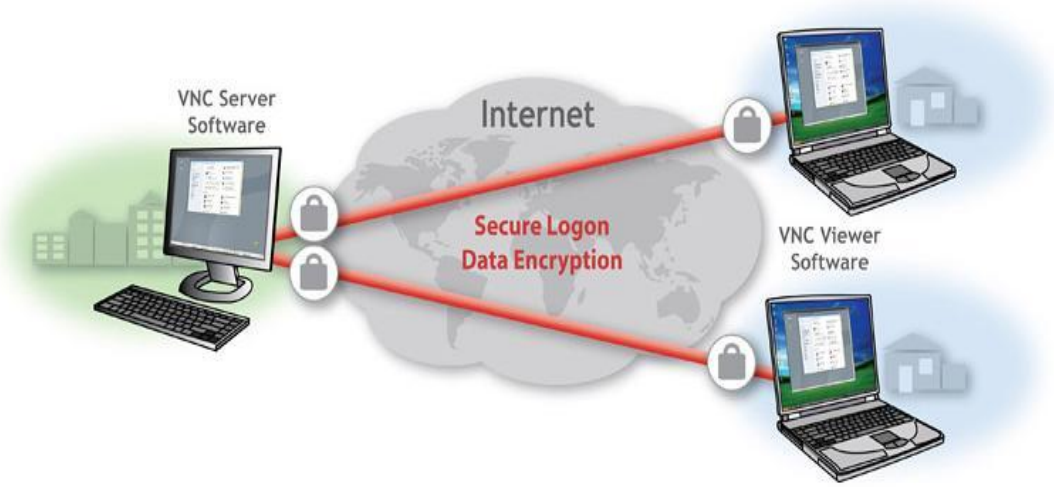
Το πλαίσιο του Metasploit παρέχει επίσης ένα μεγάλο εύρος από δυνατότητες εγκατάστασης μιας πίσω πόρτας που μπορεί να γεννήσει νέα κελύφη γραμμής εντολών που να ακροάζονται θύρες , να εκτελούν αυθαίρετες εντολές, να γεννούν κελύφη χρησιμοποιώντας καθιερωμένες συνδέσεις και να συνδέουν ένα κέφαλος εντολών με τον υπολογιστή του επιτιθέμενου, ώστε να αναφέρουμε απλώς μερικής δυνατότητες. Για επιθέσεις μέσω browser, το Metasploit έχει στοιχεία ελέγχου ActiveX μπορούν να εκτελεσθούν μέσω ενός κρυφού IEXPLORE.exe μέσω HTTP συνδέσεων.

3.3.2 Έλεγχος γραφικού περιβάλλοντος από μακριά

Ένα απομακρυσμένο κέλυφος εντολών είναι ωραίο, αλλά τα Windows είναι γραφικά για αυτό ο έλεγχος μέσω ενός γραφικού περιβάλλοντος από μακριά θα ήταν ειλικρινά κάτι αριστοτεχνικό. Εάν έχετε πρόσβαση στο Terminal Services (που εγκαθίσταται προαιρετικά στα Windows 2000 και νεότερα), μπορεί να έχετε ήδη πρόσβαση στον καλύτερο απομακρυσμένο έλεγχο που προσφέρουν τα Windows. Ελέγξτε ένα η TCP θύρα 3389 ακροάζεται στον απομακρυσμένο διακομιστή και χρησιμοποιήστε

οποιαδήποτε έγκυρα πιστοποιητικά έχετε συλλέξει σε προηγούμενες επιθέσεις για να εισέλθετε στο σύστημα.

Εάν δεν είναι διαθέσιμο το TS, τότε μπορείτε απλώς να εγκαταστήσετε το γραφικό εργαλείο του απομακρυσμένου ελέγχου. Το δωρεάν και εξαιρετικό εργαλείο **Virtual Network Computing**[10] (VNC), από την RealVNC Limited, θα πρέπει να είναι προκειμένω η επιλογή σας

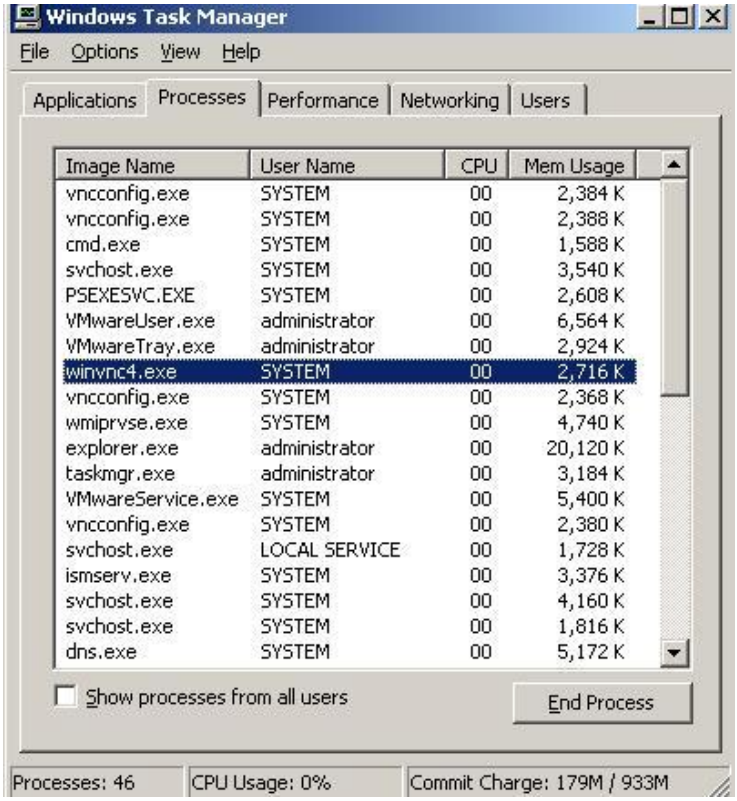


Εικόνα 123: Virtual Network Computing (VNC) RealVNC.

Ένας λόγος που ξεχωρίζει το VNC εκτός του ότι είναι δωρεάν, είναι ότι η εγκατάσταση σε μία απομακρυσμένη σύνδεση δικτύου δεν είναι πολύ δυσκολότερη από την εγκατάσταση τοπικά. Χρησιμοποιώντας ένα απομακρυσμένο κέλυφος εντολών, το μόνο που πρέπει να γίνει είναι να εγκατασταθεί η υπηρεσία VNC και να γίνει μία μόνο αλλαγή στο απομακρυσμένο Registry ώστε να εξασφαλισθεί μία μυστική εκκίνηση της υπηρεσίας. Αυτό που ακολουθεί είναι μία απλουστευμένη εκπαίδευση, αλλά συστήνουμε να δείτε την πλήρη τεκμηρίωση του VNC στο προηγούμενο URL για μία πιο πλήρη κατανόηση της λειτουργίας του VNC από την γραμμή εντολών.

Το πρώτο βήμα είναι να αντιγραφούν τα εκτελέσιμα και απαραίτητα αρχεία του VNC (WINVNC.EXE,VNCHooks.DLL, και OMNITHREAD_RT.DLL) στον διακομιστή-στόχο. Μπορείτε να χρησιμοποιήσετε οποιονδήποτε κατάλογο, αλλά θα είναι πιθανώς πιο δύσκολο να το καταλάβετε εάν είναι κρυμμένο κάπου στο %systemroot%. Ένα άλλο θέμα είναι ότι οι νεότερες εκδόσεις του WINVNC προσθέτουν αυτόματα ένα μικρό πράσινο εικονίδιο στην περιοχή ειδοποιήσεων όταν ξεκινά ο διακομιστής. Εάν οι εκδόσεις που είναι οι ίδιες ή πριν από την 3.2.2 ξεκινήσουν από τη γραμμή εντολών, είναι λίγο-πολύ αόρατες σε χρήστες που συνδέονται διαλογικά. Το WINVNC.EXE εμφανίζεται φυσικά στο Process List.

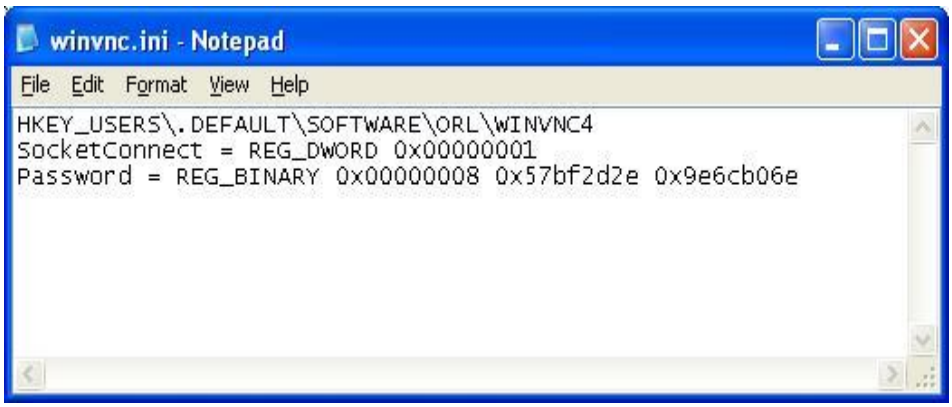
[10] *http://www.realvnc.com/index.html*



Εικόνα 124:Εμφάνιση του winvnc4.exe στο Process List.

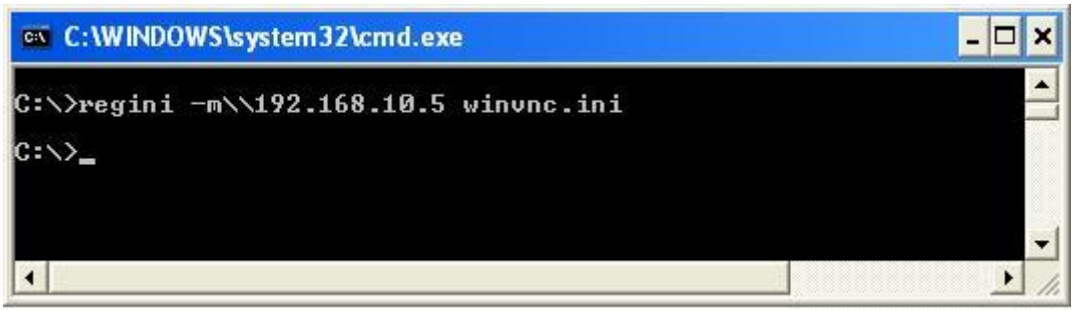
Μόλις αντιγραφεί το WINVNC.EXE, θα πρέπει να ορισθεί ο κωδικός πρόσβασης του VNC. Όταν ξεκινά η υπηρεσία WINVNC, παρουσιάζει κανονικά ένα γραφικό παράθυρο διαλόγου που απαιτεί έναν προσωπικό κωδικό πριν δεχθεί τις εισερχόμενες συνδέσεις. Επιπλέον, πρέπει να πούμε στο WINVNC να παρακολουθεί τις εισερχόμενες συνδέσεις, που επίσης ορίζεται μέσω του γραφικού περιβάλλοντος. Θα προσθέσουμε απλώς τα απαραίτητα στοιχεία κατευθείαν στο απομακρυσμένο Registry χρησιμοποιώντας το regini.exe.

Θα πρέπει να δημιουργήσουμε ένα αρχείο που ονομάζεται WINVNC.INI και να εισάγουμε τις συγκεκριμένες αλλαγές που θέλουμε στο Registry. Εδώ βλέπουμε μερικές τιμές – δείγματα από μία τοπική εγκατάσταση του WINVNC και τα οποία έχουν εξαχθεί σε ένα αρχείο κειμένου χρησιμοποιώντας το βοηθητικό πρόγραμμα regdmp του Resource Kit.



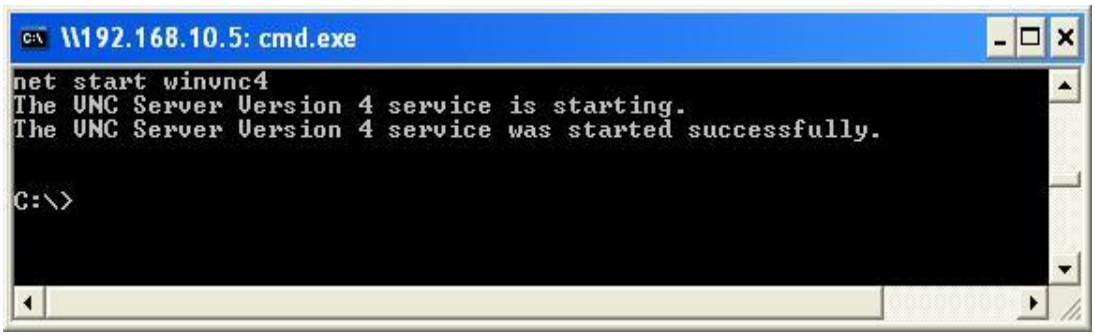
Εικόνα 125:Αρχείο WINVNC.INI.

Έπειτα, φορτώνουμε αυτές τις τιμές στο απομακρυσμένο Registry παρέχοντας το όνομα του αρχείου που περιέχει τα προηγούμενα δεδομένα (το WINVNC.INI) ως είσοδο στο εργαλείο regini:



Εικόνα 126:Φόρτωση τιμών στο εργαλείο regini.

Τέλος, εγκαθιστούμε το WINVNC ως υπηρεσία και την ξεκινούμε. Η παρακάτω απομακρυσμένη σύνοδος εντολών δείχνει την σύνταξη γι' αυτά τα βήματα (είναι ένα κέλυφος εντολών για το απομακρυσμένο σύστημα) :

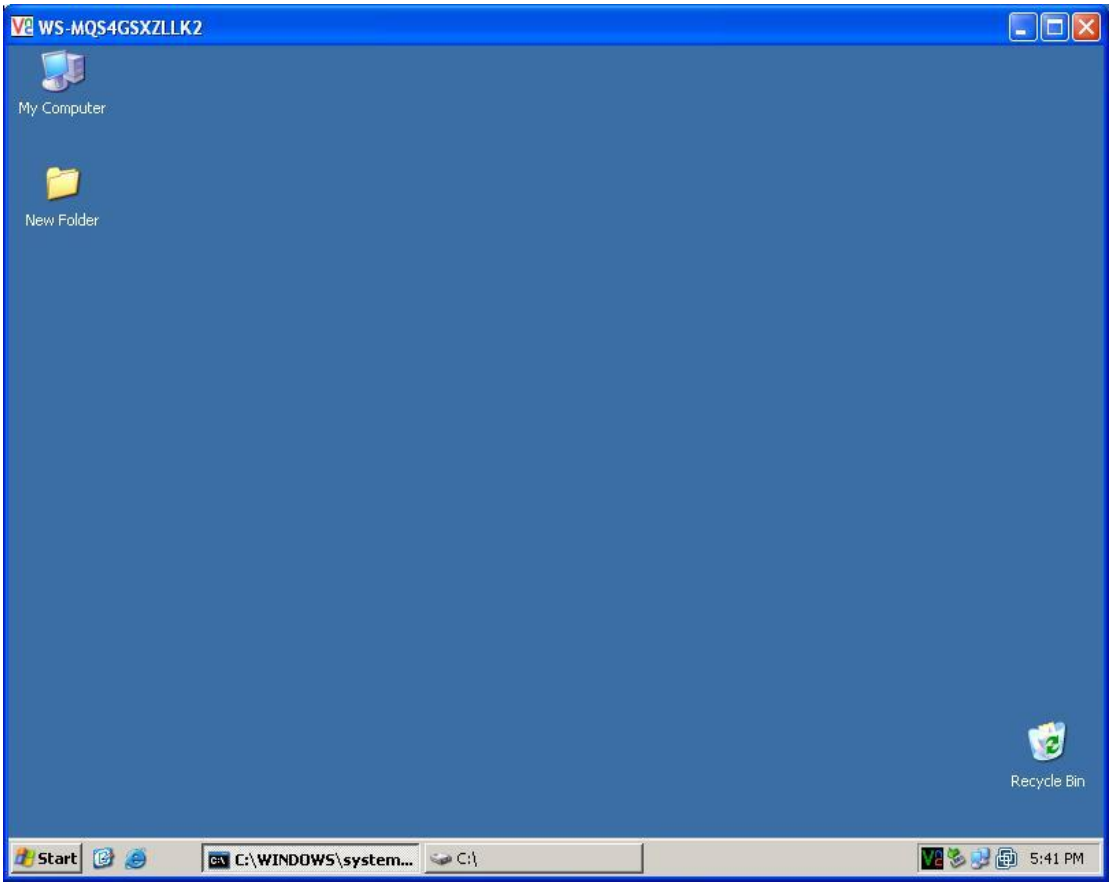


Εικόνα 127:Υπηρεσία WINVNC4 (Start)

Τώρα μπορούμε να ξεκινήσουμε την εφαρμογή vncviewer βάζοντας την IP του στόχου για να συνδεθούμε.

Εικόνα 128: Connection Details-VNC viewer

Η απομακρυσμένη επιφάνεια εργασίας εμφανίζεται σε ζωηρό χρώμα, όπως φαίνεται στην πιο κάτω στην εικόνα. Ο δρομέας του ποντικιού συμπεριφέρεται ακριβώς σαν να βρισκόσασταν στο απομακρυσμένο σύστημα. Το VNC είναι προφανώς πολύ δυνατό – μπορείτε ακόμα να στείλετε και CTRL-ALT-DEL. Οι δυνατότητες είναι ατελείωτες.



Εικόνα 129: Remote connection-winvnc.

Το WINVNC είναι συνδεδεμένο σε ένα απομακρυσμένο σύστημα.

3.4 Ανακατεύθυνση θυρών

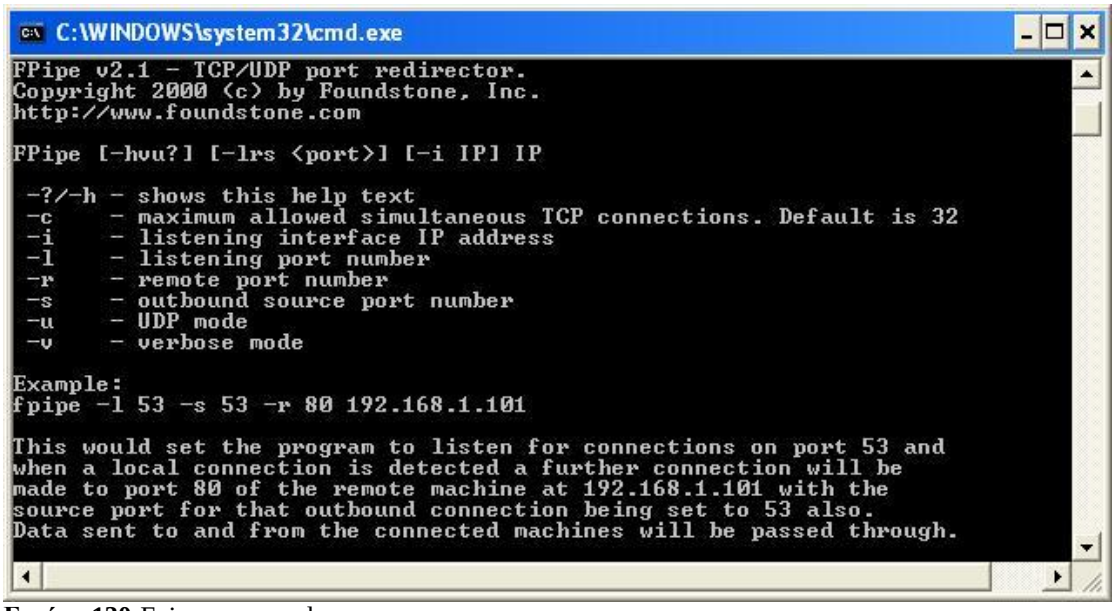
Έχουμε συζητήσει μερικά προγράμματα απομακρυσμένου ελέγχου που βασίζονται σε κέλυφος εντολών υπό το πρίσμα των απευθείας συνδέσεων απομακρυσμένου ελέγχου. Ωστόσο, ας εξετάσουμε την κατάσταση, κατά την οποία μία ενδιάμεση οντότητα, όπως ένα firewall, εμποδίζει την απευθείας πρόσβαση σ' ένα σύστημα – στόχο. Οι πολυμήχανοι επιτιθέμενοι μπορούν να βρουν τρόπους να προσπεράσουν αυτά τα εμπόδια χρησιμοποιώντας *ανακατεύθυνση θυρών*. Η ανακατεύθυνση θυρών είναι μία τεχνική που μπορεί να εφαρμοστεί σε οποιοδήποτε λειτουργικό σύστημα, αλλά θα καλύψουμε εδώ μερικά εργαλεία και τεχνικές που αφορούν στα Windows.

Μόλις οι επιτιθέμενοι μπουν σε ένα κύριο σύστημα, όπως σε ένα firewall, μπορούν να χρησιμοποιήσουν την ανακατεύθυνση θυρών για να προωθήσουν όλα τα πακέτα σε έναν συγκεκριμένο προορισμό. Ο αντίκτυπος αυτού του τύπου της εισβολής είναι σημαντικός, επειδή επιτρέπει στους επιτιθέμενους να έχουν πρόσβαση σε οποιοδήποτε και σε όλα τα συστήματα πίσω από το firewall (ή άλλους στόχους). Η ανακατεύθυνση λειτουργεί παρακολουθώντας ορισμένες θύρες και στέλνοντας τα πακέτα σ' έναν καθορισμένο δευτερεύοντα στόχο. Στην συνέχεια θα συζητήσουμε μερικούς τρόπους διαμόρφωσης ανακατεύθυνσης θυρών χρησιμοποιώντας το εργαλείο fpipe.

3.4.1 Fpipe

Το fpipe είναι ένα TCP εργαλείο προώθησης/ανακατεύθυνσης θύρας προέλευσης και έχει γίνει από την Foundstone, Inc. Μπορεί να δημιουργήσει μία TCP ροή (stream) με μία προαιρετική θύρα προέλευσης της επιλογής του χρήστη. Αυτό είναι χρήσιμο κατά της διάρκεια διείσδυσης, ώστε να περάσει ο επιτιθέμενος τα firewall που επιτρέπουν να περνούν ορισμένες τύπου κινήσεις κατευθείαν στα εσωτερικά τους δίκτυα.

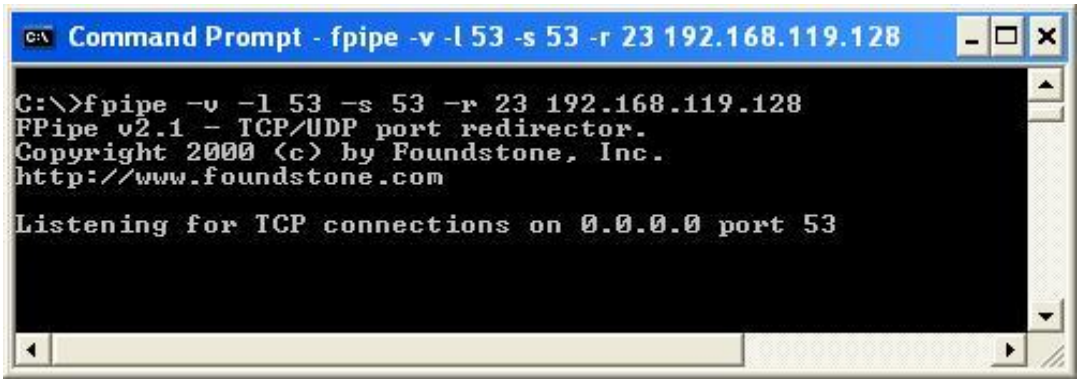
Το fpipe δουλεύει βασικά με ανακατεύθυνση. Ξεκινούμε το fpipe καθορίζοντας μία θύρα ακρόασης στον διακομιστή, μια απομακρυσμένη θύρα προορισμού (η θύρα στην οποία προσπαθούμε να φθάσουμε μέσα στο firewall) και ο (προαιρετικός) τοπικός αριθμός της θύρας προέλευσης που θέλουμε. Όταν ξεκινήσει το fpipe, θα περιμένει έναν πελάτη να συνδεθεί στην θύρα ακρόασης. Όταν γίνει μία σύνδεση ακρόασης , θα γίνει μία νέα σύνδεση στον υπολογιστή και θύρα προορισμού με την καθορισμένη τοπική θύρα προέλευσης, δημιουργώντας κατά συνέπεια ένα πλήρες κύκλωμα. Όταν ορισθεί η πλήρης σύνδεση, το fpipe προωθεί όλα τα δεδομένα που παραλαμβάνονται στην εισερχόμενη σύνδεση του προς την απομακρυσμένη θύρα προορισμού μέσα από το firewall και επιστρέφει την κίνηση με την απόκριση πίσω στο αρχικό σύστημα. Αυτό κάνει την διαμόρφωση πολλαπλών συνόδων στο netcat να μοιάζει πολύ επίμονη. Το fpipe εκτελεί τον ίδιο στόχο πολύ πιο εύκολα.



Εικόνα 130: Fpipe command.

Στην συνέχεια, θα παρουσιάσουμε τη χρήση του fpipe για να διαμορφώσουμε την ανακατεύθυνση σ' ένα σύστημα, στο οποίο έχει γίνει επίθεση που τρέχει έναν διακομιστή Telnet πίσω από ένα firewall που μπλοκάρει την θύρα 23 (Telnet) αλλά αφήνει ελεύθερη την θύρα 53 (DNS). Κανονικά, δεν θα μπορούσαμε να συνδεθούμε με την θύρα Telnet (TCP θύρα 23), αλλά διαμορφώνοντας μία ανακατεύθυνση από το fpipe στον κύριο υπολογιστή, έτσι ώστε να κατευθύνει τις συνδέσεις που λαμβάνει μέσω της TCP θύρας 53 στην θύρα του Telnet, μπορούμε να επιτύχουμε κάτι αντίστοιχο.

