Πανεπιστήμιο Πειραιώς
Τμήμα Ψηφιακών Συστημάτων
Μεταπτυχιακό Πρόγραμμα: «Δικτυοκεντρικά Συστήματα»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Θέμα: Password Cracking & Key Logging

Υπεύθυνος Καθηγητής:

Κάτσικας Σωκράτης

Σπουδαστής:

Χρόνης Ανδρέας **ΜΕ/07112** **axroniscs@gmail.com**

ΠΕΙΡΑΙΑΣ

Ακαδημαϊκό Έτος 2008 – 2009

Περιεχόμενα:

1. Εισαγωγή

Στη συγκεκριμένη μελέτη θα ασχοληθούμε με τρόπους παραβίασης και υποκλοπής δεδομένων από χρήστες. Στο επόμενο κεφάλαιο θα αναφέρουμε βασικά στοιχεία περί ασφάλειας.

Συνεχίζοντας, στο 3ο κεφάλαιο θα αναφέρουμε το Password Cracking, δηλαδή το «σπάσιμο» ή καλύτερα την παραβίαση των κωδικών που χρησιμοποιεί κάποιος χρήστης ώστε να καταφέρουμε να έχουμε πρόσβαση στα αρχεία του. Θα αναλύσουμε τις διάφορες τεχνικές που χρησιμοποιούνται για να επιτευχθεί αυτό και έπειτα θα δοκιμάσουμε και θα μελετήσουμε μερικά από τα κορυφαία προγράμματα σε αυτόν τον τομέα, για να επιτύχουμε την παραβίαση διαφόρων στόχων που θα έχουμε θέσει στα σενάρια μας.

Στο 4ο κεφάλαιο της μελέτης θα αναφερθούμε στο Key Logging, δηλαδή στην υποκλοπή των πληκτρολογήσεων (σαν βασική ιδέα) αλλά και γενικότερα όλων των κινήσεων του χρήστη ώστε να υποκλέπτουμε συνεχώς προσωπικά του δεδομένα και κωδικούς που χρησιμοποιεί. Θα αναλύσουμε διάφορες μεθόδους που χρησιμοποιούνται και έπειτα θα δοκιμάσουμε και θα μελετήσουμε μερικούς από τους κορυφαίους key loggers για να υποκλέψουμε στοιχεία από στόχους που θα έχουμε θέσει στα σενάρια μας προσπαθώντας να μη γίνουμε αντιληπτοί από τον χρήστη και από το σύστημα.

Τέλος, στο 5ο κεφάλαιο θα περιγράψουμε τη δικιά μας υλοποίηση μιας εφαρμογής password cracking. Θα την δοκιμάσουμε όπως κάναμε και στις εφαρμογές στην ενότητα 3 και θα βγάλουμε τα ανάλογα συμπεράσματα. Σαν γενικά χαρακτηριστικά του προγράμματος αναφέρουμε ότι θα επιτίθεται και με τις δυο πιο δημοφιλής τεχνικές επίθεσης, με brute forcing και dictionary attack.

2. Γενικά περί ασφάλειας

Η ασφάλεια των δεδομένων στη σημερινή εποχή παίζει πρωτεύοντα ρόλο στη ζωή μας. Θέλουμε να προφυλάξουμε τα προσωπικά μας δεδομένα, οικογενειακά στοιχεία, οικονομικά δεδομένα, εταιρικά έγγραφα, φορολογικά στοιχεία κτλ από το να τα χρησιμοποιήσουν άλλοι για να επιτύχουν κακόβουλους στόχους. Θέλουμε να έχουμε εμείς μόνο πλήρη πρόσβαση, να μπορούμε να δίνουμε πρόσβαση μόνο σε συγκεκριμένα άτομα για να τα βλέπουν και σίγουρα να μην τα αλλάζει κανένας άλλος.

Στις μέρες μας, προγράμματα παραβίασης κωδικών (password crackers) και καταγραφής πληκτρολογήσεων(key loggers) καθώς και άλλοι μέθοδοι όπως το phishing είναι ευρέως διαδεδομένα και μεγάλο πλήθος επιθέσεων πραγματοποιείται καθημερινά σε ανυποψίαστους χρήστες που δεν έχουν, και δε φροντίζουν να έχουν, τη γνώση για να προστατευτούν σωστά. Τέτοιου τύπου επιθέσεις θα αναλύσουμε παρακάτω.

Για την προστασία των χρηστών και των δεδομένων τους υπάρχουν πολλοί διαφορετικοί τρόποι. Η κρυπτογράφηση, οι κωδικοί ασφαλείας, τα τείχη προστασίας, τα anti-virus, τα permissions κτλ είναι μερικοί από αυτούς τους τρόπους και δρουν σε διαφορετικά επίπεδα και με διαφορετικούς στόχους. Κάποια από αυτά θα τα αναφέρουμε παρακάτω σε σχέση με το password cracking και το key logging.

3. Passwords - Password Cracking

Οι κωδικοί πρόσβασης είναι ένας βασικός και συνήθης τρόπος για να προστατεύσουμε τα δεδομένα μας από τρίτους. Αυτοί οι κωδικοί για την πρόσβαση σε υπολογιστικά συστήματα αποθηκεύονται συνήθως σε μια βάση δεδομένων ώστε το σύστημα να μπορεί να επαληθεύσει τον κωδικό που εισάγει κάποιος χρήστης όταν δοκιμάζει να συνδεθεί στο σύστημα ή να αποκτήσει πρόσβαση σε έναν προστατευμένο πόρο. Προφανώς, οι κωδικοί δεν αποθηκεύονται σε απλό κείμενο, αλλά κρυπτογραφούνται με διάφορες συναρτήσεις και το αποτέλεσμα αυτών αποθηκεύεται στη βάση. Αργότερα όταν ένας χρήστης προσπαθήσει να κάνει authentication ο κωδικός που δίνει σαν είσοδο, κρυπτογραφείται με τον ίδιο αλγόριθμο και το αποτέλεσμα συγκρίνεται με τον αποθηκευμένο.

Εικόνα 3-1: Παράδειγμα φόρμας σύνδεσης (login) στα windows

Παρόλο που η συνάρτηση που δημιουργεί τους κρυπτογραφημένους κωδικούς είναι, όσον αφορά την κρυπτογραφία της, ασφαλής, η κατοχή του κρυπτογραφημένων κωδικών, δυστυχώς, παρέχει έναν γρήγορο τρόπο να δοκιμαστούν πιθανοί κωδικοί που θα κρυπτογραφούνται και θα συγκρίνονται.

Το Password cracking είναι η διαδικασία της ανάσυρσης κωδικών από δεδομένα που έχουν αποθηκευτεί. Μια απλή προσέγγιση είναι η επαναλαμβανόμενη δοκιμή κωδικών μέχρι να βρεθεί ο σωστός. Λόγοι που χρησιμοποιείται το Password cracking είναι η ανάγκη για εύρεση ενός ξεχασμένου κωδικού, η μη επιτρεπτή πρόσβαση σε ένα σύστημα ή και ένας τρόπος να βλέπουν οι διαχειριστές ενός συστήματος πόσο εύκολους κωδικούς έχουν οι χρήστες τους.

Α. Κατηγορίες επιθέσεων:

1) Weak encryption

Αν ένα σύστημα χρησιμοποιεί «φτωχή» κρυπτογράφηση για την προστασία αποθηκευμένων κωδικών, ένας επιτιθέμενος μπορεί να εκμεταλλευτεί τις αδυναμίες τους συστήματος για να βρει τους κωδικούς που χρειάζεται. Ένα παράδειγμα είναι ο αλγόριθμος LM Hash που χρησιμοποιούσε η Microsoft σαν προεπιλογή για την κρυπτογράφηση των κωδικών μέχρι 15 χαρακτήρων έως και τα windows XP. Ο αλγόριθμος αυτός μετατρέπει τον κωδικό σε κεφαλαία γράμματα και σπάει τον κωδικό σε 2 κομμάτια 7 χαρακτήρων που κρυπτογραφούνται χωριστά. Έτσι ο επιτιθέμενος μπορεί να επιτεθεί χωριστά όπως θα το έκανε και σε κωδικούς 7 χαρακτήρων και έτσι χάνεται το πλεονέκτημα των περισσότερων χαρακτήρων.

Παρόλα αυτά, η κρυπτογράφηση κωδικών με δυνατότερους τρόπους κρυπτογράφησης όπως οι MD5, SHA-512, SHA-1, και RIPEMD-160 μπορούν και πάλι να είναι ευάλωτες σε επιθέσεις brute-force και precomputation όμως τέτοιες επιθέσεις δε βασίζονται σε reversing του κρυπτογραφικού αλγορίθμου. Αντίθετα, σε αυτή την περίπτωση, κρυπτογραφούν ένα μεγάλο πλήθος πιθανών κωδικών και συγκρίνουν τα αποτελέσματα με τα αποθηκευμένα. Σύγχρονοι τρόποι κρυπτογράφησης όπως ο MD5 και ο bcrypt χρησιμοποιούν επίτηδες αργούς αλγόριθμους ώστε το πλήθος των συνδυασμών που θα δοκιμαστούν να είναι σχετικά μικρός.

2) Guessing

Τους κωδικούς ασφαλείας μπορούν αρκετές φορές να τους μαντέψουν οι επιτιθέμενοι χρησιμοποιώντας προσωπικά δεδομένα του χρήστη. Παραδείγματα από συχνούς τύπους κωδικών:

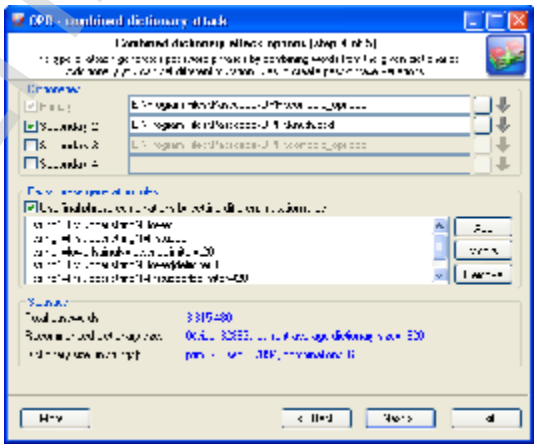
- κενό
- λέξεις όπως "password", "passcode", “passwd”, "admin" κτλ
- λέξεις όπως “god”, “sex”, “man”, “woman”, “money” κτλ
- μια σειρά γραμμάτων από qwerty πληκτρολόγιο -- *qwerty*, asdf, ή qwertyuiop)
- το όνομα χρήστη
- το όνομα συζύγου, τέκνου, κατοικίδιου
- η πόλη γέννησης, ημερομηνία γέννησης, δικά τους ή συζύγου, τέκνου κτλ

- η πινακίδα του αυτοκινήτου τους
- το νούμερο του γραφείου τους, τηλέφωνο, ταχυδρομικός κωδικός κτλ
- ένα όνομα κάποιου αγαπημένου τραγουδιστή, ηθοποιού κτλ
- βρισιές

Προσωπικά δεδομένα είναι διαθέσιμα παντού, κυρίως στο διαδίκτυο, και μπορούν να βρεθούν και χρησιμοποιώντας διάφορες τεχνικές που θα τις δούμε αναλυτικά στο επόμενο κεφάλαιο. Ιδίως οι επιτιθέμενοι που γνωρίζουν τον χρήστη μπορούν να βρουν εύκολα τέτοιες πληροφορίες.

3) Dictionary attacks

Οι χρήστες συχνά επιλέγουν αδύναμα, λίγων χαρακτήρων(<7), Passwords. Παραδείγματα είδαμε πιο πάνω, απλές λέξεις που περιέχονται στα πιο μικρά λεξικά, ονόματα και λίγοι αριθμοί. Έρευνες 40 ετών έχουν δείξει ότι περίπου το 40% των κωδικών που επιλέγουν οι χρήστες βρίσκονται άμεσα από προγράμματα cracking που χρησιμοποιούν λεξικά. Σε μια πρόσφατη έρευνα σε γνωστή σελίδα ενός social network έδειξαν ότι κωδικοί που είχαν κλαπεί με phishing, το 4% αυτών ήταν μια απλή μικρή λέξη και το 12% ήταν μια απλή λέξη συν έναν αριθμό που στο 66% των περιπτώσεων αυτό ήταν το 1!



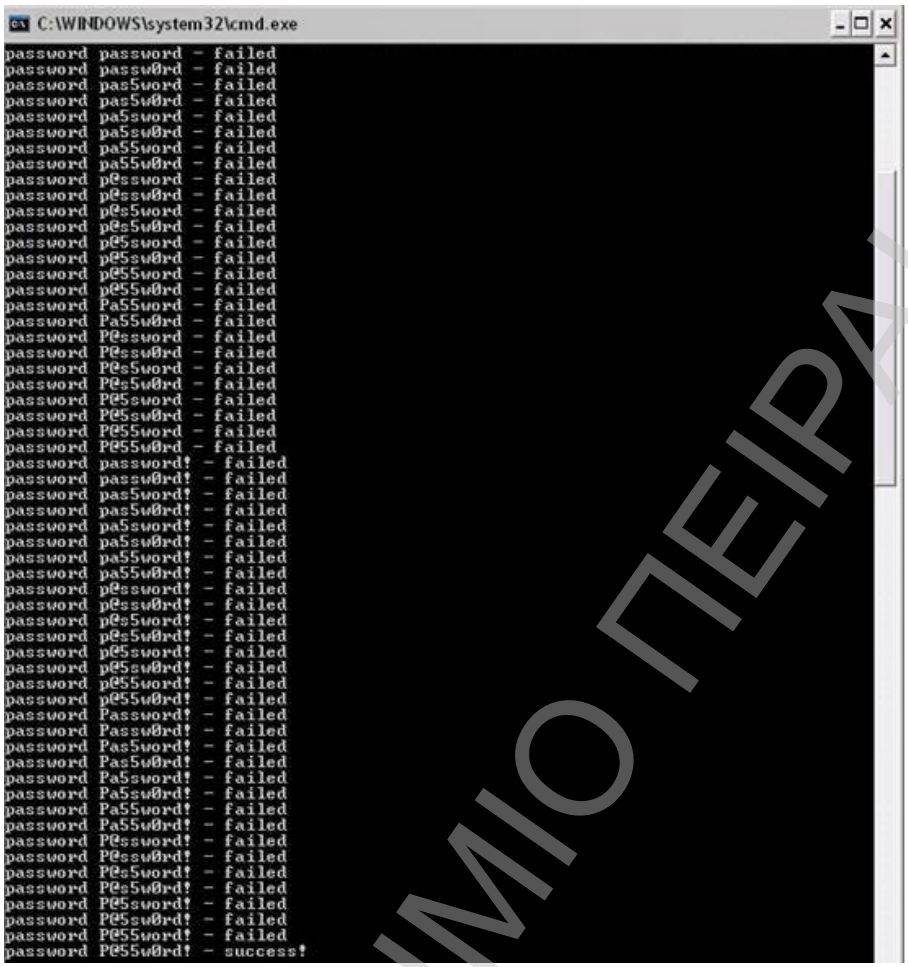
Εικόνα 3-2: Παράδειγμα Dictionary Attack

Κάποιοι χρήστες δεν αλλάζουν το προεπιλεγμένο password που είχε το υπολογιστικό τους σύστημα όπως και κάποιοι administrators δεν αλλάζουν τους κωδικούς που έχει το λειτουργικό σύστημα και διατηρούν αυτό που είχε αφήσει αυτός που έκανε την εγκατάσταση. Επίσης λίστες με τα προεπιλεγμένα passwords είναι διαθέσιμες σε σελίδες στο διαδίκτυο. Ο Gary McKinnon, είχε κατηγορηθεί στις Η.Π.Α. ως ο άνθρωπος που έκανε τη μεγαλύτερη στρατιωτική παραβίαση όλων των εποχών ενώ αυτός απλά έτρεξε ένα script που του έδειχνε που υπάρχει κενός κωδικός. Δηλαδή, απλά δεν είχε αλλαχθεί ο προεπιλεγμένος κωδικός που ήταν το κενό.

Σύγχρονα προγράμματα cracking που χρησιμοποιούν λεξικά δέχονται και προσωπικές πληροφορίες για τον χρήστη και παράγουν κωδικούς χρησιμοποιώντας αυτές.

4) Brute force attack

Μια δυνατή τεχνική που λέγεται brute force είναι να δοκιμάσεις κάθε πιθανό κωδικό. Θεωρητικά, μια τέτοια επίθεση έχει πάντα επιτυχία εφόσον οι κανόνες για τους αποδεκτούς κωδικούς είναι ευρέως γνωστοί, αλλά εφόσον το πλήθος των χαρακτήρων πάντα μεγαλώνει, μεγαλώνει και το πλήθος των πιθανών κωδικών. Οπότε αυτή η μέθοδος παραμένει πρακτική όσο το μέγεθος των κωδικών είναι μικρό. Η χρήση αυτής της τεχνικής εξαρτάται κυρίως και από το τι είδους πρόσβαση έχει ο επιτιθέμενος στο αρχείο που κρατά τους κρυπτογραφημένους κωδικούς. Αν έχει πρόσβαση και μπορεί να του επιτεθεί τότε λέμε ότι είναι offline επίθεση ενώ αν δεν έχει πρόσβαση και πρέπει να επιτεθεί μέσω κάποιας σύνδεσης τότε λέγεται online επίθεση. Η offline προφανώς είναι πιο εύκολη γιατί στην online ο επιτιθέμενος θα έχει προβλήματα με timeouts, delays και άλλα προβλήματα ασφαλείας που μπορεί να του προκαλεί η απομακρυσμένη σύνδεση.



Εικόνα 3-3: Παράδειγμα Brute Force Attack

Μια συχνή πρόταση για μήκος χαρακτήρων ενός κωδικού είναι τουλάχιστον 8 χαρακτήρες με τυχαία επιλεγμένα γράμματα, αριθμούς και ειδικούς χαρακτήρες. Η πρόταση αυτή έχει λογική όταν χρησιμοποιούνται ισχυροί αλγόριθμοι κρυπτογράφησης όπως ο md5 ή ο blowfish ενώ είναι ακατάλληλη σε συστήματα ms windows γιατί αποθηκεύουν τον κωδικό αφού τον σπάνε σε κομμάτια των 7 χαρακτήρων. Σε αυτά τα συστήματα ένας κωδικός 8 χαρακτήρων σπάει σε δυο κομμάτια όπου το δεύτερο θα είναι ενός χαρακτήρα. Επίσης σε συστήματα που δεν επιτρέπονται οι ειδικοί χαρακτήρες ή δεν υπάρχει διάκριση σε πεζά και κεφαλαία πάλι η επίθεση με brute force τεχνική είναι αποδοτική και ο χρήστης μπορεί μόνο να βάλει αρκετά μεγαλύτερο κωδικό για να δυσκολέψει λίγο την κατάσταση.

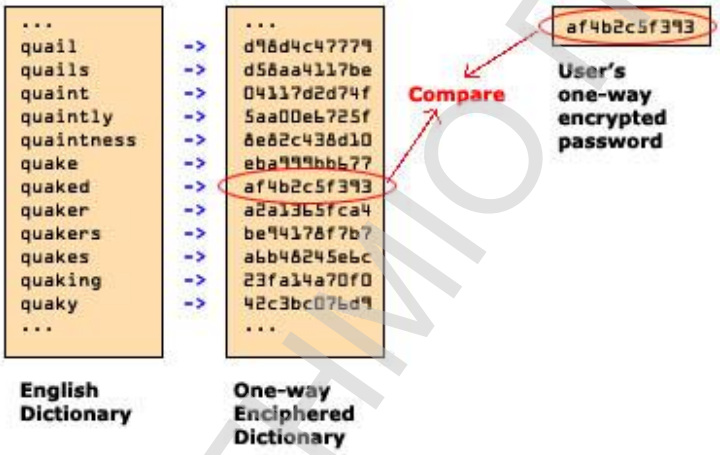
Στατιστικά οι γενικευμένες επιθέσεις της τεχνικής brute force είναι συχνά επιτυχημένες γιατί οι χρήστες δεν τηρούν τα παραπάνω μέτρα ασφαλείας και επειδή η υπολογιστική δύναμη έχει αυξηθεί πολύ. Επιπλέον, όμως, οι έξυπνες brute-force επιθέσεις που περιλαμβάνουν δεδομένα για το πώς οι χρήστες επιλέγουν κωδικούς είναι ακόμα πιο αποδοτικές.

Τέλος πρέπει να γίνει σαφές ότι τα όρια ανάμεσα στις τεχνικές brute force και σε αυτές με λεξικό δεν είναι απόλυτα. Οι τεχνικές έχουν το κοινό ότι ο επιτιθέμενος

δοκιμάζει όλους τους κωδικούς από μια προκαθορισμένη λίστα η οποία όμως προκαθορίζεται με διαφορετικό τρόπο.

5) Precomputation

Η τεχνική του precomputation, βασίζεται στη λογική της dictionary επίθεσης. Στην ουσία, στη βασική της μορφή ο αλγόριθμος ξεκινά με το να κρυπτογραφεί όλο το λεξικό, να το αποθηκεύει και μετά να δοκιμάζει να κάνει επίθεση χρησιμοποιώντας πλέον κατευθείαν τις κρυπτογραφημένες λέξεις για να τις ταυτοποιήσει με τον κωδικό του χρήστη. Έτσι, με αυτό τον τρόπο οι δοκιμές γίνονται πιο γρήγορα και μπορεί να υλοποιηθεί πιο άνετα λόγο του χαμηλού πλέον κόστος των αποθηκευτικών μέσων μιας και η κρυπτογράφηση ενός λεξικού απαιτεί πολύ μεγάλο αποθηκευτικό χώρο.



Εικόνα 3-4: Αναπαράσταση precomputation attack

Εξελιγμένες μέθοδοι precomputation είναι πολύ πιο αποτελεσματικές. Υπάρχουν παραδείγματα του αλγορίθμου που βρίσκει τον κωδικό σε συστήματα windows που χρησιμοποιούν τον Windows LAN Manager σε μερικά δευτερόλεπτα που είναι πολύ πιο γρήγορο από brute force επίθεση.

Μια τεχνική παρόμοια με το precomputation, γνωστή ως memoization, χρησιμοποιείται για να σπάει παράλληλα πολλούς κωδικούς. Αφού το πιο αργό στάδιο σε αυτή τη διαδικασία είναι η κρυπτογράφηση της λέξης και όχι η σύγκριση, κάθε φορά που κρυπτογραφείται μια λέξη χρησιμοποιείται για σύγκριση με όλους τους κωδικούς. Βέβαια οι δυο τεχνικές μπορούν να συνδυαστούν για καλύτερη απόδοση.

6) Τι είναι το salt;

Τα προτερήματα και τα επιτυχημένα αποτελέσματα των μεθόδων precomputation και memorization μπορούν να εκμηδενιστούν αν κάνουμε την διαδικασία κρυπτογράφησης να βασίζεται σε κάτι που είναι τυχαίο. Αυτό λέγεται salting. Κάθε φορά που ο χρήστης βάζει ένα password, ένα μικρό τυχαίο πλήθος χαρακτήρων προστίθεται στο τέλος του κωδικού πριν την κρυπτογράφηση του. Αυτό είναι το salt. Αφού το salt είναι σε κάθε περίπτωση διαφορετικό σε κάθε χρήστη και δεν εξαρτάται από τον χρήστη ο επιτιθέμενος δε μπορεί πλέον να δημιουργήσει πίνακες με κρυπτογραφημένους κωδικούς και δε μπορεί να χρησιμοποιήσει προσωπικά στοιχεία του. Τα αρχικά Unix συστήματα χρησιμοποιούσαν 12-bit salt. Βέβαια οι επιτιθέμενοι μπορούσαν πάλι να κωδικοποιήσουν όλους τους κωδικούς που είχαν ήδη να δοκιμάσουν μαζί με τα 4096 πιθανά salts. Βέβαια όσο μεγαλώνει το salt τόσο πιο πολύ πολλαπλασιάζονται αυτοί οι συνδυασμοί. Οπότε τώρα που οι τεχνικές md5 και bcrypt χρησιμοποιούν 48 και 128 bits για salt οι συνδυασμοί τείνουν στο άπειρο.

Β. Μελέτη και δοκιμή top password crackers

Σε αυτή την ενότητα θα μελετήσουμε την λειτουργία και την αποδοτικότητα κάποιων κορυφαίων password crackers. Η επιλογή των crackers έγινε μετά από έρευνα σε διάφορες κοινότητες καθώς και διάφορες εταιρείες και site που ασχολούνται με τέτοια εργαλεία(Insecure.org, Computer Security Institute) και έχουνε λίστες ανάλογου λογισμικού παραβίασης κωδικών. Αυτό που ψάχναμε και είχαμε σαν κριτήριο επιλογής ανάμεσα στους crackers ήταν προγράμματα που να σπάνε κωδικούς των λειτουργικών συστημάτων Windows και Linux. Η επιλογή τριών top προγραμμάτων έγινε μέσα από τη δικιά τους κατάταξη.

Θα πραγματοποιήσουμε δοκιμές με διάφορους τύπους κωδικών και θα προσπαθήσουμε να τους σπάσουμε. Οι κωδικοί αυτοί έχουν επιλεγεί συγκεκριμένα ώστε να προσομοιώνουν κωδικούς χρηστών και να παρέχουν αυξανόμενη δυσκολία και ασφάλεια για να καλύψουν την πλειοψηφία των πιθανών επιλογών και να μας δείξουν τις δυνατότητες των προγραμμάτων. Είναι οι παρακάτω:

α/α	*Χρήστης*	*Κωδικός*
1	andreas	andreas
2	andreas1	andreas01
3	andreas2	andreas222

4	andreas3	4ndr3as
5	andreas4	@ndR3@$
6	andreas5	@ndR3@$1984
7	andreas6	#Nv*Y9KfAX

Εικόνα 3-5: Πίνακας users-passwords προς επίθεση

1. Η περίπτωση αυτή αναπαριστά την επιλογή ενός μεγάλου ποσοστού χρηστών που βάζουν ίδιο όνομα χρήστη με κωδικό. Θέλει να μας δείξει πόσο εύκολο είναι να βρεθεί ο κωδικός αν είναι ακριβώς ίδιος.

2. Η δεύτερη περίπτωση αναπαριστά την επιλογή πολλών χρηστών που θέλουν ένα εύκολο κωδικό αλλά βάζουν και έναν αριθμό μετά από το όνομα τους ώστε να τον «δυσκολέψουν». Και όπως είδαμε παραπάνω σε κάποια στατιστικά στοιχεία, τα 2/3 των χρηστών χρησιμοποιούν τον αριθμό «1». Επίσης, παρατηρούμε ότι οι αριθμοί είναι από τον 8 χαρακτήρα και μετά και θα εξηγήσω αργότερα γιατί κάνω αυτή την παρατήρηση. Θα δούμε πόσο αποδοτικός είναι αυτός.

3. Παρόμοια με την προηγούμενη περίπτωση μόνο που ο αριθμός στο τέλος δείχνει σαν παράδειγμα user+αύξων αριθμός, παράδειγμα καθημερινό. Η θα μπορούσε να είναι και μια χρονολογία πχ «andreas1984» που έχει την ίδια δυσκολία. Επίσης, πάλι ο αριθμός από τον 8^{ο} χαρακτήρα και μετά.

4. Σε αυτή την περίπτωση βλέπουμε ένα όνομα στο οποίο κάποιοι χαρακτήρες του είναι αντικατεστημένοι με αριθμούς. Μια επιλογή που υποτίθεται ότι αυξάνει τα επίπεδα ασφαλείας ειδικά σε επίθεση με λεξικό.

5. Στην επόμενη περίπτωση βλέπουμε ένα όνομα στο οποίο κάποιοι χαρακτήρες του είναι αντικατεστημένοι με σύμβολα. Μια επιλογή που χρησιμοποιούν οι πιο «ψαγμένοι» στην χρήση κωδικών. Ας δούμε πόσο αποδοτικό είναι και αυτό.

6. Πιο περίεργη επιλογή με την χρήση της πιο «ψαγμένης» μεθόδου σε συνδυασμό με μερικούς χαρακτήρες ακόμα για «επιμήκυνση» του κωδικού για «περισσότερη» ασφάλεια.

7. Και τέλος ένα τελείως ακανόνιστο password, το πιο πολύπλοκο που μπορούσαμε να σκεφτούμε σε ένα λογικό μήκος 10 χαρακτήρων. Μια μίξη πεζών, κεφαλαίων, σύμβολων και αριθμών μπερδεμένα μεταξύ τους και όχι σε σειρά. Επίσης δεν είναι λέξη λεξικού με αλλαγμένους χαρακτήρες και το

μήκος του είναι μεγάλο. Δηλαδή, ένα απόλυτα μπερδεμένο password. Είναι όμως και αυτό αρκετά ασφαλές;

Δυο βασικά στοιχεία μας ενδιαφέρουν όταν πρόκειται να σπάσουμε κάποιον κωδικό. Και αυτό γιατί γνωρίζοντας τα θα μπορούσαμε να βελτιστοποιήσουμε την επίθεση και να επιταχύνουμε τη διαδικασία εύρεσης του κωδικού. Βοηθάει να ξέρουμε το μήκος του κωδικού για να το δώσουμε σαν είσοδο στην εφαρμογή. Βέβαια, θα αναρωτιέστε πως είναι δυνατόν να γνωρίζουμε το ακριβές μήκος. Αν εξαιρέσουμε τις περιπτώσεις που μπορεί να το γνωρίζουμε επειδή πχ ακούσαμε 5 πληκτρολογήσεις κατά την εισαγωγή του μια φορά, αυτό που μας ενδιαφέρει είναι το κατά προσέγγιση μήκος και αυτό για να βελτιστοποιήσουμε την επίθεση. Δηλαδή, θα μπορούσαμε πολύ απλά, να βάλουμε σαν μήκος 1 έως 20 χαρακτήρες, κάτι που θα περιλάμβανε όλες τις περιπτώσεις, και κάποια στιγμή θα το βρει αλλά αν γνωρίζαμε ότι ο κωδικός είναι 5 χαρακτήρες θα μπορούσαμε να το εισάγουμε σα δεδομένο και έτσι θα γλυτώσουμε το χρόνο που θα απαιτούσε το σύστημα να τρέξει επιθέσεις για κωδικούς μέχρι 4 χαρακτήρες. Επίσης, συνήθως η default ρύθμιση στις εφαρμογές για επίθεση είναι 1 έως 7 χαρακτήρες που είναι σύνηθες μήκος για κωδικούς χρηστών. Έτσι αν ο κωδικός είναι πάνω από 8 χαρακτήρες δε θα βρεθεί ποτέ με αυτή τη ρύθμιση.

Το δεύτερο σημαντικό στοιχείο που θα ήταν χρήσιμο αν το γνωρίζουμε είναι από τι χαρακτήρες αποτελείται ο κωδικός. Δηλαδή αν ο κωδικός είναι αριθμητικός, αν περιέχει και πεζά γράμματα, ή/και κεφαλαία ή ακόμα και σύμβολα απλά ή πιο περίεργα. Αυτό θα παίξει σημαντικό ρόλο στο χρόνο της επίθεσης. Βέβαια πάλι θα μπορούσαμε να βάλουμε μια επιλογή που θα περιλαμβάνει τα πάντα αλλά ακόμα και σε ένα μικρό κωδικό αυτό θα αύξανε κατά πολύ τον χρόνο που θα χρειαζόταν για να βρεθεί ο κωδικός. Βέβαια αυτό είναι δύσκολο να το γνωρίζεις ανά χρήστη αλλά μπορεί να το γνωρίζεις ανά σύστημα. Για παράδειγμα πολλά συστήματα δεν επιτρέπουν στους κωδικούς τους χαρακτήρες όπως {,},~ κτλ, αρκετά ασυνήθιστα σύμβολα δηλαδή, ενώ άλλα δεν επιτρέπουν καν σύμβολα οπότε μικραίνεις έτσι αρκετά το πλήθος των πιθανών συνδυασμών.

1) Cain and Abel σε Windows Attack

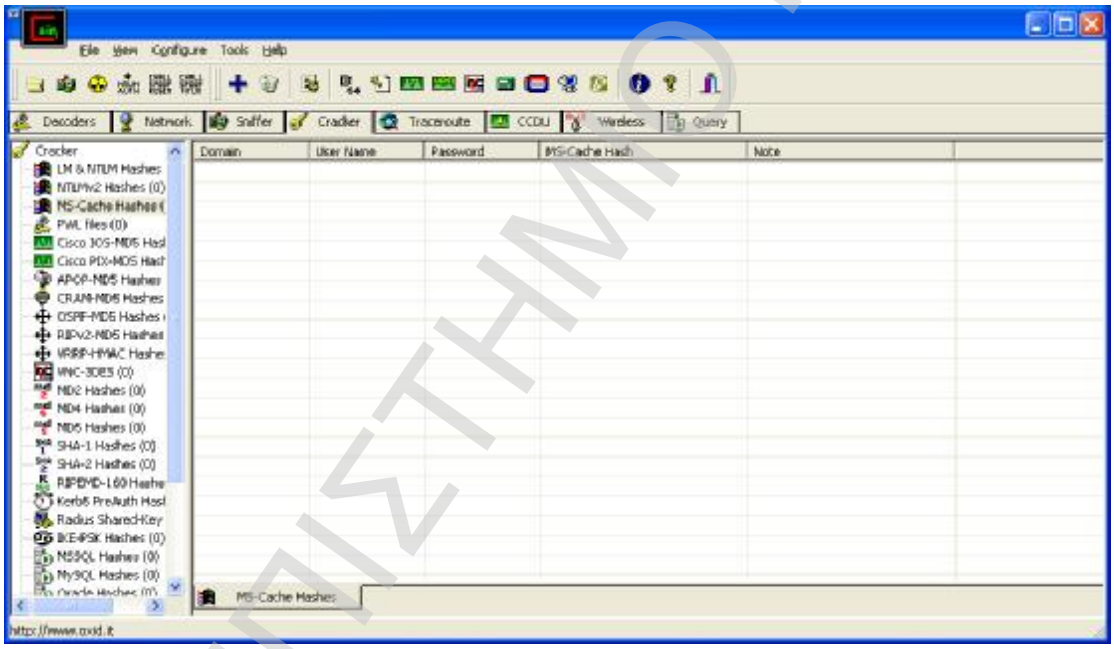
Παρουσίαση

Ένα από πιο γνωστά, τα τελευταία 3 χρόνια, προγράμματα παραβίασης κωδικών είναι το “Cain & Abel”, του οποίου δοκιμάσαμε την έκδοση 4.9.29. Οι χρήστες του Linux συνήθως περηφανεύονται ότι τα καλύτερα δωρεάν εργαλεία υποστηρίζουν τη δικιά τους πλατφόρμα πρώτα αλλά εδώ έχουμε μια από τις λίγες εξαιρέσεις καθώς η εφαρμογή αυτή είναι δωρεάν και τρέχει μόνο σε windows. Το πρόγραμμα αυτό είναι

ένα αρκετά ισχυρό πρόγραμμα που συνδυάζει ποικίλες επιλογές και δυνατότητες που δε συναντάς σε πολλούς password crackers, όπως το network sniffing, παράγοντας που αυξάνει τη δημοτικότητα του. Εμείς θα ασχοληθούμε όμως με αυτό που μας ενδιαφέρει συγκεκριμένα, το cracking των κωδικών χρηστών windows.

