

τα τέλη της δεκαετίας του '50 το κλάμη μοντελισμού σιδηροδρόμων του MIT βρέθηκε με μια δωρεά παλιών εξαρτημάτων. Τα περισσότερα από αυτά προέρχονταν από παλιές τηλεφωνικές συσκευές. Τα μέλη του κλάμη χρησιμοποίησαν όλα αυτά τα εξαρτήματα στην κατασκευή ενός πολύπλοκου συστήμα-

τος σιδηροδρόμων, όπου διαφορετικοί χειριστές μπορούσαν να ελέγχουν διαφορετικά μέρη του σιδηροδρομικού δικτύου, καλώντας, απλώς, κατάλληλα νούμερα. Για να περιγράψουν αυτή την πρωτότυπη και ευρηματική χρήση των παλιών τηλεφωνικών εξαρτημάτων, οι άνθρωποι του κλάμη επέλεξαν τη λέξη «hacking». Πολλοί ιστορικοί χαρακτηρίζουν τα μέλη αυτού του κλάμη ως τους πρώτους hacker.

Έκτοτε, ως «hacker» χαρακτηρίζεται ένας άνθρωπος που διακατέχεται από καλώς εννοούμενη περιέργεια και χρησιμοποιεί αυτή του την ορμή προκειμένου να ξεπερνά ή να «κάμπτει» τους όποιους φυσικούς ή τεχνικούς περιορισμούς. Είναι ένας άνθρωπος που γνωρίζει ότι ένα σύνολο κανόνων ή προδιαγραφών μπορεί να χρησιμοποιηθεί και με τρόπους πέρα από τους προφανείς ή προβλεπόμενους. Από νωρίς στην ιστορία της πληροφορικής ήταν φανερό ότι οι υπολογιστές θα αποτελούσαν κατεξοχήν μέσο έκφρασης κάθε hacker. Εξάλλου, οι υπολογιστές προκαλούν διαρκώς με τη φαινομενικά «άκαμπτη» λογική που διέπει τη λειτουργία τους. Τους υπολογιστές όμως και τα προγράμματα που τρέχουν τα σχεδιάζουν άνθρωποι, όντα στείλη.

Την ίδια στιγμή, ως πιστοί υπηρέτες, οι υπολογιστές δεν κάνουν ακριβώς αυτό που θέλουμε αλλά ακριβώς αυτό που τους λέμε, όπως χαρακτηριστικά επισημαίνει μια αστεία μεν, αληθήςστατη δε, ρήση. Στο ίδιο μοτίβο, τα προγράμματα των υπολογιστών συχνά δεν επιτελούν μόνο τις λειτουργίες που πρόβλεψαν οι αρχικές σχεδιαστικές προδιαγραφές. Έτσι, αν κάποιος γνωρίζει πώς να τα μεταχειριστεί, συχνά παρουσιάζουν και άλλες, ενδιαφέρουσες «όψεις» της λειτουργικής τους συμπεριφοράς. Ιδού λοιπόν μια πρώτη τάξεως πρόσκληση/πρόκληση για κάθε hacker που σέβεται τον εαυτό του! Ως στείλης ον, όμως, ο άνθρωπος συχνά ενδίδει και στον πειρασμό. Έτσι, ένας χρήστης υπολογιστή που μόλις «ανάγκασε» ένα μηχανήμα να κάνει κάτι που υπό φυσιολογικές συνθήκες δεν θα έκανε, ή έστω «σκόνταψε» πάνω στην ολιγωρία ενός διαχειριστή συστήματος, ίσως σκεφτεί να εκμεταλλευτεί τη θέση του για να προκαλέσει μια ζημιά ή να διαπράξει απάτη. Οι hacker από νωρίς είχαν ξεχωρίσει αυτά τα άτομα, στα οποία απέδωσαν το χαρακτηρισμό «cracker».