Στην πιο κάτω εικόνα δείχνει την ανακατεύθυνση fpipe που τρέχει στον κύριο υπολογιστή.



Εικόνα 131:Ανακατεύθυνση fpipe

Η απλή σύνδεση με την θύρα 53 σ' αυτόν τον κύριο υπολογιστή θα εμφανίσει μία προτροπή Telnet στον επιτιθέμενο.

Η πιο ωραία λειτουργία του fpipe είναι η δυνατότητα του να καθορίζει μία θύρα προέλευσης της κίνησης. Κατά της δοκιμές της εισβολής, αυτό είναι συνήθως απαραίτητο ώστε να παρακάμπτετε ένα firewall ή έναν δρομολογητή που επιτρέπει στην κίνηση να πηγαίνει μόνο σε ορισμένες θύρες. (Για παράδειγμα, η κίνηση που ξεκινά από την TCP 25 μπορεί να μιλήσει στον διακομιστή αλληλογραφίας). Το TCP/IP κανονικά αντιστοιχεί έναν υψηλό αριθμό θύρας προέλευσης σε συνδέσεις πελάτη, τις οποίες γενικά πιάνει ένα firewall στο φίλτρο του. Ωστόσο, το firewall μπορεί να επιτρέψει να περάσει η DNS κίνηση (στην πραγματικότητα, πιθανώς να γίνει). Το fpipe μπορεί να αναγκάσει τη ροή να χρησιμοποιεί πάντα μία συγκεκριμένη θύρα προέλευσης – σ' αυτήν την περίπτωση, την DNS θύρα προέλευσης. Κάνοντας το αυτό, το firewall 'βλέπει' τη ροή ως μία επιτρεπόμενη υπηρεσία και την αφήνει να περάσει.

3.5 Κάλυψη των Ιχνών

Μόλις οι εισβολείς αποκτήσουν δικαιώματα ισοδύναμα με του administrator ή του SYSTEM σε ένα σύστημα θα καταβάλουν προσπάθεια να αποφύγουν τον εντοπισμό της παρουσίας τους . Όταν πάρουν όλες τις πληροφορίες που τους ενδιαφέρουν από το στόχο, θα εγκαταστήσουν διαφορές πίσω πόρτες και να κρύψουν ένα κουτί «εργαλείων» προκειμένου να εξασφαλίσουν ότι θα μπορούν και στο μέλλον να έχουν εύκολες προσβάσεις και ότι θα απαιτηθεί ελάχιστη εργασία για περαιτέρω επιθέσεις σε αλλά συστήματα.

3.5.1 Απενεργοποίηση της Παρακολούθησης Συμβάντων

Εάν ο κάτοχος του συστήματος – στόχου είναι σχετικός γνωστής των θεμάτων ασφάλειας, θα έχει ενεργοποιήσει την παρακολούθηση των συμβάντων (audit), όπως εξηγήσαμε νωρίτερα σε αυτό το κεφάλαιο. Επειδή μπορεί να επιβραδυνθεί η απόδοση των ενεργών διακομιστών, ειδικά εάν παρακολουθείται η επιτυχία ορισμένων λειτουργιών όπως της User & Group Management, οι περισσότεροι διαχειριστές των Windows είτε δεν θα ενεργοποιήσουν την παρακολούθηση των συμβάντων είτε θα

ενεργοποιήσουν μόνο μερικά είδη ελέγχων . Ωστόσο, το πρώτο πράγμα που θα ελέγξουν οι εισβολείς για να αποκτήσουν δικαιώματα Administrator είναι η κατάσταση της πολιτικής Audit στο στόχο, στην σπάνια περίπτωση που παρακολουθούνται οι δραστηριότητες τους που εκτελούνται. Το εργαλείο auditpol του Resource kit το κάνει αυτό πολύ εύκολα.

Το επόμενο παράδειγμα δείχνουμε το auditpol που τρέχει με το όρισμα disable για να απενεργοποιήσει την παρακολούθηση σε ένα απομακρυσμένο σύστημα (συντομευμένη έξοδος) :

Εικόνα 132:Απενεργοποίηση της παρακολούθησης σε ένα σύστημα

Στο τέλος της παραμονής τους, οι εισβολείς θα ενεργοποιήσουν απλώς πάλι την παρακολούθηση χρησιμοποιώντας το διακόπτη auditpol/enable και όλα θα είναι καλά. Οι διάφορες μεμονωμένες ρυθμίσεις της παρακολούθησης διατηρούνται από το auditpol.

3.5.2 Εκκαθάριση του Αρχείου Καταγραφής Συμβάντων

Εάν διάφορες δραστηριότητες που οδηγούν στην απόκτηση δικαιωμάτων Administrator έχουν αφήσει ήδη αποκαλυπτικά ίχνη στο Windows Event Log, οι εισβολείς μπορούν απλώς να καθαρίσουν τα αρχεία καταγραφής με το Event Viewer. Ενώ έχουν ήδη πιστοποιηθεί στον κύριο υπολογιστή – στόχο, το Event Viewer στον κύριο υπολογιστή των επιτιθέμενων μπορεί να ανοίξει, να διαβαστεί και να καθαρίσουν οι καταχωρίσεις του απομακρυσμένου κύριου υπολογιστή. Αυτή η διαδικασία θα καθαρίσει την καταγραφή όλων των εγγράφων αλλά θα αφήσει μία νέα εγγραφή που θα λέει ότι το Event Log έχει καθαρίσει από τον «επιτιθέμενο». Φυσικά, αυτό μπορεί να προκαλέσει περισσότερες ανησυχίες στους χρήστες του συστήματος, αλλά υπάρχουν διαθέσιμες κάποιες άλλες επιλογές εκτός από την αλλαγή με το χέρι τον διαφόρων αρχείων καταγραφής που είναι στο \winnt\system32, κάτι δεν συστήνετε λόγο της σύνθετης σύνταξης των αρχείων καταγραφής των Windows.

Το βοηθητικό πρόγραμμα elsave από τον Jesper Laurutsen (http://www.ibt.ku.dk/jesper/ELSave/) είναι ένα απλό εργαλείο για καθαρισμό του Event Log . Για παράδειγμα η παρακάτω σύνταξη του elsave θα καθαρίσει το Security Log στον απομακρυσμένο διακομιστή Joel (Σημειώστε ότι απαιτούνται σωστά δικαιώματα στο απομακρυσμένο σύστημα).

```
C:\> elsave -s \\joel -l "security" -c
```

3.5.3 Απόκρυψη Αρχείων

Η αποθήκευση μιας συλλογής εργαλείων στο σύστημα-στόχο για μετέπειτα χρήση αποτελεί μεγάλη εξοικονόμηση χρόνου για κακόβουλους hacker. Ωστόσο, αυτές οι μικρές συλλογές με βοηθητικά προγράμματα μπορούν επίσης να προειδοποιήσουν τους προσεκτικούς διαχειριστές για την παρουσία ενός εισβολέα. Επομένως, θα μπορούν να λάβουν μέτρα για να κρυφθούν τα διάφορα αρχεία τα οποία είναι απαραίτητα για να ξεκινήσει η επόμενη επίθεση.

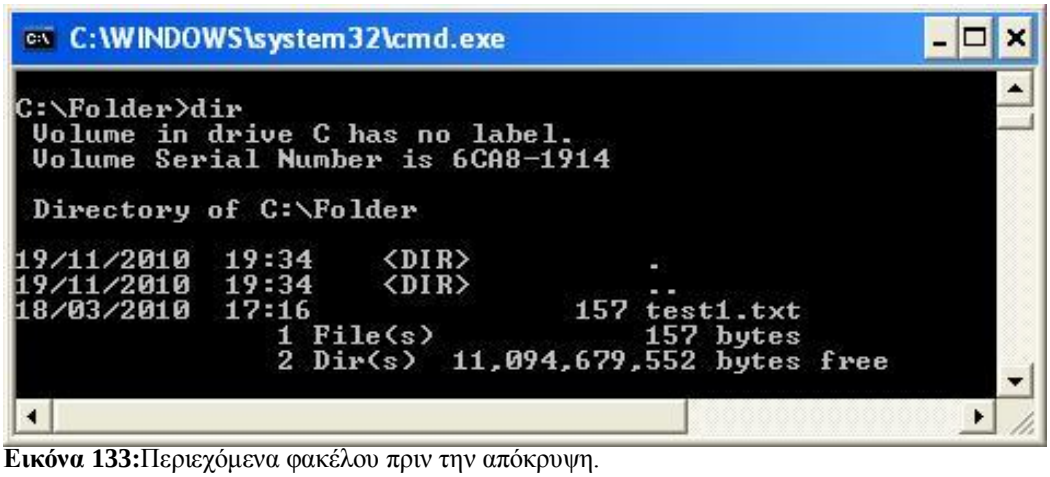
Attrib

Η απόκρυψη αρχείων απαιτεί την αντιγραφή τους σε ένα κατάλογο και την χρησιμοποίηση του παλαιού εργαλείου attrib του DOS για απόκρυψή τους, όπως φαίνεται στην παρακάτω σύνταξη :

attrib +h [directory]

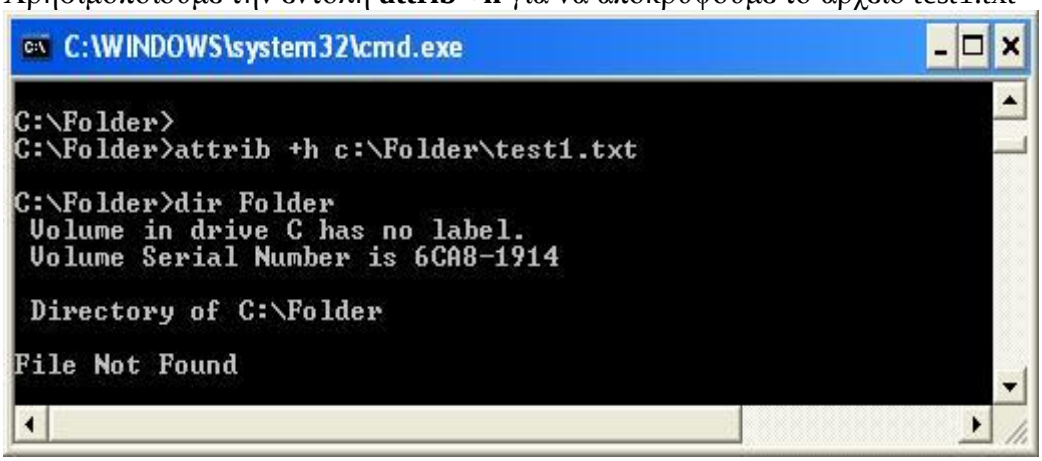
Αυτό κρύβει αρχεία και καταλόγους από εργαλεία της γραμμής εντολών, αλλά δεν τα κρύβει εάν επιλεχθεί το show All Files (εμφάνιση όλων των αρχείων) στον Windows Explorer.

Πρώτα εμφανίζουμε όλα τα αρχεία για να δούμε τι υπάρχει στον φάκελο.



Εικόνα 133:Περιεχόμενα φακέλου πριν την απόκρυψη.

Χρησιμοποιούμε την εντολή **attrib +h** για να αποκρύψουμε το αρχείο test1.txt



Εικόνα 134:Εκτέλεση της εντολής attrib +h για την απόκρυψη αρχείου.

Εφόσον το αρχείο έχει αποκρυφτεί, ελέγχουμε ξανά τον φάκελο για να το επιβεβαιώσουμε.

3.5.4 Εναλλακτικές Ροές Δεδομένων (Alternate data Streams-ADS)

Εάν το σύστημα – στόχο τρέχει το Windows File System (NTFS), είναι διαθέσιμη για τους εισβολείς μία εναλλακτική τεχνική απόκρυψης αρχείων. Το NTFS προσφέρει υποστήριξη για πολλαπλές ροές πληροφοριών μέσα σε ένα αρχείο. Η λειτουργία ροής του NTFS αναφέρεται από τη Microsoft ως «ένας μηχανισμός για προσθήκη προσθέτως ιδιοτήτων ή πληροφοριών σε ένα αρχείων» (π.χ. όταν είναι ενεργοποιημένες στα Windows λειτουργίες συμβατότητας με αρχεία Macintosh). Μπορεί επίσης να χρησιμοποιηθεί για να κρύψει το σύνολο εργαλείων ενός κακόβουλου haker (ονομάστε το αυτό adminkit)- σε ροές πίσω από αρχεία.

Στο παρακάτω παράδειγμα θα χρησιμοποιήσει το netcat.exe πίσω από ένα γενικό αρχείο που βρίσκεται στον κατάλογο winnt\system32\os2, ώστε μπορεί να χρησιμοποιηθεί σε επόμενες επιθέσεις σε άλλα απομακρυσμένα συστήματα. Αυτό το αρχείο επιλέχτηκε για την σχετική ασάφεια του, αλλά θα μπορούσε να χρησιμοποιηθεί οπουδήποτε αρχείο. Για αρχεία συνεχούς ροής, ένας επιτιθέμενος θα χρειαστεί το POSIX[11] βοηθητικό πρόγραμμα cp από το Resource Kit. Η σύνταξη είναι απλή, χρησιμοποιώντας μία άνω και κάτω τελεία στο αρχείο προορισμού για να καθορισθεί η ροή :

```
C:\>cp  <file> oso001.009: <file>
```

Εδώ βλέπετε ένα παράδειγμα :

```
C:\>cp nc so001.009:<file>: nc.exe
```

Αυτό κρύβει το nc.exe στη ροή nc.exe του oso001.009. Εδώ βλέπουμε πώς να αναλύσουμε την ροή του netcat :

```
C:\ cp oso001.009 :nc.exe nc.exe
```

Η ημερομηνία τροποποίησης του oso001.009 αλλάζει, αλλά όχι και το μέγεθός του. (Μερικές εκδώσεις του cp μπορεί να μην αλλάξουν την ημερομηνία του αρχείου). Επομένως, τα κρυφά αρχεία ροής είναι πολύ δύσκολο να εντοπισθούν.

Η διαγραφή ενός αρχείου ροής περιλαμβάνει την αντιγραφή του "εμπρός" αρχείου σε ένα διαμέρισμα FAT και μετά την αντιγραφή του ξανά στο NTFS.

Τα αρχεία ροής μπορούν να εκτελούνται ενώ κρύβονται πίσω από το "εμπρός" μέρος τους. Λόγω των περιορισμών του cmd.exe, τα αρχεία ροής δεν μπορούν να εκτελούνται κατευθείαν (δηλ., το oso001.009: nc.exe). Αντίθετα, θα προσπαθήσουμε να χρησιμοποιήσουμε την εντολή start για να εκτελέσουμε το αρχείο :

---

[11] http://homepages.cwi.nl/~aeb/linux/man2html/man1/cp.1.html

Start oso001.009: nc.exe

3.5.4.a Αντίμετρο για το ADS

Ένα εργαλείο για εύρεση αρχείων ροής NTFS είναι το sfind της Foundstone[12].

Rootkits

Οι στοιχειώδεις τεχνικές που μόλις περιγράψαμε αρκούν για να αποφύγουμε τον εντοπισμό από σχετικά απλούς μηχανισμούς. Ωστόσο αρχίζουν να εμφανίζονται πιο δόλιες τεχνικές, ειδικά η χρήση των Windows rootkits. Αν και ο όρος ξεκίνησε απλό το UNIX (όπου το «root» είναι λογισμικό του souperuser), ο κόσμος των Windows rootkit έχει περάσει μία περίοδο αναγέννησης τα τελευταία χρόνια. Το ενδιαφέρον για τα Windows rootkit ξεκίνησε από τον Greg Hoglund, ο οποίος παρήγαγε ένα από τα πρώτα βοηθητικά προγράμματα που περιγράφηκαν και ως «NT rootkit» το 1999 (αν και φυσικά υπήρχαν πολύ πριν πολλά άλλα εργαλεία εκκαθάρισης για συστήματα των Windows, χρησιμοποιώντας προσαρμοσμένα εργαλεία και διάφορα δημόσια προγράμματα). Το αρχείο rootkit του Hoglund ήταν ουσιαστικά μία πλατφόρμα για επεξήγηση της ιδέας της εναλλαγής προστατευμένων προγραμμάτων στη μνήμη (“επιδιόρθωση του πυρήνα σε τεχνική ορολογία) , ώστε να φύγει τελείως η εμπιστοσύνη προς το λειτουργικό σύστημα.

3.6 Γενικά αντίμετρα για πιστοποιημένη παραβίαση

Επειδή πολλά κενά δημιουργήθηκαν με δικαιώματα διαχειριστή σχεδόν σε όλες τις πτυχές της αρχιτεκτονικής των Windows και οι περισσότερες από αυτές τις τεχνικές μπορούν να μεταμφιεστούν για να εργάζονται με σχεδόν απεριόριστους τρόπους, ο στόχος αυτός είναι δύσκολος. Προσφέρουμε τις παρακάτω γενικές συμβουλές, που καλύπτουν τέσσερις κύριες περιοχές που αγγίζουν με κάποιο τρόπο τις διαδικασίες που μόλις περιγράψαμε :ονόματα αρχείων , κλειδιά Registry , διαδικασίες και θύρες.

3.6.1 Ονόματα Αρχείων

Οποιοσδήποτε ευφυής εισβολέας με σχετικές γνώσεις θα μετονομάσει αρχεία ή θα λάβει άλλα μέτρα για να τα κρύψει (δείτε την προηγούμενη ενότητα «Κάλυψη των Ιχνών»), αλλά η αναζήτηση αρχείων με ύποπτα ονόματα μπορεί να πιάσει μερικούς εισβολείς (τους λιγότερο δημιουργικούς) στα συστήματα μας.

Έχουμε καλύψει πολλά εργαλεία που χρησιμοποιούνται συνήθως σε δραστηριότητες μετά την εισβολή, συμπεριλαμβανομένων των nc.exe(netcat), psexec.exe, winvnc.exe, VNCHooks.dll, omnithread_rt.dll, fpipe.exe, firedaemon.exe ,srvany.exe psexec.exe. Μια άλλη συνηθισμένη τεχνική είναι να αντιγράψετε το κέλυφος εντολών των Windows (cmd.exe) σε διάφορες θέσεις στον δίσκο και με διαφορετικά ονόματα – Δείτε το root.exe, sensepost.exe και αρχεία με παρόμοια ονόματα διαφορετικών μεγεθών από το πραγματικό cmd.exe (επισκεφτείτε τη σελίδα http://www.file.net για να επαληθεύσετε πληροφορίες σχετικά με συνηθισμένα αρχεία του λειτουργικού συστήματος όπως το cmd.exe).

[12] www.foundstone.com

Επίσης να υποψιαστούμε οποιαδήποτε αρχεία που υπάρχουν σε διάφορους καταλόγους
Start Menu\PROGRAMS\STARTUP\%username% κάτω από το %SYSTEMROOT% \PROFILES. Οτιδήποτε υπάρχει σε αυτούς τους φακέλους θα ξεκινήσει κατά την εκκίνηση.

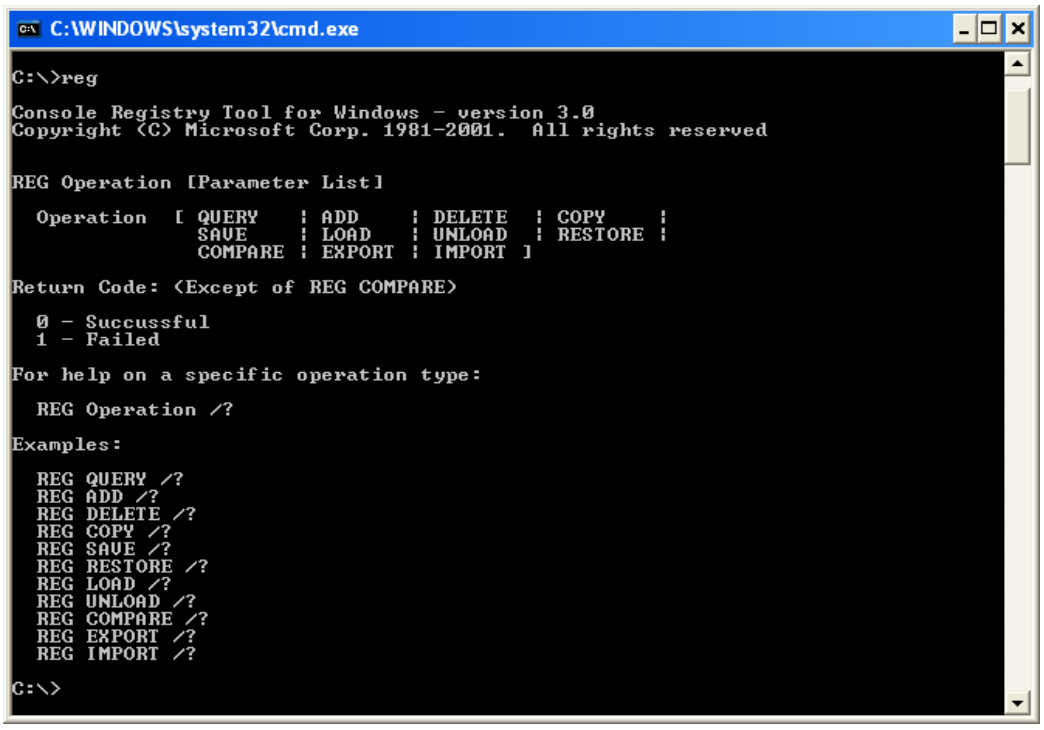
Ένας από τους κλασικούς μηχανισμούς να εντοπίσουμε και να παρεμποδίσουμε την ύπαρξη κακόβουλων αρχείων το σύστημα μας είναι να χρησιμοποιήσουμε κάποιο αντιβιοτικό λογισμικό και συστήνουμε έντονα να υπάρχει ειδικό λογισμικό για antimalware ή κάποια παρόμοια υποδομή στην επιχείρησή μας (ναι, ακόμη και στο κέντρο δεδομένων διακομιστών).

3.6.2 Καταχωρίσεις στο Registry

Σε αντίθεση της αναζήτησης αρχείων που μετονομάζονται εύκολα, η αναζήτηση ψεύτικων τιμών στο Registry μπορεί να είναι αρκετά αποτελεσματική, επειδή οι περισσότερες από τις εφαρμογές που συζητήσαμε περιμένουν να δουν και συγκεκριμένες τιμές σε συγκεκριμένες θέσεις . Ένα καλό μέρος να ξεκινήσουμε είναι το HKLM\SOFTWARE και το HKEY_USER\.DEFAULT\software, όπου βρίσκονται οι περισσότερες εγκατεστημένες εφαρμογές στο Windows Registry. Όπως έχουμε δει, δημοφιλή προγράμματα απομακρυσμένου έλεγχου , όπως το WINVNC, δημιουργούν αντίστοιχα κλειδιά κάτω από αυτούς τους κλάδους του Registry :

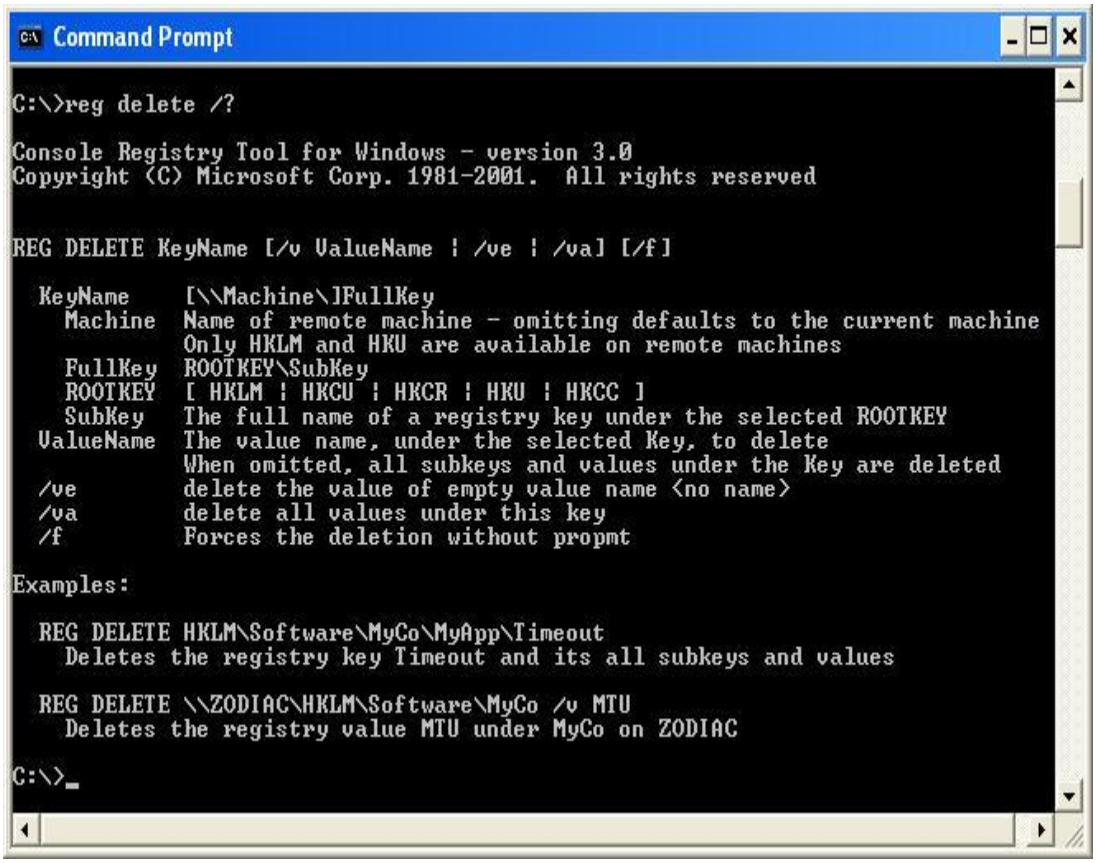
HKEY_USERS\.DEFAULT\Software\ORL\WINVNC4

Η χρησιμοποίηση του εργαλείου REG.exe της γραμμής εντολών από το Resource Kit, κάνει εύκολη την διαγραφή αυτών των κλειδιών , ακόμα και σε απομακρυσμένα συστήματα.