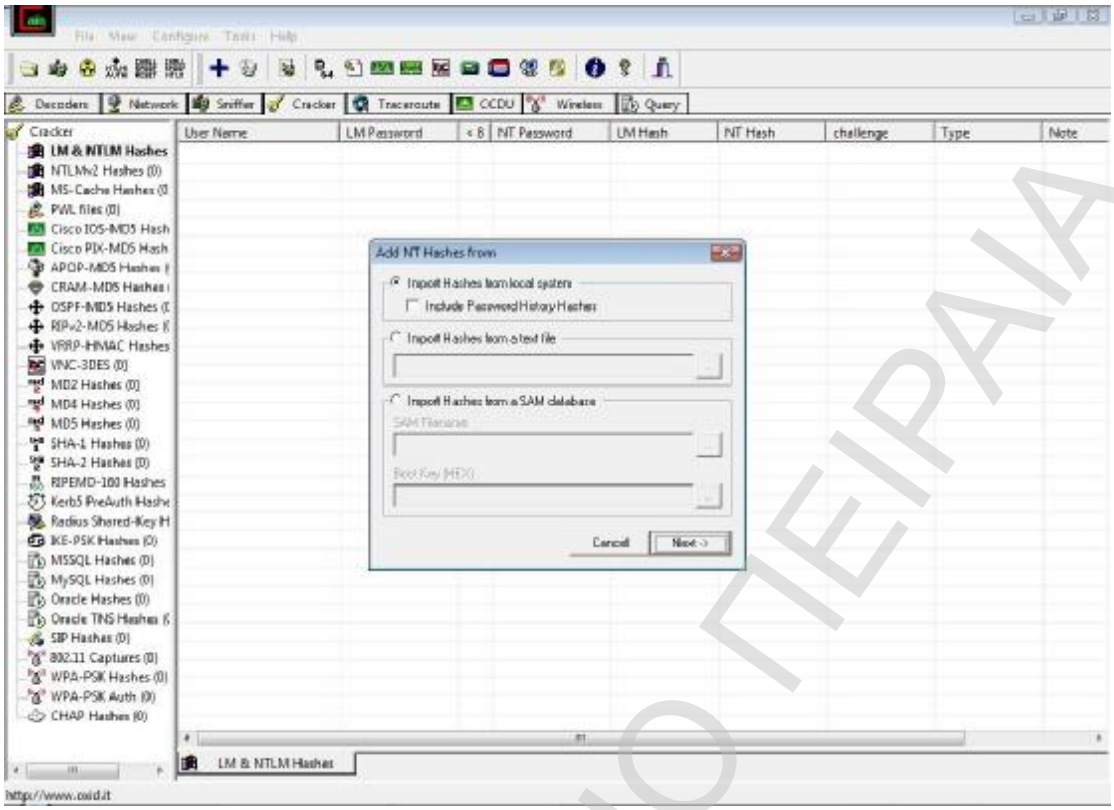
Όπως έχουμε αναφέρει η ασφάλεια των κωδικών των χρηστών στο περιβάλλον των windows βασίζεται στον αλγόριθμο LM Hash που χρησιμοποιεί η Microsoft. Μάλιστα ήταν προεπιλογή για την κρυπτογράφηση των κωδικών μέχρι 15 χαρακτήρων έως και τα Windows XP. Ο αλγόριθμος αυτός μετατρέπει τον κωδικό σε κεφαλαία γράμματα και σπάει τον κωδικό σε 2 κομμάτια 7 χαρακτήρων που κρυπτογραφούνται χωριστά. Έτσι ο επιτιθέμενος μπορεί να επιτεθεί χωριστά όπως θα το έκανε και σε κωδικούς 7 χαρακτήρων (λειτουργία που υποστηρίζει η συγκεκριμένη εφαρμογή) και έτσι χάνεται το πλεονέκτημα των περισσότερων χαρακτήρων. Οι κωδικοί αυτοί στα windows αποθηκεύονται στο αρχείο SAM το οποίο και θα εισάγουμε τώρα στην εφαρμογή.

Ξεκινάμε βλέποντας μια οθόνη του Cain & abel:



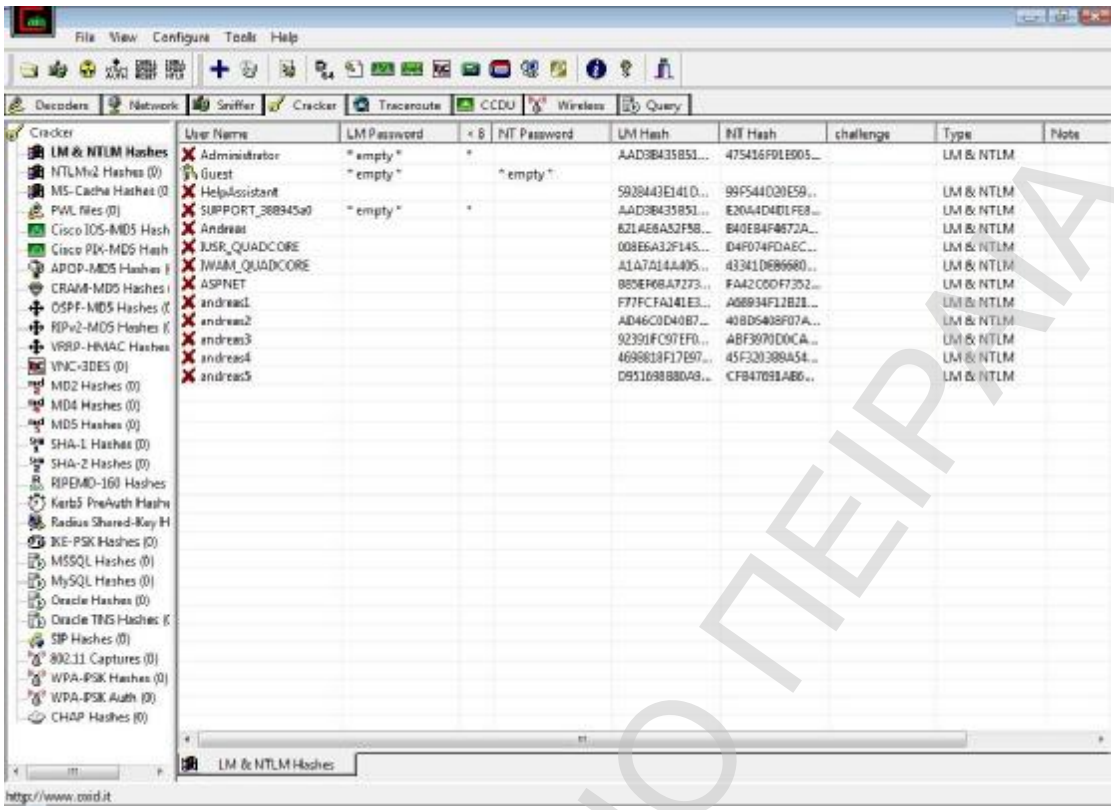
Εικόνα 3-6: Πρώτη οθόνη του Cain & abel

Η εισαγωγή του αρχείου SAM που αποθηκεύονται τα passwords των χρηστών είναι πολύ απλή. Πηγαίνοντας στο μενού “Cracker” και επιλέγοντας την επιλογή LM & NTLM Hashes βλέπεις το «+» στο κύριο μενού ενεργοποιημένο. Το πατάς και εμφανίζεται το παρακάτω παράθυρο:



Εικόνα 3-7: Προσθήκη Sam αρχείου

Μπορείς είτε να επιλέξεις να κάνει Import από το Local σύστημα είτε να εισάγεις το αρχείο Sam που έχεις πάρει από ένα άλλο σύστημα. Έπειτα, η εφαρμογή, διαβάζει το αρχείο και εμφανίζει τους χρήστες όπως βλέπουμε παρακάτω. Μια βασική στήλη που μας ενδιαφέρει εκτός από τη στήλη των usernames είναι η στήλη με τα LM passwords που είναι στην ουσία το password για τη σύνδεση του αντίστοιχου χρήστη στο σύστημα.



Εικόνα 3-8: Εμφάνιση imported users-passwords

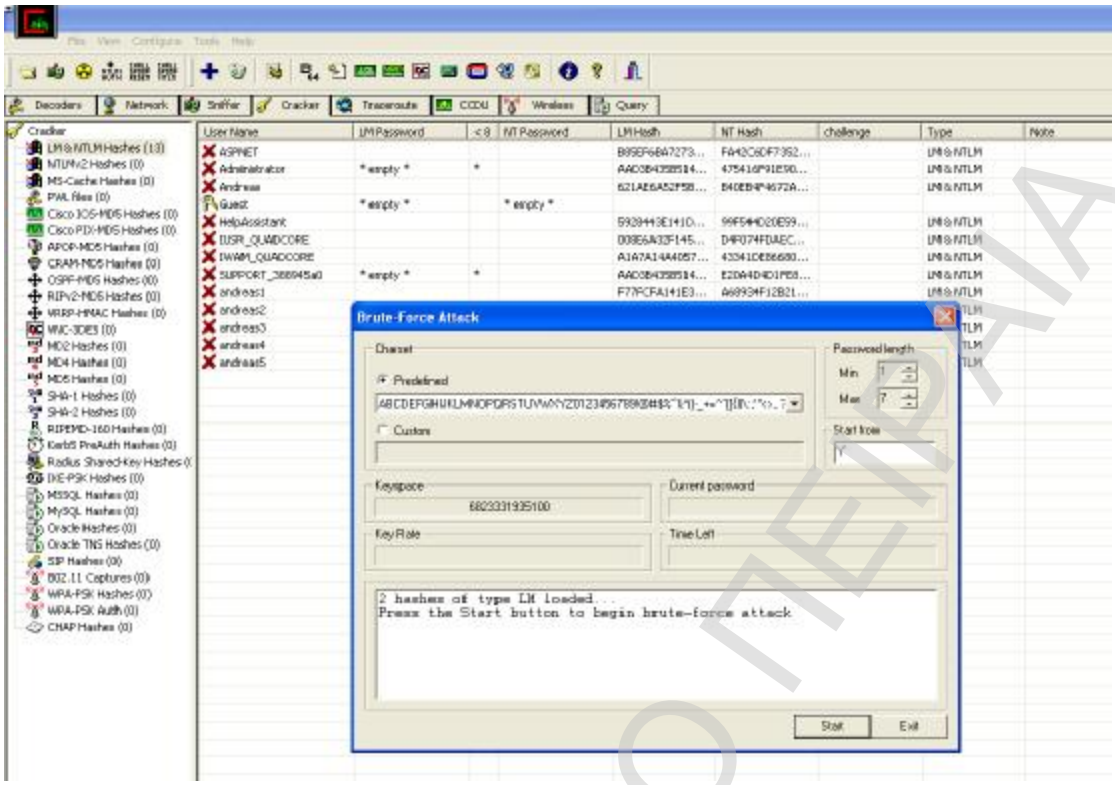
Από την αρχή με το διάβασμα του Sam, το πρόγραμμα εμφανίζει κάποια αρχικά βοηθητικά στοιχεία που ενδιαφέρουν τον επιτιθέμενο. Εμφανίζει ποιοι χρήστες έχουν κενό password, όπως επίσης εμφανίζει και ποιοι χρήστες έχουν password που έχει μήκος λιγότερο από 8 χαρακτήρες. Αυτό, όπως είπαμε και νωρίτερα, είναι πολύ χρήσιμο στις επιθέσεις γιατί το μήκος παίζει σημαντικό ρόλο.

Έχουμε λοιπόν φορτώσει και ανοίξει το αρχείο Sam και όλα είναι έτοιμα για να αρχίσουμε τις επιθέσεις.

Brute force επίθεση

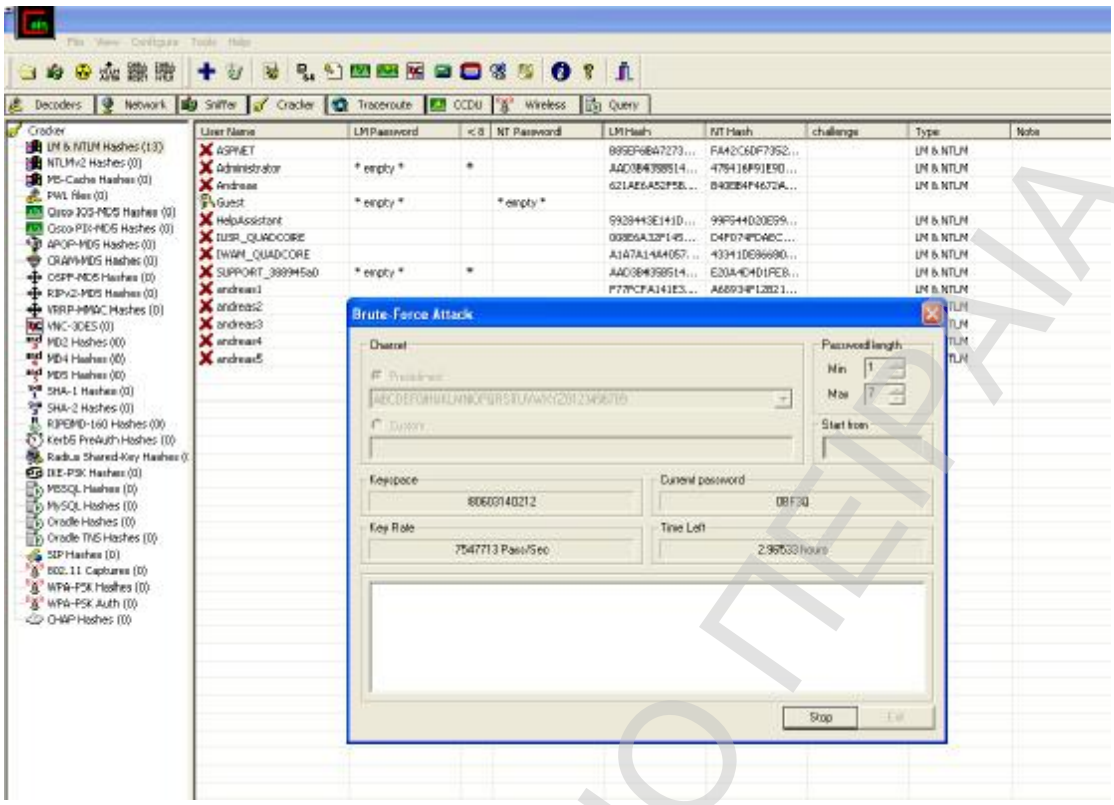
Η πρώτη επίθεση που θα δοκιμάσουμε στους «στημένους» κωδικούς που έχουμε θα είναι η brute force. Θα δοκιμάσουμε σε κάθε έναν κωδικό ξεχωριστά την επίθεση για να δούμε πόσο χρόνο χρειάζεται για να βρει η εφαρμογή ολόκληρο η μέρος του κάθε κωδικού και να βγάλουμε έτσι συμπεράσματα για την ασφάλεια που παρέχουν.

Κάνουμε δεξί κλίκ λοιπόν πάνω στον χρήστη του οποίου θέλουμε να σπάσουμε τον κωδικό και επιλέγουμε brute force attack. Εδώ βλέπετε μια εικόνα παράδειγμα για την εκκίνηση της επίθεσης:



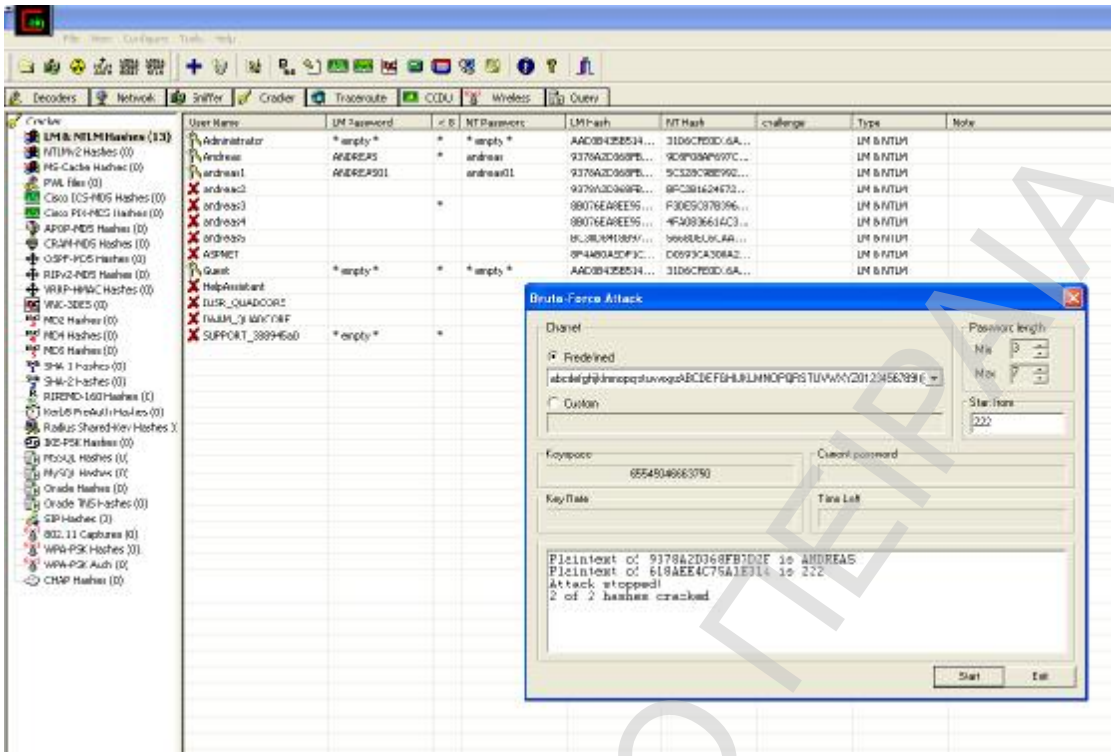
Εικόνα 3-9: Εκκίνηση brute force επίθεσης με το Cain

Όπως βλέπετε συμπληρώσαμε τα απαραίτητα πεδία, το charset, όπου ορίζουμε στην εφαρμογή τι χαρακτήρες να δοκιμάζει και το μήκος του password. Για να είναι αντικειμενικοί οι χρόνοι ευρέσεως κωδικών και να μην αναρωτιόμαστε μήπως έκανε πιο γρήγορα επειδή ήταν μικρότερο το charset, χρησιμοποιούμε πάντα στις δοκιμές μας το πλήρες charset.



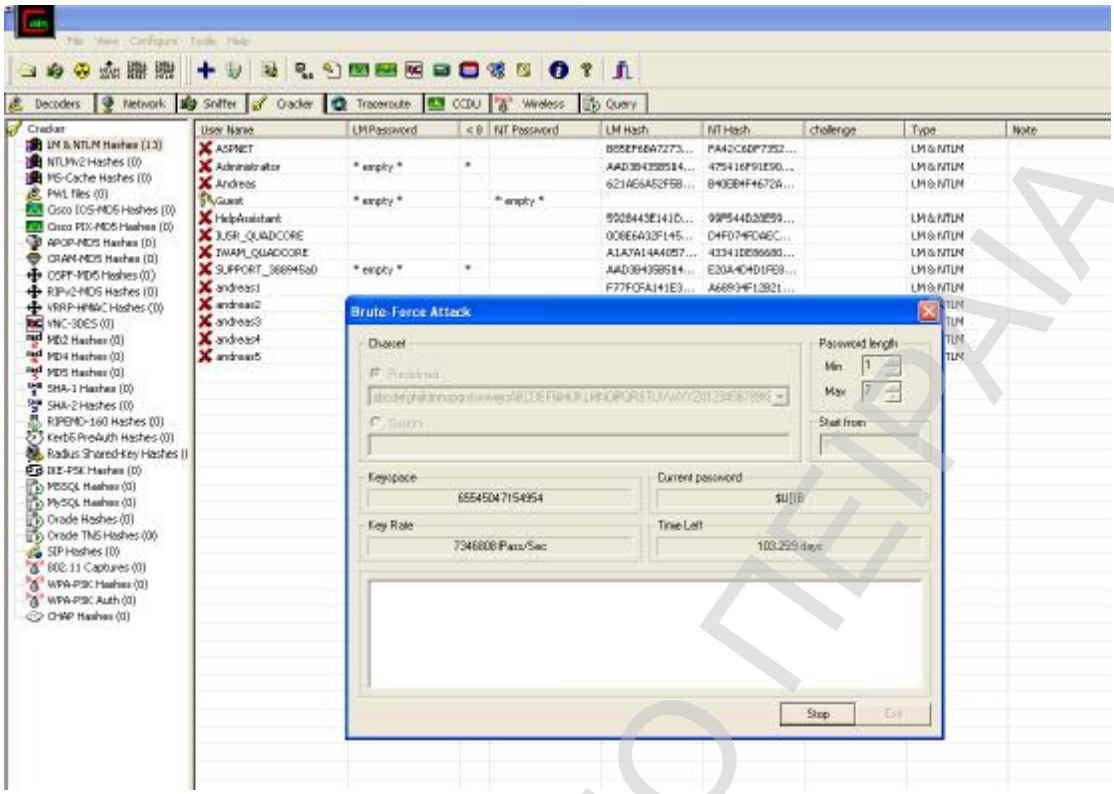
Εικόνα 3-10: Επίθεση brute force σε εξέλιξη

Όσον αφορά λοιπόν τους κωδικούς 1(andreas), 2(andreas01), 3(andreas222) και 4(4ndr3as) η εφαρμογή ήταν τόσο γρήγορη που πριν πάρουμε το ποντίκι από το κουμπί έναρξης η διαδικασία είχε τελειώσει και οι κωδικοί είχαν βρεθεί σωστά! Ήταν λοιπόν τόσο απλή υπόθεση να βρεθούν passwords τέτοιου τύπου, ποιο γρήγορα και από το χρόνο που χρειάζεται ο χρήστης να το πληκτρολογήσει, κάτι που ο μέσος χρήστης δεν το γνωρίζει και νομίζει ότι είναι ασφαλής με έναν τέτοιο κωδικό. Για τον 1ο κωδικό το πρόγραμμα έκανε απλή επίθεση brute force. Για τον 2ο και τον 3ο, τα αριθμητικά δεδομένα ήταν από τον όγδοο χαρακτήρα και έπειτα, οπότε η εφαρμογή μπορούσε να επιτεθεί ξεχωριστά σε αυτό το κομμάτι λόγω της αδυναμίας που είπαμε της συνάρτησης κρυπτογράφησης που χρησιμοποιούν τα windows. Έκανε μεν το ίδιο όπως στον 1ο, αλλά έκανε υβριδική brute force επίθεση ψάχνοντας κωδικούς της μορφής andreas01, andreas02 κτλ και αναγνώρισε τους αριθμητικούς χαρακτήρες σαν salt. Για τον τέταρτο ήταν απλά επίθεση brute force πάλι σε αλφαριθμητικούς χαρακτήρες.



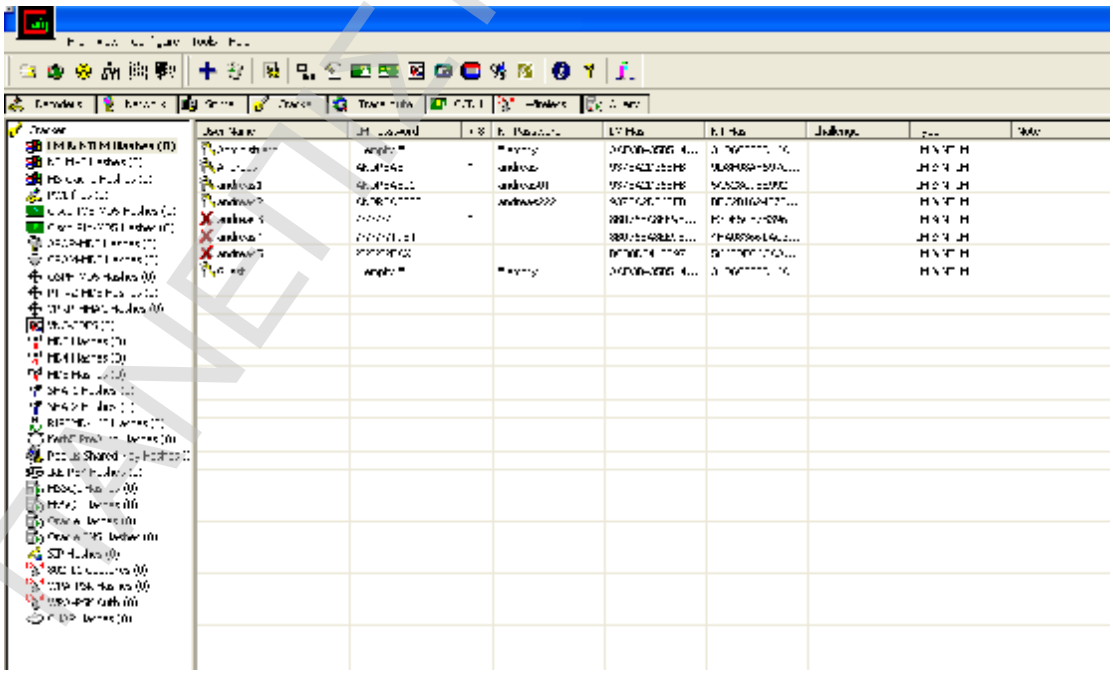
Εικόνα 3-11: Επιτυχές αποτέλεσμα brute force επίθεσης

Όσον αφορά τα υπόλοιπα passwords η εφαρμογή τα βρήκε σκούρα αλλά δεν κατέθεσε τα όπλα. Πιο συγκεκριμένα, λόγω της φύσης των passwords το μήνυμα αναμενόμενου χρόνου ολοκλήρωσης της διαδικασίας μετά την συμπλήρωση 10 ωρών έδειχνε 103 μέρες:



Εικόνα 3-12: Εμφάνιση στατιστικών κατά τη διάρκεια της επίθεσης

Παρόλα αυτά όσον αφορά τους κωδικούς που ήταν άνω των 8 χαρακτήρων η εφαρμογή αντιμετώπισε πάλι χωριστά και παράλληλα το δεύτερο κομμάτι του κωδικού, δηλαδή μετά τον 8^{ο} χαρακτήρα. Βρήκε, λοιπόν, αυτούς τους χαρακτήρες κάτι που θα μπορούσε να βοηθήσει κάποιον επιτιθέμενο για την λογική εύρεση του κωδικού:

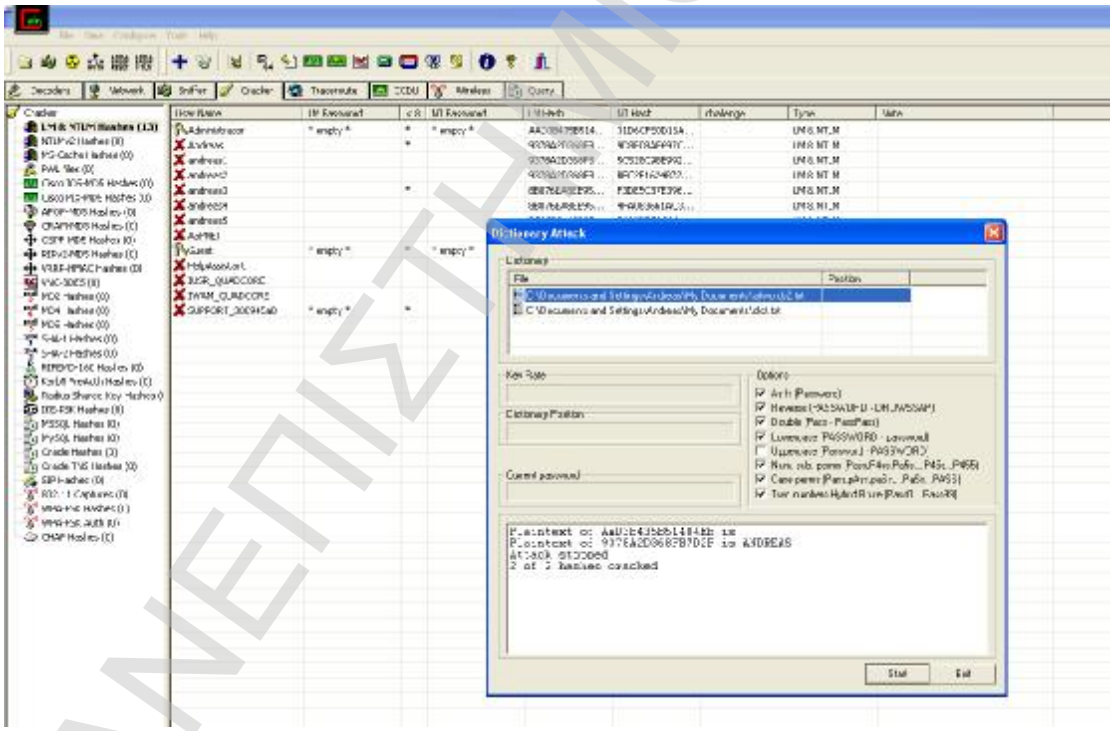


Εικόνα 3-13: Πίνακας users-passwords με τα passwords αποκαλυμμένα

Εδώ βλέπουμε ένα συγκεντρωτικό πίνακα με τους χρήστες και τους κωδικούς που αναβρέθηκαν. Εδώ ήθελα να αναφέρω ότι ένα άλλο σημαντικό σημείο επιλογής προγράμματος παραβίασης κωδικών είναι η ταχύτητα του αλγορίθμου. Υπάρχουν στην αγορά προγράμματα που όσον αφορά τις βασικές διαδικασίες, κάνουν παρόμοιες ενέργειες, δηλαδή δοκιμάζουν χαρακτήρες. Ο αλγόριθμος όμως που θα κάνει τους συνδυασμούς με τον βέλτιστο τρόπο και θα δοκιμάζει και περισσότερους χαρακτήρες έχει ένα αρκετά καλό προβάδισμα χρόνου. Στην παρούσα εφαρμογή και σε ένα σύστημα μονού επεξεργαστή με 1gb ram σύνολο, κατά μέσο όρο δοκιμάζονται 7,5 εκατομμύρια κωδικοί το δευτερόλεπτο. Φανταστείτε τι μπορεί να κάνει σε πολύ-επεξεργαστικά συστήματα.

Dictionary επίθεση

Για να σπάσουμε τους ίδιους κωδικούς χρησιμοποιώντας λεξικά χωρίς να επηρεαστούμε από τα αποτελέσματα της επίθεσης με brute force ας ξαναφορτώσουμε το Sam που έχουμε υποκλέψει. Έπειτα όπως και στη μέθοδο με brute force, κάνουμε δεξί κλικ πάνω στον χρήστη και επιλέγουμε ‘Dictionary Attack’.



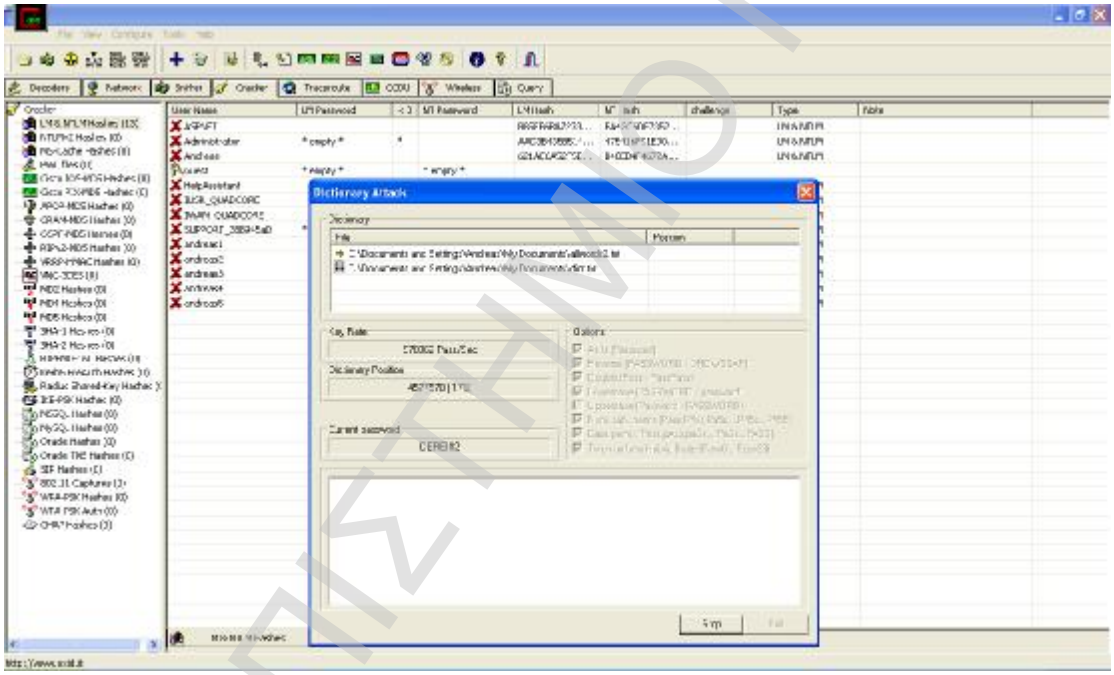
Εικόνα 3-14: Παράδειγμα επίθεσης με λεξικό με το Cain

Όπως βλέπουμε ανοίγει ένα παράθυρο με διαφορετικές επιλογές από την brute force επίθεση. Καταρχάς πρέπει να προσθέσουμε ένα η περισσότερα λεξικά. Εδώ να αναφέρουμε σαν παράληψη, ότι δεν υπάρχει ούτε ένα μικρό ενδεικτικό λεξικό για να χρησιμοποιήσει κάποιος νέος χρήστης. Προσθέσαμε, λοιπόν, ένα μικρό αγγλικό

λεξικό 400kb και ένα μεγαλύτερο αγγλικό 25mb που βρήκαμε. Σε αυτού του τύπου την επίθεση, οι δοκιμές κωδικών ήταν πιο περιορισμένες από την brute force επίθεση, βέβαια εξαρτώμενες πάντα από το μέγεθος του λεξικού. Αν ο κωδικός, όμως, που αναζητούσαμε αντιπροσώπευε μια λέξη ενός μικρού λεξικού τότε θα βρισκόταν πολύ πιο γρήγορα από την επίθεση με brute force. Αν δεν περιέχεται όμως σε αυτό τότε δε θα βρεθεί ποτέ, αντίθετα με την brute force επίθεση που θα τον βρει κάποτε.

Έπειτα έχουμε τις επιλογές που βλέπουμε για να κάνουμε επιπλέον δοκιμές. Δηλαδή αν θέλουμε να δοκιμάζουμε σαν password διπλές τις λέξεις του κωδικού ή σε πεζά ή κεφαλαία ή και στα δυο αναμειγνύοντας χαρακτήρες, πρέπει να τσεκάρουμε τις αντίστοιχες επιλογές. Επιπλέον υπάρχουν κάποιες επιλογές αρκετά 'ισχυρές' όπως η αντικατάσταση κάποιων γραμμάτων με αριθμούς πχ το A με 4, το S με 5 κτλ. Εδώ λοιπόν θα έχουμε περισσότερες πιθανότητες να βρούμε κωδικούς όπως οι 5, 6 και 7.

Ας δούμε λοιπόν τι έγινε:

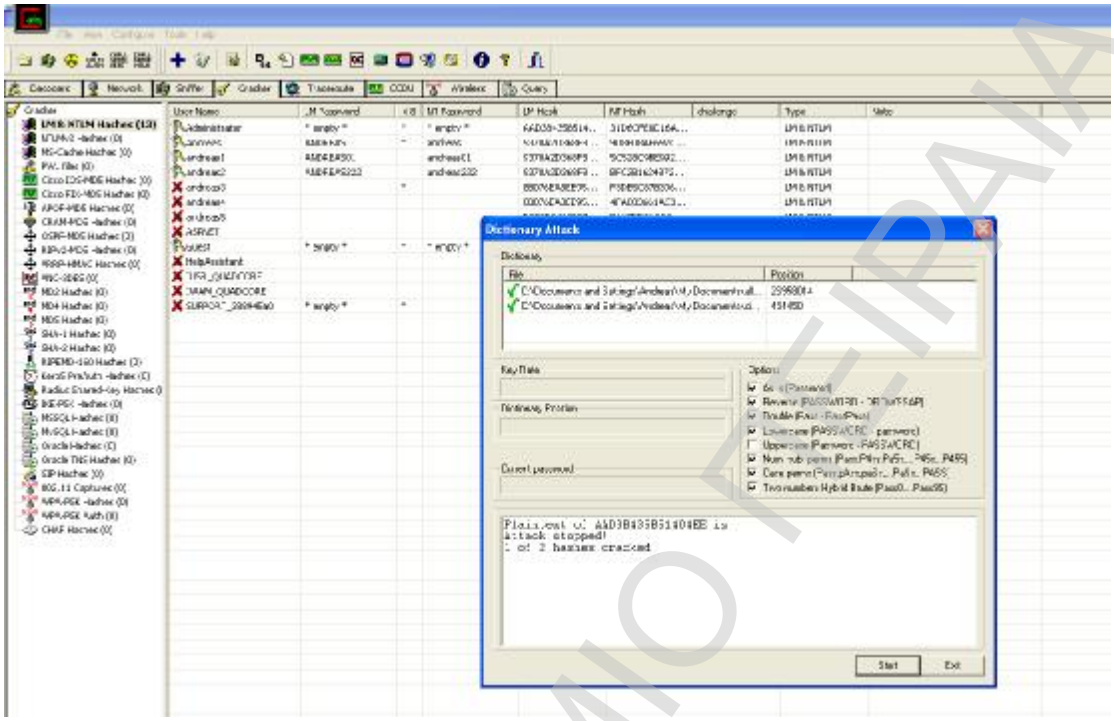


Εικόνα 3-15: Dictionary attack σε εξέλιξη με εμφάνιση στατιστικών

Όσον αφορά την αποδοτικότητα των 2 λεξικών, με τη χρήση του μικρότερου λεξικού δε βρήκαμε κανέναν κωδικό, ούτε τον πιο απλό, και εδώ φαίνεται λοιπόν πόσο μεγάλο ρόλο παίζει η επιλογή του λεξικού. Όσους κωδικούς βρήκαμε τους βρήκαμε μόνο με το μεγαλύτερο λεξικό των 25mb.