Κοντολογίς, ο cracker χρησιμοποιεί τις γνώσεις του για πονηρούς σκοπούς, ρεπώντας προς ποινικά κολλήσιμες πράξεις. Ο hacker, από την άλλη, συχνά διακατέχεται από ένα αγνό αίσθημα ελευθερίας, ενώ πάντα ως μοναδικά κίνητρα έχει τη γνώση και την καλώς εννοούμενη περιέργεια. Έτσι, αν, για παράδειγμα, ένας hacker ανακαλύψει κάποιο κενό ασφαλείας σε έναν απομα-

κρυσμένο διακομιστή, σε αντίθεση με τον cracker που θα απεύσει να το εκμεταλλευτεί προς ίδιον όφελος, εκείνος θα ειδοποιήσει τους υπεύθυνους διαχειριστές. Μολτατά, παρά το σαφή διαχωρισμό μεταξύ hacker και cracker, πολλοί δημοσιογράφοι δείχνουν μια περιέργη προτίμηση στον πρώτο όρο, χρησιμοποιώντας τον μάλλον ισοπεδωτικά. Παρόμοια αδιαφορία επιδεικνύουν και προς άλλους δύο χαρακτηρισμούς: white hat hacker (οι καλοί) και black hat hacker (οι κακοί). Όλα αυτά έχουν ως αποτέλεσμα το ευρύ κοινό να θεωρεί τους hacker κάτι σαν τους «βάνδαλους» του Internet.

Όμως η χειρότερη ζημιά στο προφίλ των (white hat) hacker δεν προκαλείται από το δημοσιογραφικό λόγο και μόνο. Δεν είναι λίγες οι φορές που οι hacker κακοχαρακτηρίζονται –ενίοτε και στιγματίζονται– εξαιτίας της εφαρμογής δύσκαμπτων ή/και ξεπερασμένων νομικών πλαισίων. Για παράδειγμα, αν κάποιος αγοράσει μια ταινία DVD και θελήσει να δημιουργήσει ένα αντίγραφο εφεδρείας, κατ' ελάχιστον θα αναγκαστεί να ξεπεράσει το σύστημα «προστασίας» CSS. Ενδέχεται, επίσης, να επιστρατεύσει εργαλεία συμπίεσης βίντεο, ώστε το αντίγραφο να χωρά σε δισκάκι χαμηλότερης χωρητικότητας σε σύγκριση με το πρωτότυπο. Όσο απλές και αν φαίνονται οι ενέργειες αυτές σε αρκετό κόσμο, δεν παύουν να αποτελούν «χακερίες», αφού κατά την εφαρμογή τους «λυγίζουν» και «παρακάμπτονται» κανόνες και περιορισμοί. Το θέμα είναι ότι, σύμφωνα με το γράμμα του νόμου, ακόμη και η δημιουργία αντιγράφων για προσωπική χρήση απαγορεύεται. Πώς, λοιπόν, χαρακτηρίζεται τώρα ο hacker που πήρε backup ενός DVD που νόμιμα κατείχε; Σύμφωνα με το νόμο, είναι απλώς ένας (black hat) hacker με «αποκλίνοια» συμπεριφορά. Το ίδιο είναι και εκείνος που αγοράζει μουσική από το Διαδίκτυο και αφαιρεί το όποιο σύστημα DRM, ώστε να μπορεί να την απολαμβάνει σε οποιοδήποτε υπολογιστή ή φορητή συσκευή αναπαραγωγής.

Αγαπητοί αναγνώστες, στο παρόν αφιέρωμα ασχολούμαστε εμπρακτά με το θέμα του «αγνού» hacking, υπό την έννοια ότι όλα όσα δείχνουμε αποσκοπούν στην απόκτηση γνώσης και μόνο. Παρουσιάζουμε έξι διαφορετικά φαινομενικά ασύνδετα μεταξύ τους θέματα. Από το game cheating και τα Google hacks έως στο ανώνυμο surfing και το sniffing, μοναδικά μας κίνητρα είναι η εξερεύνηση, ο πειραματισμός και φυσικά η «διασκέδαση! Θέλουμε επίσης να πιστεύουμε ότι αρκετά από τα θέματα που ακολουθούν θα αποτελέσουν κίνητρο για περαιτέρω μελέτη. Αν μη τι άλλο, γνωρίζοντας πώς παρακάμπτονται οι όποιοι κανόνες, μαθαίνουμε και πώς να προστατευόμαστε οι ίδιοι. Περιπτώ βέβαια να αναφέρουμε ότι όλα όσα δείχνουμε με κανέναν τρόπο δεν πρέπει να εφαρμοστούν για την πρόκληση ζημιών ή τη διάπραξη οιασδήποτε φύσεως απάτης – παραμείνετε στο στρατόπεδο των (white hat) hacker!