Εικόνα 135:Εντολές REG.exe

Η σύνταξη είναι reg delete [value] \\machine



Εικόνα 136:Εντολή reg delete

Εδώ βλέπουμε ένα παράδειγμα :

```
C:\> reg delete HKEY_USERS\.DEFAULT\Software\ORL\WinVNC4
\\192.168.202.33
```

Autostart Extensibility Points (ASEPs)

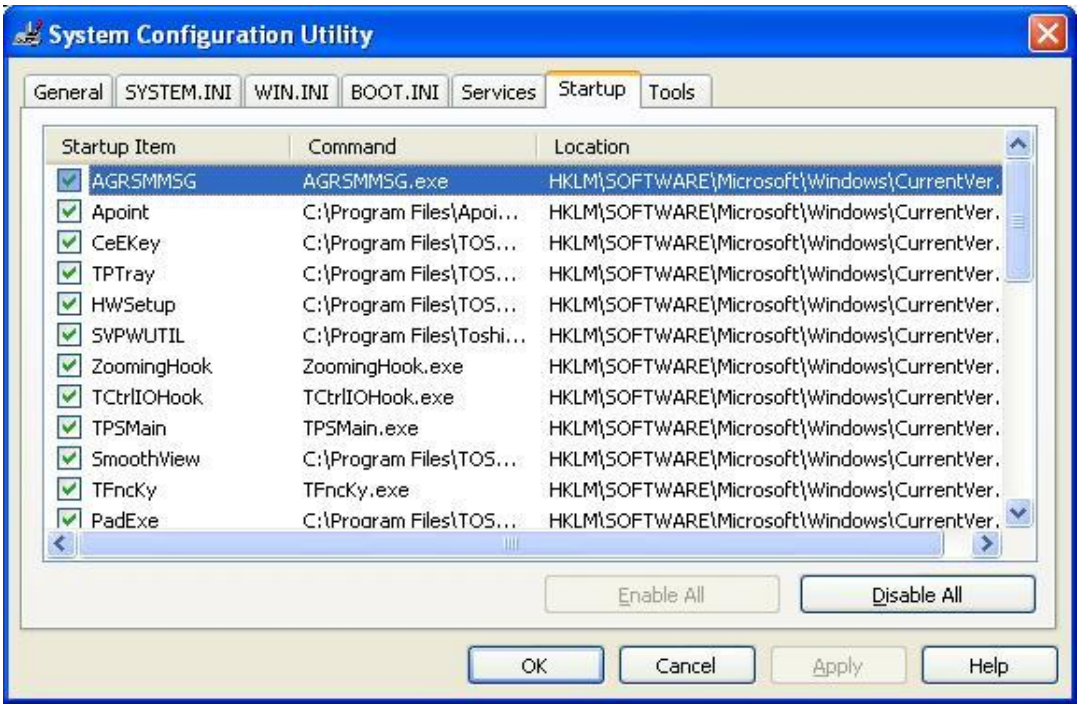
Οι επιτιθέμενοι σχεδόν πάντα βάζουν τις απαραίτητες τιμές του Registry κάτω από τα τυπικά κλειδιά εκκίνησης των Windows. Αυτές οι περιοχές θα πρέπει να ελέγχονται τακτικά για την παρουσία κακόβουλων εντολών ή παράξενων εντολών. Ως υπενθύμιση, αυτές οι περιοχές είναι το HKLM\SOFTWARE|Microsoft\Windows\CurrentVersion\Run και τα RunOnce, RunOnceEx και RunServices (μόνο στα Win 9x).

Επιπλέον, τα δικαιώματα πρόσβασης των χρηστών σε αυτά τα κλειδιά θα πρέπει να περιοριστούν. Εξ ορισμού , η ομάδα everyone των Windows έχει δικαιώματα Set Value στο HKLM\..\..\Run. Αυτό θα πρέπει να απενεργοποιηθεί χρησιμοποιώντας την ρύθμιση Security | Permissions στο regedt32.

Δεν πρέπει να ξεχνούμε να ελέγχουμε τους καταλόγους %systemroot%\profiles\%username%\Start Menu\programs\startup\ .Τα αρχεία εδώ ξεκινούν επίσης αυτόματα σε κάθε σύνδεση αυτού του χρήστη.

Η Microsoft έχει αρχίσει να μεταφέρεται στη γενική κλάση των θέσεων που επιτρέπουν την συμπεριφορά της αυτόματης εκκίνησης (autostart) ως autostart extensibility points-ASEP (σημεία επεκτασιμότητας αυτόματης εκκίνησης). Σχεδόν κάθε σημαντικό τμήμα κακόβουλου λογισμικού που είναι γνωστό σήμερα έχει χρησιμοποιήσει ASEP για να διαιωνίσει τις μολύνσεις στα Windows.

Μπορούμε επίσης να τρέξουμε το βοηθητικό πρόγραμμα msconfig για να δούμε μερικούς από αυτούς τους άλλους μηχανισμούς εκκίνησης στην καρτέλα startup (αν και η διαμόρφωση της συμπεριφοράς αυτού του εργαλείου μας αναγκάζει να βάλουμε το σύστημα σε επιλεκτική κατάσταση εκκίνησης).

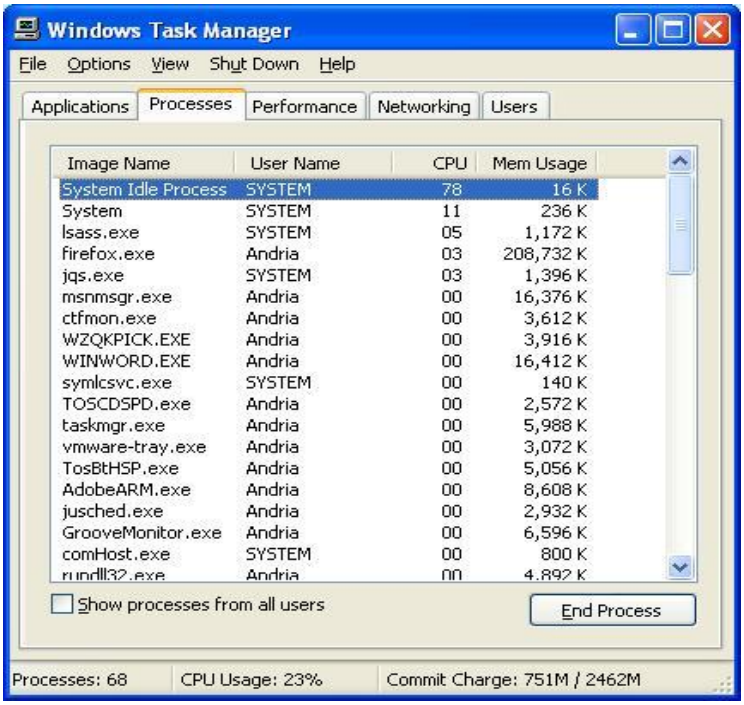


Εικόνα 137:Πρόγραμμα msconfig-Διαμόρφωση startup

3.6.3 Διεργασίες

Για αυτά τα εκτελέσιμα εργαλεία που δεν μπορούν να μετονομαστούν ή με άλλο τρόπο να ξεπακεταριστούν, μπορεί να είναι χρήσιμη η τακτική ανάλυση του Process List.

Απλώς πατάμε CTRL-DHIFT-ESC ώστε να δούμε τη λίστα των διεργασιών. Θέλουμε να ταξινομήσουμε τη λίστα ως προς τη στήλη CPU και κάνουμε κλικ σε αυτή τη στήλη, οπότε θα δείτε κάθε διεργασία σε προτεραιότητα ως προς το πόσο CPU χρησιμοποιεί.

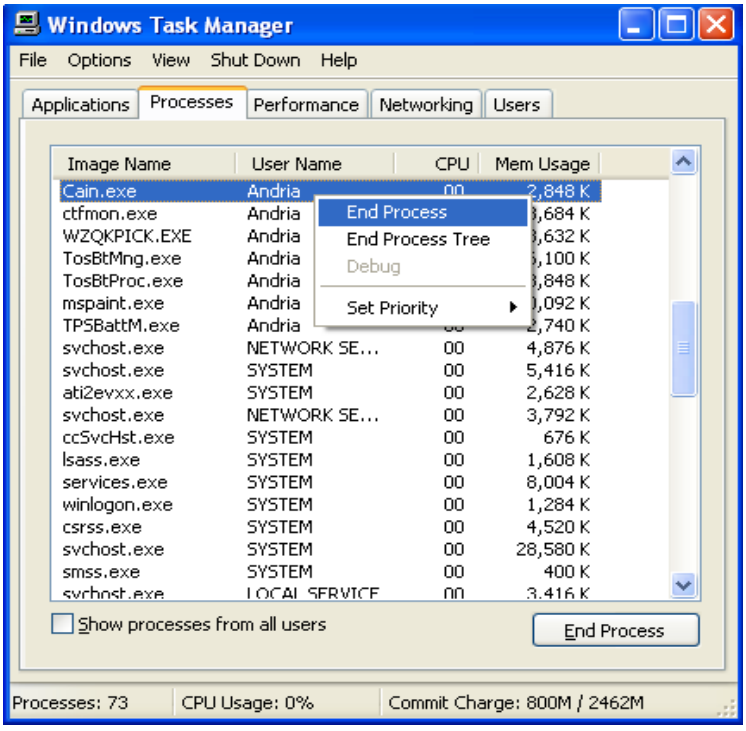


Εικόνα 138: Windows Task Manager-Processes

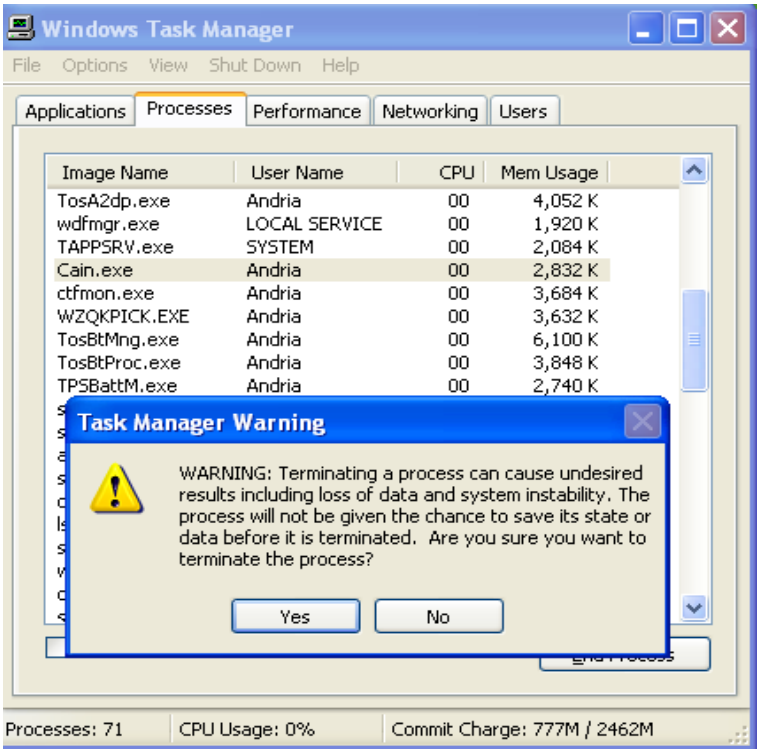
Γενικά μια κακόβουλη διαδικασία θα συμμετέχει σε κάποια διεργασία , έτσι θα βρίσκεται κοντά στην κορυφή της λίστας.

Εάν προσδιορίσουμε κάτι που δεν θα πρέπει να υπάρχει , μπορούμε να κάνουμε δεξί κλικ σε οποιεσδήποτε κακόβουλες διεργασίες και να επιλέξουμε End Process(Τέλος διεργασίας).

Παράδειγμα τερματισμού διεργασίας – Cain.



Εικόνα 139: Windows Task Manager-End Process(a)



Εικόνα 140: Windows Task Manager-End Process(b)

Μπορούμε επίσης να χρησιμοποιήσουμε το βοηθητικό πρόγραμμα Resource Kit kill.exe για να σταματήσουμε οποιεσδήποτε κακόβουλες διεργασίες που δεν αποκρίνονται στο γραφικό βοηθητικό πρόγραμμα της λίστας των διεργασιών. Το Resource Kit rkill.exe μπορεί να χρησιμοποιηθεί ώστε να το τρέξει αυτό σε απομακρυσμένους διακομιστείς ενός τομέα χρησιμοποιώντας παρόμοια σύνταξη, αν και το ID(PID) της κακόβουλης διεργασίας θα πρέπει να είναι πρώτο. Για παράδειγμα, χρησιμοποιώντας το βοηθητικό πρόγραμμα pulist.exe από το Resource kit. Ένα σωστό σύστημα θα μπορούσε να διαμορφωθεί ώστε το pulist να τρέχει τακτικά και να ψάχνει για περίεργες συμβολοσειρές, οι οποίες να τροφοδοτούνται μετά στο rkill. Φυσικά, για άλλη μία φορά, όλη αυτή η εργασία μπορεί να αντιμετωπιστεί κοινότοπα μετονομάζοντας τα κακόβουλα εκτελέσιμα αρχεία σε κάτι αβλαβές όπως WINLOG.EXE, αλλά μπορεί να είναι αποτελεσματική σε διεργασίες που δεν μπορούν να κρυφτούν, όπως το WINVNC.exe, αλλά μπορεί να είναι αποτελεσματική σε διεργασίες που δεν μπορούν να κρυφτούν, όπως το WINVNC.exe.

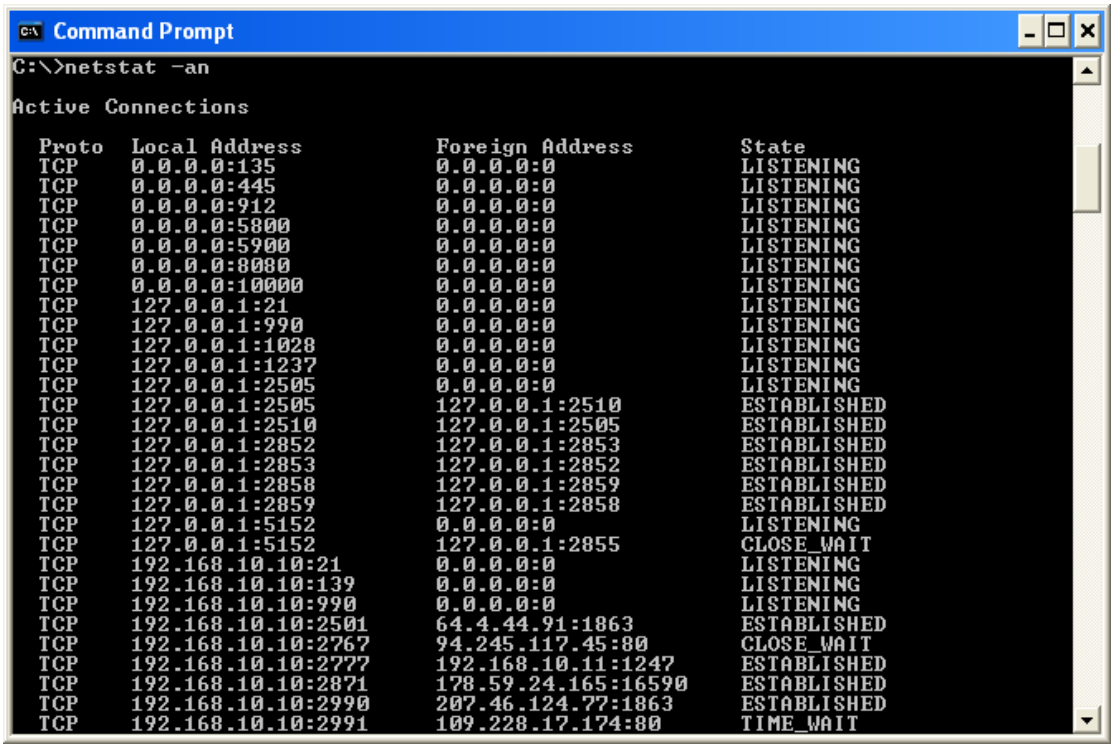
Αφού αναφέρουμε το θέμα του προγραμματισμού batch εργασιών, θα πρέπει να σημειώσουμε ότι μία καλή θέση να ψάχνουμε για αποκαλυπτικά σημάδια εισβολή είναι η ουρά αναμονής Task Scheduler των Windows. Οι επιτιθέμενοι θα χρησιμοποιήσουν συνήθως την υπηρεσία scheduler για να ξεκινήσουν κακόβουλες διεργασίες και όπως έχουμε σημειώσει σε αυτό το κεφάλαιο, το scheduler μπορεί επίσης να χρησιμοποιηθεί για να αποκτηθεί απομακρυσμένος έλεγχος ενός συστήματος και για να ξεκινήσουμε διεργασίες από τον λογαριασμό με ειδικά δικαιώματα SYSTEM. Για να ελέγξουμε την ουρά αναμονής scheduler, πληκτρολογούμε απλώς **at** σε μία γραμμή εντολής ή χρησιμοποιούμε το γραφικό περιβάλλον που είναι διαθέσιμο στο control Panel | Administrative Tools | Task Scheduler.

Πιο προχωρημένες τεχνικές όπως η ανακατεύθυνση νημάτων έχουν κάνει λιγότερο αποτελεσματική την εξέταση της λίστας των διεργασιών για προσδιορισμό εισβολών. Η ανακατεύθυνση νημάτων μπορεί να χρησιμοποιηθεί, ώστε να κάνει ένα νόμιμο νήμα να εκτελέσει κακόβουλο κώδικα (δείτε το http://www.phrack.org/issues.html ?issue=62&id=12#article)

3.6.4 Θύρες

Εάν ένας ακροατής «nc» έχει μετονομαστεί, το βοηθητικό πρόγραμμα netstat μπορεί να προσδιορίσει συνόδους ακρόασης ή συνόδους που έχουν οριστεί. Μερικές φορές ο καλύτερος τρόπος να τις βρίσκετε είναι να ελέγχετε περιοδικά το netstat για τέτοιες ψεύτικες συνδέσεις. Στο επόμενο παράδειγμα, τρέχουμε το netstat-an στον διακομιστή – στόχο μας, ενώ ένας επιτιθέμενος είναι συνδεδεμένος μέσω απομακρυσμένης συνόδου και με το nc στην 8080. Παρατηρήστε ότι η ορισμένη «απομακρυσμένη» σύνδεση λειτουργεί μέσω της TCP 139 και ότι το netcat ακούει και έχει μία ορισμένη σύνδεση στην TCP 8080. (έχει αφαιρεθεί για λόγους σαφήνειας η πρόσθετη έξοδος από το netstat).

Πληκτρολογούμε **netstat /?** σε μία γραμμή εντολής για μία επεξήγηση των διακόπτων –an.



Εικόνα 141:Χρήση εντολής netstat

Επίσης παρατηρήστε από την προηγούμενων έξοδο του netstat ότι η καλύτερη άμυνα σε μια απομακρυσμένη σύνδεση είναι να μπλοκάρετε την πρόσβαση στις θύρες 135 μέχρι 139 σε όλους τους πιθανούς στόχους, είτε στο firewall είτε απενεργοποιώντας τις συνδέσεις NetBIOS για εκτεθειμένες κάρτες, όπως είδατε στην ενότητα «Αντίμετρα στην Εύρεση Κωδικών Πρόσβασης», νωρίτερα σε αυτό το κεφάλαιο.
Η έξοδος του netstat μπορεί να διοχετευθεί μέσω της Find, ώστε να ψάχνει για συγκεκριμένες θύρες, όπως στην παρακάτω εντολή:

netstat –an | find “port” .

Εικόνα 142:Εμφάνιση μιας συγκεκριμένης θύρας

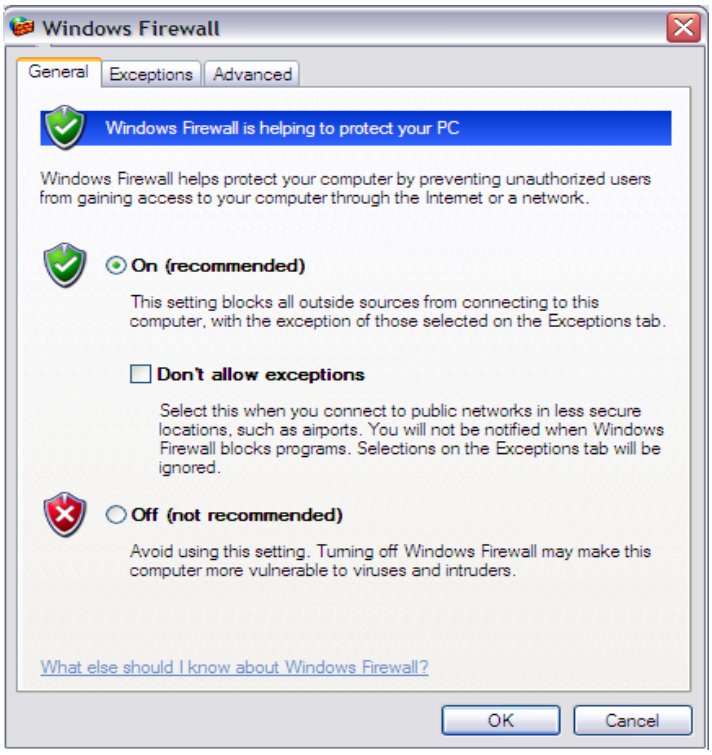
Κεφάλαιο 4 Λειτουργίες ασφάλειας των Windows

Τα Windows παρέχουν πολλά εργαλεία και λειτουργίες ασφάλειας που μπορούν να χρησιμοποιηθούν προκειμένου να εκτρέψουν τις επιθέσεις που έχουμε συζητήσει σε αυτό το κεφάλαιο. Αυτά τα βοηθητικά προγράμματα είναι εξαιρετικά για να προστατεύσουν ένα σύστημα ή απλώς για γενική διαχείριση διαμόρφωσης ώστε να διατηρεί συντονισμένα ολόκληρα περιβάλλοντα για αποφυγή κενών ασφαλείας. Τα περισσότερα από τα στοιχεία που συζητούνται σ' αυτήν την ενότητα είναι διαθέσιμα στα Windows 2000 και νεότερα.

4.1 Το firewall των Windows

Δίνουμε εύσημα στην Microsoft που συνεχίζει να βελτιώνει το firewall που εμφάνισε στα Windows XP, που ονομαζόταν πριν Internet Connection Firewall (ICF). Το νέο και με πιο απλό όνομα windows firewall προσφέρει ένα καλύτερο περιβάλλον χρήστη με μία κλασική "εξαίρεση" για εφαρμογές που επιτρέπονται και μία καρτέλα Advanced (για προχωρημένους) που εκθέτει όλες τις τεχνικές λεπτομέρειες για να τις εκμεταλλευθούν οι επιτιθέμενοι και αυτό είναι διαμορφώσιμο μέσω του Group Policy ώστε να ενεργοποιηθεί η κατανεμημένη διαχείριση των ρυθμίσεων του firewall σε μεγάλο αριθμό συστημάτων.

Από τα Windows XP SP2, το Windows firewall ενεργοποιείται εξ ορισμού με μία πολύ περιοριστική πολιτική (συνεπώς, όλες οι εισερχόμενες συνδέσεις μπλοκάρονται), κάνοντας μη προσπελάσιμα πολλά από τα τρωτά σημεία που περιγράφονται σ' αυτό το κεφάλαιο.