Τους πρώτους 4 κωδικούς λοιπόν τους βρήκε εντός λεπτών. Μπορεί, να μην ήταν τόσο γρήγορη η επίθεση αυτή (~1.000.000 δοκιμές το δευτερόλεπτο) όπως με την brute force επίθεση γιατί το μέγεθος του λεξικού ήταν μεγάλο και σίγουρα το parsing ενός αρχείου καθυστερεί λίγο τη διαδικασία, αλλά είχε θετικό αποτέλεσμα.

Όσον αφορά τους κωδικούς 5, 6, 7, επειδή εκτός από αλλαγή χαρακτήρων με αριθμούς κάναμε και έξυπνες αλλαγές χαρακτήρων με σύμβολα, οι δοκιμές απέτυχαν και δεν καταφέραμε να τους σπάσουμε.



Εικόνα 3-16: Αποτελέσματα dictionary attack

Συνοπτικά λοιπόν από τη χρήση του προγράμματος στο θέμα της παραβίασης κωδικών είδαμε τα εξής:

+ Η εφαρμογή υποστήριζε και τις δυο γνωστές τεχνικές που μας ενδιέφεραν, σαν ξεχωριστές επιθέσεις, υποστηρίζοντας αρκετές έξτρα δυνατότητες δίνοντας απόλυτη ελευθερία και δύναμη στον χρήστη να δοκιμάσει ότι ήθελε.

+ Η βοήθεια από τις «κρυφές» δυνατότητες του προγράμματος (μήκος κωδικού κτλ) ήταν πολύ καλή.

+ Η ταχύτητα και η αποδοτικότητα του προγράμματος όσον αφορά τις δοκιμές κωδικών στην brute force επίθεση ήταν παραπάνω από ικανοποιητική.

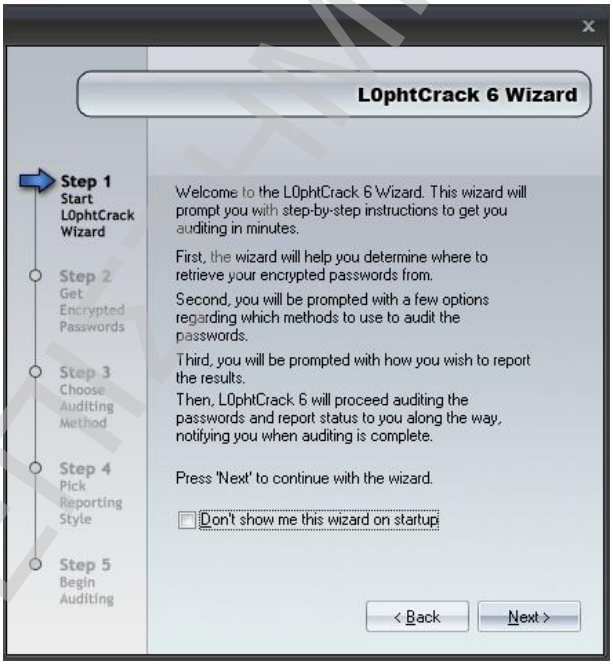
+ Η αποδοτικότητα του προγράμματος στην επίθεση με λεξικό, ανεξάρτητα από την σωστή επιλογή του λεξικού που έπρεπε να γίνει από τον χρήστη μετά από προσωπική του έρευνα, ήταν και αυτή ικανοποιητική και υποστήριζε πολλές δυνατότητες.

2) L0phtcrack σε Windows Attack

Παρουσίαση

Ένα άλλο πολύ γνωστό και αποδοτικό πρόγραμμα που ειδικεύεται στο σπάσιμο κωδικών των windows είναι το L0phtcrack. Έχει μια ιδιαίτερη ιστορία καθώς ξεκίνησε από το 1997 και το 2005 η Symantec το αγόρασε και σταμάτησε το project! Παρόλα αυτά επειδή πολύ χρησιμοποιούσαν ακόμα την τελευταία έκδοση (v5) σε σημείο που το πρόγραμμα είχε γίνει γνωστό σαν LC5, ο δημιουργός του κατάφερε να το ξαναπάρει πίσω και πλέον στα χέρια του συνεχίζει την πορεία του με ιδιαίτερη δημοτικότητα παρόλο που δεν είναι δωρεάν. Ειδικεύεται στο να σπάει κωδικούς από συστήματα windows nt και μεταγενέστερα, domain controllers, servers και active directory. Χρησιμοποιήσαμε την τελευταία έκδοση του 2009 v6.0.10.

Το L0phtcrack είναι μια εφαρμογή πολύ φιλική προς τον χρήστη αφού σε βοηθά συνέχεια στις ενέργειες που έχεις να κάνεις μέσω αυτοματοποιημένων wizards. Ξεκινώντας λοιπόν ανοίγει ένας τέτοιος wizard με βήματα και σε βοηθάει να ξεκινήσεις. Ας το δούμε στην πράξη:



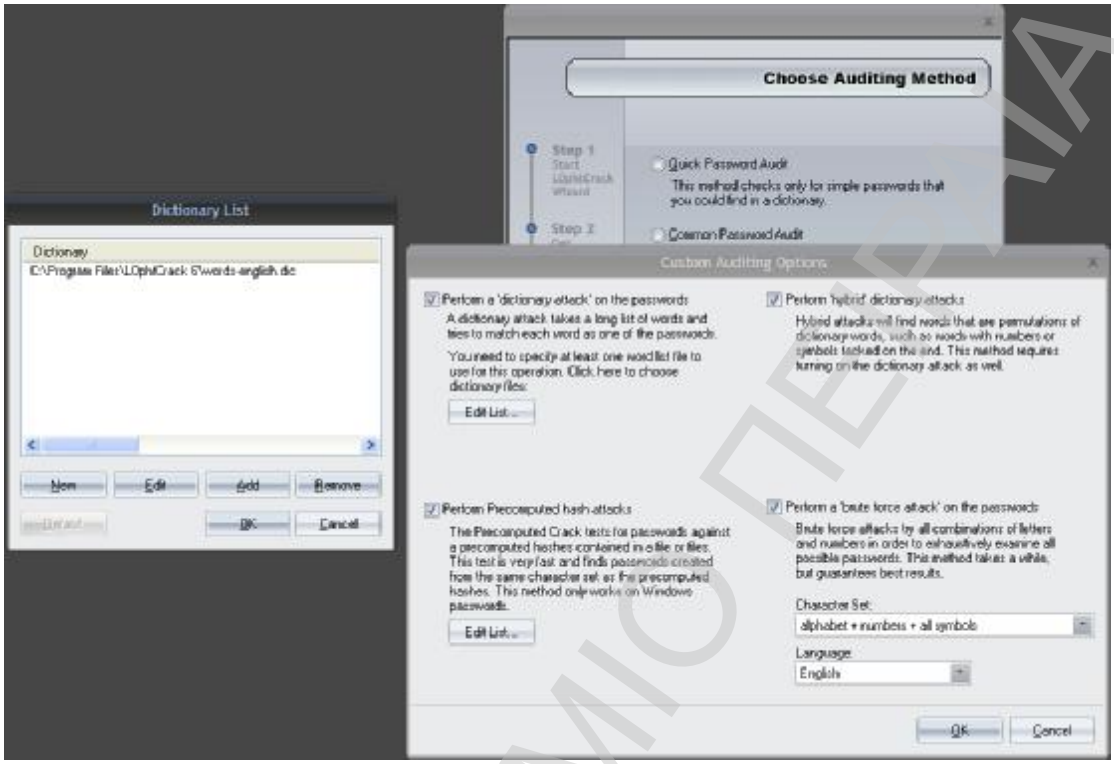
Εικόνα 3-17: Πρώτο βήμα με τον wizard εκκίνησης επίθεσης του L0pthcrack

Εικόνα 3-18: Δεύτερο βήμα με τον wizard εκκίνησης επίθεσης του L0pthcrack

Το πρώτο βήμα ήταν εισαγωγικό και στο δεύτερο σε ρωτάει με πιο τρόπο θα εισάγεις στην εφαρμογή το αρχείο με τα passwords. Αφού εισάγουμε το αρχείο Sam που χρησιμοποιήσαμε και στην δοκιμή του προηγούμενου προγράμματος προχωράμε στο βήμα 3:

Εικόνα 3-19: Τρίτο βήμα με τον wizard εκκίνησης επίθεσης του L0pthcrack

Σε αυτό το βήμα πρέπει να επιλέξουμε μέθοδο επίθεσης. Μπορούμε να δοκιμάσουμε κάποια από τις 3 γενικευμένες επιλογές ή να δούμε στο custom τι μπορούμε να κάνουμε πιο συγκεκριμένα:

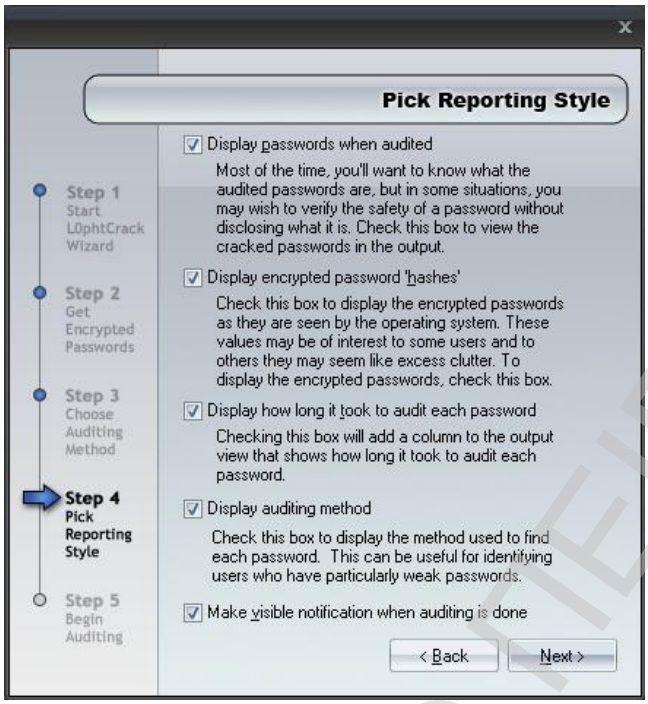


Εικόνα 3-20: Options τρίτου βήματος

Εδώ λοιπόν βλέπουμε πραγματικά τι επιλογές έχουμε:

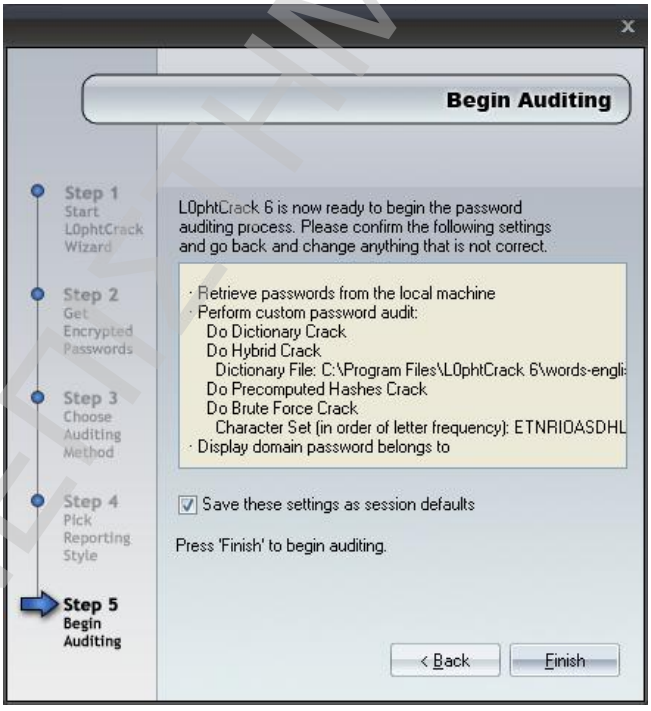
- Επίθεση με λεξικό: μπορείς να την ενεργοποιήσεις και να επεξεργαστείς τη λίστα με τα λεξικά που θα χρησιμοποιήσει η εφαρμογή στην επίθεση.
- Υβριδική επίθεση με λεξικό: σε αυτήν περίπτωση στις λέξεις που χρησιμοποιεί το λεξικό αλλάζει γράμματα με αριθμούς, προσθέτει στο τέλος αριθμούς κτλ αντίστοιχες δηλαδή με τις επιλογές που είχαμε και στο Cain.
- Precomputated επίθεση: επίθεση με προ-επεξεργασμένο λεξικό, δηλαδή λεξικό που έχει κρυπτογραφηθεί και αποθηκευτεί πριν την επίθεση.
- Brute force επίθεση: επίθεση brute force που αναφέρεις το charset αλλά και τη γλώσσα που θέλεις να κάνεις την επίθεση.

Αφού τελειώσαμε λοιπόν με τις επιλογές που είχαμε φτάνουμε στο επόμενο βήμα:



Εικόνα 3-21: Τέταρτο βήμα με τον wizard εκκίνησης επίθεσης του L0pthcrack

Εδώ απλά επιλέγουμε τι στήλες με αποτελέσματα θέλουμε να μας εμφανίζει στο πρόγραμμα κατά τη διάρκεια της επίθεσης και τέλος:

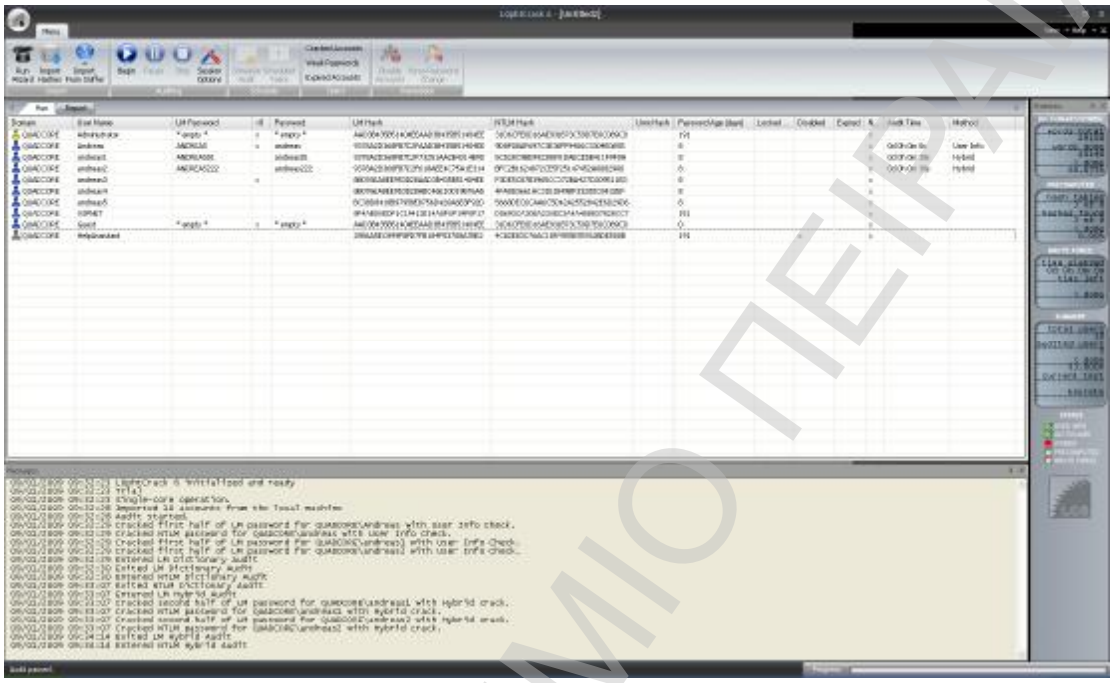


Εικόνα 3-22: Πέμπτο βήμα με τον wizard εκκίνησης επίθεσης του L0pthcrack

Στο τελευταίο βήμα μας προβάλετε μια περίληψη των επιλογών μας και διαπιστώνουμε ότι μπορούμε να σώσουμε τις επιλογές για να τις χρησιμοποιούμε

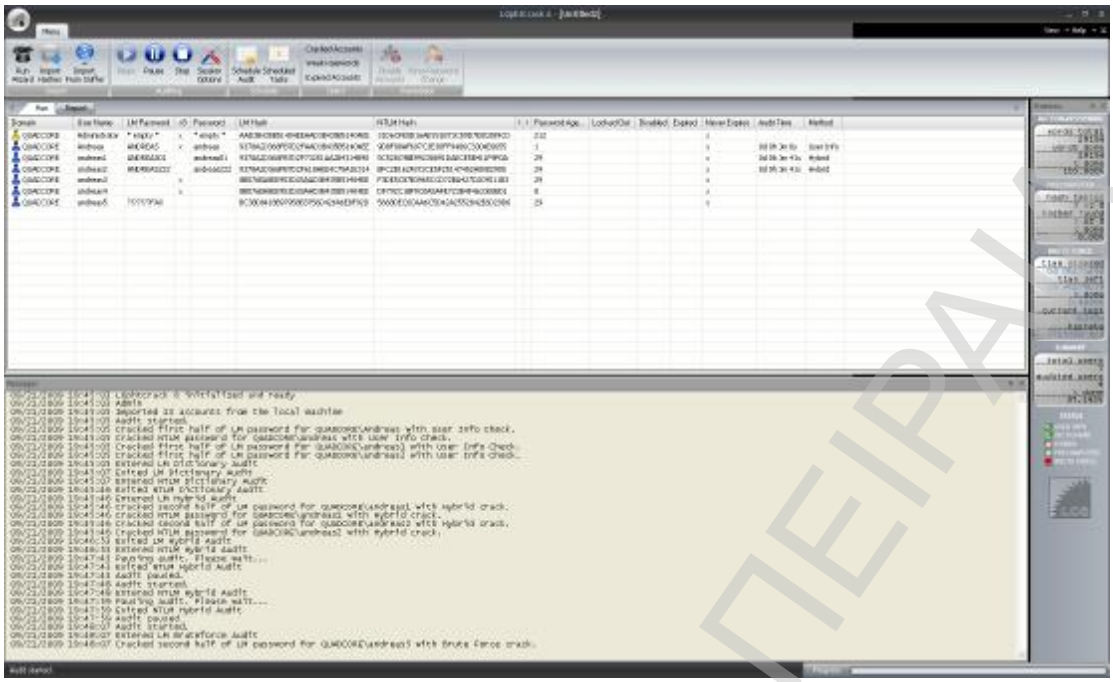
κατευθείαν σε κάθε μας επίθεση. Πατώντας λοιπόν το κουμπί ‘Finish’ ανοίγει το βασικό παράθυρο του l0pthcrack.

Πλήρης επίθεση



Εικόνα 3-23: Πίνακας imported users-passwords

Παρατηρώντας λίγο την διεπαφή διαπιστώνουμε ότι είναι λίγο πιο user friendly από το Cain καθώς παρέχει κάποια έξτρα στοιχεία όπως η δεξιά στήλη με τα επιπλέον στατιστικά δεδομένα όσον αφορά τους τύπους επιθέσεων και διάφορα δεδομένα που αφορούν την επίθεση καθώς και τα μηνύματα στο footer. Στον πίνακα που εμφανίζεται παρατηρούμε ότι μοιάζει λίγο με τον πίνακα του Cain τουλάχιστον όσον αφορά την πλειοψηφία των στοιχείων που μας ενδιαφέρουν και μας εμφανίζει. Αν σε κάποιον δημιουργήθηκε η απορία όταν επιλέγαμε τις μεθόδους επίθεσης πως θα ξέραμε τελικά ποια μέθοδος χρησιμοποιήθηκε και βρήκε τον κωδικό, εκτός από τις εμφανίσεις μηνυμάτων κάτω βλέπουμε ότι εμφανίζεται και σε μια στήλη που περιέχει δεδομένα επιτυχημένης επίθεσης ανά χρήστη. Επίσης κατά τη διάρκεια της επίθεσης υπάρχει status δεξιά που εμφανίζει ποια μέθοδος επίθεσης χρησιμοποιείται εκείνη τη στιγμή. Όπως είδαμε τις επιθέσεις τις χρησιμοποιεί κατά αυτή τη σειρά, αν έχουν επιλεγεί όλες βέβαια.



Εικόνα 3-24: Παράδειγμα επιθέσεων σε εξέλιξη με το L0pthcrack

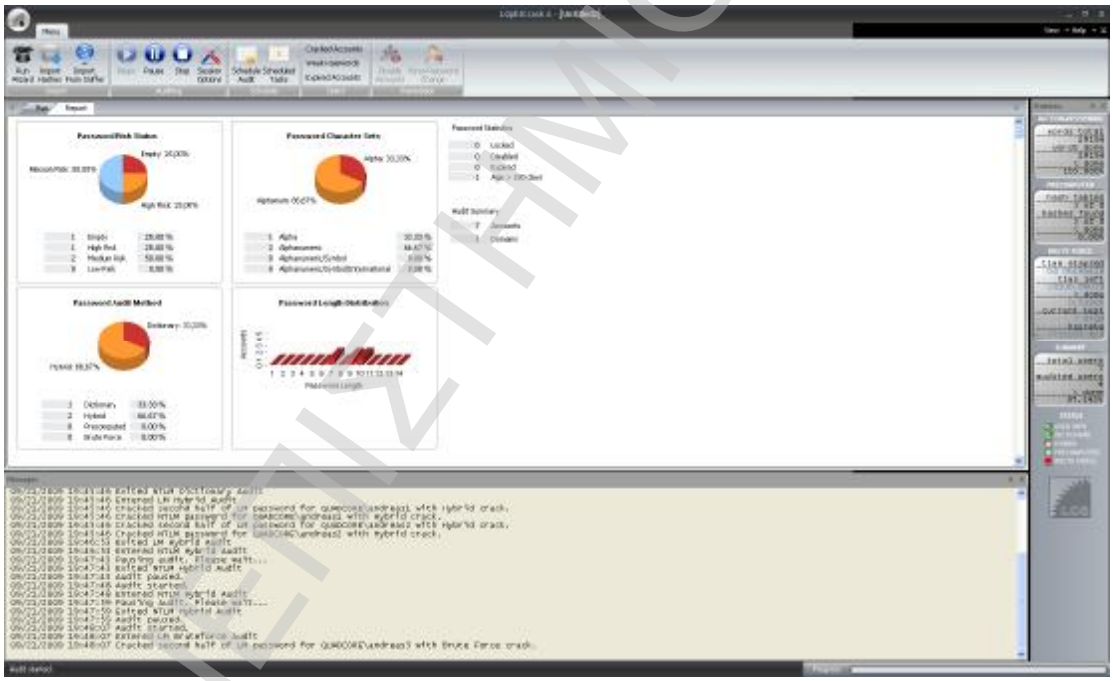
Πριν ξεκινήσουμε να αναλύουμε τι έγινε ανά κωδικό να αναφέρω ότι σε γενικές γραμμές τα επίπεδα επιτυχίας ήταν παρόμοια με του Cain. Οπότε μην περιμένετε να ακούσετε κάτι αρκετά διαφορετικό.

Ξεκινώντας, λοιπόν, και παρακολουθώντας τις επιθέσεις, είδαμε ότι πάλι η παραβίαση των 4 πρώτων κωδικών έγινε σε λίγο χρόνο όχι όμως λιγότερο του ενός δευτερολέπτου. Για την ακρίβεια στον πρώτο χρειάστηκε μηδενικό χρόνο και για τους άλλους τρεις χρειάστηκαν 34 δευτερόλεπτα και αυτό έγινε γιατί επιλέχθηκε άλλη μέθοδος επίθεσης για να σπάσει αυτό τον κωδικό. Σε αυτή την περίπτωση για να σπάσει αυτούς τους κωδικούς δεν έκανε κάποια από τις καθιερωμένες επιθέσεις αλλά χρησιμοποίησε τα ‘user info’ όπως λέει, δηλαδή τις πληροφορίες του χρήστη που είναι εμφανείς (όπως το username). Έπειτα για τα υπόλοιπα ψηφία στους άλλους δυο κωδικούς τα βρήκε με υβριδική επίθεση, κάτι αντίστοιχο που είχε κάνει και το Cain. Βλέπουμε λοιπόν, μια έξυπνη χρήση των public στοιχείων για βελτιστοποίηση των επιθέσεων. Παρόλα αυτά επειδή ο χρόνος που χρειάστηκε το Cain για να βρει και τα τέσσερα ήταν μηδενικός με Brute force επίθεση, ξανατρέξαμε την επίθεση μόνο με Brute force και είδαμε ότι ήταν εξίσου μηδενικός. Οπότε η επιλογή των μεθόδων επίθεσης είναι πολύ σημαντική για βελτιστοποίηση των αποτελεσμάτων. Παρόλα αυτά θεωρούμε ότι είναι καλύτερα να ξεκινάς με dictionary επίθεση ούτως ώστε αν το password είναι απλό να το βρει γρήγορα, αλλιώς μετά να αφήσεις την brute force επίθεση να «τρέχει» μέχρι να το βρει.

Όσον αφορά τους υπόλοιπους κωδικούς πάλι ο χρόνος που απαιτούσε για να βρεθούν ήταν εξίσου μεγάλος όπως και στο Cain. Γενικότερα οι επιθέσεις ήταν σχετικά γρήγορες καθώς έκανε ~3.500.000 δοκιμές ανά δευτερόλεπτο, όχι όμως όσο γρήγορες ήταν στο Cain. Επίσης πάλι στο password 7 βρέθηκε το δεύτερο μισό κομμάτι άμεσα όπως και στο Cain.

Ένα ωραίο κομμάτι της εφαρμογής είναι το tag για τα reports. Εφόσον αυτή την εφαρμογή την χρησιμοποιείς σαν διαχειριστής συστημάτων, για να ελέγξεις την ασφάλεια των κωδικών του συστήματος, θα ήθελες στο τέλος να βλέπεις ένα γενικό report για να έχεις μια συνολική εικόνα. Έτσι λοιπόν, πηγαίνοντας στα reports βλέπεις στατιστικά στοιχεία σε πίνακες με ποσοστά και σε γραφήματα τα εξής:

- πόσα password ήταν εύκολα και αποτελούσαν high risk, πόσα μέτριας δυσκολίας κτλ.
- τι χαρακτήρες περιέχουν οι κωδικοί, στοιχείο που δηλώνει προσδιορίζει κατά ένα μεγάλο βαθμό την αποτελεσματικότητα τους
- με τι μέθοδο επίθεσης βρέθηκαν τα passwords, στοιχείο που αναφέρατε και σε ειδική στήλη σε κάθε χρήστη ξεχωριστά
- ποιο ήταν το μήκος των κωδικών που αποτελεί και αυτό ένα σημαντικό στοιχείο ασφαλείας
- και κάποια γενικά στατιστικά για το πλήθος των χρηστών, το πόσοι έχουν κωδικό, πόσα έχουν λήξει κτλ



Εικόνα 3-25: Στατιστικά, reports και διαγράμματα

Πριν τελειώσουμε την αναφορά μας στην εφαρμογή πρέπει να αναφέρουμε ότι το L0pthcrack μπορεί και επιτίθεται με την ίδια επιτυχία και σε Linux passwords. Για επίθεση σε Linux passwords όμως έχουμε επιλέξει άλλη εφαρμογή για να σας παρουσιάσουμε.

Σε γενικές γραμμές λοιπόν το l0pthcrack σε σύγκριση με το Cain παρατηρήσαμε τα εξής:

+ Από άποψη αποτελεσματικότητας επιθέσεων καθώς και χρόνου αποκάλυψης ενός κωδικού κτλ δεν είδαμε καμία διαφορά εκτός από το ότι το l0pthcrack χρησιμοποίησε τα user info για να κάνει κάποιες έξυπνες επιθέσεις

+ Από άποψη ευκολίας χρήσης το L0pthcrack ήταν σχετικά πιο εύχρηστο για τον μέσο χρήστη με τους αυτοματοποιημένους wizards που χρησιμοποιεί και διευκολύνει τον αρχάριο χρήστη στα βήματα που κάνει. Παρόλα αυτά βέβαια, το interface του Cain δεν είχε κάποια ιδιαίτερη δυσκολία στη χρήση.

+ Από άποψη συμπερασμάτων και δημιουργία στατιστικών αποτελεσμάτων που όσο απλό και αν ακούγεται, σε διαχειριστές που θέλουν να παράγουν security reports για μια ολόκληρη εταιρεία είναι πολύ σημαντικό, το l0pthcrack είχε την υπεροχή.

- Το Cain είναι δωρεάν αντίθετα με το l0pthcrack που είναι σχετικά ακριβό, παράγοντας που απασχολεί το μέσο χρήστη που δε χρησιμοποιεί τέτοια προγράμματα για επαγγελματικούς λόγους. Και εφόσον δεν έχει διαφορά στην απόδοση(λογικά είναι και πιο γρήγορο) και πολύ πιθανόν να μην τον ενδιαφέρουν τα reports το επόμενο θέμα που θα σκεφτεί θα είναι το κόστος

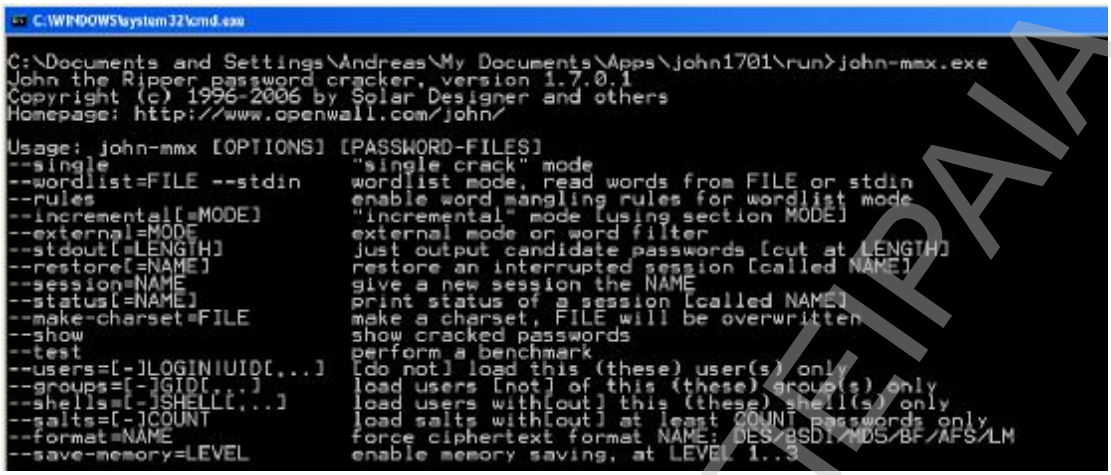
3) John the Ripper σε Linux Attack

Παρουσίαση

Ήρθε η ώρα για μια αλλαγή. Θα δοκιμάσουμε έναν password cracker για να δοκιμάσαμε να σπάσουμε τους κωδικούς χρηστών σε λειτουργικό Linux. Ο john the ripper είναι ο πιο παλιός από τους τρεις crackers που δοκιμάσαμε, ο πιο γνωστός και διαδεδομένος, ο πιο φορητός καθώς δε χρειάζεται εγκατάσταση, δουλεύει και σε Linux όσο και σε windows και κάνει επίθεση και σε κωδικούς windows όσο και Linux. Λογικό λοιπόν να θεωρείται το ιδανικό εργαλείο και να μη λείπει από την εργαλειοθήκη κάθε επιτιθέμενου.

Ο John the ripper, σαν κάθε πρόγραμμα παραβίασης που «σέβεται» τον εαυτό του, δεν εξαρτάται από γραφικά interfaces, κουμπάκια και βελάκια για να μην απαιτεί ιδιαίτερους πόρους από το σύστημα. Δουλεύει αποκλειστικά από prompt (ή αντίστοιχα terminal σε Linux). Είναι ένα ισχυρό εργαλείο και καλύπτει όλες τις

μεθόδους επίθεσης που θέλουμε να δοκιμάσουμε. Παρακάτω βλέπουμε ένα screenshot από μια λίστα με τις επιλογές που έχουμε για να επιτεθούμε σε κάποιο αρχείο κωδικών.



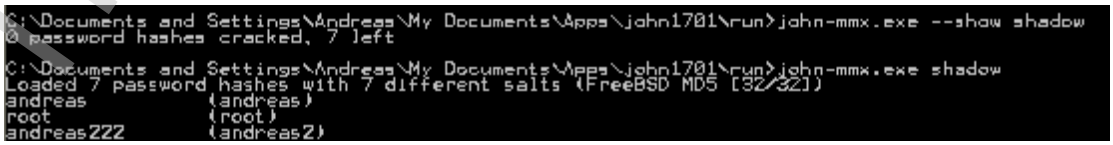
Εικόνα 3-26: Επιλογές με το John the ripper

Και εδώ και ένα screenshot επίθεσης από την έκδοση σε Linux:

Εικόνα 3-27: Παράδειγμα σε περιβάλλον Linux

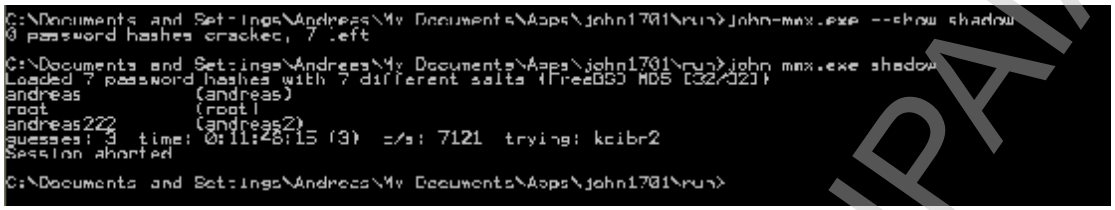
Μιας και το «θύμα» μας αυτή τη φορά δε θα είναι πάλι το αρχείο Sam όπως τις προηγούμενες δυο φορές ας αναφέρουμε μερικά πράγματα για το νέο μας θύμα. Οι κωδικοί των χρηστών στις διανομές Linux των τελευταίων χρόνων, είναι αποθηκευμένες σε ένα αρχείο που ονομάζεται shadow και βρίσκεται συνήθως (ανάλογα τη διανομή) στο /etc/. Και λέω στις εκδόσεις των τελευταίων χρόνων γιατί πιο παλιά ήταν αποθηκευμένα μαζί με όλα τα άλλα στοιχεία των χρηστών στο /etc/passwd. Προφανώς το αρχείο shadow, όπως και το Sam, είναι κρυπτογραφημένο αλλά με έναν καλύτερο αλγόριθμο κρυπτογράφησης τον Message Digest 5 (MD5) Hash. Ο MD5 σχεδιάστηκε το 1991 από τον Ron Rivest και έχει 128-bit hash. Είναι ένας ευρέως χρησιμοποιούμενος αλγόριθμος, σε λειτουργικά συστήματα, web εφαρμογές, applications κτλ. Θα προσπαθήσουμε λοιπόν τώρα να επιτεθούμε στο αρχείο shadow.

Πλήρης επίθεση



Εικόνα 3-28: Επίθεση με john the ripper σε εξέλιξη

Κλασσικά, λοιπόν, οι 4 πρώτοι κωδικοί βρέθηκαν πάλι σε μηδενικό χρόνο αν και ίσως χρειάστηκε ένα ολόκληρο δευτερόλεπτο. Η εφαρμογή είναι γενικά λιτή στα αποτελέσματα που εμφανίζει: Username, password, χρόνο επίθεσης και δοκιμές ανά δευτερόλεπτο.



Εικόνα 3-29: Διακοπή επίθεσης με το John, εμφάνιση αποτελεσμάτων

Όσον αφορά τους υπόλοιπους δύσκολους κωδικούς μετά από σχεδόν 12 ώρες δεν είχε βρεθεί τίποτα. Και λόγω της (καλύτερης) κρυπτογράφησης md5 που χρησιμοποιείται, δεν υπάρχει η κλασσική αδυναμία του LM Hash στους κωδικούς πάνω από 8 χαρακτήρες και έτσι δεν ξέρουμε τίποτα για τους κωδικούς που δεν βρήκαμε.

Επίσης, αυτό που παρατηρήσαμε ήταν ότι η ταχύτητα των δοκιμών ήταν εμφανώς μικρότερη (~7.000 δοκιμές το δευτερόλεπτο) σε σχέση με τις άλλες δυο εφαρμογές, παρόλο που βρήκε σχεδόν το ίδιο γρήγορα τα απλά passwords θα φαινόταν η διαφορά στα υπόλοιπα όταν ολοκληρωνόταν η επίθεση. Αυτό όμως δεν οφείλεται σε καθυστέρηση της εφαρμογής. Είχαμε πει ότι ένα στοιχείο ασφαλείας της κρυπτογράφησης MD5 είναι η μεγάλη καθυστέρηση του αλγορίθμου κρυπτογράφησης ώστε να δυσκολεύεται ο επιτιθέμενος σε μια τέτοια επίθεση. Οπότε υπολογίζοντας, όχι με τις δοκιμές ανά δευτερόλεπτο, αλλά με τους χρόνους που χρειάστηκε για να βρει τους κωδικούς μας, μπορούμε να πούμε ότι η ταχύτητα του αλγορίθμου της εφαρμογής είναι περίπου η ίδια με τις άλλες απλά μειώνεται λόγο της κρυπτογράφησης MD5.