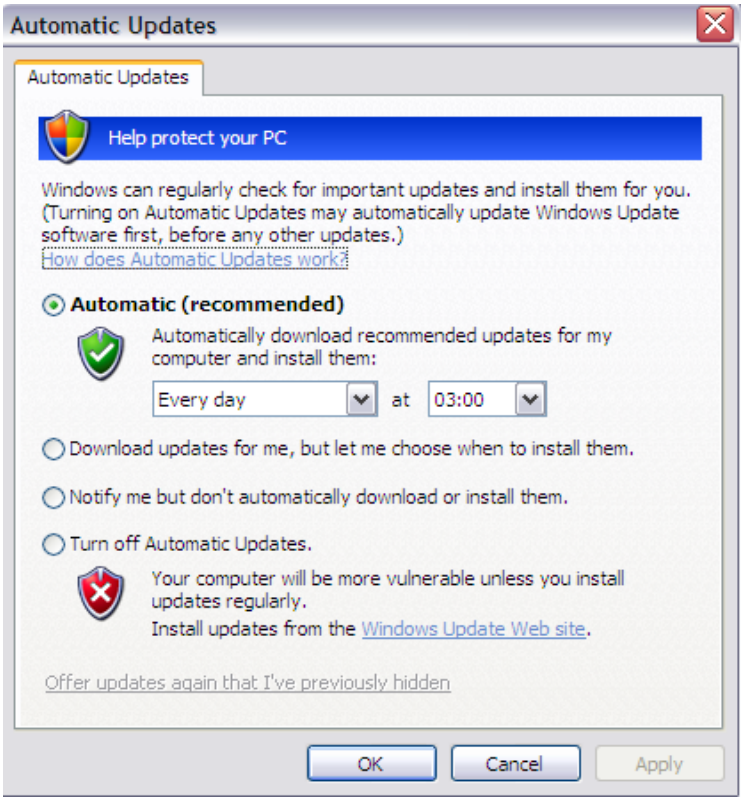


Εικόνα 143: Windows Firewall

4.1.1 Αυτοματοποιημένες Ενημερώσεις

Ένα από τα πιο σημαντικά αντίμετρα ασφάλειας που έχουμε επαναλάβει πολλές φορές σ' όλο αυτό το κεφάλαιο είναι να διατηρούμε ενημερωμένο το σύστημα μας με τις διορθώσεις και τα service pack της Microsoft. Ωστόσο, το μη αυτόματο κατέβασμα και εγκατάσταση των ενημερώσεων του λογισμικού της Microsoft αποτελούν εργασία πλήρους απασχόλησης (ή πολλές εργασίες, εάν διαχειριζόμαστε μεγάλο αριθμό συστημάτων Windows).

Ευτυχώς, η Microsoft περιλαμβάνει τώρα μια λειτουργία αυτοματοποιημένης ενημέρωσης (Automated Update) στο λειτουργικό της σύστημα. Εκτός από την εφαρμογή ενός firewall, δεν υπάρχει πιθανώς κανένα καλύτερο βήμα που μπορείτε να ακολουθήσετε από το να διαμορφώσετε το σύστημα σας, ώστε να λαμβάνει αυτόματες ενημερώσεις. Η πιο κάτω εικόνα δείχνει την οθόνη διαμόρφωσης Automatic Updates.



Εικόνα 144:Η οθόνη διαμόρφωσης Automatic Updates των Windows.

Εάν πρέπει να διαχειριστούμε διορθώσεις (patches) σε μεγάλο αριθμό υπολογιστών, η Microsoft παρέχει τις παρακάτω λύσεις (περισσότερες πληροφορίες για αυτά τα εργαλεία είναι διαθέσιμες στο www.microsoft.com/technet/security/tools) :

- Το Microsoft Update κάνεις τις διορθώσεις για τα Windows, Office και άλλα βασικά προϊόντα από μία θέση και μας επιτρέπει να επιλέξουμε αυτόματη παράδοση και εγκατάσταση των ενημερώσεων υψηλής προτεραιότητας.

- Το Windows Server Update Services (WSUS) απλοποιεί την διόρθωση συστημάτων των Windows για μεγάλες επιχειρήσεις με απλές ανάγκες διορθώσεων.

- Το System Management Server (SMS) 2003 παρέχει αναφορά κατάστασης, στοχοθέτηση, ευρύτερη υποστήριξη πακέτων, αυτοματοποιημένα rollback, διαχείριση εύρους ζώνης και άλλες πιο δυνατές λειτουργίες για επιχειρήσεις.

- Το System Center Configuration Manager 2007 παρέχει πλήρη διαχείριση πόρων των διακομιστών, υπολογιστών και φορητών συσκευών.

Μακροπρόθεσμα, το System Center θα είναι αυτό στο οποίο θα στηριχθούν οι μεγάλες επιχειρήσεις, καθώς ότι έχει σχεδιασθεί να αντικαθιστά το SMS.

Και , φυσικά, υπάρχει μία ενεργή αγορά με λύσεις διαχείρισης διορθώσεων εκτός της Microsoft. Απλώς κάνουμε αναζήτηση για το "windows patch management" σε οποιαδήποτε μηχανή αναζήτησης του Internet ώστε να πάρουμε ενημερωμένες πληροφορίες για τα τελευταία εργαλεία σ' αυτό το χώρο.

4.2 Κέντρο ασφάλειας

Ο πίνακας ελέγχου Security Center φαίνεται πιο κάτω στην εικόνα. Το Security Center είναι ένα σημείο προβολής και διαμόρφωσης για βασικές λειτουργίες ασφάλειας ενός συστήματος : Το
Windows firewall, Windows Update, Antivirus (εάν είναι εγκατεστημένο) και Internet Options.

Εικόνα 145: Windows Security Center.

Το Security Center στοχεύει σε καταναλωτές και όχι σε τεχνικούς, βασισμένο στην έλλειψη ενός πιο προχωρημένου περιβάλλοντος διαμόρφωσης ασφάλειας όπως το Security Policy, Certificate Manager κ.λπ., αλλά είναι βεβαίως μια καλή αρχή. Παραμένουμε αισιόδοξοι ότι κάποια ημέρα η Microsoft θα μάθει να δημιουργεί ένα περιβάλλον χρήστη που να ευχαριστεί τους μη τεχνικούς χρήστες, αλλά να προσφέρει και αρκετές επιλογές και κουμπιά για τους πιο τεχνογνώστες.

4.3 Πολιτική ασφάλειας και πολιτική ομάδας

Ένα από τα πιο δυνατά εργαλεία που είναι διαθέσιμα γι' αυτό είναι το Group Policy. Το Group Policy Objects (GPO) μπορεί να αποθηκευτεί στο Active Directory ή σε έναν τοπικό υπολογιστή για να ορίσουμε ορισμένους παραμέτρους διαμόρφωσης σε επίπεδο τομέα ή σε τοπική κλίμακα. Τα GPO μπορούν να εφαρμοστούν σε δικτυακούς τόπους, σε τομείς, ή οργανωτικές μονάδες (Organizational Units - OU) και κληρονομούνται από τους χρήστες ή τους υπολογιστές που περιέχουν (που ονομάζονται μέλη αυτού του GPO).

Τα GPO μπορούν να προβληθούν και να τροποποιηθούν σε οποιοδήποτε παράθυρο κονσόλας MMC και επίσης να γίνει διαχείριση τους μέσω του Group Policy Management Console (GPMC- δείτε το http://www.microsoft.com/windowsserver2003/gpmc/default.mspx - απαιτούνται δικαιώματα Administrator). Τα GPO που έρχονται με τα Windows 2000 και νεότερα είναι τα Local Computer, Default Domain και Default Domain Controller Policies. Τρέχοντας απλώς το Start | gpedit.msc, καλείται το Local Computer GPO.

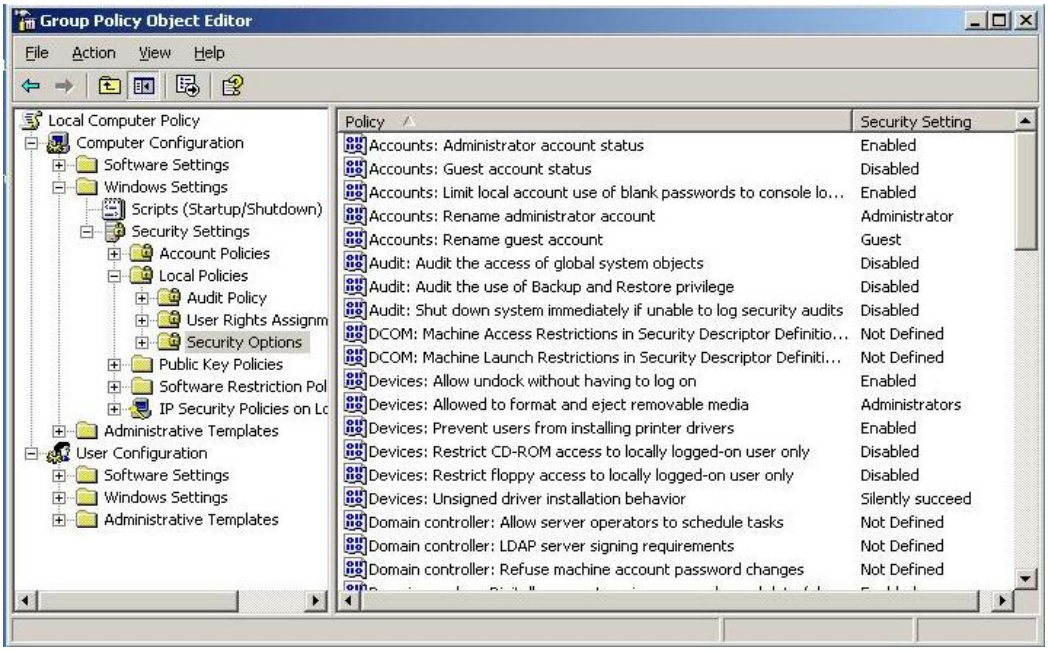
Ένας άλλος τρόπος να δούμε τα GPO είναι να δούμε τις ιδιότητες ενός συγκεκριμένου αντικειμένου καταλόγου (τομέα, OU, ή δικτυακού τόπου) και να επιλεχτεί μετά η καρτέλα Group Policy, όπως φαίνεται πιο κάτω:

Εικόνα 146: Local Computer GPO.

Αυτή η οθόνη εμφανίζει το συγκεκριμένο GPO που εφαρμόζεται στο επιλεγμένο αντικείμενο (που αναφέρεται κατά προτεραιότητα) και εάν είναι μπλοκαρισμένη η κληρονομικότητα και επιτρέπει στο GPO να τροποποιηθεί.

Η επεξεργασία ενός GPO αποκαλύπτει μεγάλο αριθμό διαμορφώσεων ασφάλειας που μπορεί να εφαρμοστεί σε αντικείμενα καταλόγου. Ιδιαίτερου ενδιαφέροντος είναι ο κόμβος Computer Configuration\WindowsSettings\Security Settings\Local Policies\Security Options.

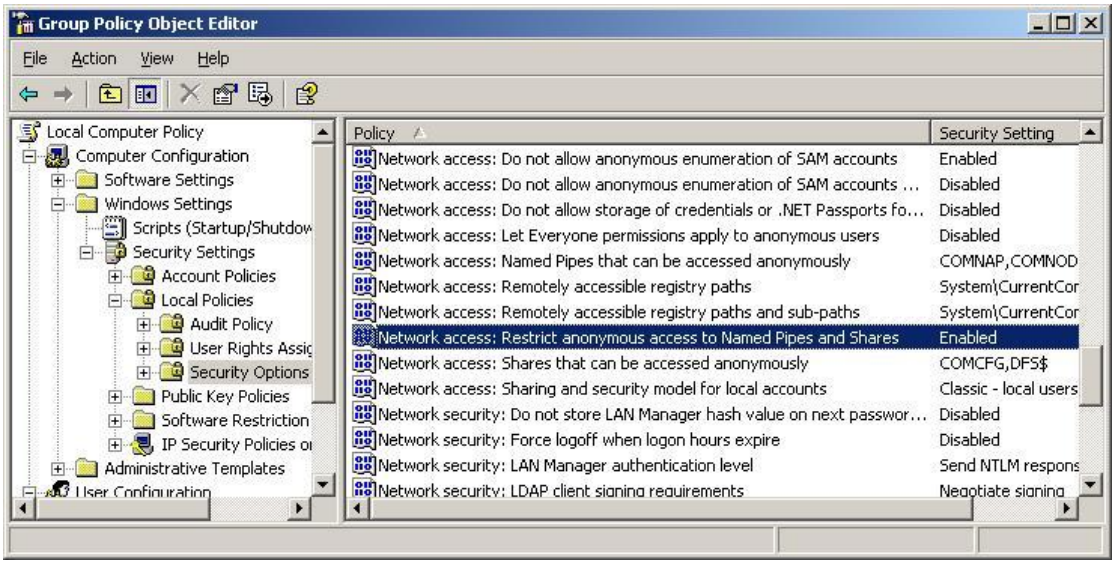
Μπορούν να διαμορφωθούν εδώ περισσότερες από 30 διαφορετικές παράμετροι ώστε να βελτιωθεί η ασφάλεια σε οποιαδήποτε αντικείμενα υπολογιστών στα οποία εφαρμόζεται το GPO.



Εικόνα 147: Security Options.

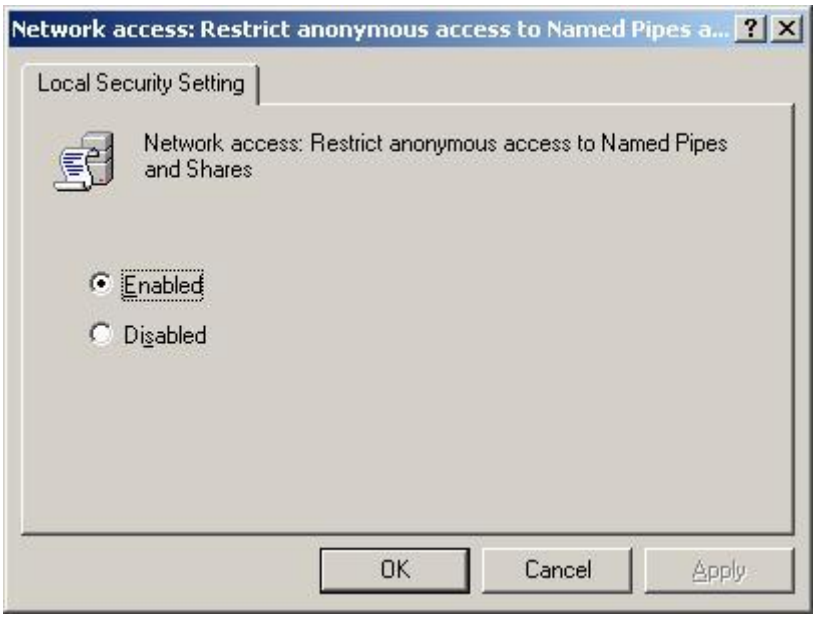
Αυτές οι παράμετροι περιλαμβάνουν το Additional Restrictions For Anonymous Connections (την ρύθμιση Restrict Anonymous), το LAN Manager Authentication Level και το Rename Administrator Account, μεταξύ πολλών άλλων σημαντικών ρυθμίσεων ασφάλειας.

Παράμετρος Additional Restrictions For Anonymous Connections (ρύθμιση Restrict Anonymous).



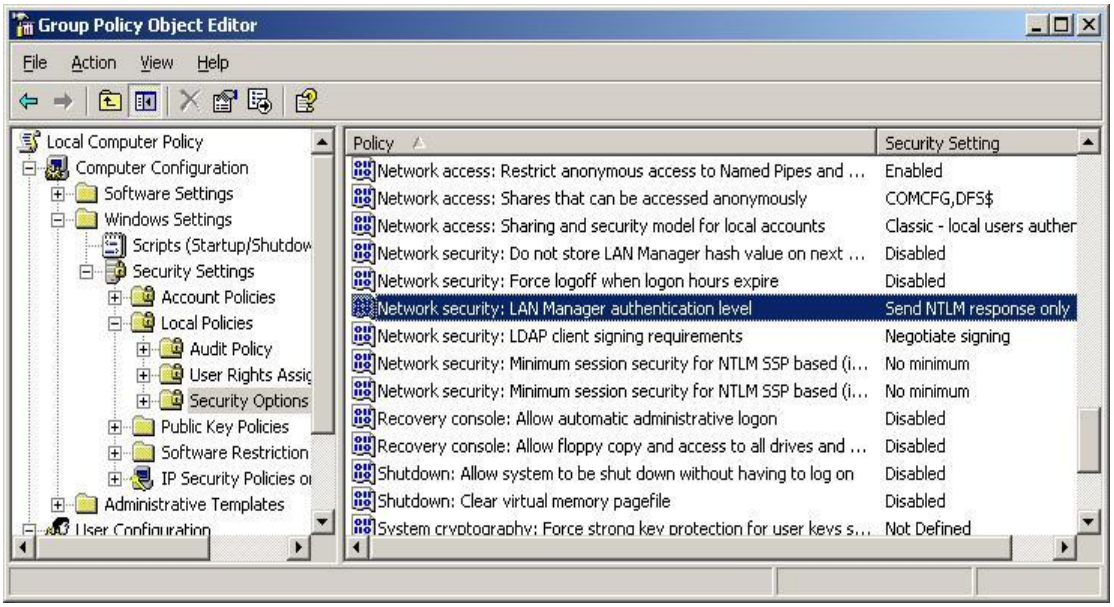
Εικόνα 148: Additional Restrictions For Anonymous Connections (ρύθμιση Restrict Anonymous)

Διαμόρφωση της παραμέτρου «Additional Restrictions For Anonymous Connections».



Εικόνα 149:Ρύθμιση της παραμέτρου «Additional Restrictions For Anonymous Connections»

Παράμετρος LAN Manager Authentication Level.

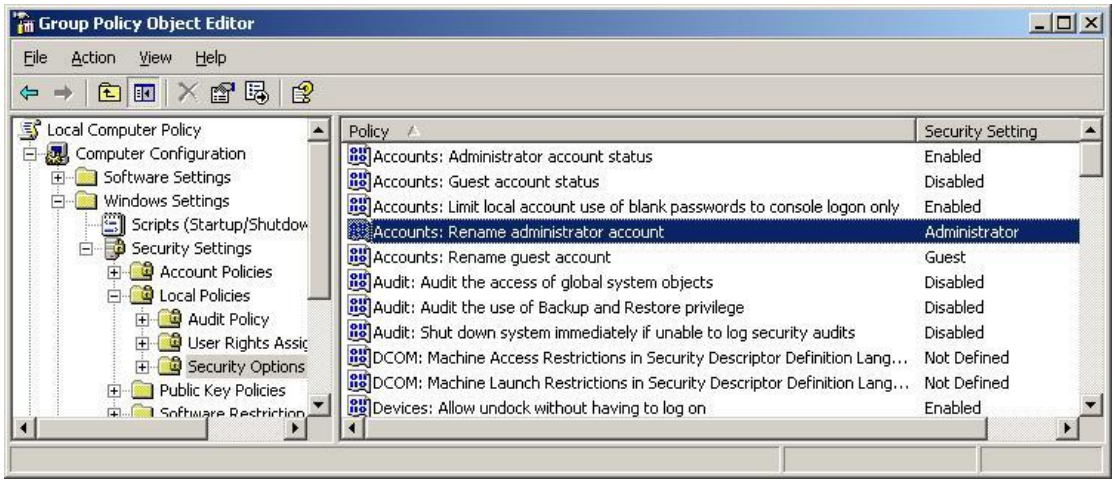


Εικόνα 150:LAN Manager Authentication Level

Διαμόρφωση της παραμέτρου LAN Manager Authentication Level.

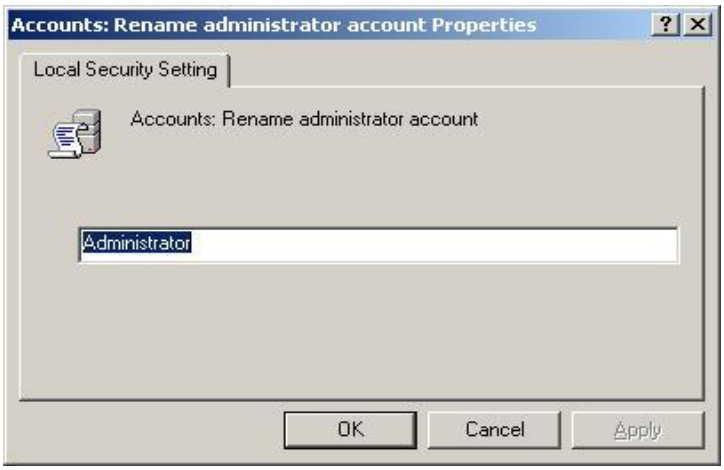
Εικόνα 151:LAN Manager Authentication Level(1).

Παράμετρος Rename Administrator Account.



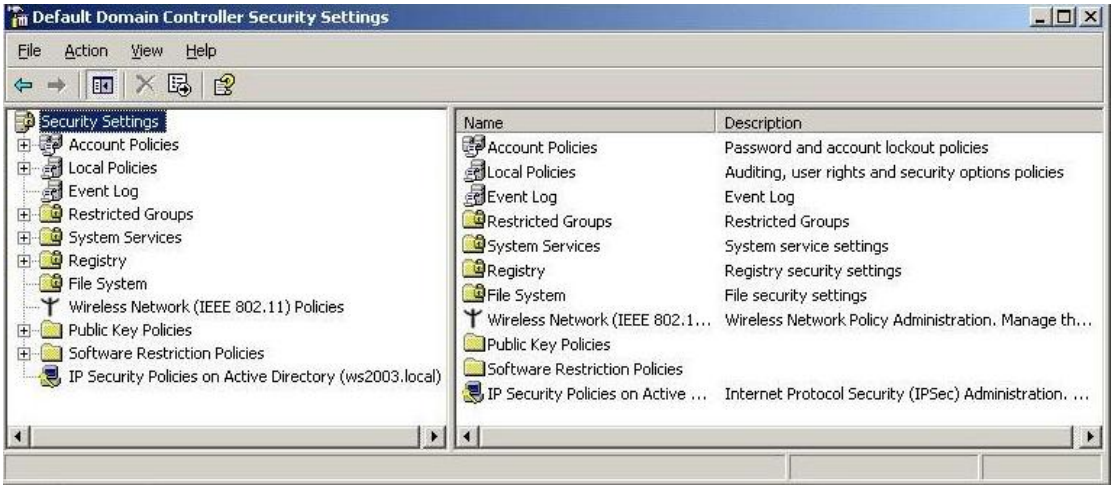
Εικόνα 152: Rename Administrator Account.

Διαμόρφωση της παραμέτρου του ονόματος Administrator Account.



Εικόνα 153:Διαμόρφωση ονόματος του Administrator Account.

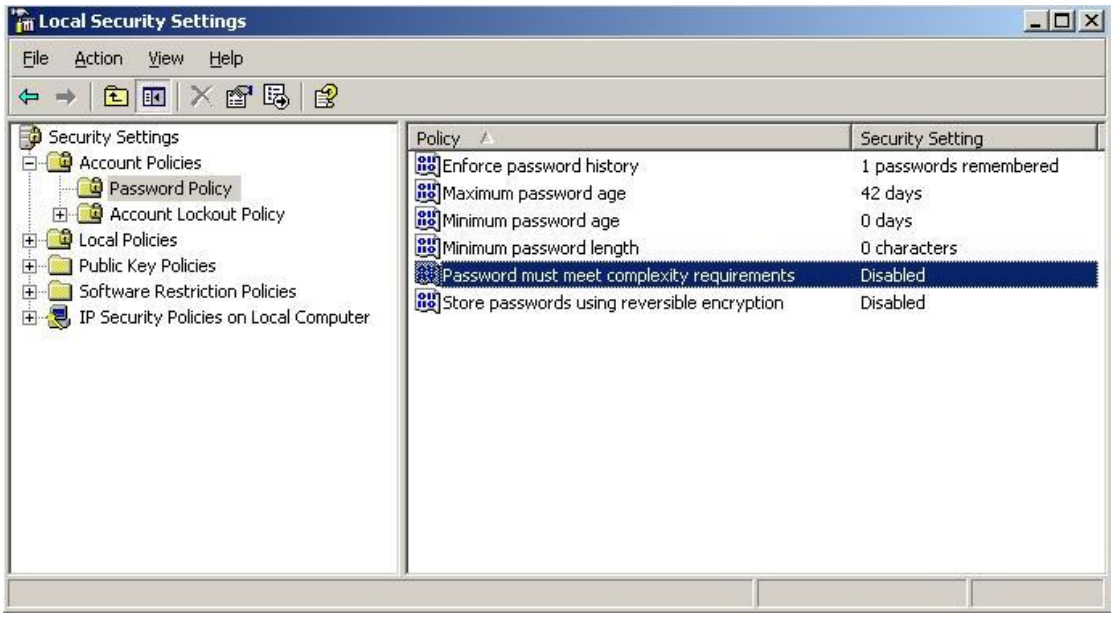
Ο κόμβος Security Settings είναι επίσης εκεί όπου μπορούν να ορισθούν ο λογαριασμός, ο έλεγχος, το Event Log, το δημόσιο κλειδί και οι πολιτικές IPSec.



Εικόνα 154:Κόμβος Security Settings.

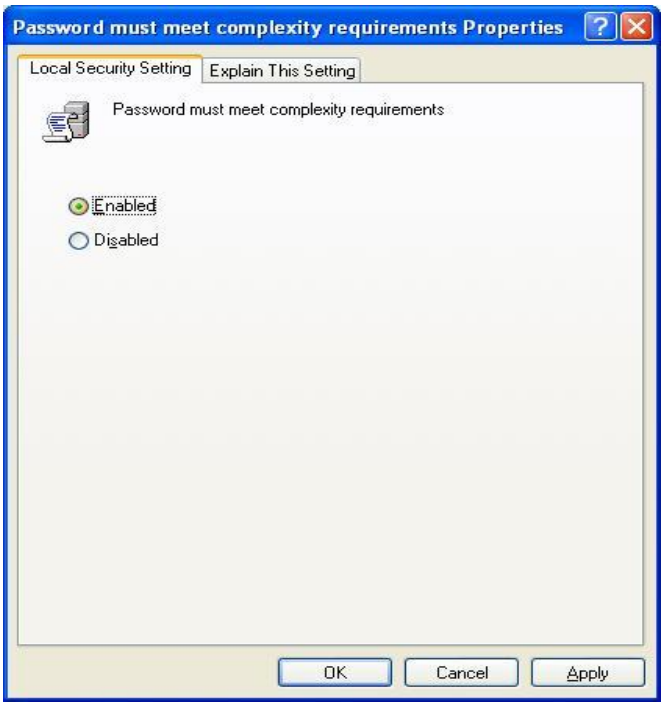
Επιτρέποντας να ορισθούν αυτές οι καλύτερες πρακτικές στον δικτυακό τόπο, τομέα ή επιπέδου οργανωτικών μονάδων (OU), μειώνεται κατά πολύ η εργασία διαχείρισης της ασφάλειας σε μεγάλα περιβάλλοντα.