Ας δούμε λοιπόν, συνοπτικά, συγκρίνοντας με τους προηγούμενους τι μας έκανε εντύπωση σε αυτή την εφαρμογή:

+ Δωρεάν, open source.

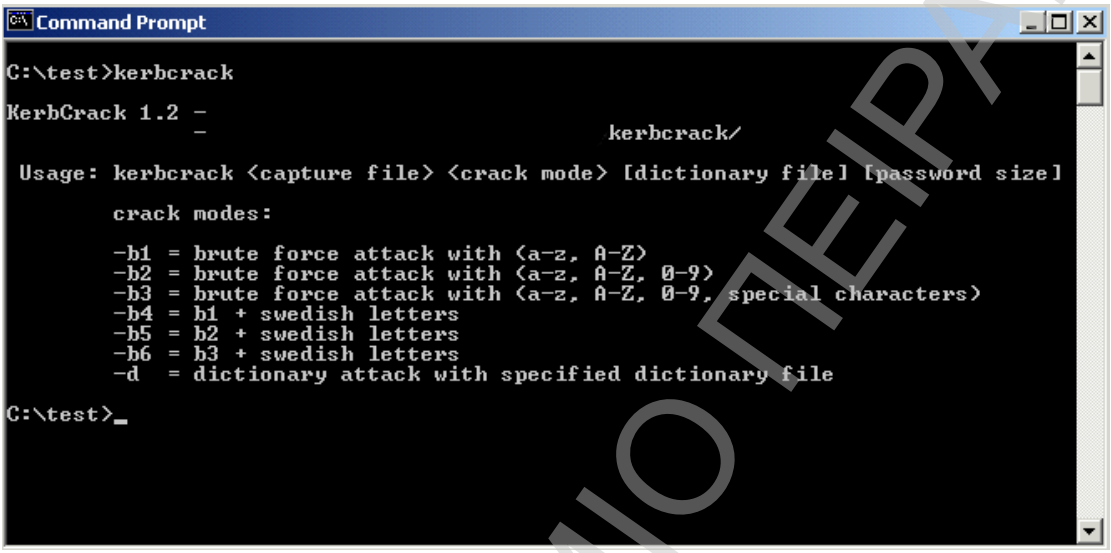
+ Λειτουργεί σε όλες τις γνωστές πλατφόρμες

+ Μπορεί να κάνει επίθεση τόσο σε Linux κωδικούς όσο και σε Windows

- Παρόλο που ήταν αποτελεσματική η εφαρμογή, ήταν λίγο αργός ο αλγόριθμος των δοκιμών

4) Νικητής;

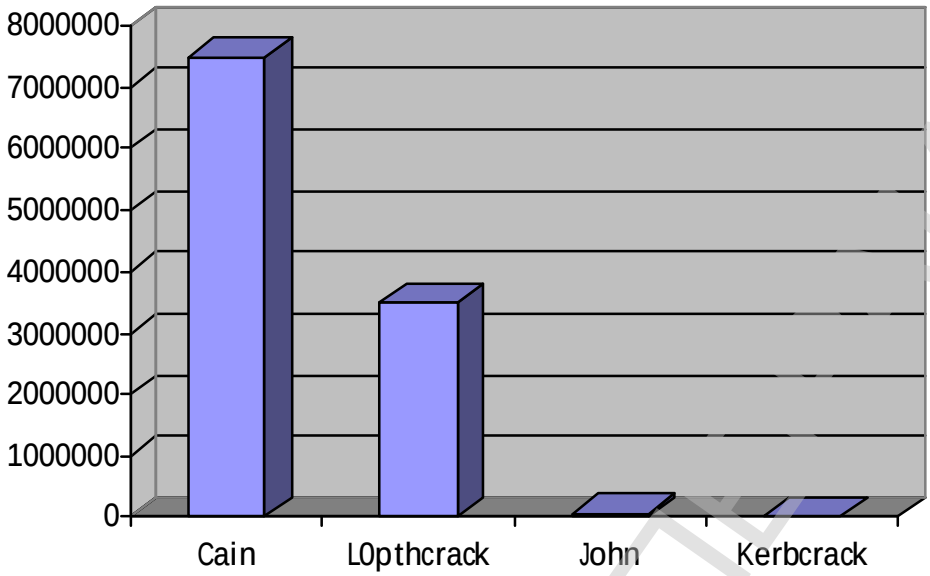
Υπάρχει νικητής σε αυτή τη δοκιμή; Οι εφαρμογές είχαν αρκετές διαφορές αλλά και αρκετές ομοιότητες. Για να εξάγουμε, όμως, ασφαλή συμπεράσματα όσον αφορά την αποτελεσματικότητα τους, σκεφτήκαμε να συγκρίνουμε τις 3 top εφαρμογές, όσον αφορά την αποτελεσματικότητας τους, με μια αντίστοιχη εφαρμογή μικρότερης «δημοτικότητας». Δοκιμάσαμε λοιπόν, το kerbcrack στην τελευταία έκδοση, v1.2.



Εικόνα 3-30: Παράδειγμα επίθεσης με το kerbcrack

Τα αποτελέσματα μας έδειξαν πόσο κορυφαίες ήταν οι προηγούμενες εφαρμογές. Το kerbcrack χρειάστηκε 10 ολόκληρα λεπτά για να βρει τον πιο απλό κωδικό με brute force επίθεση. Χρόνος υπερβολικά μεγάλος σε σχέση με την απίστευτη ταχύτητα που επέδειξαν οι άλλες εφαρμογές.

Ας δούμε λοιπόν συγκριτικά τις εφαρμογές όσον αφορά τις επιθέσεις ανά δευτερόλεπτο:



Πίνακας 1: Συγκριτικό επιθέσεων ανά δευτερόλεπτο των 4 password crackers

Όπως είδαμε λοιπόν το Cain έχει μια υπεροχή στην ταχύτητα δοκιμών σε σχέση με το L0pthcrack κατά ~4.000.000 δοκιμές περισσότερες το δευτερόλεπτο. Αυτό του δίνει ένα πολύ καλό προβάδισμα. Βέβαια αυτές οι μετρήσεις θα πρέπει να λαμβάνονται υπόψη σαν σχετικές μετρήσεις και αυτό γιατί είναι πάντα εξαρτώμενες με το hardware του υπολογιστή που τρέχουν. Δηλαδή σε έναν πιο γρήγορο προσωπικό υπολογιστή τα νούμερα θα μπορούσαν να εκτοξευτούν και πάνω από τις 10.000.000 δοκιμές ανά δευτερόλεπτο. Επίσης το γραφικό περιβάλλον που έχει είναι αρκετά εύχρηστο για τον χρήστη και έχει και ποικίλες άλλες δυνατότητες.

Αντίθετα, το L0pthcrack μπορεί να έχει τοποθετηθεί με βάση την ταχύτητα των επιθέσεων στην δεύτερη θέση όσον αφορά την αποτελεσματικότητα του αλλά το γραφικό του περιβάλλον η ποικιλία και ευκολία των επιθέσεων και τα reports το κάνουν μια αρκετά ικανή πλατφόρμα για επαγγελματικό επίπεδο.

Τέλος, το john the ripper δεν έχει ενδιαφέρον γραφικό περιβάλλον αλλά είναι μια εφαρμογή που δουλεύει παντού, επιτίθεται στα πάντα και μπορεί να είναι τελείως φορητή.

Ένας συγκεντρωτικός πίνακας:

Εφαρμογή	Cain & Abel	L0pthcrack	John the Ripper
Ταχύτητα	+++++	++++	++
Αποτελεσματικότητα	+++++	++++	+++

Κόστος	+++++	++	+++++
Φορητότητα	+	+	+++++
Αντικείμενα επίθεσης	+++	+++	+++++

Πίνακας 2: Συγκριτικός βαθμολογημένος πίνακας των 4 password crackers

Ποιος λοιπόν είναι ο νικητής στη δοκιμή; Η απάντηση είναι ποια είναι τα κριτήρια που μας ενδιαφέρουν:

- Αν θέλαμε να κάνουμε αποτελεσματικά ευρείας μορφής security tests σε περιβάλλον windows και μας απασχολούσε το κόστος η επιλογή μας θα ήταν το Cain & Abel.

- Αν εργαζόμαστε σε μια εταιρεία και θέλαμε να κάνουμε αποτελεσματικά dedicated security tests και να βλέπουμε συγκεντρωτικά reports και το κόστος δεν ήταν θέμα, η επιλογή μας θα ήταν το L0pthcrack.

- Αν απλά θέλαμε να έχουμε κάτι μαζί μας πάντα, που να δουλεύει σε οποιοδήποτε σύστημα και το οποίο θα επιτίθεται σε οτιδήποτε έστω και αν απαιτούσε περισσότερο χρόνο η επιλογή μας θα ήταν το John the Ripper.

C. Τρόποι προφύλαξης

Η καλύτερη μέθοδος για να προφυλαχθείς από το password cracking είναι να σιγουρέψεις ότι ο επιτιθέμενος δεν μπορεί να αποκτήσει πρόσβαση στους κρυπτογραφημένους κωδικούς. Για παράδειγμα στις διανομές του Unix οι κωδικοί είναι κρυπτογραφημένοι σε ένα δημόσια προσβάσιμο αρχείο το: /etc/shadow. Στις τελευταίες διανομές λοιπόν, αυτά είναι αποθηκευμένα στο αρχείο /etc/shadow, που είναι προσβάσιμα μόνο από το system. Αυτό ήδη καθιστά δυσκολότερο στο επιτιθέμενο να δοκιμάσει τους κρυπτογραφημένους κωδικούς.

Στις καινούργιες διανομές του Unix και σιγά σιγά και σε άλλα λειτουργικά συστήματα, οι παραδοσιακοί αλγόριθμοι κρυπτογράφησης (DES…) αντικαθιστώνται από τους πιο ισχυρούς md5 και blowfish. Αυτές οι μέθοδοι χρησιμοποιούν μεγάλου μήκους salt και αργούς αλγορίθμους κρυπτογράφησης για να δυσχεραίνουν τις προσπάθειες του πιθανού επιτιθέμενου.

Άλλος τρόπος προστασίας είναι η χρήση one-time κωδικών που μετά τη χρήση τους δεν έχουν καμία αξία. Τέτοιους κωδικούς παράγουν συσκευές όπως η παρακάτω και χρησιμοποιούνται συνήθως σε τραπεζικές εφαρμογές:

Εικόνα 3-31: Συσκευή για επιπλέον στιγμιαίους κωδικούς

D. Συμπέρασμα

Το password cracking έχει εξελιχθεί σε μια διαδικασία πολύ εύκολη καθώς κυκλοφορούν δεκάδες προγράμματα που υλοποιούν τις παραπάνω τεχνικές. Τηρώντας, όμως, κάποιους απλούς κανόνες ασφαλείας που αναφέραμε δυσκολεύουμε κατά πολύ τη δουλειά του επιτιθέμενου. Αυτό δε σημαίνει ότι δε θα καταφέρει να βρει κάποτε τον κωδικό μας αλλά ότι το να ασχοληθεί για να τον βρει ή να αφιερώσει ένα μηχάνημα του στο να κάνει επίθεση για μήνες θα του κοστίσει αρκετά περισσότερο από αυτά που θα κερδίσει όταν κάποτε βρει τον κωδικό. Οπότε, υπολογίζοντας το κόστος και τη ζημία που θα έχει το πιο πιθανό είναι να διακόψει την επίθεση.

4. Key logging

Το Φεβρουάριο του 2005, η Joe Lopez, μια επιχειρηματίας στην Φλόριντα των Η.Π.Α., έκανε μήνυση στην «Εθνική» τράπεζα της Αμερικής ότι άγνωστοι hackers της έκλεψαν $90.000 από τον λογαριασμό της και τα χρήματα μεταφέρθηκαν στην Λάτβια. Μετά από έρευνα βρέθηκε ότι ο υπολογιστής της κυρία Lopez είχε μολυνθεί από ένα κακόβουλο πρόγραμμα, το Backdoor.Coreflood, που καταγράφει τις πληκτρολογήσεις και στέλνει πληροφορίες σε χρήστες στο Internet. Έτσι το δικαστήριο δεν αποφάσισε υπέρ της κυρία Lopez, θεωρώντας πως αμέλησε να πάρει τις απαραίτητες βασικές προφυλάξεις στον προσωπικό της υπολογιστή.

Το keystroke logging ή key logging, στη βασική του μορφή είναι μια τεχνική καταγραφής των πληκτρολογήσεων, συνήθως συγκαλυμμένα ώστε ο χρήστης να μην γνωρίζει αυτή την ενέργεια. Υπάρχουν πολλές μέθοδοι key logging, hardware και software-based.

Υπάρχουν σοβαρά προγράμματα που χρησιμοποιούν key logging μεθόδους για να χρησιμοποιήσουν συγκεκριμένα προγράμματα που χρησιμοποιούν hotkeys, ή για να εναλλάσσονται ανάμεσα σε 2 keyboard layouts. Επίσης, υπάρχουν προγράμματα που χρησιμοποιούν διαχειριστές συστημάτων για να κρατάνε στατιστικά για το τι κάνουν οι εργαζόμενοι κατά τη διάρκεια της ημέρας αλλά το ηθικό όριο ανάμεσα στο σημείο που δικαιολογεί αυτή την καταγραφή, με την αρχή της κατασκοπίας είναι πολύ μικρό και έτσι τέτοιου είδους λογισμικό χρησιμοποιείται πολλές φορές για να υποκλαπούν πληροφορίες όπως κωδικοί χρηστών. Βέβαια όπως είπαμε δεν πρέπει να ξεχνάμε ότι υπάρχουν και hardware key loggers που πρέπει να έχουμε υπόψη μας αν και η χρήστη προγραμμάτων είναι πολύ πιο διαδεδομένη, «αόρατη», ελεγχόμενη και αποδοτική.

Οι περισσότεροι σύγχρονοι key loggers θεωρούνται νόμιμα προϊόντα που πωλούνται κανονικά στην αγορά. Οι εταιρείες που τα δημιουργούν παραθέτουν μια αρκετά μεγάλη λίστα νόμιμων περιπτώσεων που θα μπορούσαν να χρησιμοποιηθούν. Για παράδειγμα:

- Γονικός έλεγχος: οι γονείς πρέπει να βλέπουν τι κάνουν τα παιδιά στο Internet ώστε να ενημερώνονται αν υπάρχουν προσπάθειες πρόσβασης σε site με ακατάλληλο περιεχόμενο.

- Ζηλιάρες σύζυγοι που χρησιμοποιούν τέτοιου είδους λογισμικό για να ανιχνεύσουν τις πράξεις των συζύγων τους στο internet αν επικαλεστούν υποψίες «εικονικής μοιχείας»

- Εταιρική Ασφάλεια: Η ανίχνευση της χρήσης υπολογιστών στην εργασία για λόγους που δε σχετίζονται με την εργασία ή η χρήση των υπολογιστών σε χρήση τους σε περίεργες ώρες πχ πολύ μετά το πέρας του ωραρίου.

- Εταιρική Ασφάλεια: Η χρήση τους για ανίχνευση λέξεων-κλειδιά συσχετιζόμενα με πληροφορίες που η μετάδοση τους θα μπορούσε να επιφέρει ζημία στην εταιρεία.

- Και διάφοροι άλλοι λόγοι.

Βέβαια οι αιτιολογίες που αναφέρθηκαν παραπάνω είναι περισσότερο υποκειμενικές παρά αντικειμενικές. Και θα μπορούσαν όλες οι παραπάνω καταστάσεις να επιλυθούν χωρίς να χρησιμοποιηθούν τέτοιες μέθοδοι. Επιπλέον οποιοδήποτε τέτοιου είδους νόμιμο πρόγραμμα ή πρόγραμμα που γίνεται νόμιμη χρήση του μπορεί να χρησιμοποιηθεί πολύ εύκολα και για παράνομη χρήση χωρίς να γίνει αντιληπτό. Πολλοί key loggers σήμερα χρησιμοποιούνται για να υποκλέψουν προσωπικά δεδομένα χρηστών που σχετίζονται με Online πληρωμές και στοιχεία πιστωτικών καρτών. Επίσης επειδή οι περισσότεροι key loggers είναι καλά κρυμμένοι στο σύστημα (πχ με root kit λειτουργίες) είναι πολύ δύσκολο να αποκαλυφθούν ακόμα και από Trojan removers και έτσι ο χρήστης δε γνωρίζει ότι έχει πέσει θύμα υποκλοπής.

Το να φτιάξεις έναν Key loggers δεν είναι δύσκολο και όπως και άλλα τέτοιου είδους προγράμματα μπορούν να μεταδοθούν είτε μέσω ενός Trojan είτε ενός ιού. Αυτού που είναι δύσκολο είναι να καταφέρει ο επιτιθέμενος να εγκαταστήσει ένα τέτοιο πρόγραμμα χωρίς να γίνει αντιληπτή η προσπάθεια του από συστήματα ασφαλείας καθώς επίσης και να κατεβάζει τα δεδομένα που του στάλθηκαν χωρίς να αφήσει ίχνη.

Α. Γιατί οι key loggers θεωρούνται απειλή

Αντίθετα με άλλα κακόβουλα προγράμματα, οι key loggers, δεν αποτελούν απειλή στο ίδιο το σύστημα. Αυτό που κάνουν είναι να αποτελούν απειλή για τους ίδιους τους χρήστες και τα προσωπικά τους δεδομένα που εισάγουν στο σύστημα τους. Οποιοσδήποτε υποκλέψει στοιχεία καρτών, μεταφορές χρημάτων κτλ θα επιφέρει μεγάλη ζημία στον χρήστη. Μπορεί ακόμα βέβαια να προκαλέσει και μεγαλύτερη ζημιά αν χρησιμοποιηθούν σε περιπτώσεις εμπορικής/κυβερνητικής/βιομηχανικής κατασκοπίας πάλι αν υποκλαπούν πληροφορίες που είναι μυστικές. Οι key loggers και το Phishing είναι βασικοί μέθοδοι που χρησιμοποιούνται σε κυβερνο-εγκλήματα που αφορούν υποκλοπές δεδομένων. Ενώ βέβαια είναι εύκολο να αντιμετωπίσεις το phishing αν είσαι προσεκτικός κανένας χρήστης δε μπορεί με σιγουριά να πει ότι δεν υπάρχει key logger εγκατεστημένος στο σύστημα του. Γι' αυτό και οι Key loggers έχουν πλέον εκτοπίσει το Phishing από την πρώτη θέση των μεθόδων υποκλοπής εμπιστευτικών δεδομένων. Η μόνη λύση είναι να χρησιμοποιεί κατάλληλο software όπως θα αναλύσουμε αργότερα.

Η βασική ιδέα στους key loggers είναι να μπεις ανάμεσα στους δυο συνδέσμους της αλυσίδας γεγονότων από όταν πατιέται ένα πλήκτρο μέχρι να φανεί η πληκτρολόγηση στην οθόνη ή να γίνει κάποια άλλη ενέργεια. Αυτό θα δούμε με ποιους τρόπους μπορεί να γίνει. Όσο πιο σύνθετη η δομή τόσο πιο απίθανο είναι να βρεθεί σε ένα απλό Trojan και τόσο πιο πιθανό να βρεθεί σε ειδικά σχεδιασμένο Trojan που θα έχει σχεδιαστεί για να υποκλέψει οικονομικά στοιχεία ή κάτι παρόμοιο.

B. Hardware & software τύποι key loggers:

Εδώ θα αναλύσουμε τους βασικούς τύπους key loggers. Θα επικεντρωθούμε περισσότερο στους πιο συνηθισμένους, εφαρμογές των οποίων θα δοκιμάσουμε και παρακάτω στη μελέτη μας.

1) Local machine key loggers

Εδώ μιλάμε για προγράμματα που είναι σχεδιασμένα να δουλεύουν εγκατεστημένα στο λειτουργικό σύστημα του χρήστη. Από τεχνικής απόψεως υπάρχουν 4 κατηγορίες:

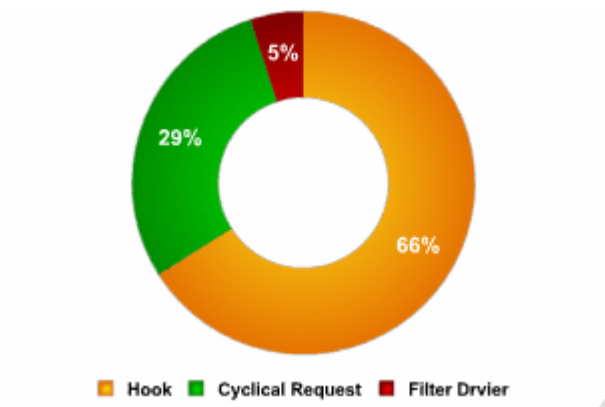
- System Hook based: Αυτοί οι key loggers κρύβονται στο σύστημα και χρησιμοποιώντας από τα APIs του λειτουργικού τις μεθόδους SetWindowsHook του πληκτρολογίου υποκλέπτουν και καταγράφουν τις πληκτρολογήσεις. Συνήθως είναι γραμμένα σε C.

- Passive Cyclic Methods: Εδώ χρησιμοποιούνται από τα APIs του λειτουργικού τα GetAsyncKeyState(), GetKeyboardState, GetForegroundWindow(), κτλ. για να καταγράφουν τις πληκτρολογήσεις. Είναι η πιο εύκολη μέθοδος αλλά αυξάνουν πολύ τη cpu και επίσης υπάρχει και η περίπτωση να μην «πιάσει» κάποια πληκτρολόγηση. Συνήθως γραμμένα σε Visual Basic ή και Delphi.

- Kernel based και Filter Drivers: Οι key loggers αυτού του τύπου είναι πολύ δύσκολο να δημιουργηθούν. Λειτουργούν σε kernel level και είναι πολύ δύσκολο να εντοπιστούν ειδικά από προγράμματα που τρέχουν σε user-mode. Φτιάχνονται συνήθως σαν root kits που ξεγελάνε το λειτουργικό και έχουν μη εξουσιοδοτημένη πρόσβαση όπου θέλουν. Συνήθως γραμμένα σε C.

- Hypervisor-based: Ο key logger μπορεί θεωρητικά να βρίσκεται σε ένα κακόβουλο πρόγραμμα που τρέχει σαν hypervisor του λειτουργικού που δουλεύει ο χρήστης (πχ σε ένα virtual machine) και να παραμένει ανέγγιχτο.

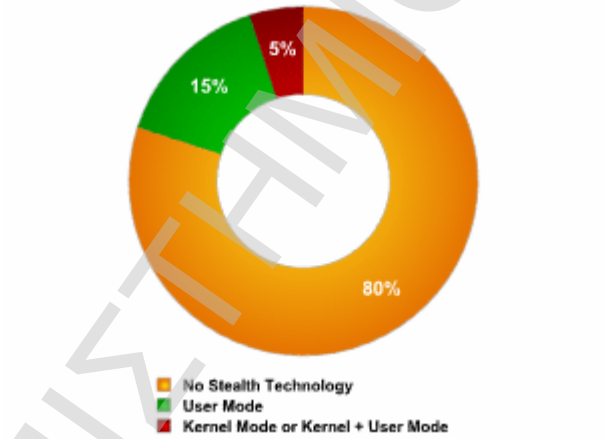
- Form Grabber: Μέθοδος που ανιχνεύει τα on submit σε φόρμες ιστοσελίδων και καταγράφει τα δεδομένα. Πολύ χρήσιμη γιατί παρακάμπτει την ασφάλεια που προσφέρει το Https.



Εικόνα 4-1: Στατιστικά της χρήσης των βασικών από τις παραπάνω τεχνολογίες

Τελευταία οι key loggers που «μεταμφιέζουν» ή κρύβουν τα αρχεία τους για να μη γίνονται αντιληπτοί από τα προγράμματα προστασίας γίνονται όλο και πιο πολλοί. Αυτές οι τεχνικές που χρησιμοποιούν λέγονται root kit τεχνικές. Υπάρχουν 2 κύριες τεχνολογίες που χρησιμοποιούνται:

- Μεταμφίεση σε user mode;
- Μεταμφίεση σε kernel mode.



Εικόνα 4-2: Στατιστικά της χρήσης των τεχνολογιών αυτών

2) Remote access software

Βασισμένοι στους παραπάνω τρόπους υποκλοπής με ένα πρόσθετο χαρακτηριστικό: να μεταδίδουν τα δεδομένα σε κάποια απομακρυσμένη τοποθεσία. Οι τρόποι είναι οι παρακάτω:

- Τα δεδομένα γίνονται Upload σε ένα website ή έναν ftp λογαριασμό.
- Τα δεδομένα στέλνονται σε κάποιο e-mail περιοδικά.
- Τα δεδομένα μεταδίδονται wireless σε σκοπό κάποιος δέκτης να τα συλλέγει.

- Ακόμα και πρόσβαση κατευθείαν στον υπολογιστή είτε φυσική είτε δικτυακή και σύνδεση σε αυτόν και εξαγωγή των log αρχείων.

Εικόνα 4-3: Παράδειγμα remote access software

3) Hardware key logging

Οι hardware-based key loggers δεν βασίζονται σε κάποιο λογισμικό καθώς επηρεάζουν κατευθείαν το hardware του υπολογιστή. Χωρίζονται στα εξής:

- Firmware-based: πρόκειται για BIOS-level firmware που χειρίζεται γεγονότα του πληκτρολογίου και τα καταγράφει. Φυσική πρόσβαση απαιτείται στο μηχάνημα και το bios πρέπει να έχει αλλαχθεί για το συγκεκριμένο σύστημα.

- Keyboard hardware: Οι Hardware key loggers έχουν σχεδιαστεί για να προσαρμόζονται κάπου ανάμεσα στο πληκτρολόγιο και τον υπολογιστή. Επιπλέον μπορούν να κατασκευαστούν πληκτρολόγια με ενσωματωμένο κάποιον key logger ώστε να μην είναι καν ορατός. Και στις δυο περιπτώσεις αποθηκεύουν σε μια εσωτερική μνήμη τις πληροφορίες και ο επιτιθέμενος μπορεί να έχει πρόσβαση σε αυτές με κάποιο μυστικό συνδυασμό πλήκτρων ή μπορεί να τις λαμβάνει χρησιμοποιώντας κάποιο ασύρματο πρωτόκολλο. Τα θετικά του Hardware key logger είναι ότι δε χρησιμοποιεί επεξεργαστική ισχύ από τον υπολογιστή, δεν εμπλέκεται σε κανένα πρόγραμμα και δεν μπορεί να ανιχνευτεί με κανένα πρόγραμμα. Παρόλα αυτά η φυσική του παρουσία μπορεί να ανιχνευτεί με το μάτι.

Εικόνα 4-4: Παράδειγμα hardware key logger

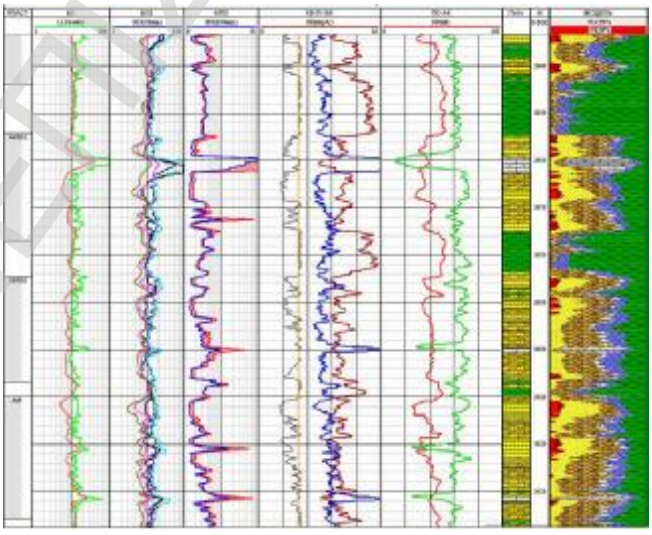
4) Wireless sniffers

Αυτοί είναι παθητικοί sniffers που συγκεντρώνουν data που μεταφέρονται από ασύρματα πληκτρολόγια στον υπολογιστή. Φυσικά, όταν χρησιμοποιείται κάποια κρυπτογράφηση δεν είναι τόσο απλό.

Εικόνα 4-5: Παράδειγμα wireless sniffer

5) Acoustic

Η ακουστική κρυπτανάλυση μπορεί να χρησιμοποιηθεί για να καταγράφει και να επεξεργάζεται κάποιος τον ήχο των πληκτρολογήσεων σε έναν υπολογιστή. Κάθε πλήκτρο στο πληκτρολόγιο κάνει έναν ελάχιστα διαφορετικό ήχο όταν πατιέται. Έτσι ο διαφορετικός ήχος, η καθυστέρηση ανάμεσα στις πληκτρολογήσεις, η γλώσσα του χρήστη κτλ βοηθάνε στο να αντιστοιχιστούν οι ήχοι με πλήκτρα!



Εικόνα 4-6: Παράδειγμα acoustic key logger

6) Electromagnetic

Επίσης είναι πιθανό να συλλάβεις τα ηλεκτρομαγνητικά κύματα του πληκτρολογίου χωρίς να είσαι φυσικά συνδεδεμένος σε αυτό. Η μέθοδος αυτή είναι σε πειραματικό στάδιο ακόμα όμως.

7) Optical surveillance

Όχι ακριβώς ένας key logger με την κλασσική έννοια, αλλά μια προσέγγιση. Μια κάμερα σωστά τοποθετημένη μπορεί να επιτρέψει στον επιτιθέμενο να βλέπει όλες τις πληκτρολογήσεις του χρήστη.

C. Μελέτη και δοκιμή top key loggers

Σε αυτή την ενότητα θα μελετήσουμε την λειτουργία και την αποδοτικότητα κάποιων κορυφαίων key loggers. Η επιλογή τους έγινε μετά από έρευνα σε διάφορες κοινότητες που ασχολούνται με τέτοια εργαλεία καθώς και διάφορα site, όπως το key logger.org και το viruslist.com, που έχουνε λίστες ανάλογου λογισμικού. Η επιλογή 3 top προγραμμάτων έγινε μέσα από τη δικιά τους κατάταξη με βάση, όμως, κάποια κριτήρια που θέσαμε εμείς σαν απαραίτητα και θα τα αναλύσουμε εδώ.

Key loggers υπάρχουν πολλοί, αλλά κάποια χαρακτηριστικά τα θεωρούμε άκρως απαραίτητα και πρέπει να τα υποστηρίζουν οι top επιλογές μας. Καταρχάς τέτοιο λογισμικό δεν πρέπει να γίνεται ποτέ αντιληπτό από τον χρήστη ή από το σύστημα και κυρίως τα προγράμματα ασφαλείας του(anti-virus κτλ). Οπότε βασικό χαρακτηριστικό είναι ο key logger να λειτουργεί σε invisible ή stealth mode όπως αναφέρεται χαρακτηριστικά σε αυτά τα προγράμματα. Για να γίνει αυτό πρέπει να μην υπάρχουν προσθήκες στο start menu, στα program files, στον πίνακα ελέγχου

στη λίστα με τα εγκατεστημένα προγράμματα, στη διαχείριση εργασιών του task manager, να λειτουργεί σαν root kit κτλ.

Επιπλέον, θεωρούμε ότι απαραίτητο στοιχείο ενός key logger είναι η αποστολή των logs είτε μέσω e-mail, είτε με ftp ή σε κάποιον απομακρυσμένο χώρο. Δεν μπορούμε να θεωρούμε δεδομένο, ο επιτιθέμενος, να έχει πάντα δυνατότητα για απομακρυσμένη σύνδεση για να ανασύρει τα log files. Οπότε δυνατότητες αποστολής των log files είναι κατά τη γνώμη μας υποχρεωτικό να υπάρχουν.

Τα υπόλοιπα χαρακτηριστικά που θα εξετάσουμε για να συγκρίνουμε τους key loggers είναι οι δυνατότητες παρακολούθησης που υποστηρίζουν. Οι σύγχρονοι key loggers δεν πρέπει να αρκούνται σε απλό key logging των key strokes του πληκτρολογίου. Πρέπει, τουλάχιστον, να παίρνουν screenshots κατά διαστήματα και υπάρχουν και πολλές εφαρμογές πλέον που καταγράφουν video. Αυτό γιατί μπορεί να θέλουμε να καταγράψουμε την κίνηση σε εφαρμογές που χρησιμοποιεί ο χρήστης και αφού ο αποθηκευτικός χώρος ακόμα και στους προσωπικούς υπολογιστές είναι συνήθως αρκετά μεγάλος στις μέρες μας πρέπει να έχουμε αυτή τη δυνατότητα. Επιπλέον μερικές φορές, μπορεί να μας ενδιαφέρουν συγκεκριμένες κινήσεις του χρήστη (πχ web browser μόνο), ή μπορεί να θέλουμε να μειώσουμε το μέγεθος του Log file, οπότε, καλό θα ήταν να είχαμε δυνατότητες επιλογής των εφαρμογών, δηλαδή να επιλέξουμε τι θα καταγράφαμε.

Για να επιλέξουμε, λοιπόν, τα 3 top από τη λίστα δεν διαλέξαμε απλώς τα 3 πρώτα σε βαθμολογία αλλά θεωρήσαμε ως σημαντικά χαρακτηριστικά τα παραπάνω, οπότε οι επιλογές μας ήταν ελαφρώς διαφορετικές. Για να φτάσουμε, μάλιστα στο να επιλέξουμε αυτά τα τρία δοκιμάσαμε εννιά από τις top εφαρμογές που βρήκαμε, που πληρούσαν, όπως διαφήμιζαν, τις απαιτήσεις μας. Έξι από τις εννιά, όμως, μας απογοήτευσαν.

Ακόμα, κατά τη δοκιμή των key loggers, διαπιστώσαμε ότι κάποιοι επηρέαζαν άλλους ή κατά την απεγκατάσταση άφηναν «κατάλοιπα» ή κάποια δεν υποστήριζαν απεγκατάσταση. Έτσι κάναμε μια νέα καθαρή εγκατάσταση του λειτουργικού την οποία την κρατήσαμε σαν image και πριν από κάθε νέα δοκιμή, ξανά-επαναφέραμε, με το Image, αυτή την εγκατάσταση και η δοκιμή γινόταν πάντα σε μια καθαρή εγκατάσταση, χωρίς επιρροές ή «κατάλοιπα» από τους προηγούμενους key loggers.

Το σενάριο που θα δοκιμάσουμε σε αυτούς τους key loggers είναι το εξής:

- Εγκατάσταση του key logger χωρίς να απαιτούνται πολλές ενέργειες(restart κτλ.)

- Λειτουργία σε stealth mode, χωρίς να ενεργοποιούνται συστήματα ασφαλείας (anti-virus κτλ) και έλεγχος της επίδρασης του στο σύστημα(καθυστέρηση απόκρισης συστήματος, περίεργη συμπεριφορά) γιατί όπως είπαμε σκοπός του είναι να μη γίνεται αντιληπτός.

- Ρυθμίσεις του key logger όσον αφορά τον τρόπο που γίνεται το logging, σε ποιες εφαρμογές (κειμενογράφοι, browsers, IM messengers), τη δυνατότητα για instant alert(άμεση ειδοποίηση), τη συχνότητα που κάνουν capture screenshot, το αν καταγράφεται βίντεο, την αποστολή e-mail ή αποστολή με ftp κτλ.

- Έναρξη καταγραφής

- Γενική χρήση: Ανοίγουμε μερικούς φακέλους και έπειτα μερικά αρχεία. Διαβάζουμε και προσθέτουμε σε κάποια αρχεία κειμένου μερικές λέξεις ακόμα.

- Έπειτα ανοίγουμε έναν web browser. Επισκεπτόμαστε έναν λογαριασμό e-mail, κάνουμε εισαγωγή Username και Password. Έπειτα μπαίνουμε στο site της τράπεζας μας και συνδεόμαστε στο e-banking account μας πάλι εισάγοντας τους απαραίτητους κωδικούς

- Τέλος, ανοίγουμε έναν Instant Messenger (googletalk) και συνομιλούμε με κάποιον που είναι συνδεδεμένος. Η επιλογή του googletalk και όχι ενός πιο διαδεδομένου όπως ο Live Messenger έγινε γιατί δε θέλαμε να δοκιμάσουμε την εύκολη περίπτωση του πιο γνωστού IM αλλά να είμαστε σίγουροι ότι θα γινόταν σωστή καταγραφή ακόμα και σε έναν όχι τόσο διαδεδομένο.

- Έλεγχος για επιτυχής καταγραφή, τρόπος καταγραφής και εμφάνισης των αποτελεσμάτων κτλ

- Έλεγχος για αποστολή των log files, τρόπος export των log files κτλ.

  Κάναμε λοιπόν απλές καθημερινές κινήσεις που θα έκαναν όλοι οι άνθρωποι και επισκεφθήκαμε καίρια σημεία τα οποία είναι σημαντικά για κάποιον αν παραβιαστούν. Ποιός θα ήθελε να υποκλαπούν προσωπικά μηνύματά του, προσωπικές συζητήσεις του ή οι κωδικοί διαχείρισης του τραπεζικού του λογαριασμού; Εδώ τελειώνει το σενάριο μας που θα δούμε σε κάθε εφαρμογή.

1) Spytech SpyAgent

Παρουσίαση – Εγκατάσταση – Αρχικές ρυθμίσεις

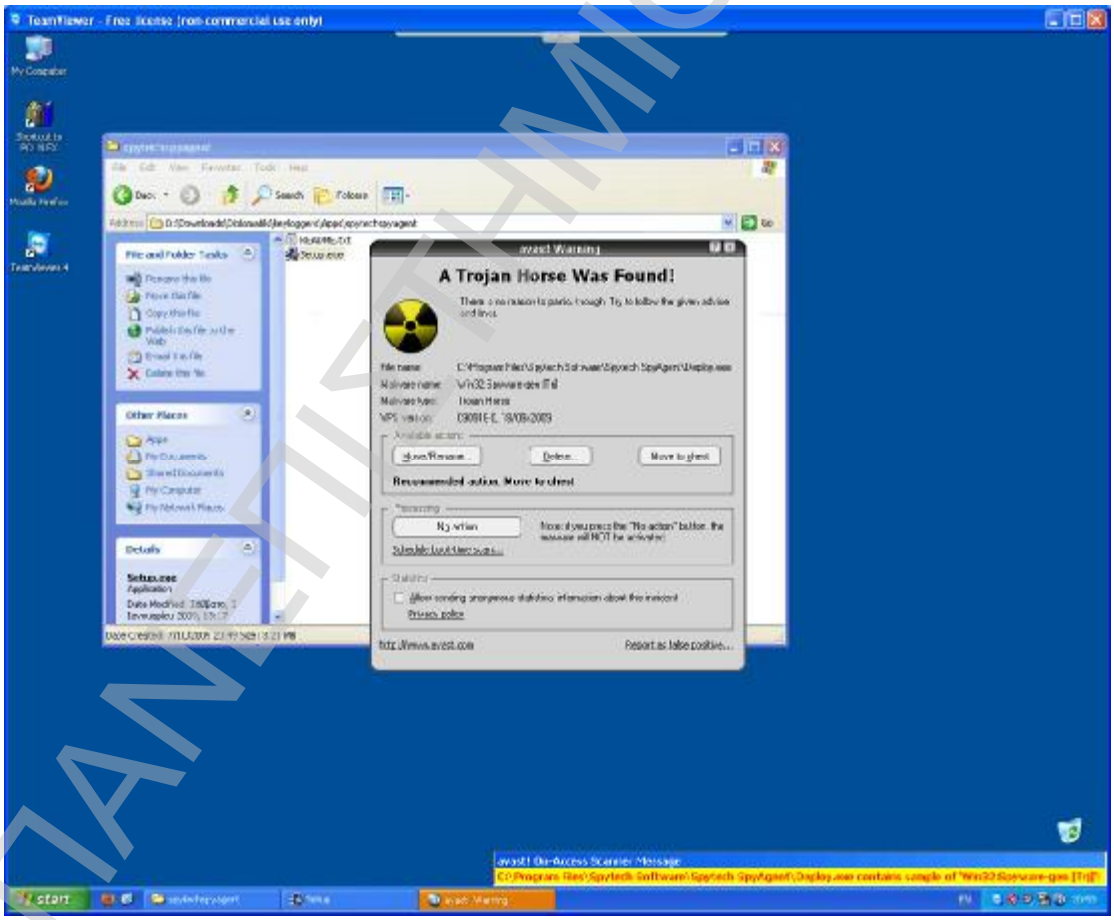
Ξεκινάμε δοκιμάζοντας την πρώτη εφαρμογή στη λίστα μας, το spyAgent της Spytech. Το SpyAgent έχει διάφορες επιλογές από εκδόσεις αναλόγως αν θες το key logging να γίνεται εμφανώς στον χρήστη ή όχι. Εφόσον έχουμε προδιαγράψει από τις απαιτήσεις μας ότι δε θέλουμε ο χρήστης να είναι γνώστης της παρακολούθησης, επιλέξαμε την stealth έκδοση στην τελευταία version της, την v.6.40. Παρεμπιπτόντως η εφαρμογή αυτή είναι η πρώτη στις λίστες των top 10 που λάβαμε υπόψη μας. Το κόστος της εφαρμογής είναι $80.

Ξεκινάμε λοιπόν και κάνουμε την εγκατάσταση του SpyAgent και επιλέγουμε όπως είπαμε εγκατάσταση μορφής «stealth» της εφαρμογής:

Εικόνα 4-7: Εκκίνηση εγκατάστασης SpyAgent

Για την ιστορία, η άλλη επιλογή μας δίνει δυνατότητες εμφάνισης των μενού, διαχείρισης των logs στον ίδιο υπολογιστή κτλ, μια μη-stealth μορφή λειτουργίας δηλαδή.

Κατά την εγκατάσταση σε όλα τα key loggers που χρησιμοποιήσαμε το antivirus ενεργοποιήθηκε, οπότε για να γίνει σωστά η εγκατάσταση έπρεπε να το απενεργοποιήσουμε προσωρινά. Ελπίζουμε τουλάχιστον να μην ενεργοποιείται και κατά την καταγραφή.



Εικόνα 4-8: Ενεργοποίηση anti-virus από την εγκατάσταση

Ολοκληρώθηκε λοιπόν η εγκατάσταση και ξεκινά ένας wizard για να μας βοηθήσει στις ρυθμίσεις τις εφαρμογής. Πρώτα επιλέγουμε τον κωδικό που θέλουμε να έχουμε για να μπούμε στην εφαρμογή.

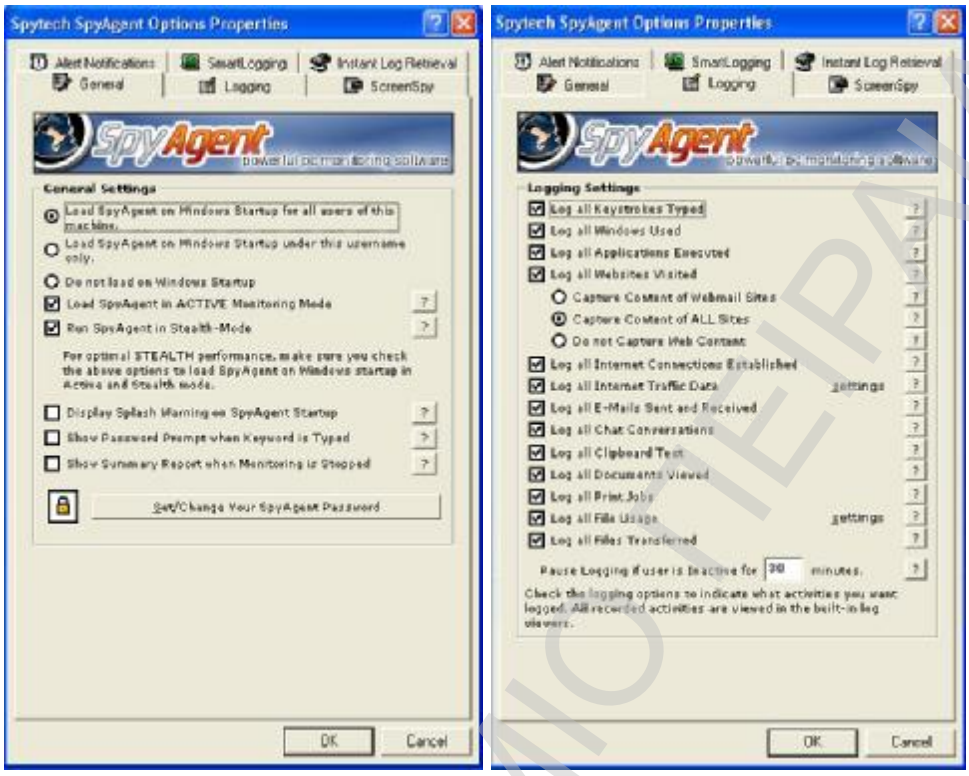
Εικόνα 4-9: Πρώτα βήματα wizard εγκατάστασης

Έπειτα επιλέγουμε τύπο εγκατάστασης που θέλουμε και μετά επιλέγουμε τρόπο αποστολής των reports. Σε κάθε επιλογή μας συμπληρώνουμε τα απαραίτητα στοιχεία πχ στην αποστολή με e-mail συμπληρώνουμε το e-mail που θέλουμε να στέλνονται τα reports. Θυμίζουμε ότι αυτές είναι οι βασικές ρυθμίσεις που κάνουμε με τον wizard και περισσότερες ρυθμίσεις θα έχουμε δυνατότητα να δούμε μετά την ολοκλήρωση της εγκατάστασης.

Εικόνα 4-10: Ρυθμίσεις με τον wizard

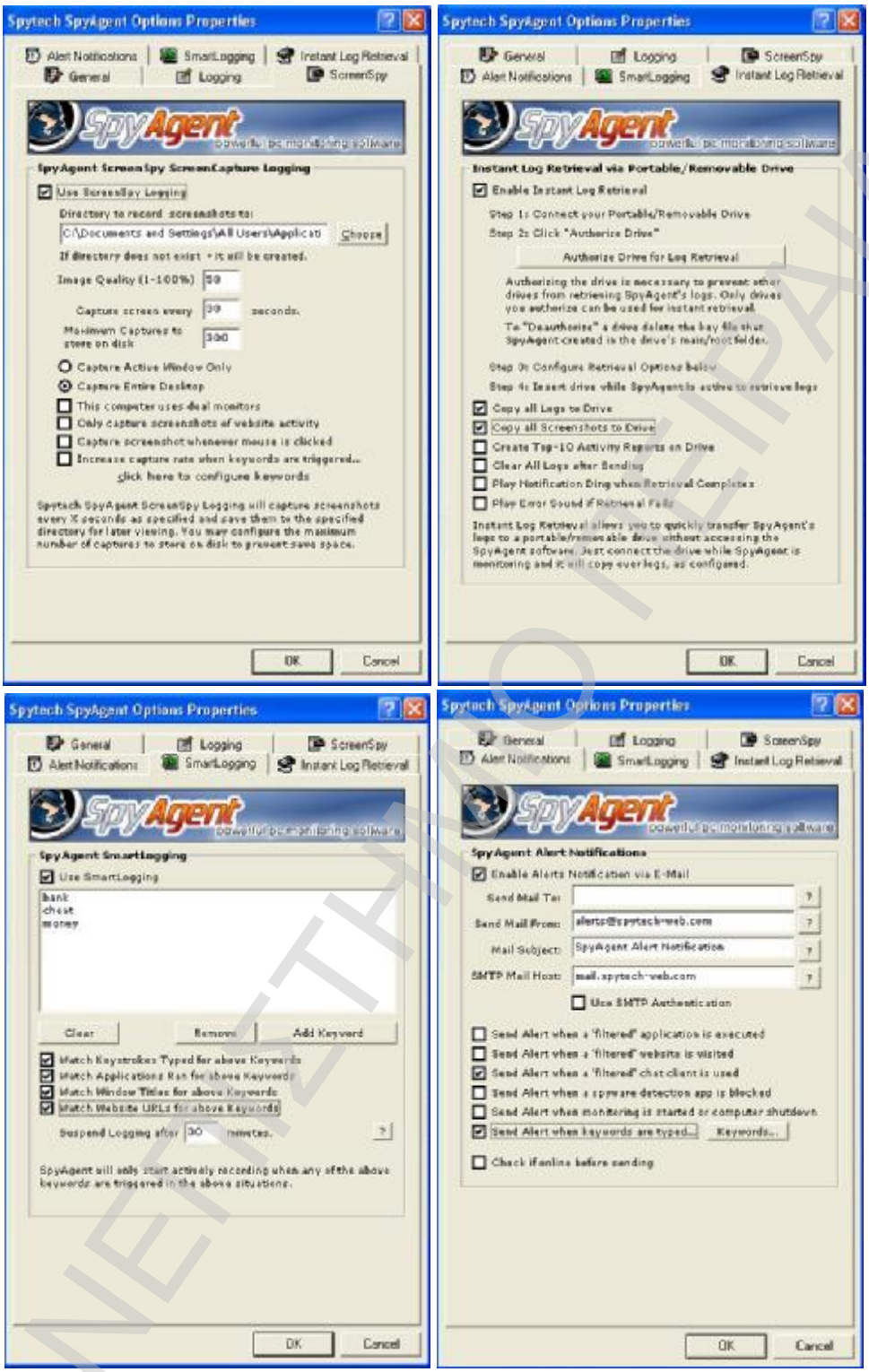
Αφού τελειώσει η εγκατάσταση ανοίγει η εφαρμογή και βλέπουμε τις καρτέλες με τις ρυθμίσεις. Ενδεικτικά θα παραθέσουμε μερικές και θα αναφέρουμε μερικές χαρακτηριστικές δυνατότητες. Βλέπουμε ότι το πρόγραμμα έχει τη δυνατότητα να ξεκινάει με την εκκίνηση του υπολογιστή και μάλιστα με ενεργή την καταγραφή. Αυτό μας έκανε να αναμένουμε ότι θα καταγράφει και το login password των χρηστών, μια λειτουργία αρκετά χρήσιμη. Δυστυχώς όμως η εκκίνηση του γινόταν μετά το login, οπότε δεν υπήρχε καμία καταγραφή πριν από αυτό. Παρατηρούμε επίσης τις αρκετές

επιλογές που έχει στην καταγραφή όσον αφορά κατηγορίες εφαρμογών και ενεργειών.



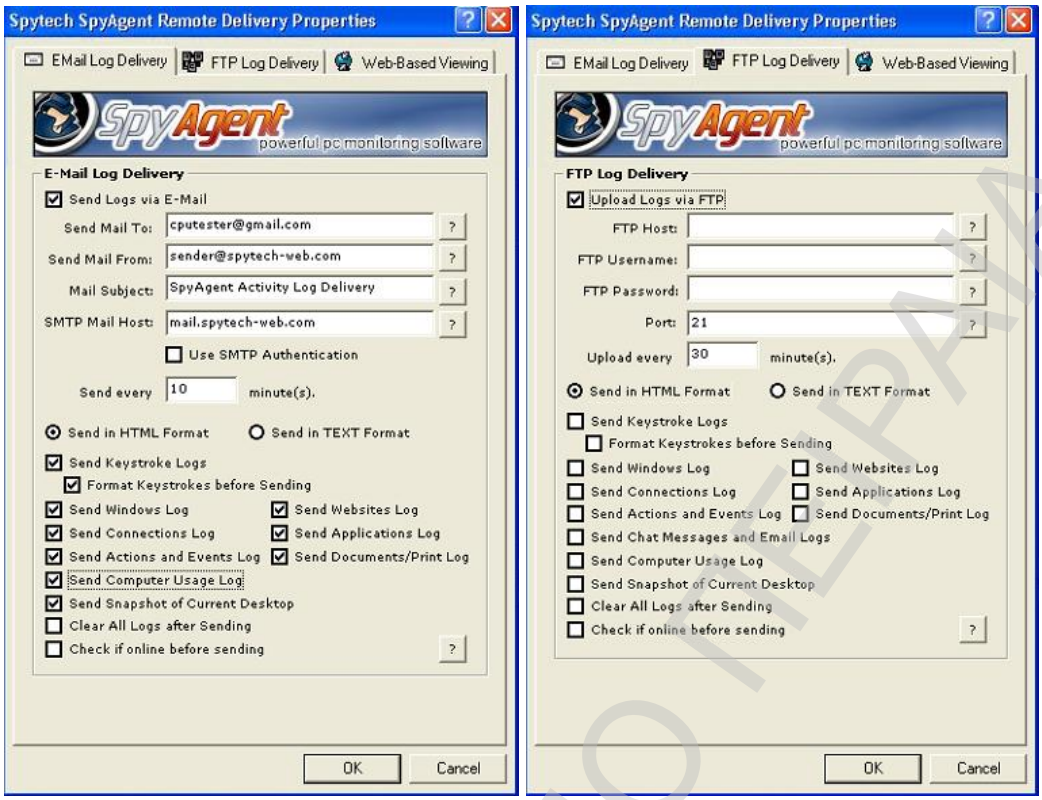
Εικόνα 4-11: Καρτέλες ρυθμίσεων SpyAgent

Ακόμα, μερικές καρτέλες με ρυθμίσεις για το που να αποθηκεύονται τα logs και τα screenshots, για δυνατότητες άμεσης ειδοποίησης, δυνατότητες smart logging όπου μπορείς να εισάγεις keywords όπως για παράδειγμα bank, money κτλ. Επίσης υποστηρίζεται η δυνατότητα alert-email, δηλαδή σε περιπτώσεις που θα του ορίσεις (πχ καταγραφή μιας λέξης) γίνεται άμεσα ενημέρωση και αποστολή του log.



Εικόνα 4-12: Καρτέλες ρυθμίσεων SpyAgent

Εδώ βλέπουμε τις δυνατότητες αποστολής των log files. Υποστηρίζεται η αποστολή μέσω e-mail όπως έχουμε πει και μέσω ftp. Πάντα κατά τη ρύθμιση μπορούμε να επιλέξουμε τι θα μας αποστέλλει ώστε να μην επιβαρύνουμε την αποστολή.



Εικόνα 4-13: Καρτέλες ρυθμίσεων SpyAgent όσον αφορά τις αποστολές των log files

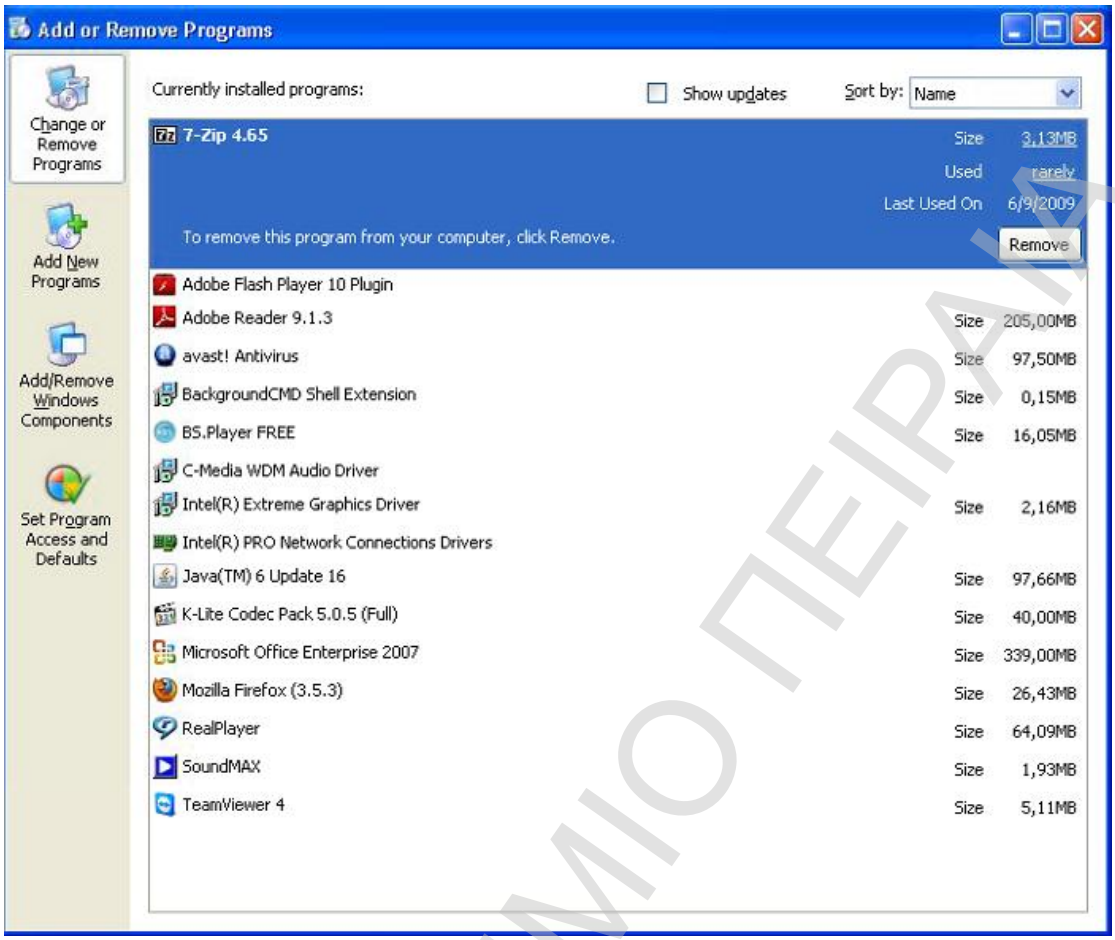
Παρακάτω βλέπουμε μερικές ακόμα ρυθμίσεις. Η εφαρμογή έχει τη δυνατότητα να καταγράφει συγκεκριμένες μέρες και ώρες, συγκεκριμένες εφαρμογές και συγκριμένους Instant Messengers.

Εικόνα 4-14: Καρτέλες ειδικευμένων ρυθμίσεων SpyAgent

Επίσης, όλοι οι Key loggers για να μην έχουν μενού και shortcuts, για να ανοίγουν ενεργοποιούνται με ειδικά hot-keys που μπορούμε να ρυθμίσουμε όπως επιθυμούμε ώστε να είναι μοναδικά.

Εικόνα 4-15: Καρτέλες ρύθμισης hot key SpyAgent

Επίσης, μετά την εγκατάσταση βλέπουμε ότι το πρόγραμμα δεν έχει αφήσει εμφανή σημεία εγκατάστασης, ούτε στο start menu, ούτε σε φακέλους, ούτε στην προσθαφαίρεση προγραμμάτων.



Εικόνα 4-16: Εμφάνιση παράθυρου προσθαφαίρεσης προγραμμάτων των Windows

Δοκιμή

Μετά τις προσεκτικές και αρκετές ρυθμίσεις λοιπόν, πάμε στο test. Ο key logger είναι αόρατος και «τρέξαμε» όλα τα βήματα του πειράματος όπως το προδιαγράψαμε στην αρχή της μελέτης.

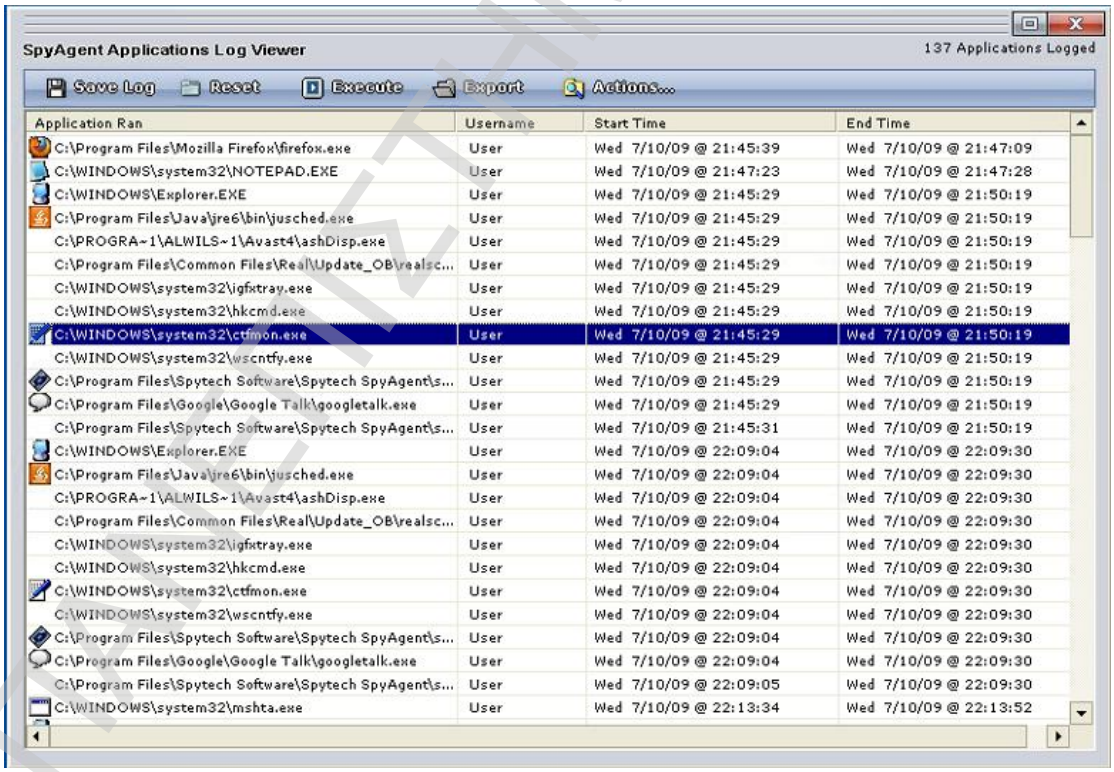
Ας δούμε λοιπόν τι κατέγραψε ο key logger μας.

Ανοίγουμε με το Hotkey μας Ctrl + Shift + Alt + S το spyagent και βλέπουμε την αρχική μας οθόνη

Εικόνα 4-17: Αρχική οθόνη SpyAgent

Όπως βλέπουμε το πρόγραμμα κατηγοριοποιεί τα καταγραμμένα γεγονότα και μπορούμε να ανακτήσουμε συγκεκριμένες εγγραφές.

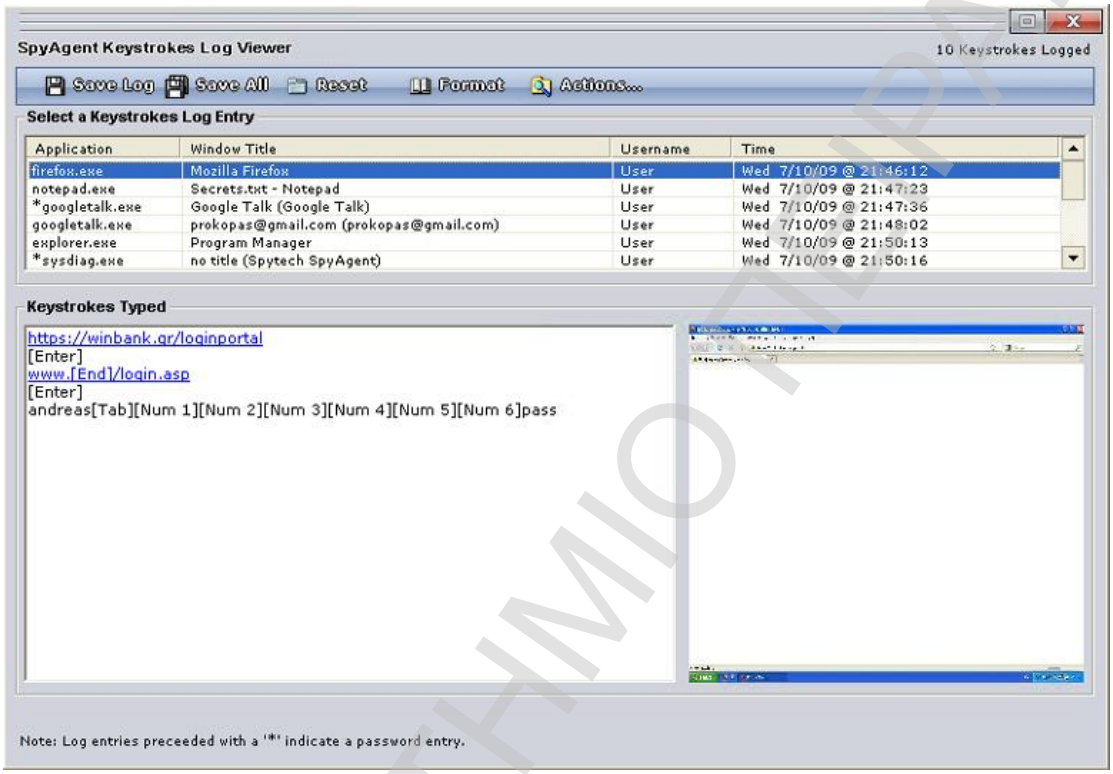
Πρώτα, μπορούμε να δούμε όλα τα προγράμματα που χρησιμοποιήσαμε και για πόση ώρα σε ένα συγκεντρωτικό report.



Εικόνα 4-18: Report για χρήση εφαρμογών

Βλέπουμε ότι μέσα σε αυτά έχουν καταγραφεί ο Firefox που χρησιμοποιήσαμε για να πλοηγηθούμε στο Internet και να μπούμε στο e-mail account μας και στο e-banking account μας καθώς και η χρήση του googletalk.

Πηγαίνοντας στην επιλογή για εμφάνιση των keystrokes που καταγράφηκαν εκεί βλέπουμε μια λίστα πάλι με τις εφαρμογές αλλά με περισσότερα στοιχεία: τις πληκτρολογήσεις που κάναμε μέσα σε κάθε εφαρμογή.

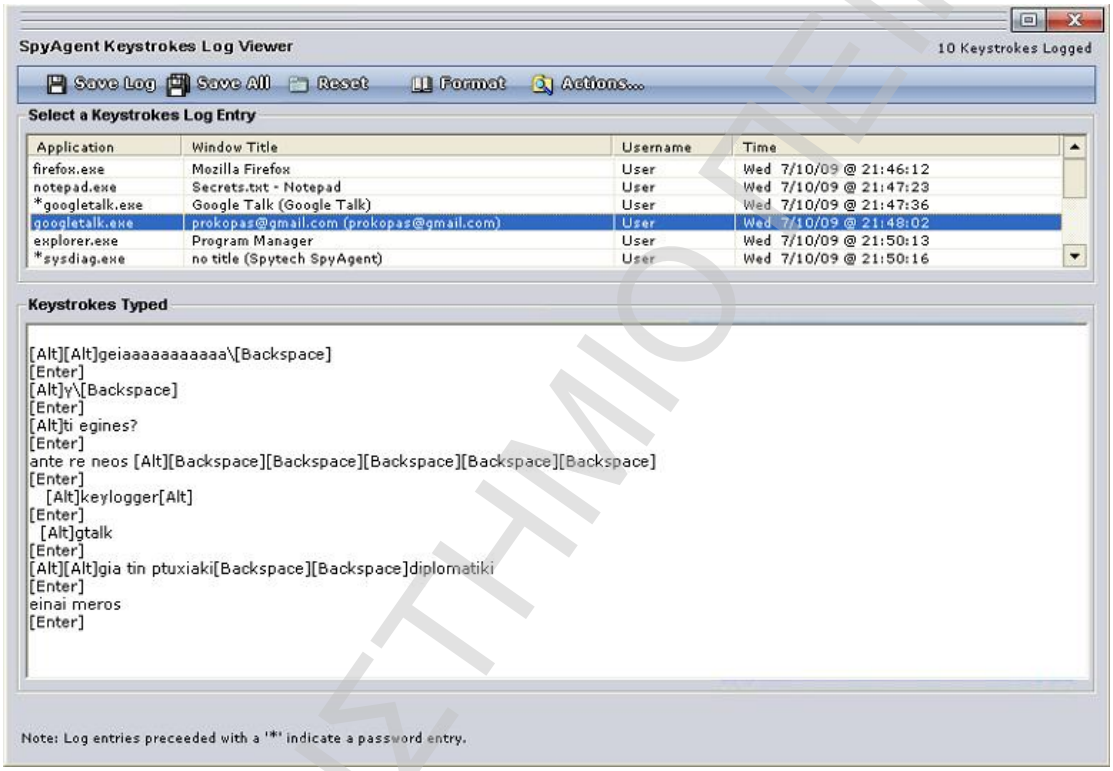


Εικόνα 4-19: Report για καταγραμμένα keystrokes

Επιλέγοντας λοιπόν πάνω στον “Firefox” βλέπουμε από κάτω στα δυο παραθυράκια τις πληκτρολογήσεις μας και ένα Screenshot που έγινε capture εκείνη τη στιγμή. Το Link λοιπόν που επισκεφθήκαμε είναι το https://www.winbank.gr/loginPortal/login.asp και σαν χρήστη βάλαμε τα “andreas” και σαν κωδικό το “1234pass”! Και μάλιστα κατέγραψε ότι χρησιμοποιήσαμε τους αριθμούς από το αριθμητικό πληκτρολόγιο κιόλας… Έτσι λοιπόν τόσο απλά υποκλέψαμε τους κωδικούς του χρήστη για τον τραπεζικό του λογαριασμό! Σε 5 λεπτά μπορούμε να μπούμε και να κάνουμε μια μεταφορά σε ένα δικό μας, όλο το διαθέσιμο υπόλοιπο του λογαριασμού! Ο λόγος, λοιπόν, που είναι σημαντικό ο Key logger να είναι αόρατος είναι για να μην υποπτευθεί τίποτα ο χρήστης κατά τη διάρκεια της υποκλοπής και αλλάξει μετέπειτα τον κωδικό, πριν πάρει ο επιτιθέμενος το log file. Επίσης παρατηρούμε ότι σε όλες τις καταγραφές χαρακτήρων καταγράφονται και οι μη-εκτυπώσιμοι χαρακτήρες (end, backspace κτλ) ώστε να έχουμε μια πλήρη αναφορά του τι έγραψε ο χρήστης ακόμα και αν το έσβησε (backspace) και σε ποιο σημείο του κειμένου (end). Δεν καταγράφονται όμως τα κλικ του ποντικιού, κάτι που θα μπορούσε να χρησιμοποιηθεί από τον χρήστη, σαν κίνηση ασφαλείας κατά την συμπλήρωση του

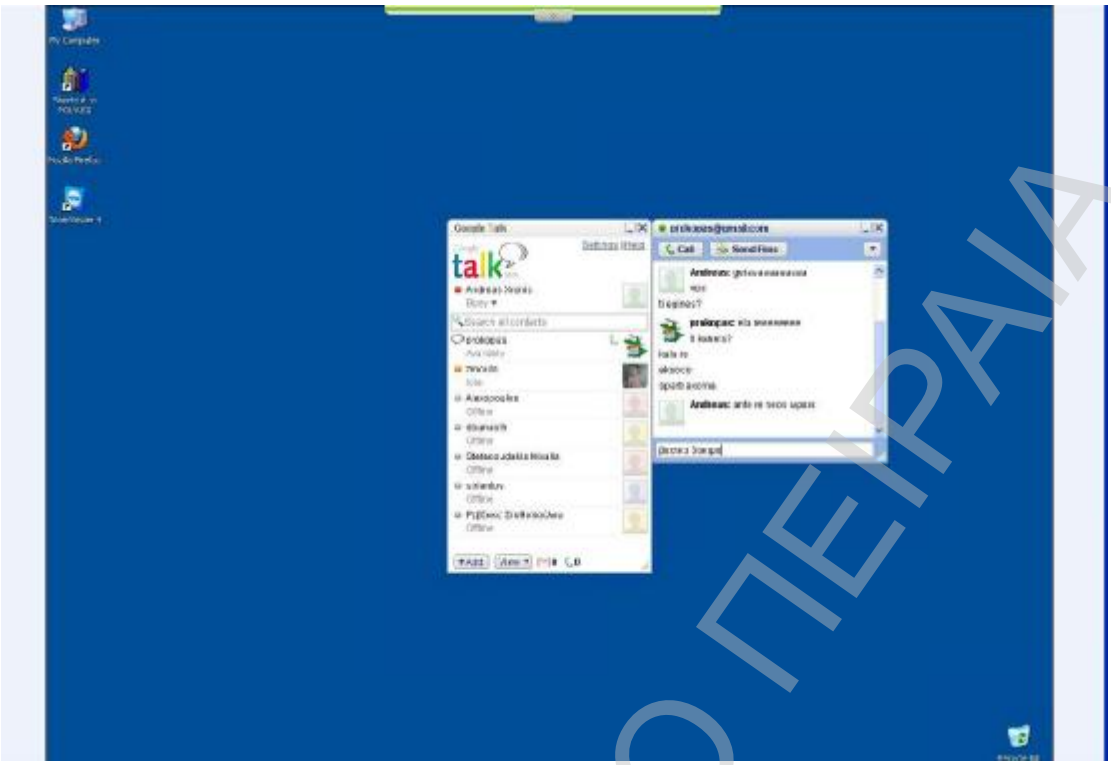
password, για να μπερδέψει τον υποκλοπέα. Για παράδειγμα αν ο χρήστης αντί 1234pass έγραφε 12pa56734ss[Backspace][Backspace][Backspace] μετακινώντας το ποντίκι κατά την εγγραφή ο υποκλοπέας θα έπαιρνε το παραπάνω αντί για το σωστό και δε θα ήξερε ούτε τη σειρά των χαρακτήρων, ούτε ποιοι σβήστηκαν.