Το Default Domain Policy GPO φαίνεται πιο κάτω.



Εικόνα 155: Default Domain Policy GPO

Μπορούμε να το ενεργοποιήσουμε για να έχουμε περισσότερη ασφάλεια χρησιμοποιώντας passwords όπου θα είναι πολύπλοκα και με βάση κάποιες απαιτήσεις.



Εικόνα 156:Διαμόρφωση Password must meet complexity requirements.

Τα GPO μοιάζουν να είναι ο καλύτερος τρόπος να διαμορφώνουμε ασφαλώς μεγάλους τομείς με Windows 2000 και νεότερα. Ωστόσο, μπορεί να δούμε αναπάντεχα αποτελέσματα όταν ενεργοποιήσουμε συνδυασμούς πολιτικών τοπικών και επιπέδου τομέα και η καθυστέρηση πριν εφαρμοστούν οι ρυθμίσεις του Group Policy μπορεί επίσης να είναι ενοχλητική. Η χρησιμοποίηση του εργαλείου secedit για άμεση ανανέωση των πολιτικών αποτελεί έναν τρόπο να αντιμετωπίζεται αυτή η καθυστέρηση. Για να ανανεώσουμε πολιτικές που χρησιμοποιούν το secedit, ανοίγουμε το παράθυρο διαλόγου Run και δίνουμε **secedit /refreshpolicy MACHINE_POLICY**. Για να ανανεώσουμε πολιτικές κάτω από τον κόμβο User Configuration, πληκτρολογούμε **secedit /refreshpolicy USER_POLICY.**

4.4 Bitlocker και Encrypting File System (EFS)

Ένα από τα πιο σημαντικά στοιχεία σχετικά με την ασφάλεια που εμφανίστηκαν στα Windows 2000 είναι το Encrypting File System (EFS). Το EFS είναι ένα σύστημα δημόσιου κλειδιού βασισμένο σε κρυπτογραφία για διαφανή κρυπτογράφηση δεδομένων επιπέδου αρχείου σε πραγματικό χρόνο, έτσι ώστε οι επιτιθέμενοι να μην μπορούν να έχουν πρόσβαση σ' αυτό χωρίς το σωστό κλειδί (για περισσότερες πληροφορίες http://www.microsoft.com/technet/
security/guidance/cryptographyetc/efs.mspx). Εν συντομία, το EFS μπορεί να κρυπτογραφήσει ένα αρχείο ή έναν φάκελο μ ' έναν γρήγορο, συμμετρικό, αλγόριθμο κρυπτογράφησης χρησιμοποιώντας ένα τυχαία παραγμένο κλειδί κρυπτογράφησης αρχείων (FEK) που είναι συγκεκριμένο γι 'αυτό το αρχείο ή φάκελο. Η πρώτη EFS χρησιμοποιούσε το Extended Data Encryption Standard (DESX) ως αλγόριθμο κρυπτογράφησης. Το τυχαία παραγμένο κλειδί κρυπτογράφησης αρχείων κρυπτογραφείται μετά μ' ένα ή περισσότερα δημόσια κλειδιά, συμπεριλαμβανομένων

αυτών του χρήστη (κάθε χρήστης στα Windows 2000 και νεότερα λαμβάνει αργότερα ένα ζευγάρι δημόσιου/ιδιωτικού κλειδιού) και έναν πράκτορα ανάκτησης (recovery agent-RA) κλειδιών. Αυτές οι κρυπτογραφημένες τιμές αποθηκεύονται ως ιδιότητες του αρχείου.

Η ανάκτηση του κλειδιού, εφαρμόζεται, για παράδειγμα , σε περίπτωση που οι υπάλληλοι που έχουν κρυπτογραφήσει μερικά ευαίσθητα δεδομένων φεύγουν από μία επιχείρηση ή χάνονται τα κλειδιά της κρυπτογράφησης τους. Για να εμποδίσει την απώλεια κρυπτογραφημένων δεδομένων που δεν μπορούν να ανακληθούν, τα Windows περιέχουν έναν πράκτορα ανάκτησης δεδομένων για το EFS. Στην πραγματικότητα, το EFS δεν θα δουλέψει χωρίς έναν πράκτορα ανάκτησης . Επειδή το FEK είναι απολύτως ανεξάρτητο από το ζευγάρι δημόσιου/ιδιωτικού κλειδιού, ένας πράκτορας ανάκτησης μπορεί να αποκρυπτογραφήσει το περιεχόμενο του αρχείου χωρίς να κλέψει το ιδιωτικό κλειδί του χρήστη. Ο προεπιλεγμένος πράκτορας ανάκτησης δεδομένων για ένα σύστημα είναι ο τοπικός λογαριασμός διακομιστή.

Αν και το EFS μπορεί να είναι χρήσιμο σε πολλές καταστάσεις, πιθανώς δεν εφαρμόζεται σε πολλαπλούς χρήστες του ιδίου τερματικού σταθμού που μπορεί να θελήσουν να προστατεύσουν τα αρχεία τους ο ένας από τον άλλο. Γι' αυτό το λόγο υπάρχουν οι λίστες ελέγχου πρόσβασης (ACL) του συστήματος αρχείων NTFS. Μάλλον, η Microsoft τοποθετεί το EFS ως επίπεδο προστασίας σε επιθέσεις, όπου το NTFS παρακάμπτεται, όπως όταν γίνεται εκκίνηση από εναλλακτικά λειτουργικά συστήματα και όταν χρησιμοποιούνται εργαλεία τρίτων για πρόσβαση σε έναν σκληρό δίσκο ή για αρχεία που είναι αποθηκευμένα σε απομακρυσμένους διακομιστές. Στην πραγματικότητα, η αναφορά της Microsoft για το EFS ειδικά υποστηρίζει : "το EFS αντιμετωπίζει ιδιαίτερα προβλήματα ασφάλειας που προκαλούνται από εργαλεία διαθέσιμα σε άλλα λειτουργικά συστήματα που επιτρέπουν σε χρήστες να έχουν πρόσβαση σε αρχεία ενός τόμου NTFS χωρίς έλεγχο πρόσβασης".

Αυτή η αξίωση είναι δύσκολο να υποστηριχτεί, εκτός αν και εφαρμοσθεί στα πλαίσια ενός τομέα των Windows. Το αρχικό τρωτό σημείο του EFS είναι ο λογαριασμός πράκτορα ανάκτησης, αφού ο τοπικός κωδικός πρόσβασης του λογαριασμού Administrator μπορεί εύκολα να αλλάξει χρησιμοποιώντας δημοσιευμένα εργαλεία τα οποία δουλεύουν όταν ξεκινά το σύστημα σ' ένα εναλλακτικό λειτουργικό σύστημα (δείτε, π.χ το εργαλείο chntpw που είναι διαθέσιμο στην διεύθυνση home.eunet.no/pnordahl/ntpasswd/).
Όταν το EFS εφαρμόζεται σ' έναν υπολογιστή συνένωσης τομέων, ο λογαριασμός του πράκτορα ανάκτησης βρίσκεται σε ελεγκτές τομέων, κατά συνέπεια διαχωρίζοντας το κλειδί της πίσω πόρτας του πράκτορα ανάκτησης και τα κρυπτογραφημένα δεδομένα, παρέχοντας πιο δυνατή προστασία.

Στα Windows Vista, η Microsoft παρουσίασε την κρυπτογράφηση Drive Bitlocker (BDE). Αν και το BDE είχε ως σκοπό αρχικά να παρέχει μεγαλύτερη διασφάλιση της ακεραιότητας του λειτουργικού συστήματος, ένα έμμεσο αποτέλεσμα από τους προστατευτικούς μηχανισμούς του είναι να αμβλύνονται οι επιθέσεις εκτός σύνδεσης, όπως η τεχνική επαναφοράς του κωδικού πρόσβασης που παρέκαμπτε το EFS. Αντί να γίνει συσχετισμός των κλειδιών κρυπτογράφησης των δεδομένων με μεμονωμένους λογαριασμούς χρηστών όπως στο EFS, το BDE κρυπτογραφεί ολόκληρους τόμους και αποθηκεύει το κλειδί με τρόπους είναι δύσκολο να

υποκλαπούν. Με το BDE, ένας επιτιθέμενος που αποκτά απεριόριστη φυσική πρόσβαση στο σύστημα (ας πούμε κλέβοντας ένα φορητό υπολογιστή) δεν μπορεί να αποκρυπτογραφήσει τα δεδομένα που είναι αποθηκευμένα στον κρυπτογραφημένο τόμο, επειδή τα Windows δεν θα ξεκινήσουν εάν έχουν πειραχτεί και η εκκίνηση σ' ένα εναλλακτικό λειτουργικό σύστημα δεν θα παράσχει πρόσβαση στο κλειδί αποκρυπτογράφησης αφού είναι αποθηκευμένο με ασφάλεια. (Μπορούμε να δούμε το en.wikipedia.org/wiki/BitLocker_Drive_Encryption για περισσότερες πληροφορίες για το BDE, που περιλαμβάνει τους διάφορους τρόπους, με τις οποίες προστατεύονται τα κλειδιά.)

Οι ερευνητές στο πανεπιστήμιο Princeton δημοσίευσαν ένα ενθουσιώδες έγγραφο για τις αποκαλούμενες *επιθέσεις ψυχρής εκκίνησης* που παρέκαμπταν το BDE (http://citp.princeton.edu/memory/). Ουσιαστικά, οι ερευνητές κρύωσαν τα τσιπ DRAM για να αυξήσουν το χρονικό διάστημα που σβήνει το φορτωμένο λειτουργικό σύστημα από την μη μόνιμη μνήμη. Αυτό έδωσε αρκετό χρόνο να συλληφθεί μία εικόνα του τρέχοντος συστήματος, από το οποίο θα μπορούσαν να εξαχθούν τα κύρια κλειδιά αποκρυπτογράφησης του BDE, αφού θα πρέπει προφανώς να είναι διαθέσιμα για να ξεκινήσει το σύστημα. Οι ερευνητές παρέκαμψαν ακόμη και ένα σύστημα μ ' ένα Trusted Platform Module (TPM), ένα διαχωρισμένο τσιπ υλικού που έχει σχεδιασθεί να αποθηκεύει προαιρετικά κλειδιά κρυπτογράφησης BDE και αποφάσισαν ότι είναι σχεδόν αδύνατο να παρακαμφθεί το BDE.

Αντίμετρα στην Ψυχρή Εκκίνηση

Όπως και με οποιαδήποτε κρυπτογραφική λύση, η κύρια πρόκληση είναι η διαχείριση των κλειδιών και είναι αναμφισβήτητα αδύνατο να προστατευθεί ένα κλειδί όταν ο επιτιθέμενος το έχει στην κατοχή του με φυσικό τρόπο (δεν έχει βρεθεί ακόμα καμία τεχνολογία ανθεκτική στην πλαστογράφηση κατά 100%).

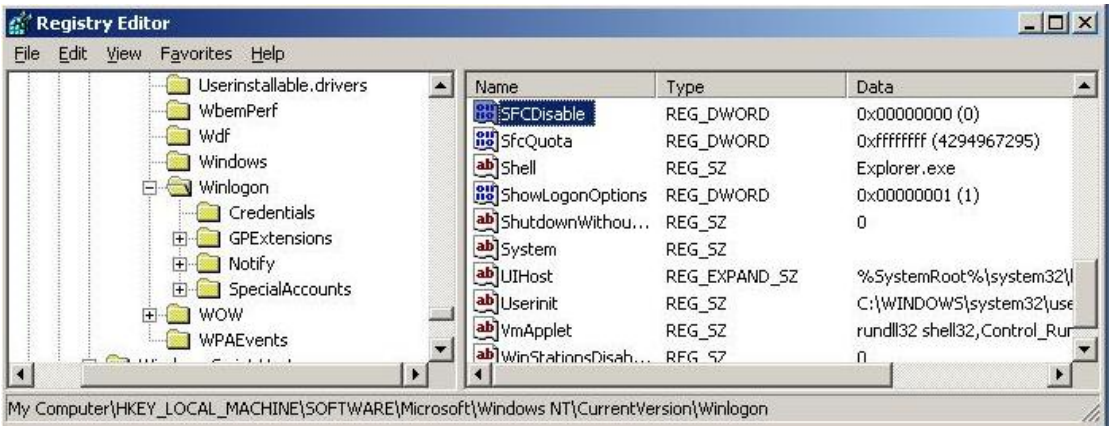
Έτσι, ο μόνος πραγματικός μετριασμός για τις επιθέσεις ψυχρής εκκίνησης είναι να χωρισθεί φυσικά το κλειδί από το σύστημα που έχει σχεδιασθεί να προστατεύει. Οι επόμενες αποκρίσεις στην έρευνα Princeton έδειξαν ότι το σβήσιμο ενός συστήματος προστατευμένου με BDE θα αφαιρέσει τα κλειδιά από τη μνήμη και έτσι θα τα κάνει μη προσπελάσιμα σε επιθέσεις ψυχρής εκκίνησης. Πιθανά, εξωτερικές λειτουργικές μονάδες που είναι φυσικά μετακινούμενες (και αποθηκευμένες χωριστά) από το σύστημα θα μπορούσαν επίσης να μετριάσουν τέτοιες επιθέσεις (π.χ το HASP dongle από την Alladin[13] μπόρεσε να τροποποιηθεί για να έχει αυτήν τη δυνατότητα).

4.5 Προστασία πόρων των Windows

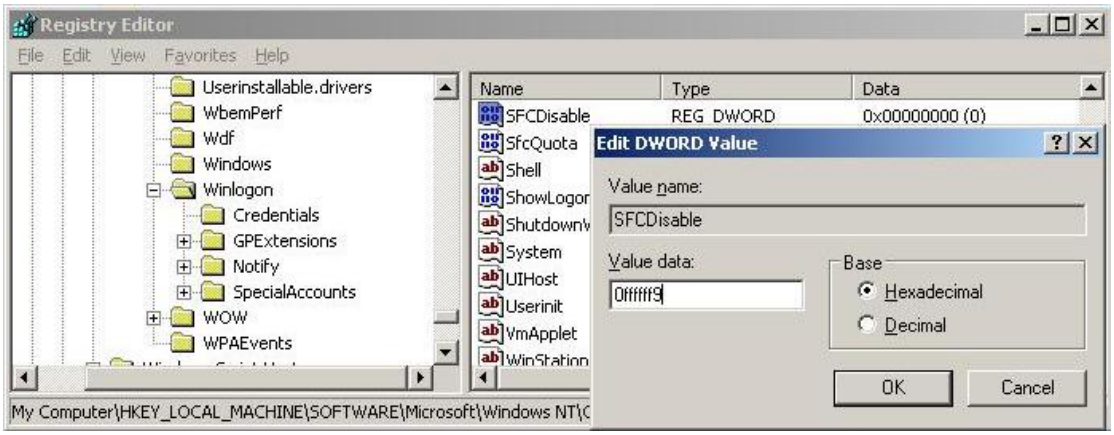
Τα Windows 2000 και Windows XP εμφανίστηκαν με μία λειτουργία που ονομάζεται Windows File Protection (WFP), το οποίο προσπαθεί να εξασφαλίσει ότι δεν θα τροποποιηθούν σκόπιμα ή ακούσια κρίσιμα αρχεία του λειτουργικού συστήματος.

[13] www.aladdin.com/hasp/

Είναι γνωστές οι τεχνικές παράκαμψης του WFP, συμπεριλαμβανομένης της μόνιμης απενεργοποίησης του ορίζοντας την τιμή του Registry SFCDisable[14] σε 0ffffff9dh στο κλειδί HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon.



Εικόνα 157:Ορισμός τιμής του Registry SFCDisable



Εικόνα 158:Αλλαγή τιμής του Registry SFCDisable

Το WFP ενημερώθηκε στα Windows Vista. Περιλαμβάνει τώρα σημαντικές τιμές του Registry, καθώς επίσης και αρχεία και έχει μετονομαστεί σε Windows Resource Protection (WRP). Όπως και το WFP, έτσι και το WRP κρύβει αντίγραφα αρχείων που είναι σημαντικά για την σταθερότητα του συστήματος. Η θέση ωστόσο, έχει μετακινηθεί από το %SystemRoot%\System32\dllcache το %Windir%\WinSxS\Backup και ο μηχανισμός για προστασία αυτών των αρχείων έχει επίσης αλλάξει λίγο. Δεν υπάρχει πλέον ένα νήμα System File Protection που να τρέχει για να εντοπίζει τροποποιήσεις σε κρίσιμα αρχεία. Αντίθετα, το WRP βασίζεται σε Access Control Lists (ACL) και έτσι προστατεύει πάντα ενεργά το σύστημα (η τιμή του Registry SFCDisable που αναφέρθηκε νωρίτερα δεν υπάρχει πλέον στον Server 2008 γι΄αυτό τον λόγο).

Στο WRP, η δυνατότητα εγγραφής ‘ έναν προστατευμένο πόρο χορηγείται μόνο στον φορέα TrustedInstaller - έτσι ακόμη και οι Administrator δεν μπορούν να τροποποιήσουν τους προστατευμένους πόρους. Στη προεπιλεγμένη διαμόρφωση, μόνο οι παρακάτω ενέργειες μπορούν να αντικαταστήσουν έναν προστατευμένο πόρο από το WRP:

[14] http://support.microsoft.com/kb/222473

- Το Windows Update που εγκαθίσταται από το TrustedInstaller.
- Τα Windows Service Pack που εγκαθίστανται από το TrustedInstaller.
- Διορθώσεις (hotfixes) που εγκαθίστανται από το TrustedInstaller.
- Βελτιώσεις του λειτουργικού συστήματος που εγκαθίστανται από το TrustedInstaller.

Φυσικά, μία προφανής αδυναμία στο WRP είναι ότι οι διαχειριστικοί λογαριασμοί μπορούν να αλλάξουν τα ACL σε προστατευμένους πόρους. Εξ ορισμού, η τοπική ομάδα των Administrator έχει το δικαίωμα SeTakeOwnership και μπορεί να πάρει την κατοχή οποιουδήποτε προστατευμένου πόρου από το WRP. Σ' αυτό το σημείο, τα δικαιώματα που εφαρμόζονται στον προστατευμένο πόρο μπορούν αυθαίρετα να αλλάξουν από τον κάτοχο και ο πόρος μπορεί να τροποποιηθεί, να αντικατασταθεί ή να διαγραφεί.

Το WRP δεν έχει σχεδιασθεί για να προστατεύεται από απατεώνες – διαχειριστές, ωστόσο. Ο αρχικός σκοπός του είναι να εμποδίζει τρίτους από το να τροποποιούν πόρους που είναι κρίσιμοι για τη σταθερότητα του λειτουργικού συστήματος.

4.6 Επίπεδα ακεραιότητας, UAC και LoRIE

Στα Windows Vista,η Microsoft εφάρμοσε μία επέκταση στο βασικό σύστημα διακριτού ελέγχου πρόσβασης που υπήρξε στήριγμα του λειτουργικού συστήματος από το ξεκίνημα του. Η βασική πρόθεση αυτής της αλλαγής ήταν να εφαρμοσθεί *υποχρεωτικός* έλεγχος πρόσβασης σε ορισμένα σενάρια. Για παράδειγμα, ενέργειες που απαιτούν διαχειριστικά προνόμια χρειάζονται μία επιπλέον έγκριση, πέρα απ' αυτήν που σχετίζεται με το σημείο πρόσβασης των χρηστών. Η Microsoft ονόμασε αυτήν την νέα επέκταση αρχιτεκτονικής *Mandatory Integrity Control (MIC).*

Για να επιτύχετε συμπεριφορά παρόμοια μ' αυτήν του υποχρεωτικού ελέγχου πρόσβασης, το MIC εφαρμόζει αποτελεσματικά ένα νέο σύνολο τεσσάρων αρχών ασφάλειας που ονομάζονται επίπεδα ακεραιότητας (Integrity Levels- ILs) που μπορούν να προστεθούν σε σημεία πρόσβασης και ACL:

- Low (χαμηλό)
- Medium (μέτριο)
- High (υψηλό)
- System (σύστημα)

Τα IL εφαρμόζονται ως SID, ακριβώς όπως οποιαδήποτε άλλη αρχή ασφάλειας. Στα Vista και νεότερα, εκτός από τον τυπικό έλεγχο πρόσβασης, τα Windows θα ελέγξουν

επίσης αν το IL του σημείου πρόσβασης ταιριάζει με το IL του πόρου στον στόχο. Για παράδειγμα, μια διαδικασία μέτριου IL μπορεί να μπλοκαριστεί από ανάγνωση , εγγραφή ή εκτέλεση ενός αντικειμένου επιπέδου υψηλού IL. Το MIC βασίζεται έτσι στο Biba Integrity Model για ασφάλεια (http://en.wikipedia.org/wiki/Biba_model) : «χωρίς γράψιμο επάνω, χωρίς ανάγνωση κάτω» έχει σχεδιασθεί να προστατεύει την ακεραιότητα. Αυτό έρχεται σε αντίθεση με το μοντέλο πολιτικής ασφάλειας που προτείνεται από την Bell και την LaPadula για το Υπουργείο Άμυνας των ΗΠΑ (DoD) πολλαπλών επιπέδων (MLS) (δείτε http://en.wikipedia.org/wiki/Bell-LaPadula_model): το χωρίς «χωρίς γράψιμο κάτω, χωρίς ανάγνωση επάνω», έχει σχεδιασθεί να προστατευτεί την εμπιστευτικότητα.

Το MIC δεν είναι άμεσα ορατό, αλλά μάλλον εξυπηρετεί ως υποστήριξη για μερικές από τις βασικές νέες λειτουργίες ασφάλειας στα Vista και νεότερα : Το User Account Control (UAC) και το Low Rights Internet Explorer (LoRIE).

Το UAC (ονομαζόταν Least User Access ή LUA, σε εκδόσεις προ των Vista) είναι ίσως η πιο ορατή νέα λειτουργία ασφάλειας στα Vista. Λειτουργεί ως εξής :

1. Οι προγραμματιστές χαρακτηρίζουν εφαρμογές ενσωματώνοντας μία προκήρυξη για την εφαρμογή (διαθέσιμη από τα XP και μετά) για να πουν στο λειτουργικό σύστημα εάν η εφαρμογή χρειάζεται περισσότερα δικαιώματα.

2. Το LSA έχει τροποποιηθεί για να χορηγεί δύο διακριτικά κατά τη σύνδεση σε διαχειριστικούς λογαριασμούς : ένα διακριτικό φιλτραρίσματος κι ένα διακριτικό σύνδεσης. Το διακριτικό φιλτραρίσματος δεν έχει κανένα από τα επιπλέον δικαιώματα (χρησιμοποιώντας τον περιορισμένο μηχανισμό διακριτικών που περιγράφεται στο msdn.microsoft.com/en-us/library/aa379316(VS.85).aspx).

3. Οι εφαρμογές τρέχουν εξ ορισμού χρησιμοποιώντας το διακριτικό φιλτραρίσματος. Το διακριτικό σύνδεσης με τα πλήρη δικαιώματα χρησιμοποιείται μόνο όταν ξεκινούν εφαρμογές οι οποίες είναι χαρακτηρισμένες ότι απαιτούν περισσότερα δικαιώματα.

4. Ο χρήστης απαντά σε μία προτροπή χρησιμοποιώντας ένα ειδικό περιβάλλον συγκατάθεσης (το υπόλοιπο μέρος της συνόδου είναι αχνό και μη προσπελάσιμο) εάν θέλει στην πραγματικότητα να ξεκινήσει το πρόγραμμα και μπορεί να του ζητηθούν τα κατάλληλα πιστοποιητικά εάν δεν είναι μέλος μιας διαχειριστικής ομάδας.

Υποθέτοντας ότι οι προγραμματιστές συμπεριφέρονται καλά, τα Vista επιτυγχάνουν έτσι υποχρεωτικό έλεγχο πρόσβασης κάποιου είδους : μόνο οι συγκεκριμένες εφαρμογές μπορούν να ξεκινήσουν με περισσότερα δικαιώματα.

Εδώ περιγράφεται πώς χρησιμοποιεί το UAC το MIC: Όλες οι μη διαχειριστικές διεργασίες χρηστών τρέχουν με μέτριο IL εξ ορισμού. Μόλις ανυψωθεί μία διαδικασία χρησιμοποιώντας UAC, τρέχει με υψηλό IL και μπορεί έτσι να έχει πρόσβαση σε αντικείμενα αυτού του επιπέδου. Κατά συνέπεια, είναι τώρα

υποχρεωτικό να υπάρχουν δικαιώματα υψηλού IL ώστε να υπάρξει πρόσβαση σε ορισμένα αντικείμενα μέσα στα Windows.