Αφού έχουμε αδειάσει τον τραπεζικό λογαριασμό του χρήστη ίσως θα μπορούσαμε να υποκλέψουμε και κάποια προσωπικά του δεδομένα ώστε να τον καταστρέψουμε ολοσχερώς. Επιλέγουμε από την ίδια λίστα την εφαρμογή googletalk. Βλέπουμε ότι η εφαρμογή για να σε «βοηθήσει» στην υποκλοπή, μαρκάρει με ένα αστεράκι τις εφαρμογές που χρειάζονται login password και έχει καταγραφεί. Ας δούμε, όμως, τι συζήταγε ο χρήστης μας λοιπόν με τους φίλους του.



Εικόνα 4-20: Report SpyAgent συνομιλίας στο googletalk

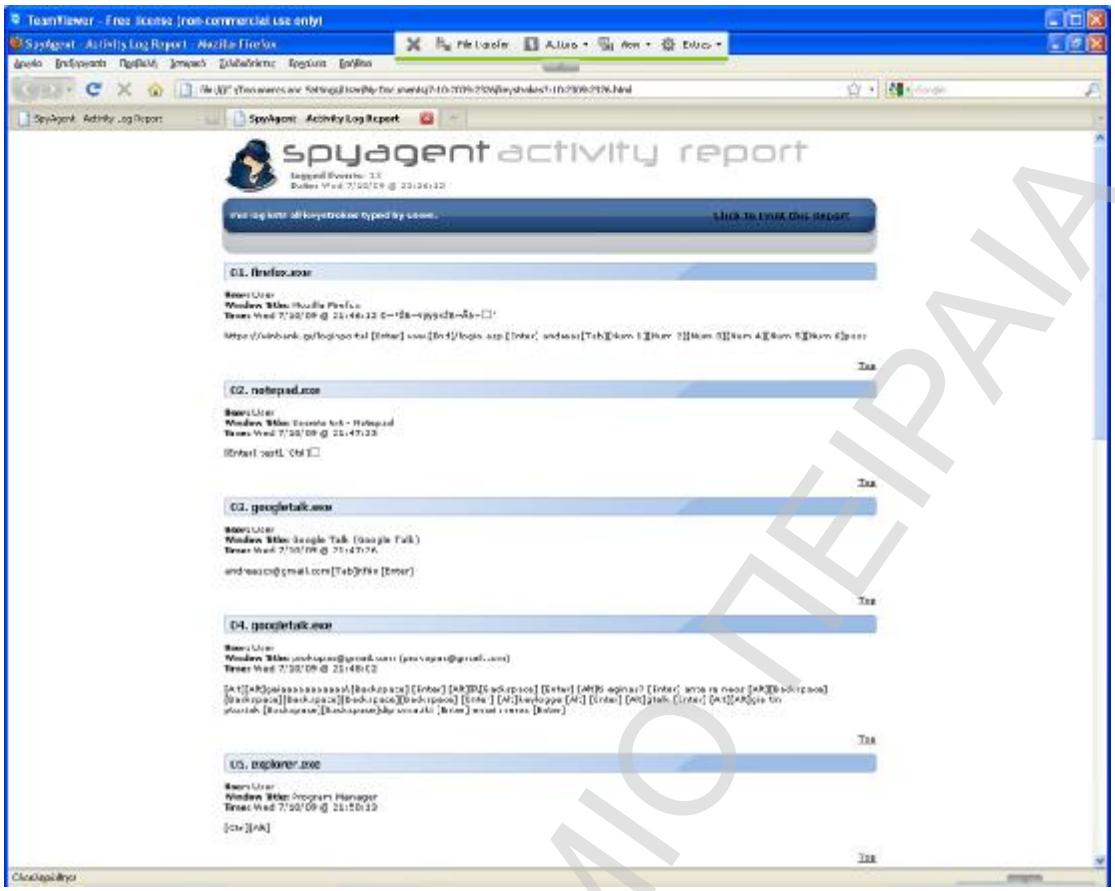
Όπως βλέπουμε έχει καταγραφεί το e-mail του χρήστη με τον οποίο συνομιλεί και όλη η κουβέντα τους! Για να βοηθηθούμε βέβαια, όπως είπαμε η εφαρμογή παίρνει κάθε χ δευτερόλεπτα (30 έχουμε ορίσει στη δοκιμή μας) screenshot. Ας δούμε ένα από τη συγκεκριμένη συνομιλία.



Εικόνα 4-21: Αυτοματοποιημένο screenshot SpyAgent

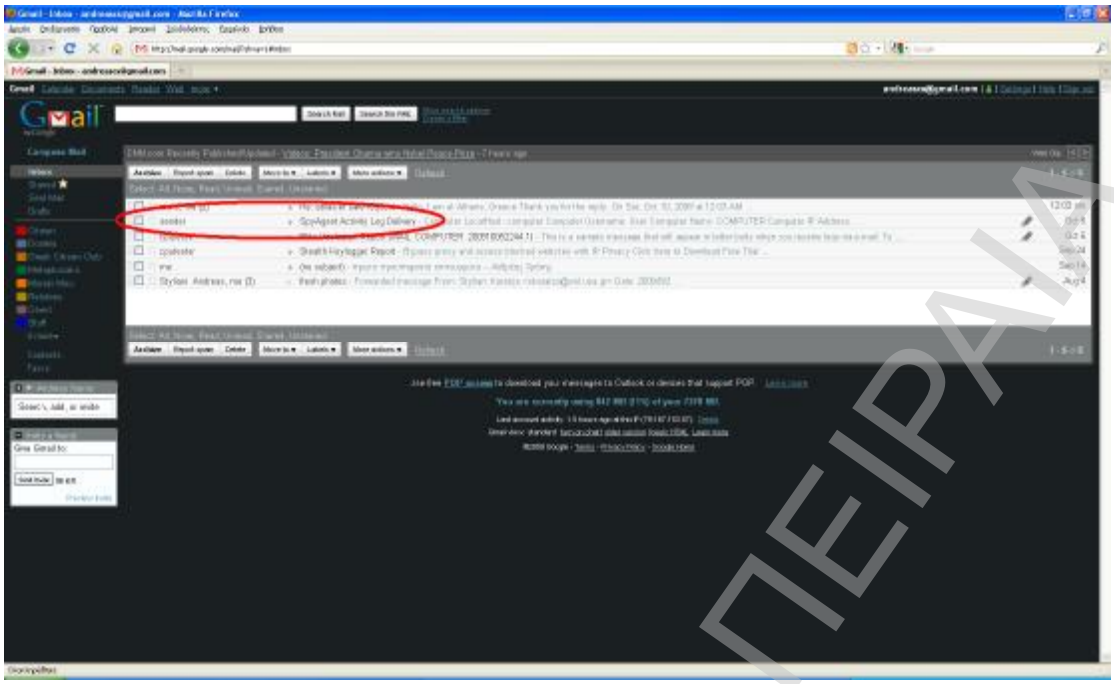
Τα screenshot είναι σε πολύ καλή ποιότητα και θα μπορούσαμε να διαβάσουμε και από εδώ τη συνομιλία για να μη μπερδευόμαστε με τους μη-εκτυπώσιμους χαρακτήρες. Παρατηρούμε, όμως, σε σύγκριση με την καταγραφή κάποιες ελλείψεις. Στην εφαρμογή δεν έχουν καταγραφεί καθόλου οι λέξεις που γράφτηκαν με ελληνικούς χαρακτήρες. Σημαντική παράληψη λοιπόν, για τους υποκλοπείς της χώρας μας, ή χρήσιμο μέτρο ασφαλείας για τους χρήστες.

Ένα ακόμα ωραίο χαρακτηριστικό της εφαρμογής είναι η παραγωγή ενός ωραίου, ευκολοδιάβαστου report σε html.

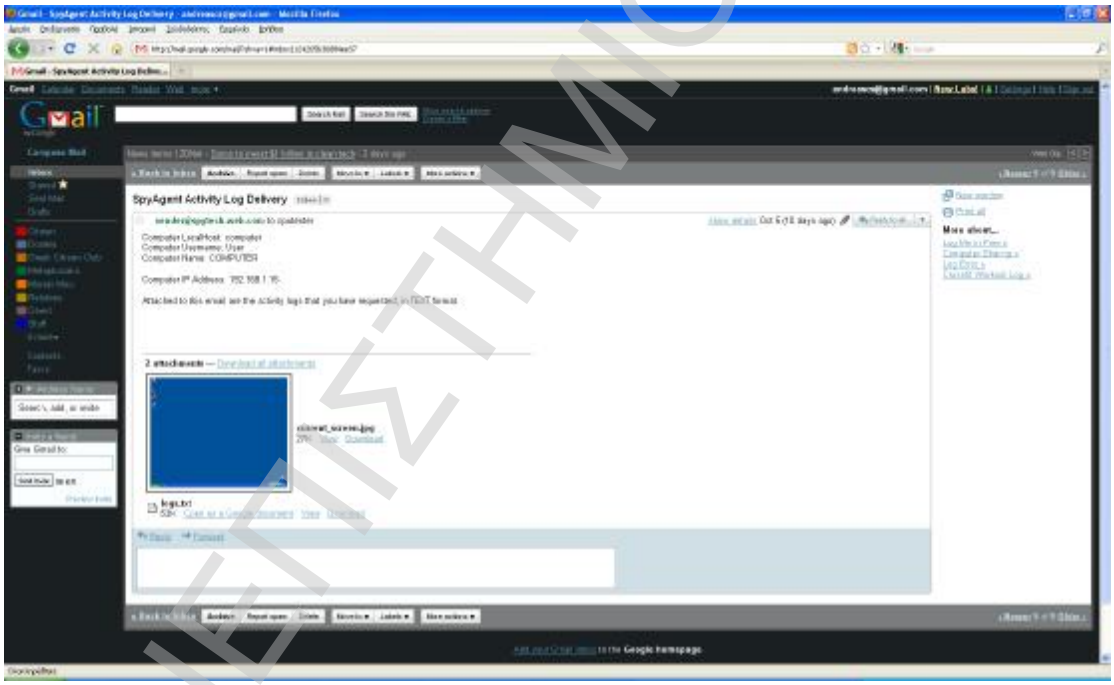


Εικόνα 4-22: Συνολικό report SpyAgent

Όπως είπαμε η εφαρμογή στέλνει τα reports στο e-mail μας όποτε όλα αυτά που είδαμε τοπικά θα τα δούμε στο e-mail μας. Μπορούμε να επιλέξουμε αν θέλουμε να μας στέλνονται και τα screenshots ή όχι. Ανοίγοντας το e-mail μας βλέπουμε το αυτόματο e-mail από την εφαρμογή.



Εικόνα 4-23: Επιβεβαίωση αυτοματοποιημένου e-mail



Εικόνα 4-24: Εμφάνιση αυτοματοποιημένου e-mail

Συμπεράσματα

Σε γενικές γραμμές η εφαρμογή μας ικανοποίησε. Ας δούμε όμως πιο συγκεκριμένα τα θετικά:

+ Ο αρχικός wizard για ρύθμιση της εφαρμογής ήταν πολύ χρήσιμος για έναν αρχάριο χρήστη για να γίνουν οι βασικές ρυθμίσεις

+ Όσον αφορά τις επιλογές της καταγραφής, σίγουρα είχε πάρα πολλές, για να καλύψει κάθε πιθανή περίπτωση.

+ Η «κατηγοριοποίηση» των καταγραφών είναι εύστοχη.

+ Η αποστολή των log files μέσω e-mail ήταν επιτυχής, παρακάμπτοντας firewall και σημεία ασφαλείας.

+ Η απόκρυψη της εφαρμογής από τον χρήστη ήταν επιτυχής. Ούτε μενού, ούτε στοιχεία εγκατάστασης, πραγματικά αόρατη.

+ Η καταγραφή σε γενικές γραμμές ήταν επιτυχής. Δεν «ξέφευγε» καμία κίνηση από την εφαρμογή και τα screenshots συμπλήρωναν το καλό αποτέλεσμα.

+ Τα συνολικά reports σε μορφή html είναι αρκετά καλά.

Η εφαρμογή όμως είχε και αρκετά αρνητικά:

- Κατά την εκκίνηση της καταγραφής η «λύση» του προβλήματος για να μην ανιχνεύεται από το antivirus ήταν να απενεργοποιεί αυτό καθώς και τον task manager. Σε περίπτωση ενεργοποίησης του antivirus ο key logger ανιχνευόταν από αυτό. Πολύ ανεπιτυχής τρόπος απόκρυψης από το σύστημα λοιπόν.

- Κατά την καταγραφή δεν ανιχνεύονταν και δεν καταγράφονταν οι ελληνικοί χαρακτήρες. Δεν υπήρχε καν ένδειξη πληκτρολόγησης εκείνη τη στιγμή. Σαν να προσπαθούσε το πρόγραμμα να κρύψει την αδυναμία του.

- Όσον αφορά τις επιλογές της καταγραφής, σίγουρα είχε πάρα πολλές, άλλα ίσως ήταν υπερβολικά πολλές.

- Η «κατηγοριοποίηση» των καταγραφών ήταν μεν εύστοχη αλλά η εφαρμογή είχε πολλά μενού με αποτέλεσμα να χάνεσαι λίγο κατά τη χρήση της.

- Δεν καταγράφονταν διαδικασίες στο login, όπως η είσοδος κωδικού χρήστη. Αρκετά σημαντική παράληψη.

- Δεν καταγράφονταν τα κλικ του ποντικιού.

2) Stealth Key logger

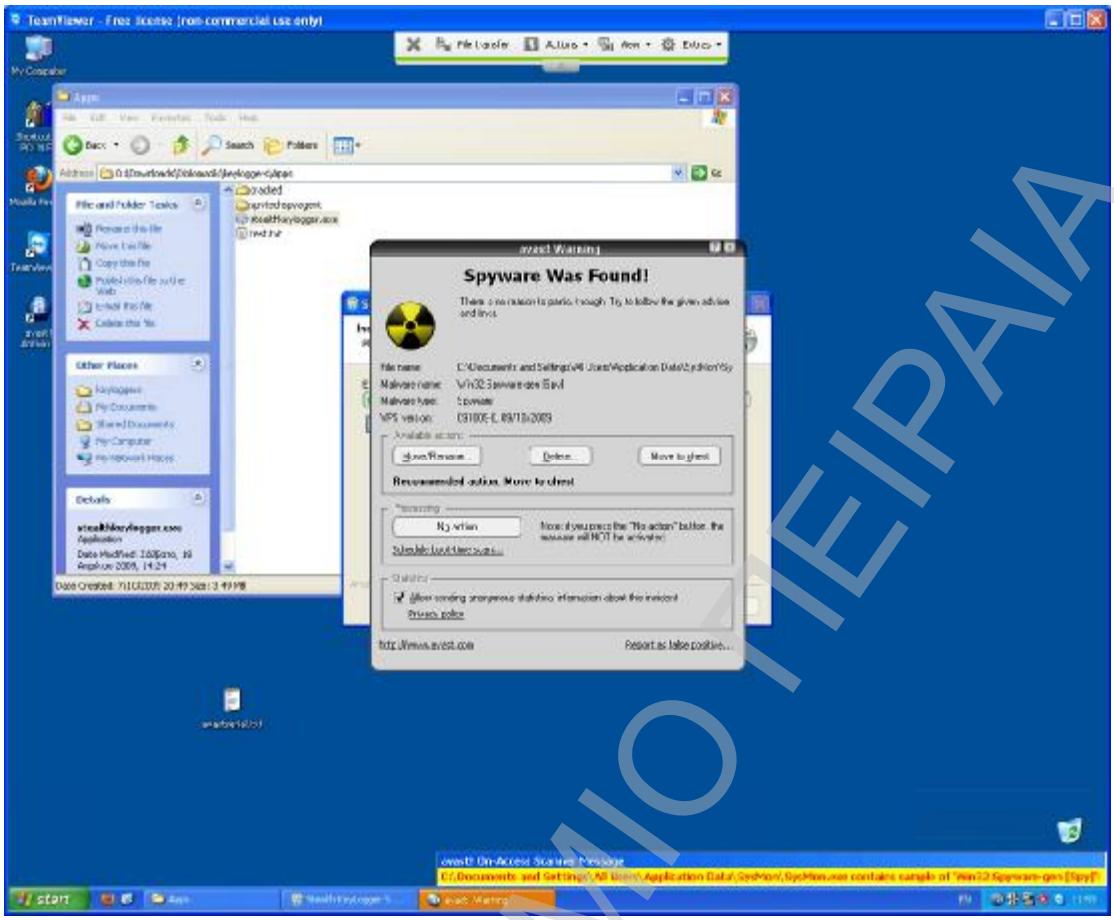
Παρουσίαση – Εγκατάσταση – Αρχικές ρυθμίσεις

Ο δεύτερος Key logger που θα δοκιμάσουμε είναι ο Stealth και είναι και αυτός μέσα στο στις 5 πρώτες επιλογές των λιστών με τις top 10 που έχουμε βρει. Είναι προϊόν της AmplusNet και υπόσχεται πολλές δυνατότητες σε χαμηλή τιμή. Η έκδοση που δοκιμάσαμε είναι η v.5.0 και το κόστος της εφαρμογής ήταν $40.

Ξεκινάμε, λοιπόν, με την εγκατάσταση της εφαρμογής σε «καθαρή εγκατάσταση» όπως αναλύσαμε και νωρίτερα.

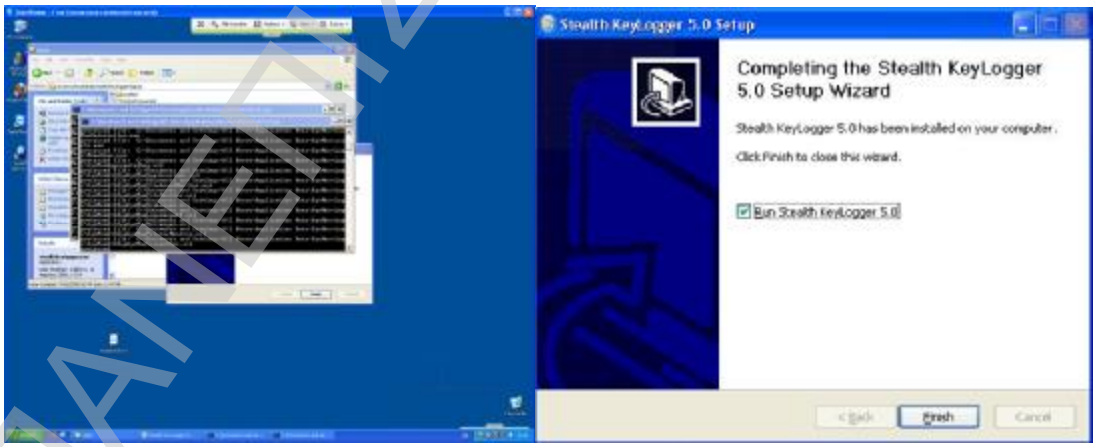
Εικόνα 4-25: Εκκίνηση εγκατάστασης Stealth

Όπως και στις άλλες περιπτώσεις το antivirus ανίχνευσε το κακόβουλο λογισμικό και ενεργοποιήθηκε.



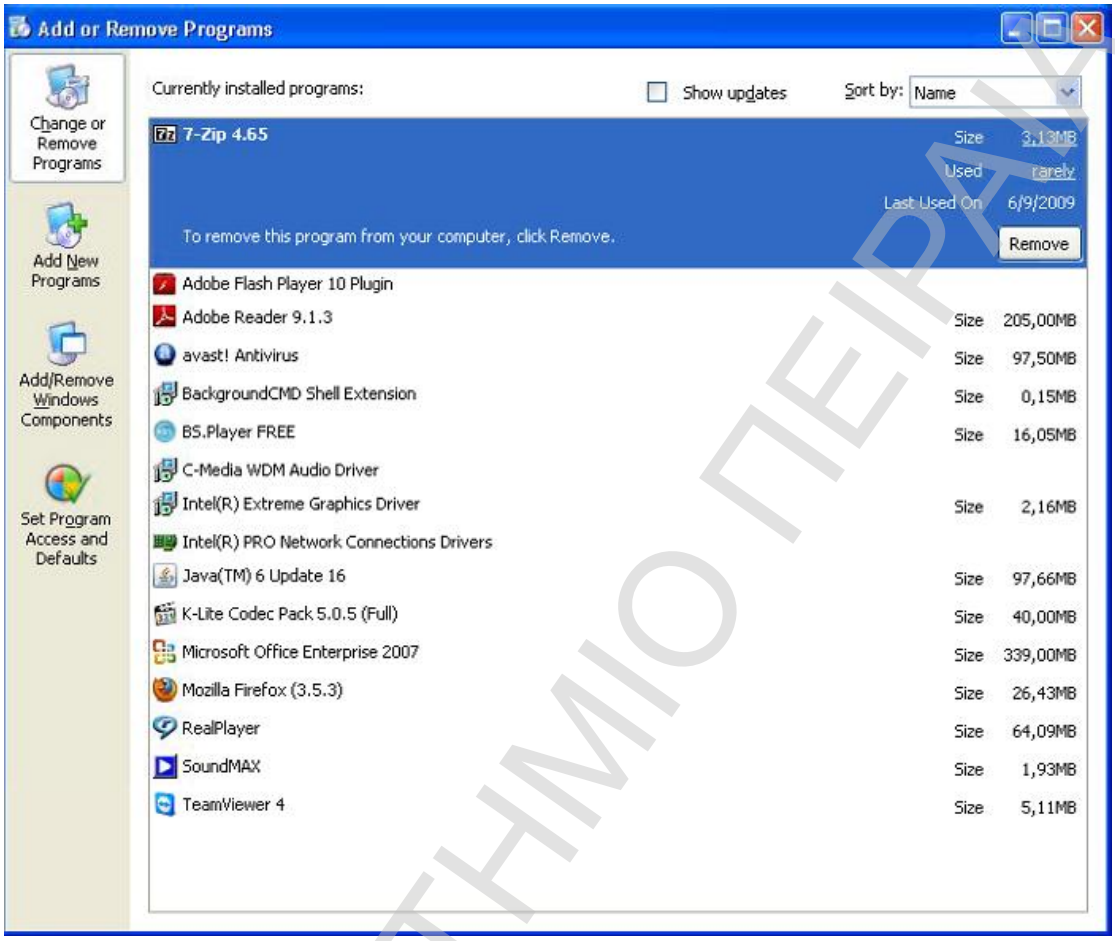
Εικόνα 4-26: Ενεργοποίηση anti-virus

Μετά την απενεργοποίηση του και την επανεκκίνηση της εγκατάστασης αυτή συνεχίζεται και ολοκληρώνεται



Εικόνα 4-27: Ολοκλήρωση εγκατάστασης

Όπως και στον spyagent, μετά την εγκατάσταση βλέπουμε ότι το πρόγραμμα δεν έχει αφήσει εμφανή σημεία εγκατάστασης, ούτε στο start menu, ούτε σε φακέλους, ούτε στην προσθαφαίρεση προγραμμάτων.



Εικόνα 4-28: Εμφάνιση παραθύρου προσθαφαίρεσης προγραμμάτων των windows

Κατά την εκκίνηση της εφαρμογής, είτε τώρα μετά την εγκατάσταση, είτε αργότερα μέσω του hotkey εμφανίζεται παράθυρο για την εισαγωγή του κωδικού πρόσβασης στο κυρίως παράθυρο του Key logger.

Εικόνα 4-29: Παράθυρο εισαγωγής στον Stealth

Ο default κωδικός για την πρώτη φορά είναι «user». Έπειτα ενημερώνεσαι και ποιο είναι το default hotkey (Ctrl + Shift + Alt + S) για να ανοίξεις την εφαρμογή.

Εικόνα 4-30: Εμφάνιση βασικών στοιχείων στην εκκίνηση του Stealth

Ανοίγοντας το αρχικό παράθυρο του Stealth βλέπουμε μια πολύ πιο διακριτική εφαρμογή με λιγότερα μενού. Στο Status βλέπουμε σε τι κατάσταση λειτουργίας είναι τώρα ο key logger. Επίσης, και στο status αλλά και στα δυο επόμενα μενού βλέπουμε τις επιλογές για reports των καταγραφών. Είτε τα current, είτε ημερήσια, είτε γενικά, είτε δημιουργία custom reports. Άποψη μας ότι είναι λίγο υπερβολικό τόσα διαφορετικά μενού για το ίδιο θέμα για αυτό τα παρουσιάζουμε όλα μαζί.

Εικόνα 4-31: Μενού για reports στον Stealth

Έπειτα βλέπουμε ένα επιπλέον μενού για screenshots.

Εικόνα 4-32: Μενού για screenshots στον Stealth

Πηγαίνοντας στα settings βλέπουμε μερικές απλές ρυθμίσεις για τον Key logger: Ρύθμιση hot key, μερικές απλές ρυθμίσεις για logging και για screenshots .

Εικόνα 4-33: Ρυθμίσεις στον Stealth

Και στο τελευταίο tab ρυθμίσεις για τα reports και την αποστολή σε e-mail.

Εικόνα 4-34: Μενού για ρύθμιση αποστολής reports στον Stealth

Δοκιμή

Τελειώνοντας οι ρυθμίσεις, κάναμε τα βήματα του πειράματος που αφορούν την καταγραφή όπως και στον προηγούμενο key logger. Ας δούμε τι κατέγραψε ο Stealth key logger. Πρώτα θα δούμε ένα γενικό report με τις εφαρμογές που καταγράφηκαν.

3.	10:53:03	User	Firefox	winbank internet
4.	10:52:52	User	Firefox	The page cannot be found
5.	10:52:36	User	Firefox	Error
6.	10:52:09	User	Firefox	winbank internet
7.	10:51:35	User	Firefox	winbank internet
8.	10:51:31	User	Firefox	winbank internet
9.	10:50:39	User	Firefox	winbank internet
10.	10:50:30	User	Firefox	Gmail: Çëåêôñïíéêû ôá÷ôäñîåßï áðü ôçí Google
11.	10:49:05	User	Firefox	Gmail: Çëåêôñïíéêû ôá÷ôäñîåßï áðü ôçí Google
12.	10:45:30	User	Firefox	winbank internet
13.	10:45:09	User	Firefox	winbank internet
14.	10:45:04	User	Firefox	winbank internet
15.	10:44:53	User	Firefox	Error
16.	10:44:43	User	Firefox	Ðñûâëçìá öüñôùóçò óåëßäáò

Find Keyword
OK

Εικόνα 4-35: Reports για χρήση καταγραμμένων προγραμμάτων στον Stealth

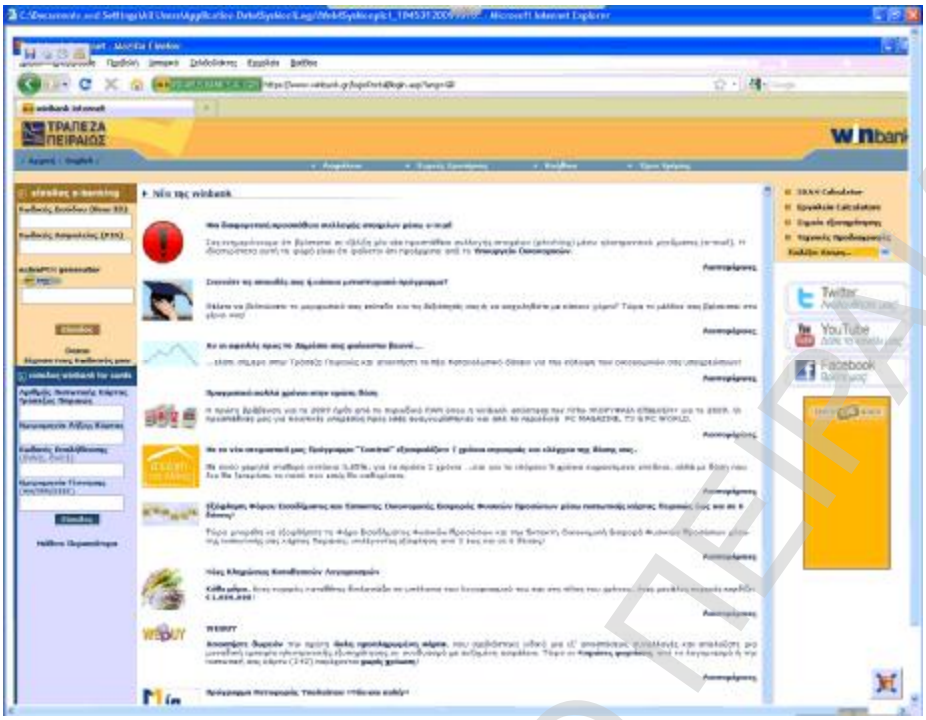
Βλέπουμε λοιπόν ότι καταγράφηκε η χρήση του Firefox και η επίσκεψη μας στο e-banking μας και στο webmail μας. Ας πάμε να δούμε όμως και την καταγραφή των πληκτρολογήσεων για να δούμε αν υποκλέψαμε τους κωδικούς.

Εικόνα 4-36: Reports των keystrokes στον Stealth

Το report που εμφανίζει η εφαρμογή δεν ενθουσιάζει εμφανισιακά και δεν είναι ευανάγνωστο. Παρόλα αυτά η καταγραφή πέτυχε.

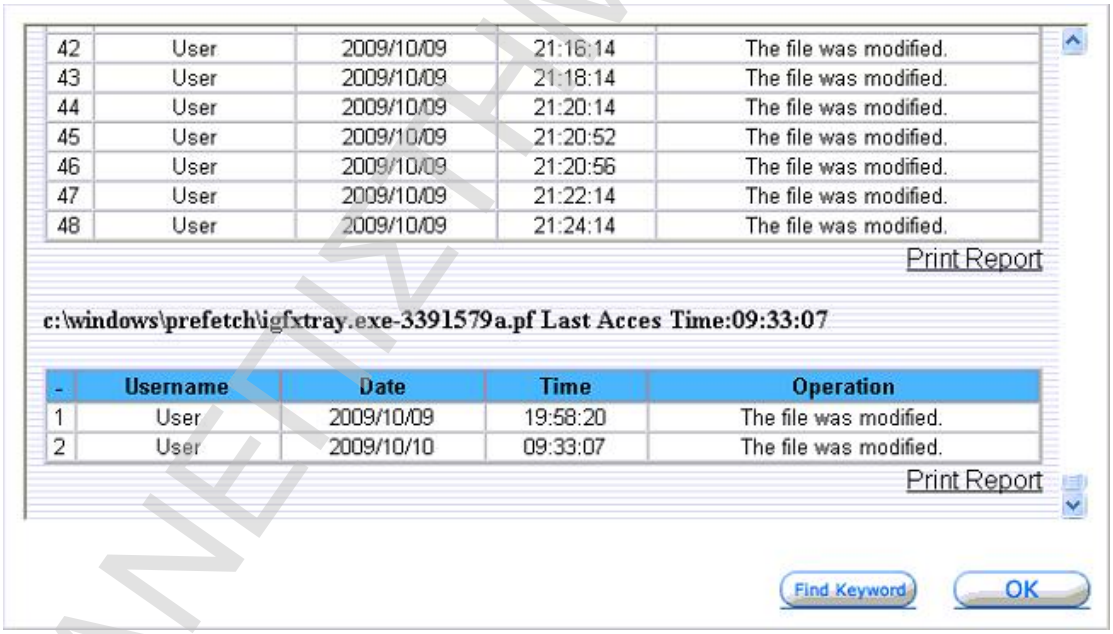
Όσον αφορά το e-banking ο key logger κατέγραψε το link που επισκεφθήκαμε, το όνομα χρήστη και έπειτα και τον κωδικό. Προσπαθήσαμε να τον μπερδέψουμε λίγο αλλάζοντας παράθυρα και εισάγοντας τον κωδικό αργότερα αλλά οι κινήσεις που κάναμε ήταν λίγες τελικά για να μπερδευτεί ο επιτιθέμενος και οι καταγραφές είναι κατηγοριοποιημένες ανά εφαρμογή αν και δεν είναι τόσο εμφανές από την αρχή. Πάντως, έτσι, πολύ απλά, πήραμε και τους κωδικούς του e-banking του χρήστη. Επίσης παρακάτω ένα screenshot που τραβήχτηκε την ώρα της επίσκεψης στο e-banking και θα βοηθούσε τον επιτιθέμενο περισσότερο.

Προφανώς παρόμοια αποτελέσματα είχε και η προσπάθεια καταγραφής των κωδικών του e-mail. Το όνομα χρήστη και ο κωδικός καταγράφηκαν επιτυχώς και θα τα βρούμε μέσα στα καταγεγραμμένα keystrokes.



Εικόνα 4-37: Screenshots αυτόματα δημιουργημένα από τον Stealth

Όσον αφορά τη γενική χρήση και την επεξεργασία ενός αρχείου δυστυχώς το μόνο διαθέσιμο report είναι το παρακάτω:



42	User	2009/10/09	21:16:14	The file was modified.
43	User	2009/10/09	21:18:14	The file was modified.
44	User	2009/10/09	21:20:14	The file was modified.
45	User	2009/10/09	21:20:52	The file was modified.
46	User	2009/10/09	21:20:56	The file was modified.
47	User	2009/10/09	21:22:14	The file was modified.
48	User	2009/10/09	21:24:14	The file was modified.

Print Report

c:\windows\prefetch\igfxtray.exe-3391579a.pf Last Acces Time:09:33:07

-	Username	Date	Time	Operation
1	User	2009/10/09	19:58:20	The file was modified.
2	User	2009/10/10	09:33:07	The file was modified.

Print Report

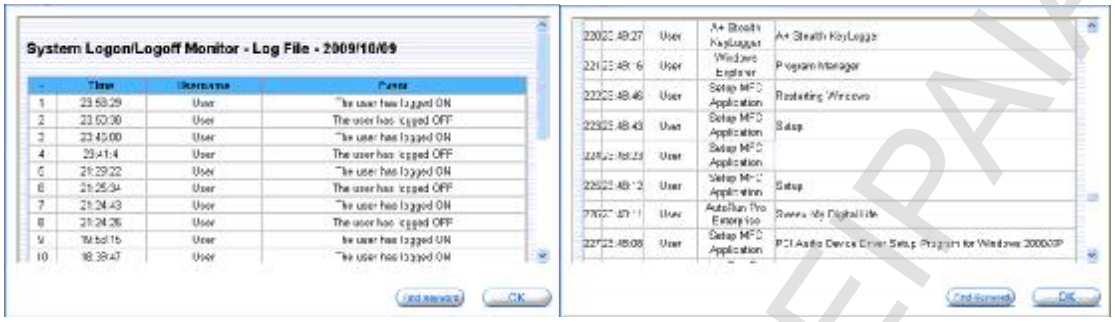
Find Keyword OK

Εικόνα 4-38: Reports για επεξεργασία αρχείων στον Stealth

Εδώ αναφέρεται ποια αρχεία άλλαξαν και τι ώρα από τον χρήστη. Έτσι μόνο σε συνδυασμό με το report των keystrokes μπορείς να δεις τι αλλαγές έγιναν. Επιπλέον στο παραπάνω report αναφέρονται και όλα τα αρχεία συστήματος που τροποποιήθηκαν χωρίς βέβαια ο ίδιος ο χρήστης να έχει κάνει κάτι με αποτέλεσμα η

λίστα να είναι τεράστια. Περισσότερο χρήσιμη λειτουργία σε recovery tool παρά σε key logger.

Ακόμα μερικά reports παρακάτω που δείχνουν τις εισόδους-εξόδους των χρηστών στο σύστημα και καταγραφή λειτουργίας εφαρμογών.