Το MIC βρίσκεται κάτω από την υλοποίηση LoRIE στα Vista : η διεργασία Internet Explorer (iexplore.exe) τρέχει με Low IL και, σ' ένα σύστημα με την προεπιλεγμένη διαμόρφωση, μπορεί να γράψει μόνο σε αντικείμενα που έχουν χαρακτηρισθεί με Low IL SID (εξ ορισμού, αυτό περιλαμβάνει μόνο το φάκελο %USERPROFILE%\AppData\LocalLow). Το LoRIE δεν μπορεί έτσι να γράψει εξ ορισμού σε οποιοδήποτε άλλο αντικείμενο στο σύστημα, περιορίζοντας κατά πολύ την ζημιά που μπορεί να γίνει εάν η διεργασία καταληφθεί από έναν ιό (malware) κατά την πλοήγηση στο διαδίκτυο.

Με την εμφάνιση των Vista, υπάρχουν δυνατότητες να επιτρέπουν να τρέχει μη χαρακτηρισμένος κώδικας με διαχειριστικά δικαιώματα. Σε μελλοντικές εκδόσεις , ο μόνος τρόπος να τρέχει μια εφαρμογή με υψηλά δικαιώματα θα είναι να υπάρχει μια υπογεγραμμένη διακήρυξη που να προσδιορίζει το επίπεδο δικαιωμάτων της εφαρμογής.

Το UAC μπορεί να απενεργοποιηθεί σε επίπεδο συστήματος κάτω από το User Accounts Control Panel, ρύθμιση «Turn User Account Control Off». (Απενεργοποίηση ελέγχουν λογαριασμού χρηστών).

Η ερευνήτρια ασφάλειας Joanna Rutkowska έγραψε μερικές ενδιαφέρουσες κριτικές για το UAC και το MIC στα Vista στο http://theinvisiblethings.blogspot.com/2007/02/running-vista-everyday.
html.. Ο γκουρού της τεχνολογίας των Windows Jesper Johansson έχει γράψει μερικά διορατικά άρθρα σχετικά με το UAC στο blog του στο http://msinfluentials.com/blogs/jesper/.

4.7 Data Execution Prevention (DEP)

Για πολλά χρόνια, οι ερευνητές ασφάλειας έχουν συζητήσει την ιδέα του χαρακτηρισμού τμημάτων της μνήμης ως μη εκτελέσιμων. Ο κύριος στόχος αυτής της λειτουργίας ήταν να αποτραπούν οι επιθέσεις στο αδύνατο σημείο του λογισμικού , την υπερχείλιση buffer . Οι υπερχειλίσεις buffer (και σχετικά τρωτά σημεία της μνήμης) βασίζονται γενικά στην εμφύτευση κακόβουλου κώδικα σε εκτελέσιμα μέρη της μνήμης, συνήθως την στοίβα εκτέλεσης της CPU ή στον σωρό. Κάνοντας την στοίβα μη εκτελέσιμη, για παράδειγμα, κλείνετε έναν από τους πιο αξιόπιστους μηχανισμούς για εκμετάλλευσης τρωτών λογισμικού που είναι διαθέσιμοι σήμερα: την υπερχείλιση buffer με βάση στοίβα .

Η Microsoft έχει μετακινηθεί πιο κοντά προς αυτό το << ιερό δισκοπότηρο>> υλοποιώντας αυτό που ονομάζεται Data Execution Prevention, ή DEP (δείτε το support.microsoft.com/kb/875352 για πλήρεις πληροφορίες). Όταν τρέχει σε συμβατό υλικό, το DEP ξεκινά αυτόματα και σημειώνει κάποια μέρη της μνήμης ως μη εκτελέσιμα εκτός αν περιέχουν εκτελέσιμο κώδικα. Φαινομενικά αυτό θα εμποδίσει τις περισσότερες επιθέσεις υπερχείλισης buffer που βασίζονται στην στοίβα. Εκτός από το DEP που υλοποιείται μέσω υλικού, το XP SP2 και νεότερο

χειρίζεται επίσης DEP μέσω λογισμικού που προσπαθεί να εμποδίσει την εκμετάλλευση μηχανισμών Structured Exception Handling(SEH) στα Windows, οι οποίοι έχουν υπάρξει ιστορικά για τους επιτιθεμένους ένα αξιόπιστο σημείο εμφύτευσης για το shellcode (για παράδειγμα, δείτε το www.securiteam.com/windowsntfocus/5DP0M2KAKA.html).

4.8 Θωράκιση Υπηρεσιών

Όπως έχουμε δει σε όλο αυτό το κεφάλαιο, η παραβίαση ή η εισβολή σε υπηρεσίες των Windows με υψηλά δικαιώματα είναι μία συνηθισμένη τεχνική επίθεσης . Αυτό έχει κινητοποιήσει τη Microsoft να συνεχίσει να σκληραίνει την υποδομή των υπηρεσιών στα Windows XP και Server 2003 και στα Vista και Server 2008 έχουν προχωρήσει ακόμα περισσότερο το επίπεδο των υπηρεσιών ασφαλείας με το Windows Service Hardening το οποίο περιλαμβάνει τα εξής:

- Απομόνωση πόρων των υπηρεσιών
- Λιγότερες προνομιούχες υπηρεσίες
- Απομόνωση συνόδου 0
- Περιορισμένη δυνατότητα πρόσβασης σε δίκτυο .

4.8.1 Απομόνωση Πόρων των Υπηρεσιών

Πολλές υπηρεσίες εκτελούνται στα πλαίσια του ίδιου τοπικού λογαριασμού, όπως του LocalService. Εάν οποιαδήποτε από αυτές τις υπηρεσίες χρησιμοποιηθεί από ένα hacker, θα μπορεί επίσης να παραβιαστεί η ακεραιότητα όλων των άλλων υπηρεσιών που εκτελούνται ως ο ίδιος χρήστης . Για να αντιμετωπίσουμε αυτό το θέμα χρησιμοποιούνται δυο τεχνολογίες :

- SID ειδικά για υπηρεσίες
- Περιορισμένα SID

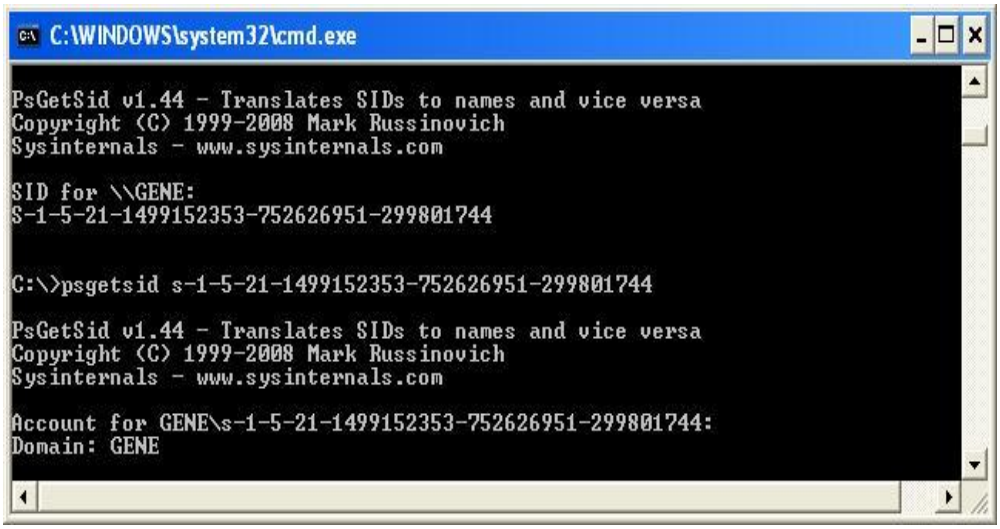
Αντιστοιχώντας σε κάθε υπηρεσία ένα μοναδικό SID, οι πόροι υπηρεσιών, όπως ένα αρχείο ή ένα κλειδί του Registry, μπορούν να μπουν σε λίστες ελέγχου πρόσβασης(ACL) για να επιτρέψουμε μόνο σε αυτήν την υπηρεσία να τα τροποποιεί. Το παρακάτω παράδειγμα παρουσιάζει τα εργαλεία της Microsoft sc.exe και PsGetSid (www.microsoft.com) για να δείξουμε το SID της υπηρεσίας WLAN και εκτελώντας μετά την αντίστροφη μετάφραση του SID για να παραχθεί το όνομα λογαριασμού που είναι κατανοητό από τον άνθρωπο :

Πιο κάτω φαίνεται η εγκατάσταση του εργαλείου PsGetSid.

Εικόνα 159:Εγκατάσταση του εργαλείου PsGetSid

Στην συνέχεια πληκτρολογούμε στην γραμμή εντολών C:/>sc showsid wlansvc και μας εμφανίζει το SID της υπηρεσίας.

Ακολούθως πληκτρολογούμε C:/>psgetsid.



Εικόνα 160:SID της υπηρεσίας WLAN

Στο τέλος βλέπουμε ότι μας εμφανίζει το Domain.

Για να μετριάσουμε τις υπηρεσίες που πρέπει να τρέχουν κάτω από το ίδιο πλαίσιο επηρεάζοντας η μία την άλλη, χρησιμοποιούνται περιορισμένα ως προς την εγγραφή SID : η υπηρεσία SID, μαζί με περιορισμένα ως προς την εγγραφή SID (S-1-5-33), προστίθεται στην περιορισμένη λίστα SID της διεργασίας της υπηρεσίας. Όταν μία περιορισμένη διεργασία ή ένα νήμα προσπαθεί να έχει πρόσβαση σε ένα αντικείμενο, εκτελούνται δύο

έλεγχοι πρόσβασης : ο ένας χρησιμοποιεί τα ενεργοποιημένα διακριτικά SID και ο άλλος χρησιμοποιεί τα περιορισμένα SID. Μόνο εάν επιτύχουν και οι δυο έλεγχοι χορηγείται η πρόσβαση. Αυτό εμποδίζει περιορισμένες υπηρεσίες να αποκτήσουν πρόσβαση σε οποιοδήποτε αντικείμενο το οποίο δεν χορηγεί ρητά πρόσβαση στην υπηρεσία SID.

4.8.2 Υπηρεσίες Με τα Λιγότερα Δικαιώματα

Ιστορικά, πολλές υπηρεσίες των Windows λειτουργούσαν κάτω από το πλαίσιο του LocalSystem, το οποίο χορηγεί τη δυνατότητα να κάνει σχεδόν τα πάντα. Στα Vista, τα προνόμια που χορηγούνται σε μία υπηρεσία δεν είναι πλέον αποκλειστικά συνδεδεμένα με τον λογαριασμό, με τον οποίο έχει διαμορφωθεί να τρέχει – μπορούν να ζητηθούν απευθείας.

Για να επιτευχθεί αυτό, έχει αλλάξει το Service Control Manager (SCM). Οι υπηρεσίες είναι τώρα σε θέση να παρέχουν το SCM με μία λίστα συγκεκριμένων δικαιωμάτων τα οποία ζητούν(φυσικά, δεν μπορούν να ζητήσουν δικαιώματα που δεν είχαν από αρχή από τον φορέα, από τον οποίο έχουν διαμορφωθεί να ξεκινούν). Κατά την έναρξη της υπηρεσίας, το SCM κόβει όλα τα προνόμια από τη διεργασία των υπηρεσιών που δεν έχουν ζητηθεί άμεσα.

Για υπηρεσίες που μοιράζονται μία διεργασία, όπως το svchost, το διακριτικό της διεργασίας θα περιέχει ένα σύνολο όλων των δικαιωμάτων που απαιτούνται από κάθε μεμονωμένη υπηρεσία της ομάδας, κάνοντας αυτήν την διεργασία ένα ιδανικό σημείο επίθεσης. Αφαιρώντας τα δικαιώματα που δεν χρειάζονται, μειώνεται η γενική επιφάνεια της επίθεσης.

Όπως και στις προηγούμενες εκδόσεις των Windows, μπορούν να διαμορφωθούν υπηρεσίες μέσω του εργαλείου γραμμής εντολών sc.exe. Έχουν προστεθεί δύο νέες επιλογές σε αυτό το βοηθητικό πρόγραμμα, η qprivs και η privs, που επιτρέπουν δικαιώματα αναζήτησης και ορισμού δικαιωμάτων υπηρεσιών, αντίστοιχα. Εάν θέλετε να ελέγξετε ή να κλειδώσετε τις υπηρεσίες που τρέχουν στον υπολογιστή σας που έχει Vista ή Server 2008, αυτές οι εντολές είναι ανεκτίμητες.

4.8.3 Ανακατασκευή Υπηρεσίας

Η ανακατασκευή υπηρεσιών (service refactoring) είναι ένα εντυπωσιακών όνομα για την εκτέλεση υπηρεσιών σε λογαριασμούς με μειωμένα δικαιώματα και είναι ο καλύτερος τρόπος να τρέχουν υπηρεσίες με λιγότερα δικαιώματα. Στα Vista, η Microsoft έχει μετακινήσει οκτώ υπηρεσίες από το πλαίσιο SYSTEM στο LocalService. Τέσσερεις πρόσθετες υπηρεσίες SYSTEM έχουν μετακινηθεί, ώστε να τρέχουν επίσης στο πλαίσιο του λογαριασμού NetworkService.

Επιπλέον, έχουν εμφανιστεί έξι νέοι κύριοι υπολογιστές υπηρεσιών (svchosts). Αυτοί οι κύριοι υπολογιστές παρέχουν και πρόσθετη ευελιξία όταν κλειδώνουμε υπηρεσίες και αναφέρονται εδώ από τα λιγότερα δικαιώματα στα μεγαλύτερα:

- LocalServiceNoNetwork
- LocalServiceRestricted

- LocalServiceNetworkRestricted
- NetworkServiceRestricted
- NetworkServiceNetworkRestricted
- LocalSystemNetworkRestricted

LocalServiceNetworkRestricted

Μια από τις υπηρεσίες που μπορούμε να κλειδώσουμε και να τρέχει με λιγότερα δικαιώματα είναι η Windows Security Center Service.

Η υπηρεσία WSCSVC (Windows Security Center) παρακολουθεί και αναφέρει τις ρυθμίσεις για την υγεία ασφάλεια του υπολογιστή. Οι ρυθμίσεις αυτές περιλαμβάνουν firewall (on / off), antivirus (on / off / out of date), antispyware (on / off / out of date), το Windows Update (αυτόματη / χειροκίνητη λήψη και εγκατάσταση ενημερώσεων), το User Account Control (για / off), και τις ρυθμίσεις Internet (συνιστώνται /μη συνιστώνται). Η υπηρεσία παρέχει COM APIs για τους ανεξάρτητους προμηθευτές λογισμικού την καταγραφή της κατάστασης των προϊόντων τους στην υπηρεσία του Κέντρου ασφαλείας. Το Κέντρο Δράσης (AC) UI χρησιμοποιεί την υπηρεσία για την παροχή ειδοποιήσεις Systray και μια γραφική άποψη των καταστάσεων της υγείας της ασφάλειας στον πίνακα ελέγχου του AC.
Το Network Access Protection (NAP) χρησιμοποιεί την υπηρεσία για να αναφέρει τις καταστάσεις της ασφάλειας των πελατών του NAP Network Policy Server για να πάρει αποφάσεις καραντίνας του δικτύου.
Η υπηρεσία έχει επίσης ένα δημόσιο API που επιτρέπει σε εξωτερικούς καταναλωτές να ανακτήσουν τον προγραμματισμό της συγκεντρωτική κατάσταση της ασφάλειας της υγείας του συστήματος.

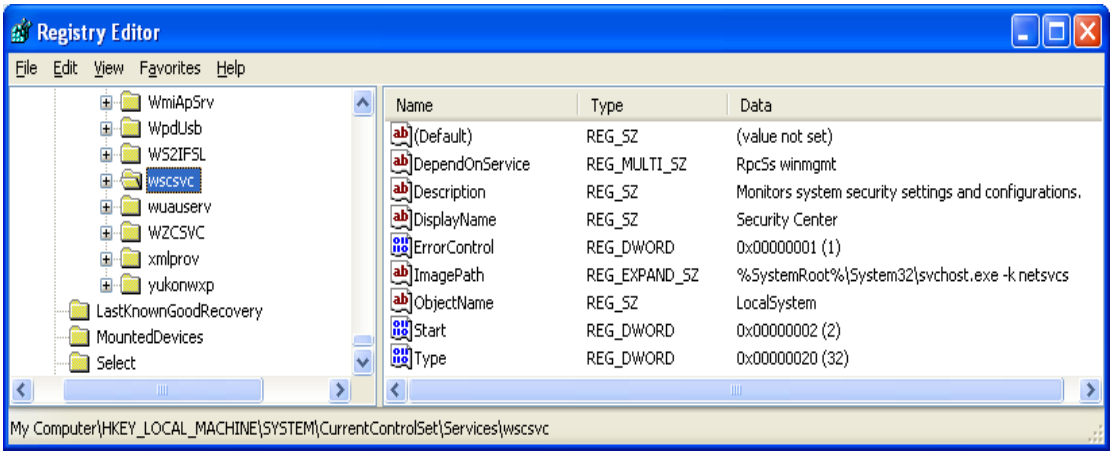
Windows Security Center Service

Service Host Group Name	LocalServiceNetworkRestricted
Service Short Description	Windows Security Center Service
Service Full Description	The WSCSVC (Windows Security Center) service monitors and reports security health settings on the computer. The health settings include firewall (on/off), antivirus (on/off/out of date), antispyware (on/off/out of date), Windows Update (automatically/manually download and install updates), User Account Control (on/off), and Internet settings (recommended/not recommended). The service provides COM APIs for independent software vendors to register and record the state of their products to the Security Center service. The Action Center (AC) UI uses the service to provide systray alerts and a graphical view of the security health states in the AC control panel. Network Access Protection (NAP) uses the service to report the security health states of clients to the NAP Network Policy Server to make network quarantine decisions. The service also has a public API that allows external consumers to programmatically retrieve the aggregated security health state of the system.
Service Executable File Path	c:\windows\system32\wscsvc.dll
Service Host Launch Command	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
Service Privileges	SeChangeNotifyPrivilege SeImpersonatePrivilege
Registry Key	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wscsvc
Depends on	Ole resource dll WMI

Εικόνα 161: Windows Security Center Service

Για να τροποποιήσουμε ή να δούμε τις επιλογές για αυτή την υπηρεσία πηγαίνουμε από το menu Start επιλέγουμε το Run και ακολούθως γράφουμε regedit. Στην συνέχεια εμφανίζεται το Registry Editor και ακολουθούμε τα εξής βήματα :

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wscsvc



Εικόνα 162: Windows Security Center Service-Registry Key

Σε αυτή την διεύθυνση (http://localservicenetworkrestricted.svchost-exe.net/) μπορούμε να δούμε κι άλλες υπηρεσίες του LocalServiceNetworkRestricted.

NetworkServiceRestricted

Μια από τις υπηρεσίες του NetworkServiceRestricted που μπορούμε να κλειδώσουμε έτσι ώστε να τρέχει με λιγότερα δικαιώματα είναι η Terminal Service.

Επιτρέπει στους χρήστες να συνδέονται αλληλεπιδραστικά σε έναν απομακρυσμένο υπολογιστή. Remote Desktop και Remote Desktop Session Host Server εξαρτώνται από αυτή την υπηρεσία. Για να αποφευχθεί η απομακρυσμένη χρήση κάποιου υπολογιστή, απενεργοποιούμε τα checkboxes στην καρτέλα Remote από τις ιδιότητες του συστήματος του πίνακα ελέγχου.

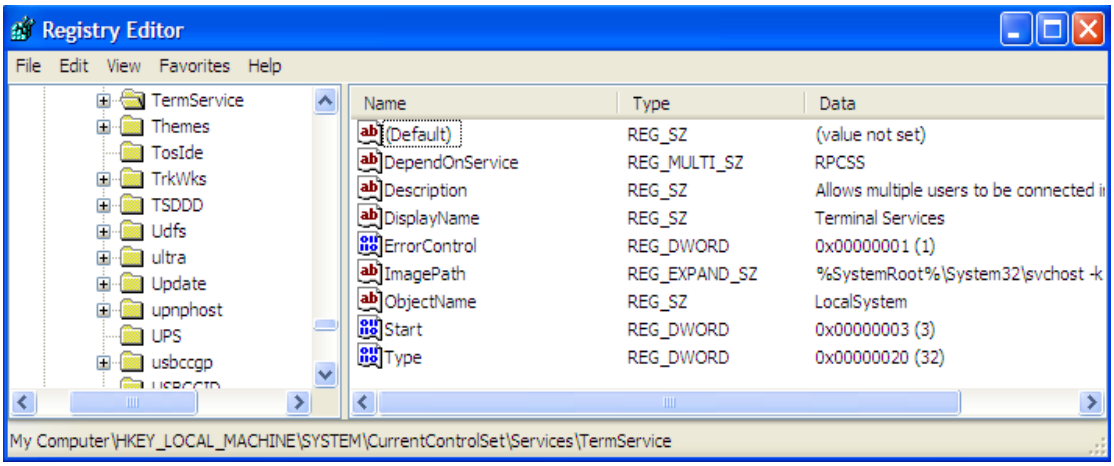
Remote Desktop Session Host Server Remote Connections Manager

Service Host Group Name	NetworkService
Service Short Description	Remote Desktop Session Host Server Remote Connections Manager
Service Full Description	Allows users to connect interactively to a remote computer. Remote Desktop and Remote Desktop Session Host Server depend on this service. To prevent remote use of this computer, clear the checkboxes on the Remote tab of the System properties control panel item.
Service Executable File Path	c:\windows\system32\termsrv.dll
Service Host Launch Command	C:\Windows\System32\svchost.exe -k NetworkService
Service Privileges	**SeAssignPrimaryTokenPrivilege** **SeAuditPrivilege** **SeChangeNotifyPrivilege** **SeCreateGlobalPrivilege** **SeImpersonatePrivilege** **SeIncreaseQuotaPrivilege**
Registry Key	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermService
Depends on	**Ole resource dll** TermDD

Εικόνα 163: Remote Desktop Session Host Server Remote Connections Manager

Για να τροποποιήσουμε ή να δούμε τις επιλογές για αυτή την υπηρεσία πηγαίνουμε από το menu Start επιλέγουμε το Run και ακολούθως γράφουμε regedit. Στην συνέχεια εμφανίζεται το Registry Editor και ακολουθούμε τα εξής βήματα :

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermService



Εικόνα 164: Remote Desktop Session Host Server Remote Connections Manager-Registry Key

Σε αυτή την διεύθυνση (http://networkservice.svchost-exe.net/) μπορούμε να δούμε κι άλλες υπηρεσίες του NetworkServiceRestricted.

NetworkServiceNetworkRestricted

Μια από τις υπηρεσίες του NetworkServiceNetworkRestricted που μπορούμε να κλειδώσουμε έτσι ώστε να τρέχει με λιγότερα δικαιώματα είναι η PolicyAgent.

Το (IPsec) υποστηρίζει δίκτυο σε επίπεδο ταυτότητας peer, τα στοιχεία ταυτότητας προέλευσης, την ακεραιότητα των δεδομένων, της εμπιστευτικότητας των δεδομένων (κρυπτογράφηση) και την προστασία επανάληψης. Η υπηρεσία αυτή επιβάλλει IPsec πολιτικές που δημιουργούνται μέσω της IP Security Policies τοποθετώντας το πρόγραμμα ή το εργαλείο γραμμής εντολών netsh IPSec ". Εάν σταματήσουμε αυτή την υπηρεσία, ενδέχεται να αντιμετωπίσουμε ζητήματα σύνδεσης δικτύου εάν η πολιτική μας απαιτεί συνδέσεις χρήση IPsec. Επίσης, η απομακρυσμένη διαχείριση του Firewall των Windows δεν είναι διαθέσιμη όταν αυτή η υπηρεσία διακοπεί.