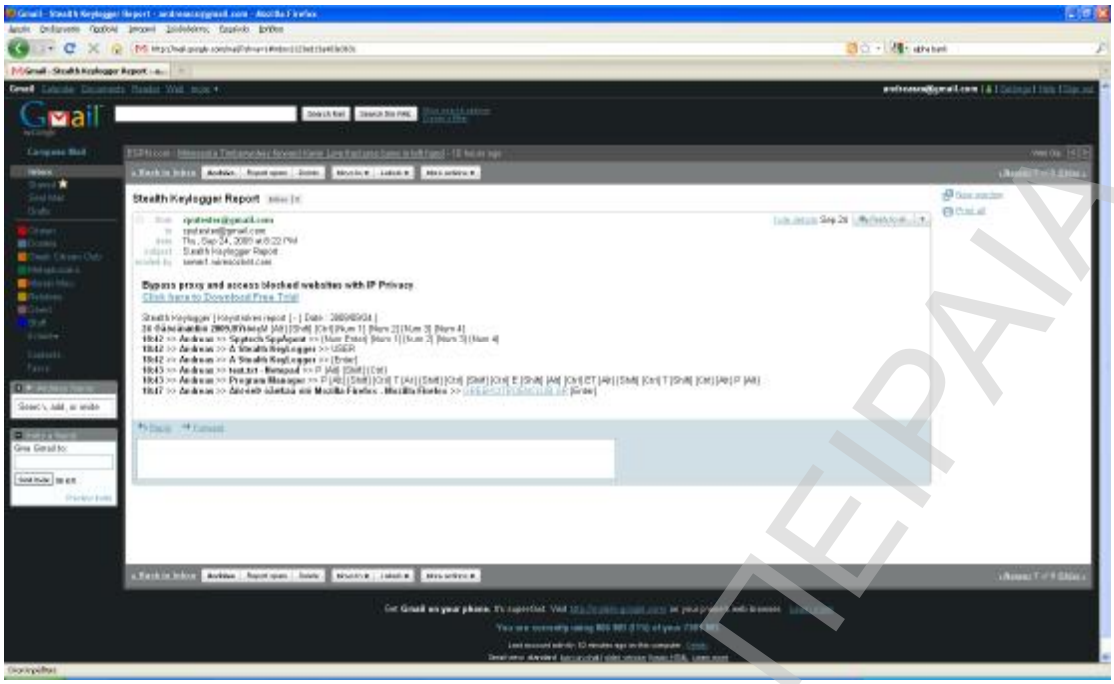


Εικόνα 4-39: Reports για logon-logoff στον Stealth

Τι έγινε όμως με τη συνομιλία στο googletalk που κάναμε;

Δυστυχώς, στο μενού των reports “Chat Monitor”, ο stealth key logger δεν είχε καταγράψει τίποτα. Μετά από μερικές δοκιμές ακόμα διαπιστώσαμε ότι η λειτουργία της καταγραφής του googletalk στις εφαρμογές που «έτρεξαν» γινόταν κανονικά, όπως και στα keystrokes όπως μπορούμε να διακρίνουμε ανάμεσα στις «συστάδες» χαρακτήρων, απλώς ο stealth δεν αναγνώρισε τον googletalk σαν IM και έτσι η συνομιλία δεν καταγράφηκε πουθενά σαν συνομιλία ολοκληρωμένη, δηλαδή να υπάρχει και το κείμενο του συνομιλητή. Θα μπορούσαμε να δούμε βέβαια στα χιλιάδες καταγεγραμμένα keystrokes αυτά που έγραφε ο χρήστης μας και όχι ο συνομιλητής και να τα συνδυάσουμε και με μερικά κομμάτια που φαίνονται στα screenshots αλλά αυτό προφανώς είναι μια χρονοβόρα διαδικασία.

Όσον αφορά την αποστολή των logs σε e-mail ήταν επιτυχής αν και όλα τα reports που παρήγαγε η εφαρμογή ήταν μέσα στο κείμενο του e-mail χωρίς να υπήρχε κάποια ιδιαίτερη κατηγοριοποίηση.



Εικόνα 4-40: Εμφάνιση αυτοματοποιημένου e-mail από τον Stealth

Συμπεράσματα

+ Η εφαρμογή ήταν σχετικά απλή αν και αποδοτική. Ας δούμε τα θετικά της:

+ Απλή η ρύθμιση για τον αρχάριο χρήστη χωρίς πολλά μενού και προσαρμογές.

+ Η αποστολή e-mail ήταν επιτυχής.

+ Χαμηλό κόστος

Και τα αρνητικά της:

- Πολύ απλό γραφικό περιβάλλον, σε σημείο που φαίνεται χαζό στον πιο εξειδικευμένο χρήστη.

- Ενώ, σε γενικές γραμμές, ήταν λίγες οι επιλογές των μενού τα λίγα αυτά μενού που υπήρχαν ήταν σχεδόν όλα για το ίδια πράγμα. Πολλά διαφορετικά μενού, όλα για reports ενώ ένα από όλα θα ήταν υπεραρκετό.

- Πολύ λίγες επιλογές όσον αφορά τις δυνατότητες καταγραφής. Δεν υπήρχε υποστήριξη για επιλογή εφαρμογών καταγραφής, ωρών, χρηστών και γενικά υπήρχαν πολλές παραλήψεις σε αυτό.

- Δεν αναγνωρίζεται το googletalk σαν IM οπότε και δεν καταγράφεται η συνομιλία

- Δεν υπήρχε ούτε εδώ υποστήριξη ελληνικών.

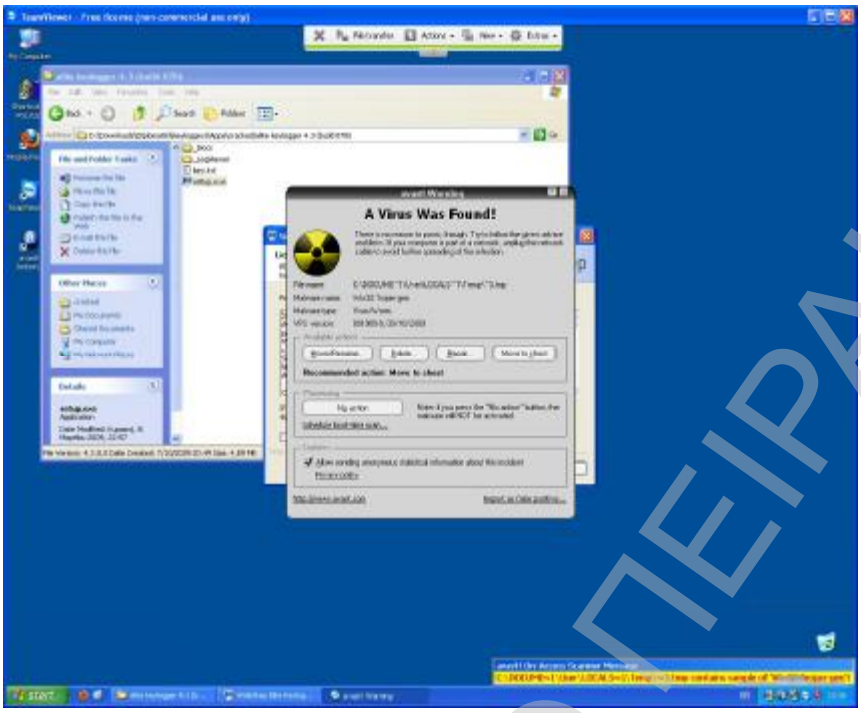
- Δεν υπήρχε δυνατότητα καταγραφής κατά το login.
- Δεν γινόταν καταγραφή των κλικ του ποντικιού.
- Η περιοδικότητα των screenshots είχε χρονικούς περιορισμούς και δεν υπήρχε η δυνατότητα να είναι αρκετά συχνή.
- Ενώ υπήρχαν τόσα πολλά μενού για τα reports, αυτά, εμφανισιακά, αντί να διευκολύνουν τον αναγνώστη τους τον ταλαιπωρούσαν. Αδιανόητη γραφική εργασία με διπλά >> αντί για στήλες και διάσπαρτες πληκτρολογήσεις κτλ

3) Elite Key logger

Παρουσίαση – Εγκατάσταση – Αρχικές ρυθμίσεις

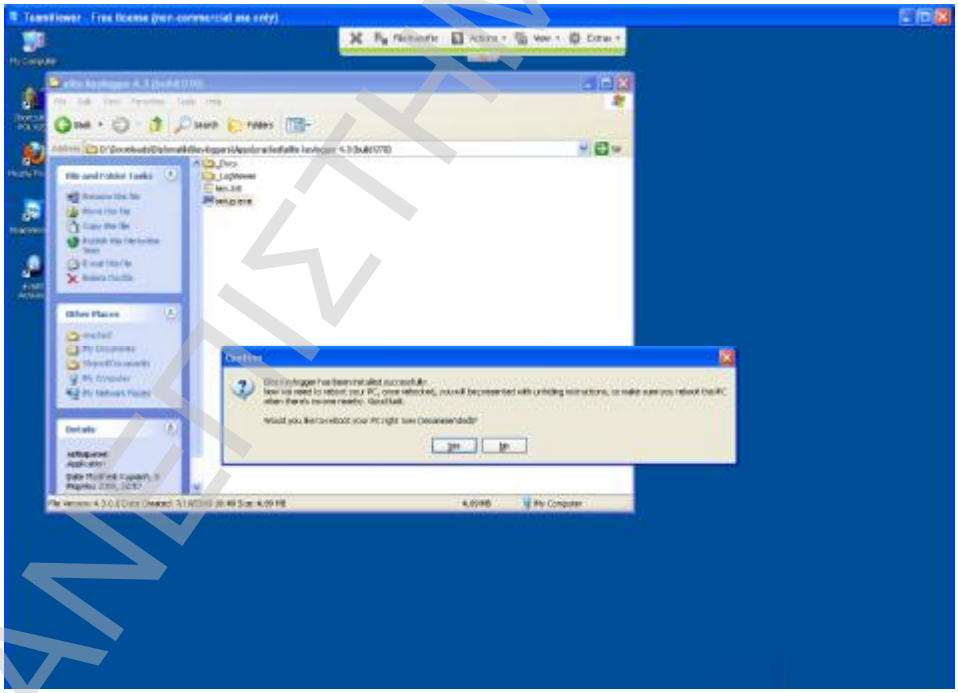
Έχοντας ανάμεικτες εντυπώσεις από τους 2 προηγούμενους Key loggers συνεχίζουμε στον τρίτο. Ο Elite key logger, κάθε άλλο παρά elite, ένα προϊόν της WideStep με κόστος $70. Η έκδοση που δοκιμάσαμε ήταν η v.4.3.

Αφού ξεκινάμε πάλι με καθαρή εγκατάσταση του λειτουργικού μας, κάνουμε την εγκατάσταση του elite key logger. Αναμενόμενη ήταν η ενεργοποίηση του antivirus κατά την εγκατάσταση.



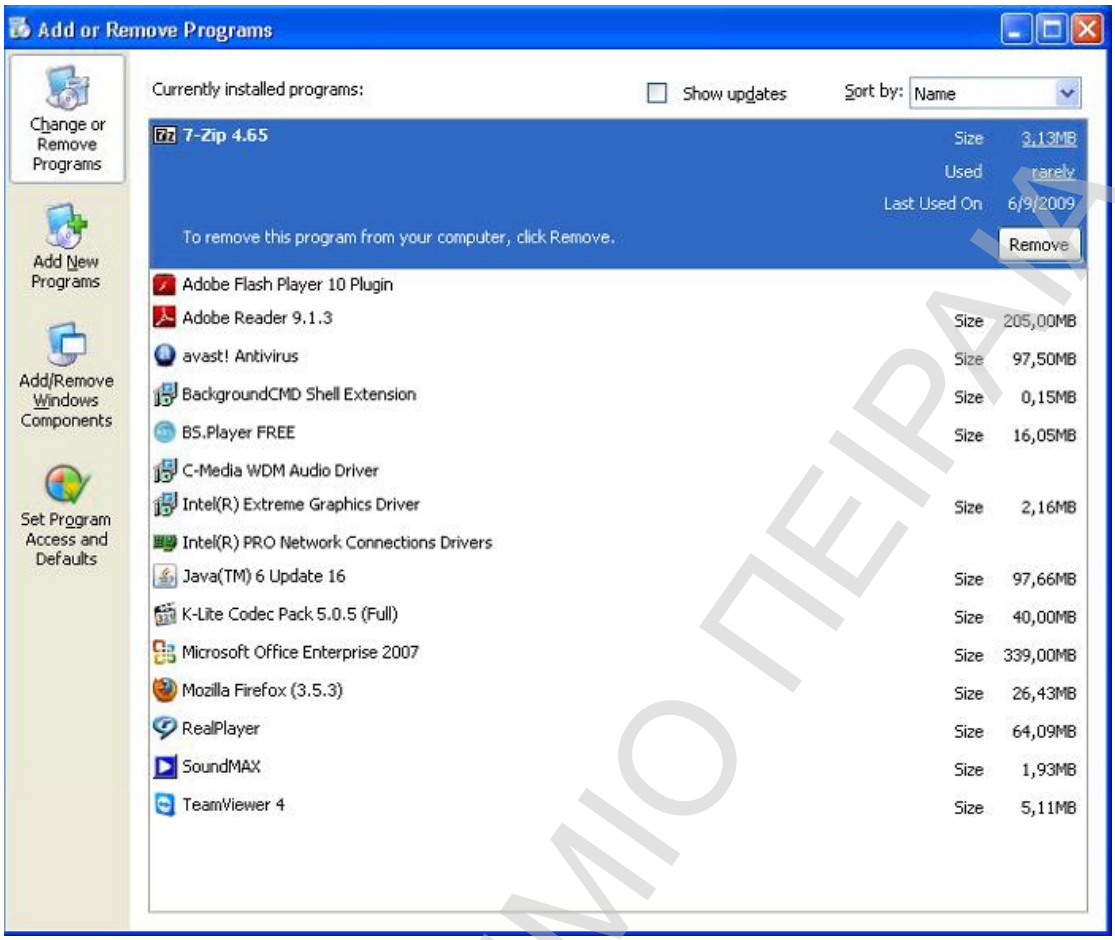
Εικόνα 4-41: Εκκίνηση εγκατάστασης στον Elite

Ένα πρόσθετο στοιχείο που δε μας άρεσε είναι ότι ο elite key logger χρειάζεται επανεκκίνηση για να εγκατασταθεί πλήρως.



Εικόνα 4-42: Απαίτηση restart στην εγκατάσταση του Elite

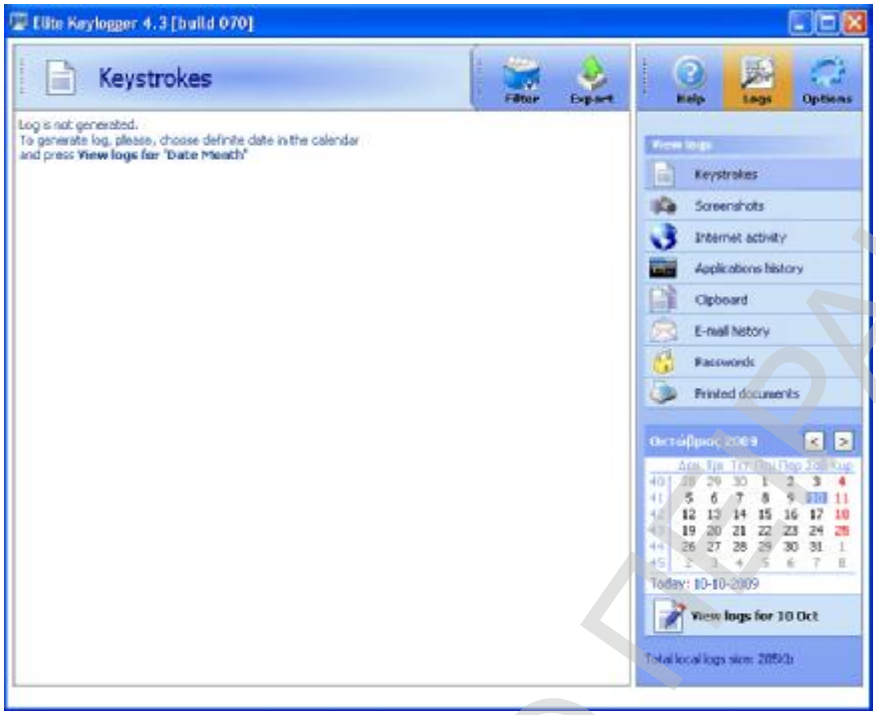
Όπως και στα άλλα δυο, μετά την εγκατάσταση βλέπουμε ότι το πρόγραμμα δεν έχει αφήσει εμφανή σημεία εγκατάστασης, ούτε στο start menu, ούτε σε φακέλους, ούτε στην προσθαφαίρεση προγραμμάτων.



Εικόνα 4-43: Εμφάνιση παραθύρου προσθαφαίρεσης προγραμμάτων των windows

Ένα διαφορετικό χαρακτηριστικό του elite με τους άλλους είναι ότι δε χρησιμοποιεί κάποιο hot key για να ανοίξει αλλά μόνο το password. Γράφοντας δηλαδή οπουδήποτε το password ανοίγει το παράθυρο του elite στο οποίο απαιτείται ξανά η εισαγωγή του κωδικού για επιβεβαίωση. Αυτό έχει και θετικά και αρνητικά. Γενικότερα, η ύπαρξη hot key σε προφυλάσσει από την αποκάλυψη του key logger σε ανύποπτο χρόνο γιατί οι συνδυασμοί που χρησιμοποιούνται είναι σχετικά απίθανο να πληκτρολογηθούν ενώ ένα password του χρήστη αν δεν είναι σωστά επιλεγμένο δεν θεωρείται απίθανο. Η δυνατότητα όμως αυτή σου δίνει την επιλογή να χρησιμοποιήσεις κάτι προσωπικό και ίσως ακόμα πιο απίθανο να πληκτρολογηθεί από ένα προεπιλεγμένο hot key.

Στο κεντρικό παράθυρο της εφαρμογής βλέπουμε το κουμπί των ρυθμίσεων καθώς και δυνατότητες εμφάνισης των logs και export αυτών.



Εικόνα 4-44: Αρχική οθόνη του Elite

Πηγαίνοντας στο παράθυρο των ρυθμίσεων βλέπουμε μερικές επιλογές καταγραφής και έναρξης της εφαρμογής, ρύθμισης του κωδικού, επιλογής χρηστών για καταγραφή καθώς και δυνατότητα επιλογής συγκεκριμένων εφαρμογών. Ένα παράθυρο με όλες τις ρυθμίσεις μαζί και όμως χωρίς να σε κουράζει.

Εικόνα 4-45: Οθόνη ρυθμίσεων στον Elite

Πηγαίνοντας να ρυθμίσουμε την αποστολή με e-mail μας ανοίγει ένα άλλο παράθυρο για να ρυθμίσουμε τις λεπτομέρειες.

Εικόνα 4-46: Οθόνη ρύθμισης αποστολής e-mail του Elite

Εδώ στην αρχή δυσκολευτήκαμε λίγο γιατί δεν αρκούσε απλά το e-mail όπως στις άλλες δυο εφαρμογές αλλά ήθελε και πρόσθετα στοιχεία όπως ο smtp server του e-mail μας κτλ. Βέβαια τέτοια χαρακτηριστικά απαιτούσαν και άλλες εφαρμογές που δοκιμάσαμε εκτός από τις 2 προηγούμενες που έχουμε αναλύσει.

Δοκιμή

Αφού ρυθμίσαμε και αυτά λοιπόν, «τρέξαμε» τα βήματα του πειράματος για την καταγραφή. Ας δούμε και σε αυτή την περίπτωση τι διαφορετικό έχει να μας προτείνει αυτός ο key logger.

Ανοίγοντας τα logs ενθουσιαστήκαμε από την προσεγμένη γραφική δουλεία που έχει γίνει. Μπορεί να φαίνεται ανούσιο και αστείο το να προσέχουμε σχεδιαστικά τις εφαρμογές αλλά η ευανάγνωστη παρουσίαση των reports σε έναν key logger που μπορεί να καταγράφει τα πάντα είναι πολύ σημαντική ώστε ο επιτιθέμενος να μπορεί να βρει εύκολα αυτό που ψάχνει και να μη χαθεί μέσα σε ένα κυκεώνα πληκτρολογήσεων.

Εικόνα 4-47: Συνολικό report στον Elite

Βλέπουμε λοιπόν ότι ανοίγοντας απλά ένα report βλέπουμε τα πάντα συγκεντρωμένα και συνδυασμένα-ταιριασμένα μεταξύ τους. Ότι βλέπαμε πριν σε δυο και τρία reports χωριστά(keystrokes, application run, IM reports) τα έχουμε εδώ σε ένα τέλειο συνολικό report, χωρίς το παραμικρό να σε δυσκολεύει στην ανάγνωση. Βέβαια υποστηρίζεται και η μεμονωμένη εμφάνιση των logs.

Ας δούμε λοιπόν τι καταγράφηκε όσον αφορά τις κινήσεις μας.

Εικόνα 4-48: Εμφάνιση καταγραμμένων κωδικών στον Elite

Όπως βλέπουμε στο μικρό παραθυράκι της καταγραφής του Firefox, έχει γίνει πλήρης καταγραφή της επίσκεψης μας στο e-banking μας. Καταγράφηκαν κανονικά και το username και ο κωδικός και εμφανίζονται εδώ. Επιπλέον ένα screenshot κατέγραψε και την επίσκεψη μας εκείνη την ώρα και όπως βλέπουμε το username είναι ήδη συμπληρωμένο.

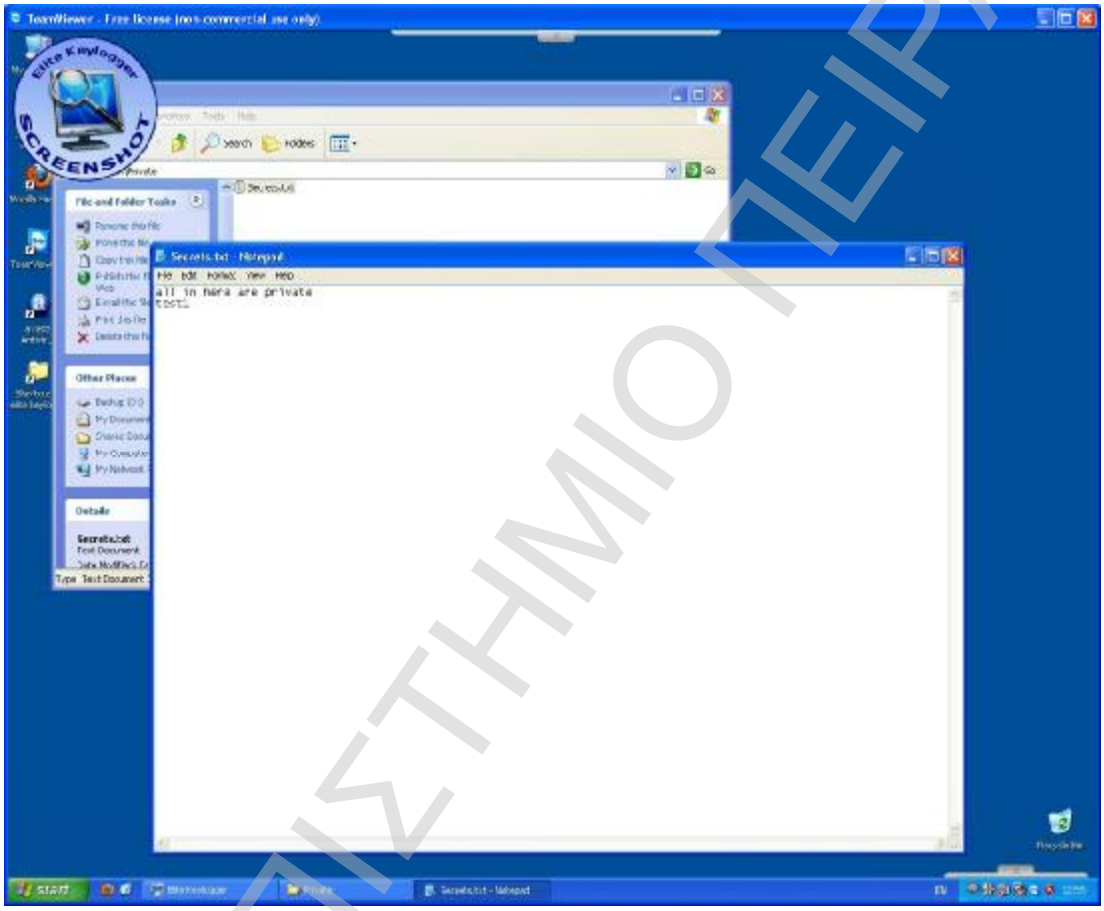
Εικόνα 4-49: Screenshot του Elite

Επιπλέον όσον αφορά το googletalk ο key logger λειτούργησε σωστά και εκεί και κατέγραψε username και password και αναγνώρισε σωστά τον IM.

Εικόνα 4-50: Εμφάνιση report για παρακολούθηση συνομιλίας του googletalk στον Elite

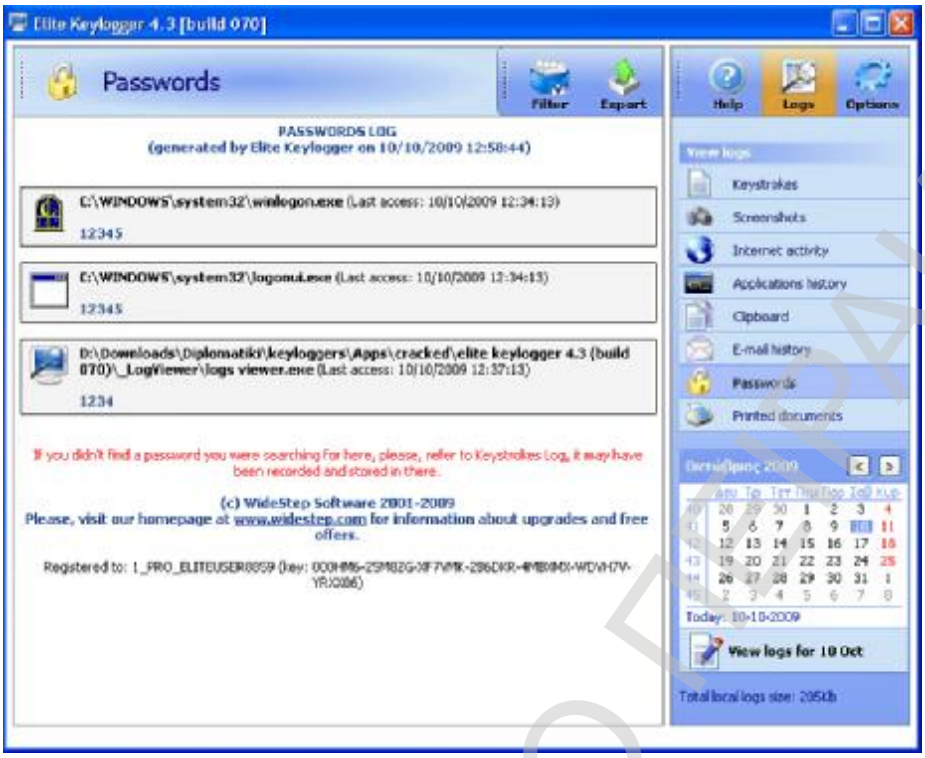
Παρατηρούμε ακόμα ότι και σε αυτό και στο προηγούμενο report δεν εμφανίζονται πολλοί μη-εκτυπώσιμοι χαρακτήρες(shift κτλ). Αυτό δεν οφείλεται στο ότι δεν τα χρησιμοποιήσαμε αλλά στο ότι η εφαρμογή λειτουργεί έξυπνα και καταγράφει το τελικό αποτέλεσμα. Όπως παραπάνω δηλαδή αντί να καταγράψει mail[Shift]i[Shift]mpin κατέγραψε mailIMpin. Τέτοια χαρακτηριστικά διευκολύνουν αρκετά τον επιτιθέμενο.

Επιπλέον όσον αφορά τη γενικότερη χρήση και την αξιολόγηση των screenshot αυτά γίνονταν πάντα την κατάλληλη ώρα:



Εικόνα 4-51: Screenshot του Elite

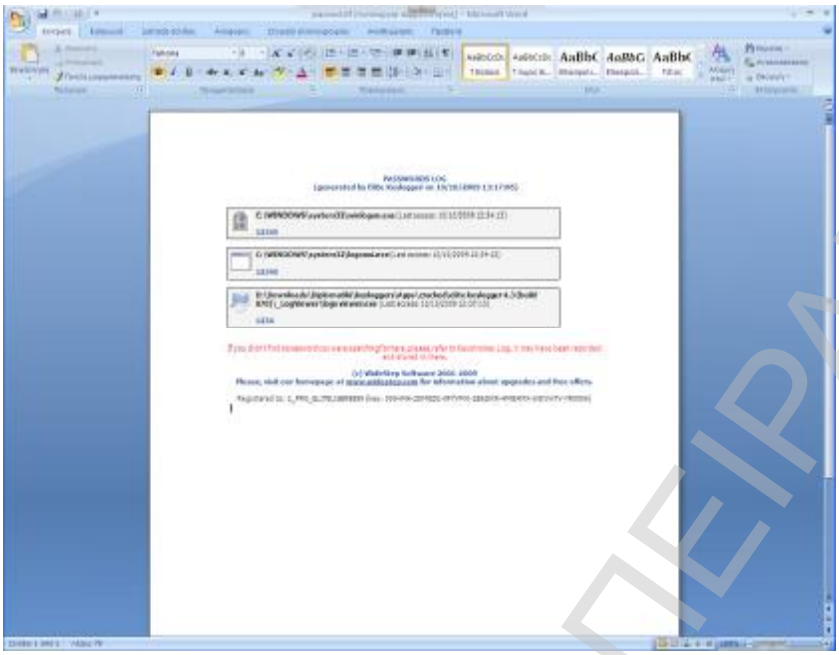
Βλέπουμε όμως, ότι ένα από τα reports που υπάρχει έχει τίτλο «passwords». Για να δούμε τι έχει κάνει ο elite για να μας εντυπωσιάσει. Η εφαρμογή έχει αναγνωρίσει και καταγράψει εφαρμογές που ζήτησαν και συμπληρώθηκε password και τις έχει συγκεντρώσει σε ένα ξεχωριστό report για να βοηθήσει τον επιτιθέμενο να μην ψάχνει πολλά reports!



Εικόνα 4-52: Report συγκεντρωμένων κωδικών στον Elite

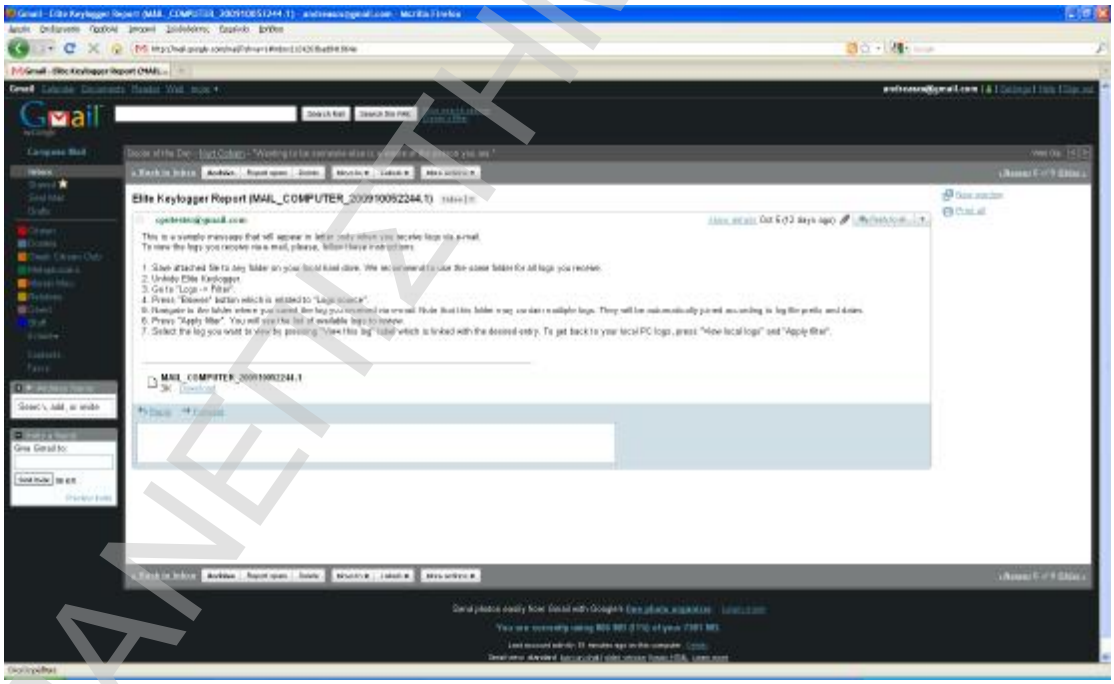
Παρατηρώντας, όμως, αυτό το report εντυπωσιαστήκαμε ακόμα περισσότερο όταν διαπιστώσαμε ότι η εφαρμογή υποστηρίζει (και το είχε κάνει κιόλας) την καταγραφή πριν το login. Το πρώτο password λοιπόν που βλέπετε είναι ο κωδικός του χρήστη μας! Αυτή η δυνατότητα είναι ιδιαίτερα σημαντική γιατί δίνει την ευκαιρία στον επιτιθέμενο να έχει φυσική πρόσβαση στον επιτιθέμενο κατά τη διάρκεια της απουσίας του χρήστη.

Επιπλέον τα reports αυτά γίνονται export σε αρχεία word, ιδιαίτερα χρήσιμη λειτουργία για τον απλό χρήστη.



Εικόνα 4-53: Εξαγόμενο report του Elite

Τέλος, η αποστολή e-mail ήταν επιτυχής. Και το export αυτό, δεν είναι στατικό(html κτλ) αλλά γίνεται import στην εφαρμογή, η οποία έρχεται και μόνο με τον log viewer. Το εξαγόμενο αρχείο γίνεται εισαγωγή και φαίνονται κανονικά τα reports σαν να βρίσκεσαι στον υπολογιστή-στόχο.



Εικόνα 4-54: Εμφάνιση αυτοματοποιημένου e-mail του Elite

Συμπεράσματα

Η εφαρμογή αυτή μας ικανοποίησε ιδιαίτερα. Λειτουργώντας με μια συγκεντρωτική τακτική ενσωματώνοντας τα πάντα σε 2-3 φόρμες αλλά με τέτοιο τρόπο ώστε όχι να δυσκολεύει αλλά να βοηθάει στο έργο του επιτιθέμενου. Ας δούμε τα θετικά όμως ένα-ένα:

+ Επιτυχής καταγραφή σε όλες τις εφαρμογές
+ Καταγραφή του login password
+ Άψογος τρόπος εμφάνισης και matching των καταγραφών και ομαδοποιημένα ανά εφαρμογή
+ Επιτυχής ομαδοποιημένη συγκέντρωση των ρυθμίσεων σε μια οθόνη
+ Έξυπνη καταγραφή όσον αφορά τους μη-εκτυπώσιμους χαρακτήρες
+ Ξεχωριστό report μόνο για τα passwords
+ Προσωποποιημένο hot key

Και τα αρνητικά:

- Απαιτείται restart κατά την εγκατάσταση
- Δυσκολία στις ρυθμίσεις αποστολής e-mail
- Δεν υποστήριζε ελληνικά στην καταγραφή ούτε και αυτό

4) Νικητής;

Όπως και στην προηγούμενη ενότητα έτσι και εδώ θα κάνουμε σύγκριση ανάμεσα στους key loggers που δοκιμάσαμε.

Καταρχάς, όπως είπαμε και στην αρχή της ενότητας, δοκιμάσαμε 9 από τους 10 των λιστών με τους top key loggers. Για την ιστορία απλώς αναφέρω ότι ο ένας από τους 10 που δε δοκιμάστηκε δεν υποστήριζε καμία δικτυακή αποστολή ή ανάσυρση log files (τοπικός) και για αυτό το λόγο δεν δοκιμάστηκε καν. Οι υπόλοιποι δοκιμάστηκαν και μας άφησαν ποικίλες εντυπώσεις και οι τρεις που καταλήξαμε ήταν κοντά στην κορυφή των λιστών που είχαμε υπόψη μας. Παρόλα αυτά δε μπορούμε να πούμε ότι μείναμε απόλυτα ικανοποιημένοι από το σύνολο των top εφαρμογών. Δηλαδή καμία από τις εφαρμογές δεν πληρούσε όλες τις απαιτήσεις μας. Καμία εφαρμογή δεν κατάφερε να «ξεφύγει» από το antivirus κατά την εγκατάσταση, οι περισσότερες (6 από τις 9) δεν κατάφεραν να παραμείνουν πλήρως κρυφές ούτε καν από τον χρήστη,

1 από τις 3 top που καταλήξαμε ανιχνευόταν από το anti-virus κατά τη διάρκεια της εκκίνησης καταγραφής και οι περισσότερες (6 από τις 9) ενώ υποστήριζαν αποστολή e-mail δεν κατάφεραν να το κάνουν γιατί κάποιο στοιχείο ασφαλείας τις εμπόδιζε. Δεν μπορώ να πιστέψω ότι οι εταιρείες παραγωγής τέτοιων προγραμμάτων δεν κάνουν αρκετή δουλειά πάνω στον τομέα τους, απλά θέλω να υποθέσω ότι οι εταιρείες που ασχολούνται με την ασφάλεια των συστημάτων έχουν πάρει στα σοβαρά τον ρόλο τους και χρειάζεται κάτι παραπάνω από μια εγκατάσταση εφαρμογής για να υποκλέψεις προσωπικά δεδομένα.