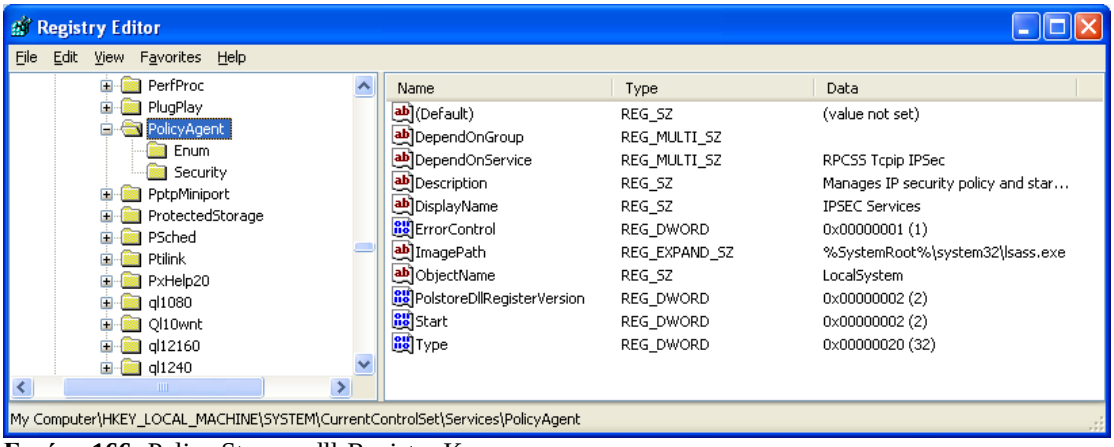
Policy Storage dll

Service Host Group Name	NetworkServiceNetworkRestricted
Service Short Description	Policy Storage dll
Service Full Description	Internet Protocol security (IPsec) supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. This service enforces IPsec policies created through the IP Security Policies snap-in or the command-line tool "netsh ipsec". If you stop this service, you may experience network connectivity issues if your policy requires that connections use IPsec. Also,remote management of Windows Firewall is not available when this service is stopped.
Service Executable File Path	c:\windows\system32\polstore.dll
Service Host Launch Command	C:\Windows\system32\svchost.exe -k NetworkServiceNetworkRestricted
Service Privileges	SeAuditPrivilege SeChangeNotifyPrivilege SeCreateGlobalPrivilege SeImpersonatePrivilege
Registry Key	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent
Depends on	Tcpip Base Filtering Engine

Εικόνα 165: Policy Storage dll

Για να τροποποιήσουμε ή να δούμε τις επιλογές για αυτή την υπηρεσία πηγαίνουμε από το menu Start επιλέγουμε το Run και ακολούθως γράφουμε regedit. Στην συνέχεια εμφανίζεται το Registry Editor και ακολουθούμε τα εξής βήματα :

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent



Εικόνα 166: Policy Storage dll-Registry Key

Σε αυτή την διεύθυνση (http://networkservicenetworkrestricted.svchost-exe.net/) μπορούμε να δούμε κι άλλες υπηρεσίες του NetworkServiceNetworkRestricted.

LocalSystemNetworkRestricted

Μια από τις υπηρεσίες του LocalSystemNetworkRestricted που μπορούμε να κλειδώσουμε έτσι ώστε να τρέχει με λιγότερα δικαιώματα είναι η Netman.

Διαχειρίζεται αντικείμενα στο φάκελο Network and Dial-Up Connections, στον οποίο μπορούμε να δούμε τοπικές συνδέσεις δικτύου όσο και απομακρυσμένες.

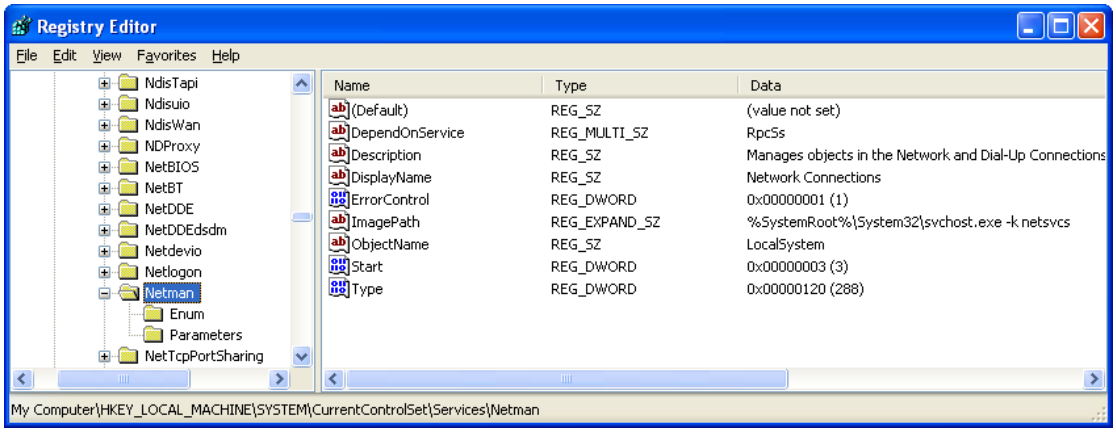
Network Connections Manager

Service Host Group Name	LocalSystemNetworkRestricted
Service Short Description	Network Connections Manager
Service Full Description	Manages objects in the Network and Dial-Up Connections folder, in which you can view both local area network and remote connections.
Service Executable File Path	c:\windows\system32\netman.dll
Service Host Launch Command	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted
Service Privileges	SeImpersonatePrivilege SeChangeNotifyPrivilege SeLoadDriverPrivilege
Registry Key	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netman
Depends on	Ole resource dll Network Store Interface RPC server

Εικόνα 167: Networks Connections Manager

Για να τροποποιήσουμε ή να δούμε τις επιλογές για αυτή την υπηρεσία πηγαίνουμε από το menu Start επιλέγουμε το Run και ακολούθως γράφουμε regedit. Στην συνέχεια εμφανίζεται το Registry Editor και ακολουθούμε τα εξής βήματα :

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netman



Εικόνα 168: Networks Connections Manager-Registry Key

Σε αυτή την διεύθυνση (http://localsystemnetworkrestricted.svchost-exe.net/) μπορούμε να δούμε κι άλλες υπηρεσίες του LocalSystemNetworkRestricted.

Κάθε ένα από αυτά τα έξι λειτουργεί με ένα διακριτικό περιορισμένης εγγραφής όπως περιγράφηκε νωρίτερα σ' αυτό το κεφάλαιο, με την εξαίρεση αυτών με επίθεμα NetworkRestricted.Περιορίζουν τη δυνατότητα πρόσβασης σε δίκτυα της υπηρεσίας σ' ένα σταθερό σύνολο θυρών, το οποίο θα καλύψουμε τώρα με λίγο περισσότερες λεπτομέρειες.

4.8.4 Περιορισμένη Πρόσβαση στο Δίκτυο

Με τη νέα έκδοση του Window Firewall (τώρα με Advanced Security) στα Vista και Server 2008, μπορούν να εφαρμοστούν πολιτικές περιορισμού δικτύου επίσης και σι υπηρεσίες. Το νέο firewall επιτρέπει σε διαχειριστές να δημιουργούν κανόνες που σέβονται τα παρακάτω γενικά χαρακτηριστικά σύνδεσης:

- **Κατευθυντικότητα** Μπορούν τώρα να εφαρμοστούν κανόνες και στην εισερχόμενη και στην εξερχόμενη κίνηση.
- **Πρωτόκολλο** Το firewall μπορεί τώρα να πάρει αποφάσεις με βάση ένα επεκταμένο σύνολο τύπου πρωτοκόλλου.
- **Φορέας** Μπορούν να διαμορφωθούν κανόνες που να ισχύουν μόνο για ένα συγκεκριμένο χρήστη.
- **Διεπαφές** Οι Administrator μπορούν τώρα να εφαρμόζουν κανόνες σε ένα δεδομένο σύνολο διεπαφών όπως Wireless, Local Area Network κ.λπ.

Η αλληλεπίδραση μ' αυτές και άλλα λειτουργίες του firewall αποτελούν απλώς μερικούς από τους τρόπους που μπορούν να ασφαλιστούν πρόσθετα υπηρεσίας.

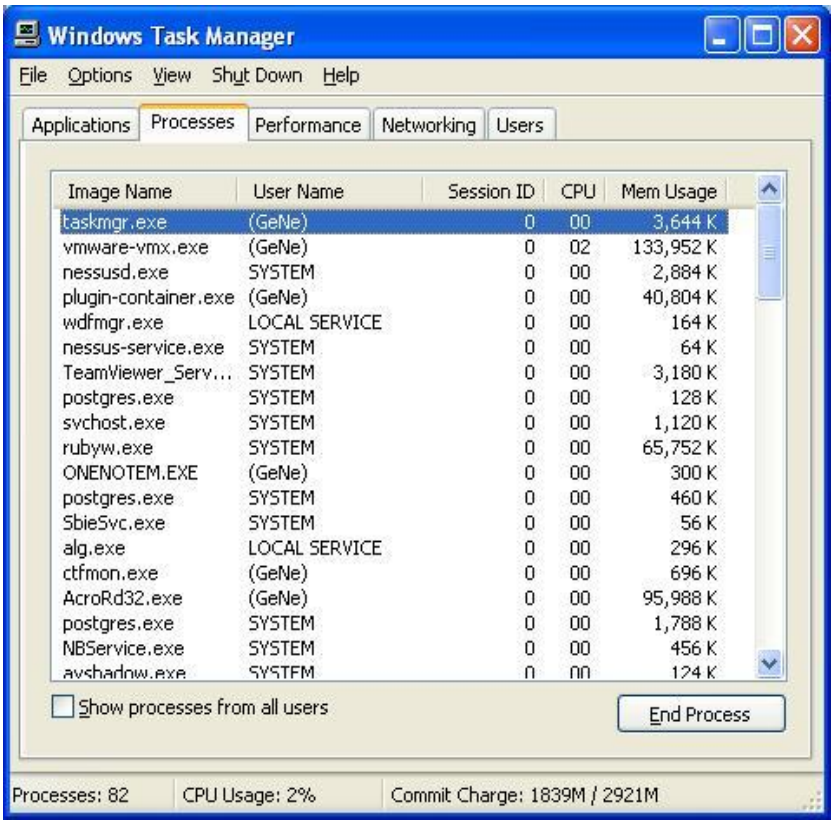
4.8.5 Απομόνωση Συνοδού 0

Το 2002, ο ερευνητής Chris Paget παρουσίασε μία νέα τεχνική επίθεσης για τα Windows, το «Shatter Attack»[15]. Η τεχνική περιελάμβανε ένα επιτιθέμενο με χαμηλότερα δικαιώματα που στέλνει ένα μήνυμα σε μία υπηρεσία με υψηλότερα δικαιώματα ώστε να την αναγκάσει να εκτελέσει αυθαίρετες εντολές, ανυψώνοντας τα δικαιώματα του επιτιθεμένου σ' αυτή την υπηρεσία. Στην απάντησή της στο έγγραφο του Paget, η Microsoft σημείωσε ότι: «από το σχεδιασμό τους, όλες οι υπηρεσίες μέσα στην διαλογική επιφάνεια εργασίας είναι ομότιμες και μπορούν να επιβάλουν αιτήματα η μία στην άλλη. Κατά συνέπεια, όλες οι υπηρεσίες στην διαλογική επιφάνεια εργασίας έχουν δικαιώματα ισοδύναμα με αυτά των πιο προνομιούχων υπηρεσιών.

[15] http://en.wikipedia.org/wiki/Shatter_attack

Σε πιο τεχνικό επίπεδο, αυτό ο σχεδιασμός επιτρέπει στους επιτιθέμενους να στέλνουν μηνύματα παραθύρων σε προνομιούχες υπηρεσίες επειδή μοιράζονται τη προεπιλεγμένη σύνοδο σύνδεσης, την Session 0[16].
Με το διαχωρισμό των συνόδων χρηστών και υπηρεσιών, μετριάζονται οι επιθέσεις τύπου shatter. Αυτή είναι η ουσία της απομόνωσης της συνόδου 0: στα Vista, οι υπηρεσίες και οι διεργασίες παραμένουν σε Session 0, ενώ οι σύνοδοι χρηστών αρχίζουν στην Session 1.

Αυτό μπορεί να παρατηρηθεί μέσα στο Task Manager εάν πάμε από το μενού Veiw και επιλέξουμε τη στήλη Session ID.



Εικόνα 169: Task Manager-Processes-Session ID

Μπορούμε να δούμε στην εικόνα, ότι οι περισσότερες διεργασίες υπηρεσιών και συστημάτων υπάρχουν στην Session 0, ενώ οι διεργασίες χρηστών υπάρχουν στην Session 1. Αξίζει να αναφέρουμε ότι δεν εκτελούνται όλες οι διεργασίες συστημάτων στην Session 0. Για παράδειγμα, το winlogon.exe και ένα στιγμιότυπο του csrsss.exe υπάρχουν σε συνόδους χρηστών κάτω από το πλαίσιο SYSTEM. Ακόμα κι έτσι, η απομόνωση συνόδου, σε συνδυασμό με άλλες λειτουργίες όπως τη MIC που συζητήθηκαν προηγουμένως, αντιπροσωπεύει έναν αποτελεσματικό μετριασμό για μία δυνατότητα που κάποτε χρησιμοποιούταν από τους επιτιθέμενους.

[16] http://www.microsoft.com/whdc/system/sysinternals/Session0Changes.mspx

4.9 Βελτιώσεις βασισμένες σε μεταγλωττιστή

Όπως έχουμε δει μέχρι τώρα, μερικά από τα χειρότερα τρωτά προκύπτουν από επιθέσεις μνήμης όπως υπερχείλιση buffer. Αρχίζοντας από τα Windows Vista και Server 2008 (οι προηγούμενες εκδόσεις εφαρμόζουν μερικές από αυτές τις λειτουργίες), η Microsoft εφάρμοσε μερικές λειτουργίες για να αποτρέψει τέτοιες επιθέσεις, που περιλαμβάνουν :

- GS
- SafeSEH
- Address Space Layout Randomization (ASLR)

Αυτές είναι λειτουργίες κυρίως κρυφές κατά τη μεταγλώττιση που δεν είναι διαμορφώσιμες από διαχειριστές η χρήστες. Παρέχουμε συνοπτικές περιγραφές αυτών των λειτουργιών ώστε να επεξηγήσουμε εδώ τη σημασία τους στην αποτροπή συνηθισμένων επιθέσεων.

Το GS είναι μία τεχνολογία κατά τη μεταγλώττιση η οποία στοχεύει να εμποδίσει την εκμετάλλευση υπερχειλίσεων buffer με βάση την στοίβα στην πλατφόρμα των Windows.Το GS το επιτυγχάνει αυτό τοποθετώντας μία τυχαία τιμή ή το cookie, στην στοίβα μεταξύ τοπικών μεταβλητών και την διεύθυνση επιστροφής. Μέρη του κώδικα σε πολλά προϊόντα της Microsoft μεταγλωττίζονται τώρα με το GS.

Όπως αρχικά περιγράφεται στο έγγραφο του Dave Litchfield ‘Defeating the Stack Based Overflow Prevention Mechanism of Microsoft Windows 2003 Server’ (αμυνόμενοι στον μηχανισμό υπερχείλισης με βάση την στοίβα του Microsoft Windows 2003 Server) (δείτε την διεύθυνση http://www.ngssoftware.com/papers/defeating-w2k3-stack-protection.pdf), ένας επιτιθέμενος μπορεί να επικαλύψει τον χειριστή εξαιρέσεων με μία ελεγχόμενη τιμή και να επιτύχει την εκτέλεση κώδικα μ ‘ έναν πιο αξιόπιστο τρόπο από την κατευθείαν επικάλυψη της διεύθυνσης επιστροφής. Για να αντιμετωπισθεί αυτό, εμφανίστηκε το SafeSEH στα Windows XP SP2 και Windows Server 2003 SP1. Όπως και το GS, έτσι και το SafeSEH (επίσης γνωστό ως Software Data Execution Prevention ή DEP) είναι μία τεχνολογία ασφάλειας κατά τη μεταγλώττιση. Αντίθετα, από το GS, αντί να προστατεύει τον δείκτη πλαισίων και την διεύθυνση επιστροφής, ο σκοπός του SafeSEH είναι να εξασφαλίζει το πλαίσιο των χειριστών εξαίρεσης δεν χρησιμοποιείται σωστά.

Το ASLR έχει σχεδιασθεί να μετριάζει την δυνατότητα ενός επιτιθέμενου να προβλέπει θέσεις στην μνήμη όπου βρίσκονται χρήσιμες οδηγίες και ελεγχόμενα δεδομένα. Πριν από το ASLR, οι εικόνες των Windows φορτώνονταν με συνεπείς τρόπους οι οποίοι επέτρεπαν να δουλεύουν αξιόπιστα οι επιθέσεις υπερχείλισης στοίβας σχεδόν σε κάθε υπολογιστή που έτρεχε μία τρωτή έκδοση του συγκεκριμένου λογισμικού, όπως έναν πανδημικό ιό που θα μπορούσε να μολύνει παγκοσμίως όλες τις εγκαταστάσεις των Windows. Για να το αντιμετωπίσει αυτό ή Microsoft υιοθέτησε προγενέστερες προσπάθειες που ήταν εστιασμένες στην τυχαιοποίηση της θέσης , όπου βρίσκονται οι εκτελέσιμες εικόνες (DLL, EXE κ.λπ.), ο σωρός και δεσμεύσεις της στοίβας. Όπως και το GS και το SafeSEH, έτσι και το ASLR

ενεργοποιείται επίσης μέσω μιας παραμέτρου κατά τη μεταγλώττιση, την επιλογή του linker /DYNAMICBASE.

Από την σκοπιά ενός απομακρυσμένου επιτιθέμενου, το ASLR παραμένει ένας αποτελεσματικός προστατευτικός μηχανισμός καθώς δεν υπάρχει κανένας τρόπος να προσδιοριστεί ή διεύθυνση φόρτωσης των εικόνων. Ωστόσο, ένας τοπικός επιτιθέμενος μπορεί να παράγει τις διευθύνσεις από χρήσιμα DLL επισυνάπτοντας ένα debugger σε οποιαδήποτε διεργασία. Επειδή η διεύθυνση φόρτωσης των DLL είναι αρκετά σταθερή σε μία διεργασία, είναι μεγάλη η πιθανότητα φόρτωσης του ίδιου DLL στην ίδια θέση μέσα σε μία προνομιούχο διεργασία. Υπό αυτήν την μορφή, η αποτελεσματικότητα του ASLR στον τοπικό υπολογιστή είναι αρκετά μειωμένη. Για να είμαστε δίκαιοι, το ASLR δεν έχει σχεδιασθεί να προστατεύεται από τοπικές επιθέσεις.

Κεφάλαιο 5 Συμπεράσματα

Στις μέρες μας η εγκληματικότητα αυξάνεται όλο και περισσότερο στον τομέα της πληροφορικής. Δεν υπάρχει αμφιβολία πως το έντονο ενδιαφέρον σήμερα για τα κενά ασφαλείας έχει καταστήσει πιο δύσκολη την ανάδειξη νέων σφαλμάτων ασφαλείας. Ωστόσο, η βιομηχανία παραγωγής λογισμικού ανεβάζει τον πήχη στην ασφάλεια/θωράκιση των εφαρμογών, έτσι με την σειρά τους και οι hackers αντιδρούν χρησιμοποιώντας πιο εξελιγμένες τεχνικές και εργαλεία διείσδυσης. Όπως και να έχει το να ασφαλίσουμε τους εαυτούς μας ενάντια στο κυβερνο-έγκλημα δεν είναι καθόλου εύκολη υπόθεση και χρειάζεται μια συνεχή προσπάθεια. Πρέπει να ακολουθούμε και να ενημερωνόμαστε για την τεχνολογία και να προσαρμοζόμαστε κατάλληλα με αυτήν έτσι ώστε να παραμένουμε ασφαλής. Οι επαγγελματίες τις ασφάλειας χρειάζονται τουλάχιστον διπλάσιες γνώσεις από αυτές που έχουν οι εγκληματίες ώστε να μπορέσουν να αντιμετωπίσουν τους κινδύνους.

Ο τομέας με τον οποίο έχουμε ασχοληθεί στη πτυχιακή αυτή βρίσκεται σε συνεχή εξέλιξη οπότε πάντοτε θα υπάρχει μελλοντική έρευνα ώστε να αντιμετωπίσουμε τις πιθανές αδυναμίες και τα τρωτά σημεία των συστημάτων για την ασφάλεια μας.

Συμβουλές για ενίσχυση της ασφάλειας του δικτύου

- **Διατηρείτε τον υπολογιστή σας ενημερωμένο**

Για να διατηρήσετε τους υπολογιστές του δικτύου σας ασφαλέστερους, ενεργοποιήστε τη δυνατότητα Αυτόματων ενημερώσεων σε όλους τους υπολογιστές. Τα Windows εγκαθιστούν αυτόματα σημαντικές και προτεινόμενες ενημερώσεις ή μόνο σημαντικές ενημερώσεις. Οι σημαντικές ενημερώσεις παρέχουν σημαντικά οφέλη, όπως βελτιωμένη ασφάλεια και αξιοπιστία. Οι συνιστώμενες ενημερώσεις μπορούν να αντιμετωπίσουν μη κρίσιμα προβλήματα και να βοηθήσουν στη βελτίωση της εμπειρίας σας κατά τη χρήση ηλεκτρονικών υπολογιστών. Οι προαιρετικές ενημερώσεις δεν λαμβάνονται ή εγκαθίστανται αυτόματα.

- **Χρήση τείχους προστασίας**

Το τείχος προστασίας εμποδίζει εισβολείς ή κακόβουλο λογισμικό (όπως ιούς τύπου worm) να αποκτήσουν πρόσβαση στον υπολογιστή σας μέσω δικτύου ή του Internet. Το τείχος προστασίας εμποδίζει επίσης τον υπολογιστή σας να στείλει λογισμικό κακόβουλης λειτουργίας σε άλλους υπολογιστές.

- **Εκτελείτε λογισμικό προστασίας από ιούς**

Τα τείχη προστασίας εμποδίζουν τους ιούς τύπου worm και τους εισβολείς να προσβάλουν τον υπολογιστή σας, αλλά δεν είναι σχεδιασμένα για να προστατεύουν από ιούς. Γι' αυτό θα πρέπει να εγκαταστήσετε και να χρησιμοποιείτε ένα λογισμικό προστασίας από ιούς. Οι ιοί μπορεί να προέρχονται από συνημμένα σε μηνύματα ηλεκτρονικού ταχυδρομείου, από αρχεία σε CD ή DVD ή από αρχεία που λαμβάνετε

από το Internet. Βεβαιωθείτε ότι το λογισμικό προστασίας από ιούς που χρησιμοποιείτε έχει ρυθμιστεί έτσι ώστε να εκτελεί σάρωση του υπολογιστή σας σε τακτά διαστήματα.

- **Χρησιμοποιήστε έναν δρομολογητή για να κάνετε κοινή χρήση μιας σύνδεσης στο Internet**

Εξετάστε το ενδεχόμενο χρήσης ενός δρομολογητή (ή συσκευή οικιακής πύλης) για να κάνετε κοινή χρήση μιας σύνδεσης στο Internet. Αυτές οι συσκευές διαθέτουν συνήθως ενσωματωμένα τείχη προστασίας και άλλες δυνατότητες, οι οποίες παρέχουν στο δίκτυό σας καλύτερη προστασία από τους εισβολείς.

- **Μην παραμένετε συνδεδεμένοι ως διαχειριστής**

Όταν χρησιμοποιείτε προγράμματα, τα οποία απαιτούν σύνδεση στο Internet, όπως είναι τα προγράμματα περιήγησης στο Web ή ένα πρόγραμμα ηλεκτρονικού ταχυδρομείου, συνιστούμε να συνδέεστε ως τυπικός χρήστης και όχι ως διαχειριστής. Αυτό ισχύει επειδή πολλοί ιοί και worm δεν μπορούν να αποθηκευτούν και να εκτελεστούν στον υπολογιστή σας, παρά μόνον εάν είστε συνδεδεμένοι ως διαχειριστής.

Βιβλιογραφία

Βιβλίο «Ασφάλεια Δικτύων» έκτη έκδοση των Stuart McClure, Joel Scambray και George Kurtz.

EBooks

Ebook Hacking Exposed Windows third Edition Widows Security Secrets & Solutions, Joel Scambray και Stuart McClure.

Ηλεκτρονική Βιβλιογραφία

Google → *www.google.com*

Microsoft Support → *http://support.microsoft.com/kb/129266*

Ss64 →*http://ss64.com/nt/*

Windows → *http://windows.microsoft.com/*

Windows server → *http://technet.microsoft.com/en-us/windowsserver*

Wikipedia → *http://www.wikipedia.org/*

Microsoft security →*http://www.microsoft.com/security/default.aspx*

Παράρτημα Α Ακρωνύμια - Συντομογραφίες

Τα ακρωνύμια και οι συντομογραφίες που χρησιμοποιήθηκαν στον οδηγό, ορίζονται παρακάτω.

A	
ACL	*Access Control Lists*
AD	*Active Directory*
AES	*Advanced Encryption Standard*
ARP	*Address Resolution Protocol*
ASLR	*Address Space Layout Randomization*
B	
BIOS	*Basic Input/Output System*
BCD	*Binary Coded Decimal*
C	
CPU	*Central processing unit*
D	
DCOM	*Distributed Component Object Model*
DEP	*Data Execution Prevention*
DESX	*Extended Data Encryption Standard*
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name System*
E	
EFS	*Encrypting File System*
F	
FEK	*File Encryption Key*
FTP	*File Transfer Protocol*
G	
GPMC	*Group Policy Management Console*
GPU	*Graphics Processing Unit*
H	
HKLM	*HKEY_Local_Machine*
HTTP	*Hypertext Transfer Protocol*
HTTPS	*HTTP Over SSL*
I	
ICF	*Internet Connection Firewall*
IDS	*Intrusion Detection System*
ILs	*Integrity Levels*
IMAP	*Internet Message Access Protocol*
IPv4	*Internet Protocol Version 4*

IPv6	*Internet Protocol Version 6*
IPsec	*Internet Protocol Security*
J	
K	
KDC	*Kerberos Key Distribution Center*
KEK	*Key Encrypting Key*
L	
LM	*LanManager*
LSA	*Local Security Authority*
LoRIE	*Low Rights IE*
M	
MIC	*Mandatory Integrity Control*
MITM	*Man in the middle*
MSRPC	*Microsoft Remote Procedure*
N	
NAP	*Network Access Protection*
NTLM	*NT LAN Manager*
NTFS	*New Technology File System*
NSA	*National Security Agency*
O	
OMB	*Office of Management and Budget*
OVAL	*Open Vulnerability and Assessment Language*
P	
PIN	*Personal Identification Number*
PKI	*Public Key Infrastructure*
Q	
QoS	*Quality of Service*
QRA	*Quantitative Risk Analysis*
R	
RA	*Remote Assistance*
RAS	*Remote Access Services*
RID	*User Relative ID*
RPC	*Remote Procedure Call*
S	
SACL	*System Access Control List*
SAM	*Security Accounts Manager*
SMB	*Server Message Block*
SCM	*Service Control Manager*

SCTP	*Stream Control Transmission Protocol*
SID	*Security Identifier*
SMS	*System Management Server*
SMTP	*Simple Mail Transfer Protocol*
SSH	*Secure Shell*
SSL	*Secure Sockets Layer*
T	
TCP	*Transmission Control Protocol*
TGS	*Ticket Granting Service*
TLS	*Transport Layer Security*
TPM	*Trusted Platform Module*
TS	*Terminal Service*
U	
UAC	*User Account Control*
UDP	*User Datagram Protocol*
UMDF	*User-Mode Driver Framework*
V	
VNC	*Virtual Network Computing*
VPN	*Virtual Private Network*
W	
WFP	*Windows File Protection*
WINS	*Windows Internet Naming Service*
WPA	*Wi-Fi Protected Access*
WRP	*Windows Resource Protection*
WSUS	*Windows Server Update Services*
X	
Y	
Z	

Πίνακας 2 : Συντομογραφίες

Παράρτημα Β Επεξήγηση Όρων

Β.1

Ένα κρυφό κοινόχρηστο στοιχείο αναγνωρίζεται από το σύμβολο του δολαρίου ($) στο τέλος του ονόματος του κοινόχρηστου στοιχείου. Τα κρυφά κοινόχρηστα στοιχεία δεν εμφανίζονται στη λίστα όταν πραγματοποιείτε αναζήτηση κοινόχρηστων στοιχείων σε έναν υπολογιστή ή όταν χρησιμοποιείτε η εντολή **net view.**
Το κοινόχρηστο στοιχείο **IPC$**[17] (Inter – Process Communication) χρησιμοποιείται για ανταλλαγή δεδομένων μεταξύ των εφαρμογών και των ηλεκτρονικών υπολογιστών. Το IPC$ με τη χρήση RPC (Remote Procedure Call), επιτρέπει στον πελάτη να στείλει διαφορετικές εντολές στον κεντρικό υπολογιστή:

- Λίστα όλων των κοινόχρηστων πόρων
- Λίστα όλων των χρηστών
- Κατάλογος αρχείων με κοινόχρηστο περιεχόμενο
- Stop / Start υπηρεσίες

Τα γράμματα μονάδων δίσκου C και D είναι κοινόχρηστα ως C$ και D$.
Σε Windows XP το κοινόχρηστο στοιχείο **C$** χρησιμοποιείται για διαχειριστικούς σκοπούς.
Τα κρυφά κοινόχρηστα στοιχεία διαχείρισης που δημιουργούνται από τον υπολογιστή (όπως το ADMIN$ και το C$) μπορούν να διαγραφούν, αλλά ο υπολογιστής τα δημιουργεί ξανά, αφού διακόψουμε και επανεκκινήσουμε την υπηρεσία διακομιστή ή επανεκκινήσουμε τον υπολογιστή μας. Τα κρυφά κοινόχρηστα στοιχεία που δημιουργούνται από χρήστες μπορούν να διαγραφούν και δεν δημιουργούνται ξανά μετά την επανεκκίνηση του υπολογιστή μας. Τα Microsoft Windows XP Home Edition δεν δημιουργούν κρυφά κοινόχρηστα στοιχεία διαχείρισης.

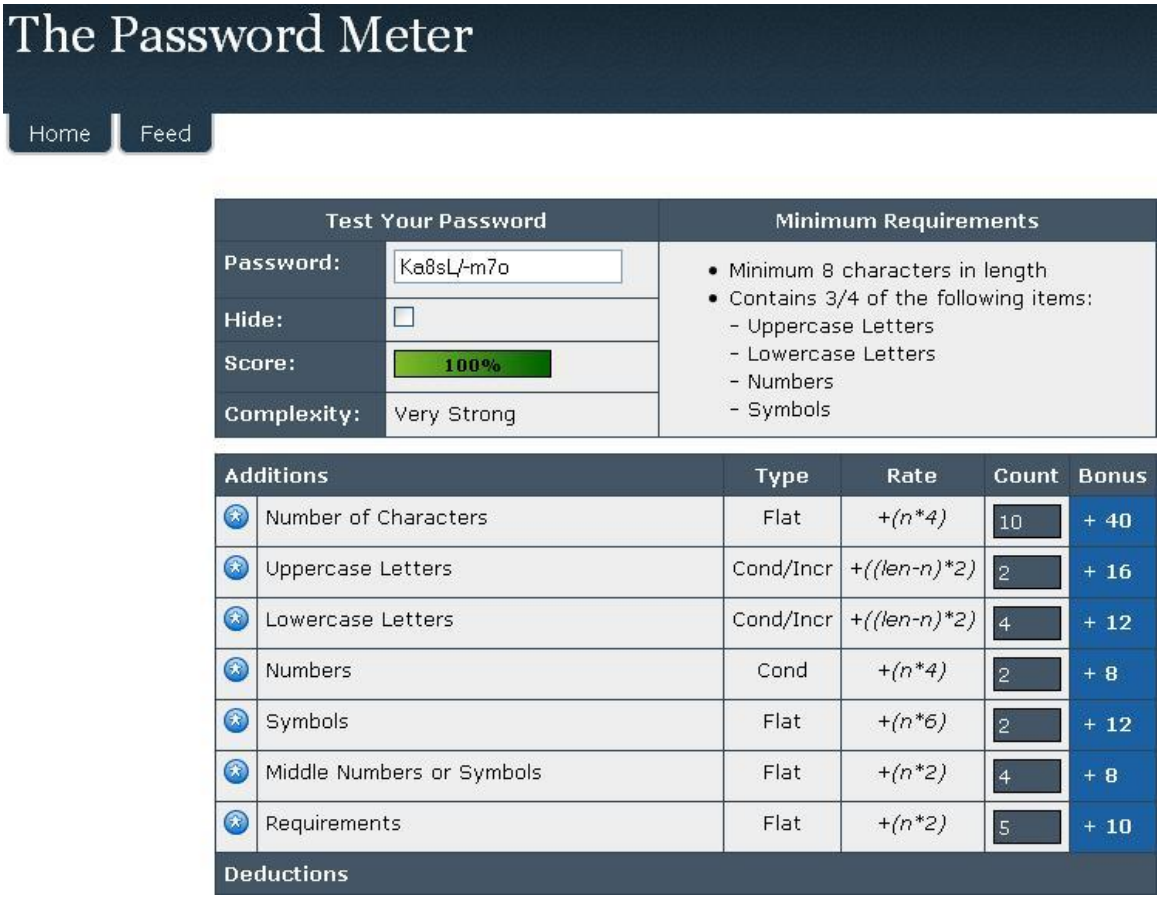
[17] http://support.microsoft.com/kb/314984
http://www.computercare.ca/forum/showthread.php?t=311

Παράρτημα Γ Password Meter

Γ.1

Πιο κάτω παρουσιάζουμε ένα τρόπο ώστε να ελέγξουμε τη δύναμη κάποιου κωδικού πρόσβασης .

Πηγαίνουμε στη σελίδα http://www.passwordmeter.com/ και εκεί εισάγουμε τον κωδικό μας.
Εάν το ποσοστό ασφαλείας όπου σας βγάζει είναι μικρό τότε θα πρέπει να αλλάξετε κωδικό. Ακολουθείστε τις ενδείξεις της σελίδας για καλύτερα αποτελέσματα.



✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
✓	Repeat Characters (Case Insensitive)	Comp	-	0	0
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
✓	Consecutive Lowercase Letters	Flat	-(n*2)	0	0
✓	Consecutive Numbers	Flat	-(n*2)	0	0
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0
✓	Sequential Numbers (3+)	Flat	-(n*3)	0	0
✓	Sequential Symbols (3+)	Flat	-(n*3)	0	0

Εικόνα 170:Έλεγχος ασφάλειας κωδικού πρόσβασης

Πολιτικές ασφάλειας κωδικού πρόσβασης

Ο κωδικός πρόσβασης πρέπει να πληροί τα πάρα κάτω κριτήρια :

Ο κωδικός πρέπει να αποτελείται από πολλούς χαρακτήρες. Κάθε χαρακτήρας που προσθέτετε στον κωδικό πρόσβασης αυξάνει την ασφάλεια που σας παρέχει στο πολλαπλάσιο. Οι κωδικοί πρόσβασής σας θα πρέπει να έχουν μήκος 8 χαρακτήρες ή περισσότερους.

Πολλά συστήματα επίσης υποστηρίζουν τη χρήση του διαστήματος στους κωδικούς πρόσβασης, έτσι ώστε να μπορείτε να δημιουργείτε μια φράση που να αποτελείται από πολλές λέξεις (μια "κωδική φράση"). Μια κωδική φράση είναι συχνά ευκολότερο να τη θυμηθείτε από έναν απλό κωδικό πρόσβασης, ενώ είναι μεγαλύτερη και πιο δύσκολο να τη μαντέψει κανείς.

Συνδυάστε γράμματα, αριθμούς και σύμβολα (για παράδειγμα: ! $ # ή %). Όσο μεγαλύτερη ποικιλία χαρακτήρων έχει ο κωδικός πρόσβασής μας, τόσο δυσκολότερο είναι να τον μαντέψουν. Άλλα σημαντικά στοιχεία είναι τα εξής:

- Όσο λιγότερους τύπους χαρακτήρων συμπεριλάβουμε σε έναν κωδικό πρόσβασης τόσο πιο μακρύς πρέπει να είναι. Ένας κωδικός πρόσβασης 15 χαρακτήρων που αποτελείται μόνον από τυχαία γράμματα και αριθμούς είναι περίπου 33.000 φορές ισχυρότερος από έναν κωδικό πρόσβασης 8 χαρακτήρων που αποτελείται από χαρακτήρες από ολόκληρο το πληκτρολόγιο. Αν δεν μπορούμε να δημιουργήσουμε έναν κωδικό πρόσβασης που να αποτελείται από σύμβολα, για να έχουμε τον ίδιο βαθμό προστασίας θα πρέπει να τον κάνουμε πολύ πιο μακρύ. Ένας ιδανικός κωδικός πρόσβασης συνδυάζει μήκος και διαφόρους τύπους συμβόλων.

- Καλό είναι να χρησιμοποιούμε ολόκληρο το πληκτρολόγιο, όχι μόνον τους πιο κοινούς χαρακτήρες. Τα σύμβολα που πληκτρολογούνται κρατώντας πατημένο το πλήκτρο "Shift" και πληκτρολογώντας έναν αριθμό είναι πολύ συνηθισμένα στους κωδικούς πρόσβασης. Ο κωδικός πρόσβασής μας θα είναι

πολύ πιο ισχυρός αν επιλέξετε από όλα τα σύμβολα του πληκτρολογίου, συμπεριλαμβανομένων των σημείων στίξης που δεν βρίσκονται στην κορυφαία σειρά του πληκτρολογίου και οποιωνδήποτε συμβόλων που είναι μοναδικά στη δική μας γλώσσα.

- Χρησιμοποιούμε λέξεις και φράσεις που εμείς τις θυμόμαστε εύκολα αλλά οι άλλοι δύσκολα θα τις μαντέψουν. Ο πιο εύκολος τρόπος να θυμόμαστε τους κωδικούς πρόσβασης και τις κωδικές φράσεις είναι να τα σημειώσουμε. Οι περισσότεροι πιστεύουν ότι είναι κακό να σημειώνει κανείς τους κωδικούς πρόσβασης. Αυτό είναι λάθος, αλλά θα πρέπει να τους προστατεύουμε προκειμένου να είναι ασφαλείς και αποτελεσματικοί.

Γενικά, οι κωδικοί πρόσβασης που γράφονται σε ένα κομμάτι χαρτί είναι δυσκολότερο να αποκαλυφθούν στο Internet από τους κωδικούς που αποθηκεύονται σε λογισμικό διαχείρισης κωδικών πρόσβασης, τοποθεσία Web ή άλλο εργαλείο αποθήκευσης λογισμικού.

Στρατηγικές δημιουργίες κωδικών πρόσβασης που πρέπει να αποφεύγουμε

Ορισμένες από τις συνηθισμένες μεθόδους που χρησιμοποιούνται για τη δημιουργία κωδικών πρόσβασης είναι εύκολο να τις μαντέψουν οι επιτιθέμενοι. Για να αποφύγουμε τους ανίσχυρους και εύληπτους κωδικούς πρόσβασης:

- Αποφεύγουμε τις ακολουθίες ή τους επαναλαμβανόμενους χαρακτήρες. Τα "12345678", "222222", "abcdefg" ή τα γράμματα που γειτονεύουν στο πληκτρολόγιο δεν χρησιμεύουν για τη δημιουργία ισχυρών κωδικών.

- Αποφεύγουμε την αντικατάσταση αριθμών ή συμβόλων αποκλειστικά στη βάση της ομοιότητας. Οι εγκληματίες και οι άλλοι κακόβουλοι χρήστες που γνωρίζουν αρκετά για να προσπαθήσουν να σπάσουν τους κωδικούς σας δεν θα ξεγελαστούν από συνηθισμένες αντικαταστάσεις στη βάση της ομοιότητας, π.χ. με το να αντικαταστήσετε το 'i' με '1' ή το 'a' με το '@', π.χ. "M1cr0$0ft" ή "P@ssw0rd". Αυτές οι αντικαταστάσεις όμως μπορούν να είναι αποτελεσματικές όταν συνδυάζονται με άλλα μέτρα, όπως το μήκος, οι ανορθογραφίες ή η χρήση πεζών-κεφαλαίων, για την αύξηση της ισχύος του κωδικού μας.

- Αποφεύγουμε να χρησιμοποιήσουμε το όνομα σύνδεσης. Είναι κακό να χρησιμοποιούμε το όνομα ή το επίθετό μας, τον αριθμό μητρώου μας, την ημερομηνία των γενεθλίων μας ή παρόμοια στοιχεία των αγαπημένων μας. Αυτά θα προσπαθήσουν να χρησιμοποιήσουν πρώτα οι επιτιθέμενοι.

- Αποφεύγουμε τις λέξεις του λεξικού, σε οποιαδήποτε γλώσσα. Οι επιτιθέμενοι χρησιμοποιούν εξελιγμένα εργαλεία που μαντεύουν γρήγορα τους κωδικούς πρόσβασης που βασίζονται σε λέξεις πολλών λεξικών, συμπεριλαμβανομένων

λέξεων γραμμένων ανάποδα, συνηθισμένων ανορθογραφιών και αντικαταστάσεων.

- Να χρησιμοποιούμε πολλαπλούς κωδικούς παντού. Αν κάποιος από τους υπολογιστές μας ή τα διαδικτυακά συστήματα που χρησιμοποιούν αυτό τον κωδικό πρόσβασης εκτεθεί, τότε θα πρέπει να θεωρηθεί ότι εκτέθηκαν και όλες οι άλλες πληροφορίες που προστατεύονται από αυτόν τον κωδικό πρόσβασης. Είναι πολύ σημαντικό να χρησιμοποιούνται διαφορετικοί κωδικοί πρόσβασης για διαφορετικά συστήματα.

- Αποφεύγουμε τη χρήση διαδικτυακών εργαλείων αποθήκευσης. Αν οι κακόβουλοι χρήστες βρουν αυτούς τους κωδικούς πρόσβασης αποθηκευμένους διαδικτυακά ή σε δικτυωμένο υπολογιστή, έχουν πρόσβαση σε όλες μας τις πληροφορίες.

Η επιλογή "κενού κωδικού πρόσβασης"

Ένας κενός κωδικός πρόσβασης (κανένας κωδικός πρόσβασης) στο λογαριασμό μας είναι ασφαλέστερος από έναν ανίσχυρο κωδικό πρόσβασης, όπως ο "1234". Οι εγκληματίες μπορούν να μαντέψουν εύκολα κάποιον απλούστερο κωδικό πρόσβασης αλλά, σε υπολογιστές που χρησιμοποιούν Windows XP, δεν μπορεί να προσπελαστεί από απόσταση ένας λογαριασμός μέσω δικτύου ή του Internet.(Αυτή η επιλογή δεν είναι διαθέσιμη για λειτουργικό σύστημα Microsoft Windows 2000, Windows Me ή νεότερες εκδόσεις). Μπορούμε να επιλέξουμε να χρησιμοποιήσουμε κενό κωδικό πρόσβασης στο λογαριασμό του υπολογιστή μας εάν πληρούνται τα παρακάτω κριτήρια:

- Έχουμε μόνον έναν υπολογιστή ή έχουμε πολλαπλούς υπολογιστές αλλά δεν χρειάζεται να προσπελαύνουμε πληροφορίες από τον έναν υπολογιστή στον άλλον.

- Ο υπολογιστής είναι φυσικά ασφαλής (εμπιστεύεστε όλους όσους έχουν φυσική πρόσβαση στον υπολογιστή).

- Η χρήση κενού κωδικού πρόσβασης δεν είναι πάντοτε καλή ιδέα. Για παράδειγμα, ένας φορητός υπολογιστής που τον παίρνουμε μαζί μας μάλλον δεν είναι φυσικά ασφαλής, οπότε θα πρέπει να έχει ισχυρό κωδικό πρόσβασης.

Κρατάμε τους κωδικούς πρόσβασης μυστικούς

Να διαχειριζόμαστε τους κωδικούς πρόσβασης και τις κωδικές φράσεις με την ίδια φροντίδα που διαχειριζόμαστε και τις πληροφορίες που προστατεύουν.

- Να μην τους αποκαλύπτουμε σε άλλους. Να κρατάμε τους κωδικούς πρόσβασής μας μυστικούς από τους φίλους και τα μέλη της οικογένειάς μας (ιδιαίτερα τα παιδιά) που μπορεί να τους αποκαλύψουν σε άλλα, μη έμπιστα πρόσωπα. Μόνες εξαιρέσεις είναι οι κωδικοί πρόσβασης που πρέπει να μοιραζόμαστε με άλλους, όπως είναι ο κωδικός πρόσβασης για το διαδικτυακό τραπεζικό σας λογαριασμό που πρέπει να είναι κοινός με τη σύζυγό μας.

- Να προστατεύουμε τους καταγεγραμμένους κωδικούς πρόσβασης. Να προσέχετε που αποθηκεύουμε τους κωδικούς πρόσβασης που καταγράφουμε ή που τους σημειώνουμε. Να μην αφήνουμε τα αρχεία μας έκθετα, όπως δεν θα αφήναμε και τα στοιχεία που προστατεύουν.

- Ποτέ να μην αποκαλύψουμε τον κωδικό πρόσβασης μέσω ηλεκτρονικού ταχυδρομείου και να μην τον καταγράφουμε σε αιτήσεις που αποστέλλονται μέσω ηλεκτρονικού ταχυδρομείου. Οποιοδήποτε μήνυμα ηλ. ταχυδρομείου που ζητά τον κωδικό πρόσβασης ή μας ζητά να μεταβείτε σε τοποθεσία Web για να επιβεβαιώσουμε τον κωδικό μας είναι σχεδόν βέβαια απάτη. Αυτό αφορά και τις αιτήσεις αξιόπιστων εταιρειών ή προσώπων. Τα μηνύματα ηλεκτρονικού ταχυδρομείου μπορούν να υποκλαπούν κατά τη μεταφορά και τα μηνύματα που απαιτούν την καταγραφή πληροφοριών ίσως να μην προέρχονται από τον αποστολέα που ισχυρίζονται. Οι απάτες ηλεκτρονικού "ψαρέματος" (phishing) μέσω Internet χρησιμοποιούν μηνύματα ηλεκτρονικού ταχυδρομείου για να μας παρασύρουν να αποκαλύψουμε ονόματα χρήστη και κωδικούς πρόσβασης, να κλέψουν στοιχεία ταυτότητας και άλλα.

- Να αλλάζουμε τακτικά τους κωδικούς πρόσβασης. Έτσι μπορεί να κρατήσουμε μακριά τους εγκληματίες και τους άλλους κακόβουλους χρήστες. Η ισχύς του κωδικού πρόσβασης θα μας βοηθήσει να τον διατηρήσουμε για περισσότερο χρόνο. Ένας κωδικός πρόσβασης μικρότερος από 8 χαρακτήρες θα παραμένει ισχυρός για μία περίπου εβδομάδα, ενώ ένας κωδικός πρόσβασης 14 χαρακτήρων ή μεγαλύτερος (που ακολουθεί και τους άλλους κανόνες που περιγράφηκαν παραπάνω) μπορεί να παραμείνει ισχυρός για χρόνια.

- Να μην πληκτρολογούμε κωδικούς πρόσβασης σε υπολογιστές που δεν ελέγχουμε. Οι υπολογιστές που υπάρχουν Internet café, εργαστήρια υπολογιστών, συστήματα κοινής χρήσης, συστήματα σε κιόσκια και αίθουσες αναμονής αεροδρομίων δεν θα πρέπει να θεωρούνται ασφαλείς για οποιαδήποτε χρήση εκτός από ανώνυμη περιήγηση στο Internet. Να μην χρησιμοποιούμε τους υπολογιστές αυτούς για να ελέγχουμε το ηλεκτρονικό σας ταχυδρομείο, να μπαίνουμε σε χώρους ηλεκτρονικής συνομιλίας, να ελέγχουμε το τραπεζικό σας υπόλοιπο και το επιχειρηματικό σας ταχυδρομείο ή για να μπαίνουμε σε οποιονδήποτε άλλον λογαριασμό που να απαιτεί όνομα χρήστη και κωδικό πρόσβασης. Οι εγκληματίες μπορούν να αγοράσουν πολύ φθηνά συσκευές σύνδεσης με πλήκτρα, που εγκαθίστανται σε ελάχιστο χρόνο. Οι συσκευές αυτές επιτρέπουν στους κακόβουλους χρήστες να συλλέγουν όλες τις πληροφορίες που πληκτρολογούνται σε έναν υπολογιστή μέσω

Internet—οι κωδικοί πρόσβασης και οι κωδικές σας φράσεις είναι το ίδιο σημαντικοί με τις πληροφορίες που προστατεύουν.

Τι πρέπει να κάνουμε αν κλαπεί ο κωδικός πρόσβασης

Να φροντίσουμε να παρακολουθούμε όλες τις πληροφορίες που προστατεύουμε με τους κωδικούς πρόσβασης, όπως οι μηνιαίες οικονομικές μας αναφορές, οι αναφορές της πιστωτικής μας κάρτας, οι λογαριασμοί διαδικτυακών αγορών κ.λπ. Οι ισχυροί κωδικοί πρόσβασης που απομνημονεύονται εύκολα μπορούν να μας προστατεύσουν από τις απάτες και την κλοπή στοιχείων ταυτότητας, αλλά δεν υπάρχουν εγγυήσεις. Όσο ισχυρός και να είναι ο κωδικός πρόσβασης, αν κάποιος "σπάσει" το σύστημα όπου είναι αποθηκευμένος τότε θα έχει πρόσβαση και σε αυτόν. Αν παρατηρήσουμε ύποπτη δραστηριότητα που υποδεικνύει ότι έχει κάποιος προσπελάσεις τις πληροφορίες μας, ειδοποιήστε τις αρχές το συντομότερο δυνατό. Περισσότερες πληροφορίες σχετικά με το τι πρέπει να κάνουμε αν πιστεύουμε ότι έχουν κλαπεί τα στοιχεία της ταυτότητάς μας ή ότι έχουμε πέσει θύμα παρόμοιας απάτης.

Κλείνουμε όλους τους λογαριασμούς που επηρεάζονται

Επικοινωνούμε με την αρχική εταιρεία ή τον οργανισμό εάν πιστεύουμε πως δώσαμε ευαίσθητες πληροφορίες σε άγνωστη πηγή, η οποία προσποιήθηκε πώς ήταν η πραγματική εταιρεία ή οργανισμός. Εάν επικοινωνήσουμε αμέσως με την πραγματική εταιρεία, ίσως μπορέσουν να περιορίσουν τη ζημιά προς εμάς και προς τους υπολοίπους. Κατόπιν:

- Επικοινωνούμε με το τμήμα ασφάλειας ή απάτης κάθε τράπεζας ή πιστωτικού ιδρύματος με το οποίο συνεργαζόμαστε, συμπεριλαμβανομένων των εταιριών πιστωτικών καρτών, οργανισμών κοινής ωφέλειας, εταιρειών παροχής υπηρεσιών Internet και άλλων τοποθεσιών όπου χρησιμοποιούμε την πιστωτική μας κάρτα, για κάθε ύποπτη πρόσβαση ή άνοιγμα λογαριασμού.

- Στη συνέχεια, στέλνουμε μία επιστολή και κρατούμε και ένα αντίγραφο για εμάς.

Αλλάζουμε τους κωδικούς πρόσβασης σε όλους μας τους λογαριασμούς στο Internet.

Όταν αλλάξουμε τους κωδικούς ή όταν ανοίξετε νέους λογαριασμούς, χρησιμοποιήστε ισχυρούς κωδικούς πρόσβασης.

Προσθέτουμε ειδοποίηση απάτης στους πιστωτικούς μας λογαριασμούς.