Συγκεντρωτικά τώρα, όσον αφορά την ποικιλία ρυθμίσεων και επιλογών πρώτο έρχεται το spyagent. Οι δυνατότητες που έχει για ρύθμιση είναι πάρα πολλές κα καλύπτουν όλες τις πιθανές περιπτώσεις. Ακολουθεί, λίγο πιο πίσω, ο elite χωρίς να του λείπει κάτι ουσιώδες.

Όσον αφορά τις δυνατότητες καταγραφής μπορεί το spyagent να είχε τις περισσότερες επιλογές αλλά ο elite υποστήριζε και εκκίνηση της καταγραφής πριν το login για καταγραφή του login password.

Όσον αφορά την επιτυχία αποστολής e-mail με τα log files, πρώτο έρχεται το stealth. Αυτό γιατί παρόλο που όλα το κατάφεραν σε αυτό το θέμα, το stealth μπόρεσε και έκανε περισσότερες παρακάμψεις και θα εξηγήσω τι εννοώ. Στην αρχή οι key loggers δοκιμάστηκαν σε περιβάλλον Virtual Machine και μόνο ο stealth κατάφερνε να στέλνει e-mail ακόμα και μέσα από αυτό, ενώ κανένα άλλο από τα 9 δεν το κατάφερε. Και οι άλλες δυο εφαρμογές όμως σε κανονική εγκατάσταση υπολογιστή παρέκαμπταν τις δικλίδες ασφαλείας.

Όσον αφορά τα reports, θέμα που εξηγήσαμε ότι είναι πολύ σημαντικό γιατί ο επιτιθέμενος πρέπει να ξεδιαλέξει ένα password ανάμεσα σε χιλιάδες keystrokes, ο elite είναι νικητής και με διαφορά. Απόλυτο ταίριασμα όλων των καταγραφών σε συνολικά ευανάγνωστα reports και διευκολύνσεις για τον αναγνώστη με reports για passwords, ήταν τα κύρια δυνατά σημεία του.

Όσον αφορά την παραβίαση ασφαλείας κατά την εγκατάσταση κανένα δεν τα κατάφερε. Παρόλα αυτά, παραβλέπουμε το συγκεκριμένο σημείο καθώς ο επιτιθέμενος εφόσον έχει φυσική πρόσβαση στον υπολογιστή του χρήστη μπορεί να το απενεργοποιήσει. Η παράκαμψη, όμως, της ασφάλειας κατά την καταγραφή είναι αναγκαία κάτι στο οποίο το spyagent δεν είχε μεγάλο βαθμό επιτυχίας γιατί ανιχνευόταν στην εκκίνηση. Τα άλλα δυο ανιχνεύονταν μόνο κατά το άνοιγμα των εφαρμογών κάτι το οποίο όμως δεν θα κάνει ούτε ο χρήστης ούτε ο επιτιθέμενος ο οποίος θα βλέπει τα logs από άλλο υπολογιστή.

Εφαρμογή	SpyAgent	Stealth	Elite
Ποικιλία Επιλογών	+++++	+	++++
Αποστολή E-mail	++++	+++++	++++
Δυνατότητα Καταγραφών	+++++	++	+++++
Reports	++++	+	+++++
Παράκαμψη ασφαλείας	+	++++	++++

Πίνακας 3: Συγκριτικός βαθμολογημένος πίνακας των 3 εφαρμογών key logging

Σε γενικές γραμμές λοιπόν:

Αν κάποιος ψάχνει έναν απλό Key logger θα μπορούσε να επιλέξει είτε τον stealth είτε τον elite.

Αν ψάχνει για κάποιον που να έχει πολλές επιλογές μπορεί να επιλέξει τον spyagent ή τον elite.

Αν ψάχνει κάτι που να καλύπτει τα πάντα, ίσως με ελάχιστες και όχι σημαντικές παραχωρήσεις, τότε μπορεί να επιλέξει τον elite.

D. Τρόποι προφύλαξης

Οι περισσότερες εταιρείες antivirus και anti-spyware έχουν ήδη προσθέσει στις βάση δεδομένων που έχουν με κακόβουλα προγράμματα και γνωστούς key loggers. Έτσι σε περίπτωση που έχετε τέτοιο λογισμικό και βρεθούν key loggers τα antivirus τα χειρίζονται όπως όλα τα άλλα κακόβουλα προγράμματα.

Υπάρχουν βέβαια και anti-key logging προγράμματα που είτε έχουν κάποιες στάνταρ λίστες με key loggers και ψάχνουν να τα αφαιρέσουν είτε ανιχνεύουν σε διάφορα modules του συστήματος για περίεργη «λειτουργία».

Άλλος τρόπος προστασίας είναι η χρήση one-time κωδικών γιατί και να υποκλαπούν οι κωδικοί δεν θα έχουν καμία αξία. Τέτοιους κωδικούς παράγουν συσκευές όπως αυτή:

Εικόνα 4-55: Τραπεζική συσκευή παραγωγής επιπλέον On-line κωδικών

Τέτοιες συσκευές χρησιμοποιούνται συνήθως σε τραπεζικές εφαρμογές εδώ και 3-4 χρόνια.

Επίσης η χρήση εικονικού πληκτρολογίου όπως αυτό που βρίσκουμε στα εργαλεία των περισσότερων λειτουργικών είναι ένας έξυπνος τρόπος. Βέβαια αυτά δεν σχεδιάστηκαν για αυτό το λόγο αλλά για ανθρώπους με ειδικές ανάγκες.

Εικόνα 4-56: Εικονικό πληκτρολόγιο

Παρόλα αυτά και τα click σε αυτό το πληκτρολόγιο μπορούν να υποκλαπούν από σύγχρονους key loggers.

Επίσης στην εγκατάσταση προγραμμάτων θα πρέπει να προσέχουμε τι εγκαθιστούμε. Πλέον λειτουργικά, όπως τα 64-bit Windows Vista και Server 2008 απαιτούν υποχρεωτική ψηφιακή υπογραφή για kernel-mode device drivers, ώστε να αποφευχθεί η εγκατάσταση key-logging root kits.

Επίσης η εγκατάσταση Firewall και Network monitors δεν μπλοκάρει τη λειτουργία των key logger αλλά θα βοηθήσει στο να αποφευχθεί μια απομακρυσμένη εγκατάσταση και θα ενημέρωνε τον χρήστη για εφαρμογές που προσπαθούν να επικοινωνήσουν μέσω δικτύου.

Μια έξυπνη λύση είναι η αλλαγή του Keyboard layout. Οι περισσότεροι key loggers υποθέτουν ότι ο χρήστης χρησιμοποιεί qwerty πληκτρολόγιο οπότε αν αλλαχθεί το layout για παράδειγμα σε Dvorak, 99% θα αποτύχει η υποκλοπή.

Μια άλλη έξυπνη μέθοδος είναι η αναγνώριση ομιλίας. Χρησιμοποιώντας προγράμματα που μετατρέπουν τη φωνή σε κείμενο δεν είναι εύκολο να υποκλαπούν τα δεδομένα μιας και δεν υπάρχουν ενδιάμεσες πληκτρολογήσεις. Βέβαια είναι πολύ σημαντικό πως στέλνεται αυτό το κείμενο γιατί μπορεί να υποκλαπεί μετά την ψηφιοποίηση του σε text.

Τέλος η χρήση smart cards είναι πολύ αποτελεσματική γιατί δεν επηρεάζονται από key loggers. Η κάρτα περιέχει τα στοιχεία και δεν μπορεί να υποκλαπεί τίποτα από κάποιον key logger. Παρόλα αυτά ο smart card reader μπορεί να χρησιμοποιηθεί για hardware key logger.

Κάποιες μη τεχνολογικές αλλά αποδοτικές λύσεις είναι η πληκτρολόγηση ενδιάμεσων χαρακτήρων. Για παράδειγμα αν θες να γράψεις έναν κωδικό μπορείς να πληκτρολογήσεις τα 2 πρώτα γράμματα στο πεδίο του κωδικού, μετά να πληκτρολογήσεις 4-5 γράμματα εκτός του πεδίου πηγαίνοντας εκεί με το ποντίκι και μετά να συνεχίσεις μέσα στο πεδίο. Η να γράφεις κάποιους άσχετους χαρακτήρες και μετά να τους επιλέγεις και να γράφεις από πάνω. Ο Key logger θα έχει «πιάσει» όλες τις πληκτρολογήσεις σαν κωδικό χρήστη!

Ε. Συμπέρασμα

Στην ενότητα αυτή αναφέραμε με λίγα λόγια πως λειτουργούν οι Key loggers. Είδαμε τις κατηγορίες στις οποίες χωρίζονται ανάλογα με τις μεθόδους που χρησιμοποιούν. Αναφέραμε ότι στην ουσία όλα αυτά τα προγράμματα μπορούν να παρουσιαστούν σα νόμιμα οπότε δεν είναι εύκολο να απαγορευτούν παρά μόνο ανάλογα με τη χρήση που γίνεται. Επισημάναμε ότι υπάρχουν τρόποι αντιμετώπισης που συνδυάζουν την προσοχή και την εξυπνάδα του χρήστη, τη χρήση ειδικού λογισμικού και την χρήση ειδικών κωδικών όπως One-time κωδικοί κτλ. Τέλος, για να είμαστε ξεκάθαροι πρέπει να πούμε ότι είναι δύσκολο στην καθημερινή μας εργασία να προσέχουμε όλα τα παραπάνω για να μην πέσουμε θύμα υποκλοπής και ότι πλέον οι σύγχρονοι Key loggers που συνδυάζουν και λήψη βίντεο εκτός από όλα τα παραπάνω δεν είναι τόσο εύκολο να ξεγελαστούν. Παρόλα αυτά όμως πρέπει να παίρνουν κάποια αναγκαία βασικά μέτρα ώστε να μην πέσουμε θύματα υποκλοπής από απλούς απατεώνες που χρησιμοποιούν απλά προγράμματα που βρίσκουν στο διαδίκτυο.

5. Παρουσίαση και δοκιμή του δικού μας password cracker ‘CreamCracker’

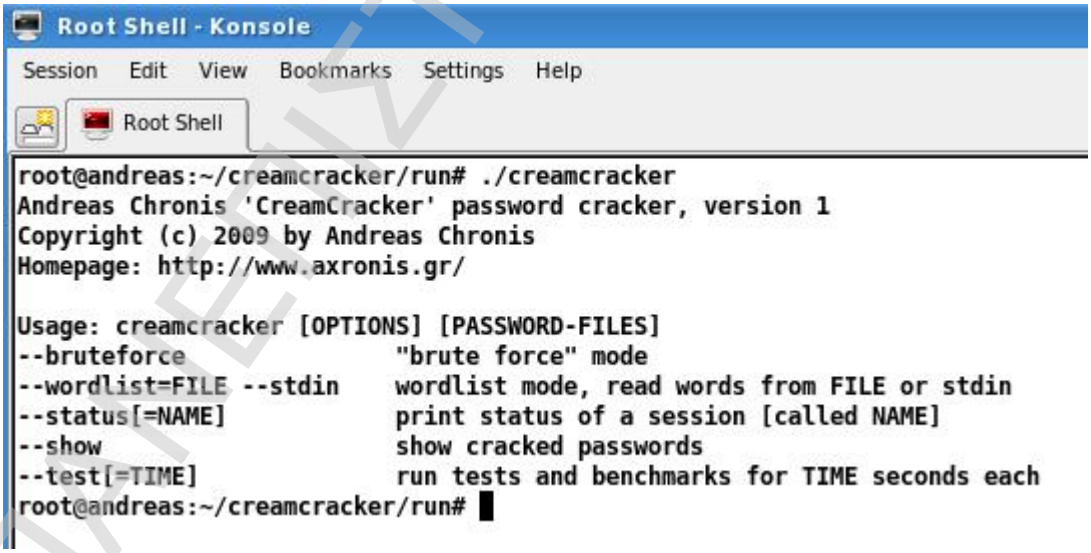
Α. Παρουσίαση

Μετά τη μελέτη μας και τις δοκιμές μας στους Password Crackers ήρθε η ώρα να φτιάξουμε και ένα δικό μας. Ο password cracker που θα φτιάξουμε θα είναι γραμμένος σε γλώσσα c χρησιμοποιώντας τον compiler gcc-4.3 και όσον αφορά το γραφικό του περιβάλλον θεωρούμε ότι όπως κάθε πρόγραμμα παραβίασης που «σέβεται» τον εαυτό του έτσι και αυτό για βέλτιστη απόδοση θα τρέχει στο console του Linux. Σκοπός μας σε αυτή την ενότητα δεν είναι να αναλύσουμε προγραμματιστικά πως θα δημιουργήσουμε την εφαρμογή μας, αλλά να δούμε αυτό που φτιάξαμε πόσο αποδοτικό είναι και αν μπορεί να συγκριθεί με τις εφαρμογές που συγκρίναμε σε προηγούμενη ενότητα. Ο κώδικας της εφαρμογής περιέχεται στο cd.

Ο cracker που δημιουργήσαμε λοιπόν, και του δώσαμε το όνομα CreamCracker, είναι μια μικρή εφαρμογή σε c που έχει τη δυνατότητα δυο ειδών επίθεσης:

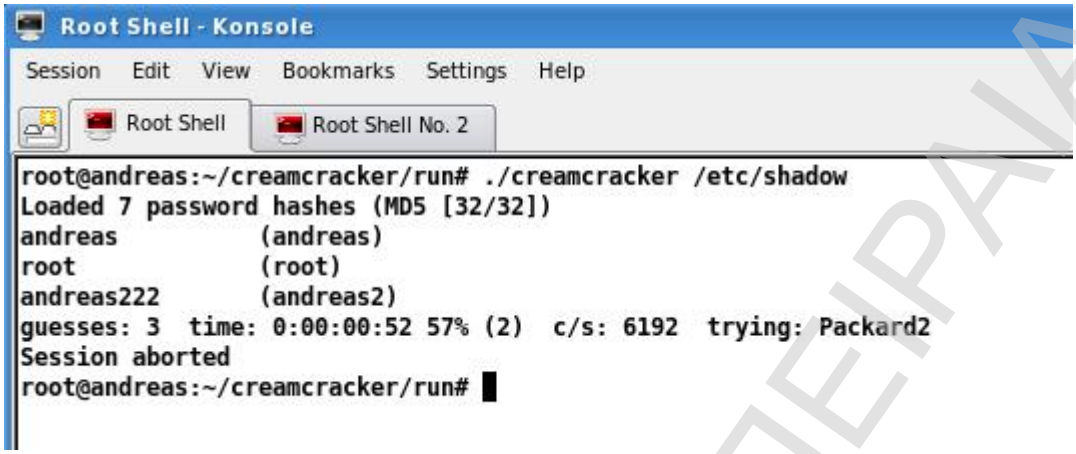
1. Brute force επίθεση: επίθεση όπως την έχουμε αναφέρει παραπάνω με υποστήριξη Latin character set καθώς και αριθμών και όλων των συμβόλων. Προσπαθήσαμε ο αλγόριθμος της επίθεσης να είναι όσο πιο βέλτιστος γίνεται

2. Dictionary επίθεση: επίθεση με λεξικό, όπως την έχουμε αναφέρει και παραπάνω χρησιμοποιώντας ένα λεξικό περίπου 25mb που χρησιμοποιήσαμε και στις δοκιμές μας στην ενότητα 3.



Εικόνα 5-1: Επιλογές εφαρμογής

Όμως, η εφαρμογή μας έχει σχεδιαστεί και λειτουργεί και συνδυασμένα. Δηλαδή μπορεί ο χρήστης να μην επιλέξει μέθοδο επίθεσης και έτσι η εφαρμογή θα χρησιμοποιήσει και τους 2 τρόπους ξεκινώντας από την brute force επίθεση.



Εικόνα 5-2: Παράδειγμα εφαρμογής

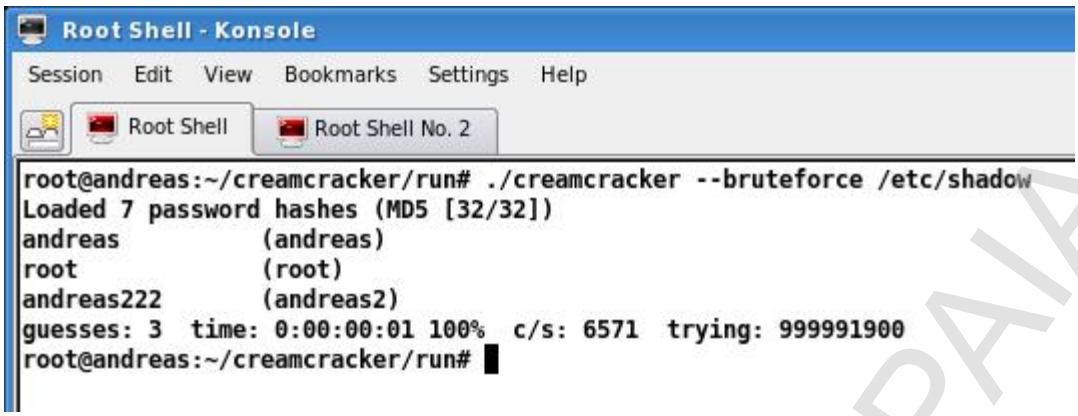
Ας δοκιμάσουμε όμως την εφαρμογή μας. Ο καλύτερος τρόπος για να την δοκιμάσουμε είναι να χρησιμοποιήσουμε ένα αρχείο κωδικών που χρησιμοποιήσαμε και πριν στις δοκιμές μας και να βάλουμε τον creamcracker να επιτεθεί σε αυτό. Χρησιμοποιούμε λοιπόν το αρχείο shadow.

B. Brute force επίθεση

Ανοίγουμε λοιπόν το console για να τρέξουμε από εκεί τον creamcracker. Για να επιτεθούμε με brute force επίθεση γράφουμε:

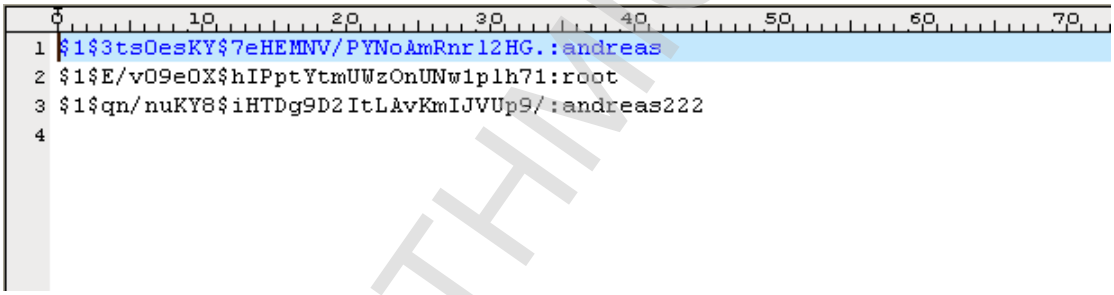
```
#./creamcracker –bruteforce /etc/shadow
```

και πατάμε enter.



Εικόνα 5-3: Παράδειγμα Brute force επίθεσης

Πρώτα βλέπουμε στην οθόνη μας μερικά στοιχεία όπως το πλήθος των passwords που έχουν φορτωθεί και στους οποίους θα γίνει επίθεση καθώς και τον τύπο της κρυπτογράφησης. Έπειτα στις επόμενες γραμμές εμφανίζονται σταδιακά κάθε password που βρίσκει η εφαρμογή και δίπλα το όνομα του χρήστη στον οποίο ανήκει το password. Αυτές οι γραμμές λοιπόν, θα εμφανίσουν στο τέλος τις επίθεσης όλα τα passwords που θα παραβιαστούν. Επίσης, για λόγους διευκόλυνσης, τα passwords που αποκαλύπτονται, αποθηκεύονται σε ένα αρχείο που δημιουργείται.



Εικόνα 5-4: Παράδειγμα αποθήκευσης κωδικών στο αρχείο

Και επιπλέον η εφαρμογή κρατάει κάποια logs για την επίθεση, όπως η ώρα εκκίνησης του session, κανόνες που χρησιμοποιήθηκαν και όλες τις επιτυχημένες προσπάθειες παραβίασης.

```
 1 0:00:00:00 Starting a new session
 2 0:00:00:00 Loaded a total of 7 password hashes with 7 different salts
 3 0:00:00:00 Remaining 7 password hashes with 7 different salts
 4 0:00:00:00 - Hash type: FreeBSD MD5 (lengths up to 15)
 5 0:00:00:00 - Algorithm: 32/32
 6 0:00:00:00 - Candidate passwords may be buffered and tried in chunks of 8
 7 0:00:00:00 Proceeding with "single crack" mode
 8 0:00:00:00 - 956 preprocessed word mangling rules
 9 0:00:00:00 - Allocated 7 buffers of 8 candidate passwords each
10 0:00:00:00 - Rule #1: ':' accepted as ''
11 0:00:00:00 - Rule #2: '-s x**' rejected
12 0:00:00:00 - Rule #3: '-c (?acQ' accepted as '(?acQ'
13 0:00:00:00 - Rule #4: '-c lQ' accepted as 'lQ'
14 0:00:00:00 - Rule #5: '-s-c x**MlQ' rejected
15 0:00:00:00 - Rule #6: '>6'6' accepted
16 0:00:00:00 + Cracked andreas
17 0:00:00:00 - Rule #7: '>7l'7' accepted
18 0:00:00:00 - Rule #8: '>6/?ul'6' accepted
19 0:00:00:00 - Rule #9: '>5'5' accepted
20 0:00:00:00 - Rule #10: '<*d' accepted
21 0:00:00:00 - Rule #11: 'rc' accepted
22 0:00:00:00 - Rule #12: '<*dMcQ' accepted
23 0:00:00:00 - Rule #13: '>5/?ul'5' accepted
24 0:00:00:00 - Rule #14: 'uQ' accepted
25 0:00:00:00 - Rule #15: 'r(?al' accepted
26 0:00:00:00 + Cracked root
27 0:00:00:00 - Rule #16: '<*!?Alp' accepted
28 0:00:00:00 - Oldest still in use is now rule #14
29 0:00:00:00 - Rule #17: '<*!?Acp' accepted
30 0:00:00:00 - Rule #18: '<*cQd' accepted
31 0:00:00:00 - Rule #19: '>7/?u'7' accepted
32 0:00:00:00 - Rule #20: '>4l'4' accepted
33 0:00:00:00 - Rule #21: '<+(?lcr' accepted
34 0:00:00:00 - Oldest still in use is now rule #20
35 0:00:00:00 - Rule #22: '<+r(?lcr' accepted
36 0:00:00:00 - Rule #23: '>3'3' accepted
```

Εικόνα 5-5: Log επίθεσης

Στο τέλος της λειτουργίας, ή στη διακοπή της, η εφαρμογή εμφανίζει κάποια στατιστικά στοιχεία όπως ο χρόνος επίθεσης, ταχύτητα δοκιμών καθώς και σε ποιο password διακόψαμε, ή τελείωσε η εφαρμογή.

Όπως παρατηρούμε, η ταχύτητα δοκιμών είναι περίπου 6500 δοκιμές το δευτερόλεπτο. Ένας αρκετά καλός χρόνος, αν και δεν μπορεί να συγκριθεί με τις top εφαρμογές που δοκιμάσαμε που έχουν χρόνους πάνω από 8 εκατομμύρια δοκιμές το δευτερόλεπτο.

Η εφαρμογή έτρεξε αρκετές ώρες για να βρει περισσότερους κωδικούς από ότι εμφανίζουμε άλλα δεν πέτυχε. Πως θα μπορούσε άλλωστε όταν ούτε οι top εφαρμογές δεν το κατάφεραν.

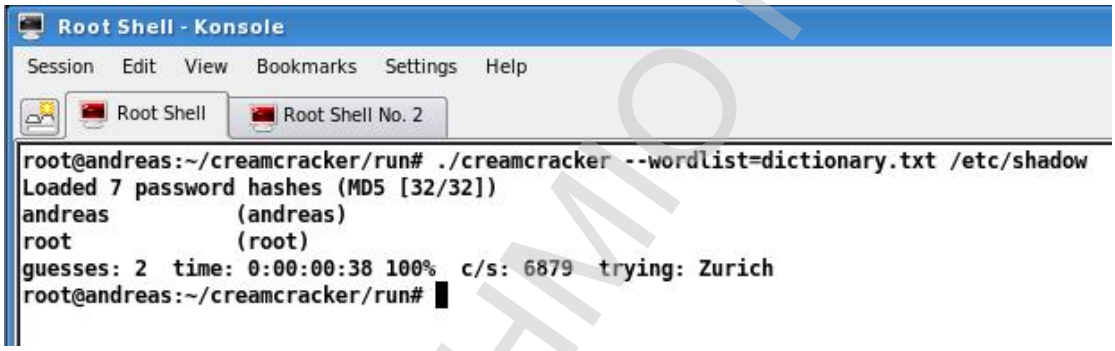
C. Dictionary επίθεση

Αφού δοκιμάσαμε λοιπόν την brute force επίθεση ας δοκιμάσουμε και πόσο καλά δουλεύει η εφαρμογή μας και στην επίθεση με λεξικό. Το λεξικό που χρησιμοποιήσαμε είναι το ίδιο λεξικό που χρησιμοποιήσαμε και στις δοκιμές των top crackers για να είμαστε απόλυτα αντικειμενικοί. Ανοίγουμε λοιπόν το console για να τρέξουμε από εκεί τον creamcracker και να επιτεθούμε πάλι στο αρχείο shadow. Για να επιτεθούμε με dictionary επίθεση γράφουμε:

```
#./creamcracker --wordlist=dictionary.txt /etc/shadow
```

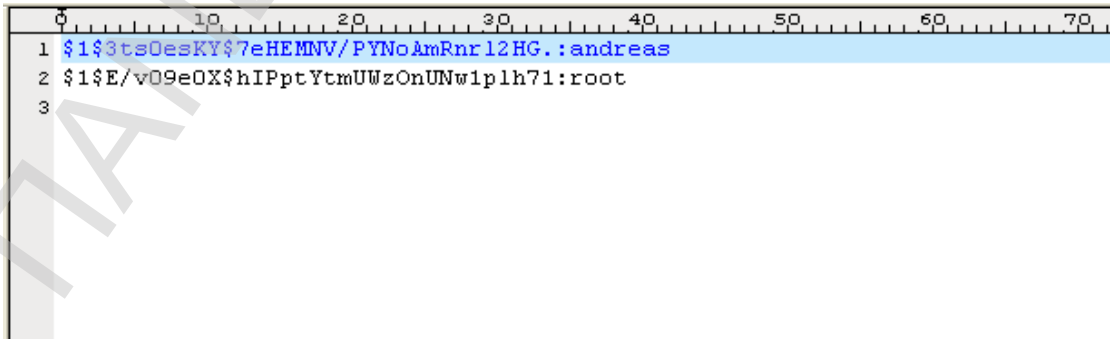
και πατάμε enter.

Η διαφορά δηλαδή στην ουσία είναι ότι προσθέτουμε ένα επιπλέον όρισμα που ορίζει στην εφαρμογή να επιτεθεί με λεξικό.



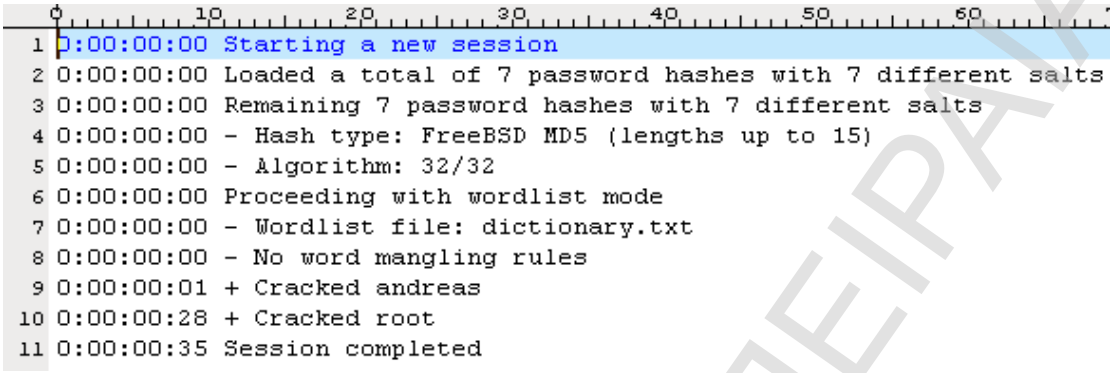
Εικόνα 5-6: Παράδειγμα Dictionary επίθεσης

Όπως και στην προηγούμενη επίθεση, πρώτα βλέπουμε στην οθόνη μας μερικά στοιχεία όπως το πλήθος των passwords που έχουν φορτωθεί και στους οποίους θα γίνει επίθεση καθώς και τον τύπο της κρυπτογράφησης. Έπειτα στις επόμενες γραμμές εμφανίζεται σταδιακά κάθε password που βρίσκει η εφαρμογή και δίπλα το όνομα του χρήστη στον οποίο ανήκει το password. Αυτές οι γραμμές λοιπόν, θα εμφανίσουν στο τέλος τις επίθεσης όλα τα passwords που θα παραβιαστούν. Επίσης, και σε αυτή την επίθεση, για λόγους διευκόλυνσης, τα passwords που αποκαλύπτονται, αποθηκεύονται σε ένα αρχείο που δημιουργείται.



Εικόνα 5-7: Παράδειγμα αποθήκευσης κωδικών στο αρχείο

Και επιπλέον η εφαρμογή κρατάει κάποια logs για την επίθεση, όπως η ώρα εκκίνησης του session, κανόνες που χρησιμοποιήθηκαν και όλες τις επιτυχημένες προσπάθειες παραβίασης.



Εικόνα 5-8: Log επίθεσης

Όπως παρατηρούμε εδώ η επίθεση χρειάστηκε πολύ μικρότερο χρονικό διάστημα για να βρει τα δυο passwords αλλά έκανε μόνο αυτό. Σταμάτησε δηλαδή αφού τελείωσε το λεξικό και κατάφερε με αυτή την μέθοδο να βρει μόνο τα 2 από τα 7 passwords. Αναμενόμενο βέβαια. Επίσης παρατηρούμε ότι οι χρόνοι που χρειάστηκαν για αυτή την επίθεση ήταν παραπλήσιοι με τους χρόνους της brute force επίθεσης, σε αρκετά καλά επίπεδα δηλαδή.

6. Επίλογος

Στην μελέτη αυτή είδαμε πολλά σημαντικά θέματα που αφορούν την ασφάλεια του μέσου χρήστη. Είδαμε καταρχήν πόσο εύκολο είναι να παραβιάσουμε συνήθεις κωδικούς που χρησιμοποιούνται κατά κόρον από το μέσο χρήστη. Αντιληφθήκαμε πόσο σημαντικό είναι να επιλέγουμε σοβαρά τους κωδικούς που χρησιμοποιούμε αν θέλουμε να εξασφαλίσουμε τα προσωπικά μας δεδομένα.

Επιπλέον είδαμε, πως μπορεί κάποιος κακόβουλος συνάδερφος, φίλος, χρήστης του ίδιου δικτύου να υποκλέψει σημαντικά προσωπικά μας δεδομένα. Πόσο εύκολα μπορεί να γίνει γνώστης των προσωπικών μας δεδομένων και να χάσει ακόμα και το υπόλοιπο των χρημάτων του τραπεζικού του λογαριασμού.

Τέλος κάναμε μια ενδιαφέρουσα και σοβαρή προσπάθεια να φτιάξουμε τον δικό μας password cracker, να δούμε πόσο αποτελεσματικός είναι και να εξάγουμε κατάλληλα στατιστικά συμπεράσματα.

Διαπιστώνουμε λοιπόν ότι ο χρήστης πρέπει να λαμβάνει κάποια βασικά μέτρα ασφαλείας για να προστατευθεί. Ο κωδικός που επιλέγει ο χρήστης πρέπει να πλήρη κάποιους κανόνες που έχουμε αναφέρει στο κεφάλαιο 3, ώστε η πολυπλοκότητα του να είναι αυξημένη και η παραβίαση του να είναι χρονοβόρα. Περισσότερο χρονοβόρα από ότι αξίζει να ασχοληθεί ο επιτιθέμενος για αυτά που θα κερδίσει αν τον σπάσει.

Ακόμα, λογισμικό ασφαλείας όπως antivirus κτλ πρέπει να είναι εγκατεστημένα στο σύστημα και ενημερωμένα για να προσφέρουν κάποια ασφάλεια κατά την εγκατάσταση key loggers. Ειδικά προγράμματα anti-key logging υπάρχουν όπως αναφέραμε στο κεφάλαιο 4 και ο χρήστης πρέπει να χρησιμοποιεί και αυτά αν έχει υποψίες παρακολούθησης.

Εν τέλει λοιπόν, η ασφάλεια σε ένα προσωπικό υπολογιστή είναι πιο σημαντική από ότι ο κάθε χρήστης πιστεύει και πρέπει να λαμβάνονται σοβαρά μέτρα προστασίας όταν υπάρχουν σοβαρά δεδομένα που αξίζουν σοβαρή προστασία.

7. Βιβλιογραφία

- Password security
- ZDNet Report: Net users picking safer passwords
- Default Password List *Pnenoelit.de* Retrieved on 2007-05-07
- British hacker fights extradition, BBC News, February 14, 2007
- Transcript of the interview, BBC Click
- John the Ripper project, John the Ripper cracking modes
- Bruce Schneider, Choosing Secure Passwords
- "How to prevent Windows from storing a LAN manager hash of your password in Active Directory and local SAM databases". Microsoft. http://support.microsoft.com/kb/299656. Retrieved on 2009-02-18.
- ophcrack
- Password Protection for Modern Operating Systems
- No Plaintext Passwords
- Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol
- A Future-Adaptable Password Scheme
- MDCrack FAQ 1.8
- "Top 10 Password Crackers". Sectools. http://sectools.org/crackers.html. Retrieved on 2008-11-01.
- Rainbow table
- Brute Force Attack
- Dictionary attack
- MD5
- Insecure.org
- Key logger.org
- Viruslist.com
- Jonathan Brossard (2008-09-03) (PDF). *Bypassing pre-boot authentication passwords by instrumenting the BIOS keyboard buffer (practical low level attaks*

against x86 pre-boot authentiation softwares). Iviz Technosolutions. http://www.ivizsecurity.com/research/preboot/preboot_whitepaper.pdf. Retrieved on 2008-09-23.

- "Keyghost". keyghost.com. http://www.keyghost.com/sx/. Retrieved on 2009-04-19.
- Jeremy Kirk (2008-12-16). "Tampered Credit Card Terminals". IDG News Service. http://www.pcworld.com/article/155525/.html?tk=rss_news. Retrieved on 2009-04-19.
- "Remote monitoring uncovered by American techno activists". ZDNet. 2000-10-26. http://news.zdnet.co.uk/security/0,1000000189,2082190,00.htm. Retrieved on 2008-09-23.
- "ATM camera". snopes.com. http://www.snopes.com/fraud/atm/atmcamera.asp. Retrieved on 2009-04-19.
- A. Young, M. Yung, "Deniable Password Snatching: On the Possibility of Evasive Electronic Espionage," IEEE Symposium on Security & Privacy, pages 224-235, May 4-7, 1997.
- John Leyden (2000-12-06). "Mafia trial to test FBI spying tactics: Keystroke logging used to spy on mob suspect using PGP". The Register. http://www.theregister.co.uk/2000/12/06/mafia_trial_to_test_fbi/. Retrieved on 2009-04-19.
- "Kernel-Mode Code Signing Policy (Windows Server 2008 and Windows Vista)". Msdn. http://msdn.microsoft.com/en-us/library/aa906239.aspx. Retrieved on 2008-11-16.
- Austin Modine (2008-10-10). "Organized crime tampers with European card swipe devices". The Register. http://www.theregister.co.uk/2008/10/10/organized_crime_doctors_chip_and_pin_machines/. Retrieved on 2009-04-18.
- Cormac Herley and Dinei Florencio (2006-02-06). "How To Login From an Internet Cafe Without Worrying About Key loggers" (PDF). Microsoft Research. http://cups.cs.cmu.edu/soups/2006/posters/herley-poster_abstract.pdf. Retrieved on 2008-09-23.
- Electromagnetic Radiation

8. Παράρτημα

Α. Πίνακες

Β. Εικόνες