Καλύτερα όμως να αφήσουμε τα πολλά λόγια και να αρχίσουμε αμέσως τώρα την εξερεύνηση ενός νέου, συναρπαστικού κόσμου. Παρεμπιπτόντως, συχνά οι θύρες αυτών των κόσμων είναι δίπλα μας αλλά εμείς τείνουμε να τις αγνοούμε. Ε, λοιπόν, καιρός να πάψουμε!

Ανασφάλεια στον Ιστό

Τα πράγματα στο Διαδίκτυο δεν είναι τόσο αθώα όσο αρχικά δείχνουν. Οι «επιτήδριοι» εύκολα μπορούν να εκμεταλλευτούν τις όποιες αδυναμίες διακομιστών Web, πληκτρολογώντας απλά μερικές γραμμές σε ένα πρόγραμμα πλοήγησης!

ΣΤΙΣ ΑΡΧΕΣ ΤΗΣ ΔΕΚΑΕΤΙΑΣ ΤΟΥ '90 ο Tim Berners-Lee δημιούργησε το γνωστό σε όλους μας Παγκόσμιο Ιστό ή WWW (World Wide Web). Οι δυνατότητες που παρείχε η τεχνολογία που κρυβόταν πίσω από αυτόν αλλά και η δωρεάν φύση του συντέλεσαν στην ραγδαία ανάπτυξη και διάδοσή του, σε σχέση με τη ήδη δοκιμασμένο και ανταγωνιστικό Gopher. Από τότε έως σήμερα το Web έχει αλλάξει πολλά πρόσωπα, ωθώντας τις εταιρείες λογισμικού να αναπτύσσουν νέες τεχνολογίες και δυνατότητες, καθιστώντας το WWW την υπ' αριθμό ένα σε χρήση υπηρεσία. Την ίδια στιγμή αναδείχθηκε σε δημοφιλή στόχο επίθεσης για τους απανταχού cracker, οι οποίοι έσπευσαν να εκμεταλλευτούν τη μεγάλη διάδοση και την αποδοχή του από το ευρύ κοινό.

Σε γενικές γραμμές μπορούμε να πούμε ότι ένα σύγχρονο σύστημα εφαρμογών του Παγκόσμιου Ιστού (web application system) αποτελείται από τέσσερα βασικά μέρη. Κατ' αρχάς έχουμε το πρόγραμμα που τρέχει ο χρήστης, το οποίο αναλαμβάνει αφενός την αποστολή αιτήσεων προς τους διακομιστές (server) και αφετέρου τη λήψη απαντήσεων από αυτούς.

Τα προγράμματα που τρέχει ο χρήστης ονομάζονται πελάτες (clients) και ένα δημοφιλές παράδειγμα αποτελεί η εφαρμογή πλοήγησης ιστοσελίδων (browser). Ένα άλλο παράδειγμα είναι κάποιο πρόγραμμα αυτόματου κατεβάσματος δικτυακών τόπων (non-interactive web downloader).

Το δεύτερο μέρος ενός συστήματος εφαρμογών WEB είναι ο διακομιστής, ο οποίος διαχειρίζεται την κίνηση και τα ερωτήματα των πελατών. Στους πελάτες «σερβίρει» σελίδες HTML, έτσι ώστε αυτοί να τις εμφανίζουν στο χρήστη, να τις αποθηκεύουν στο δίσκο κ.ο.κ. Εσωτερικά, ένας διακομιστής ιστοσελίδων (Web server) επικοινωνεί με ποικίλες εφαρμογές, ανάλογα με τον τρόπο που έχει γίνει η εγκατάστασή του αλλά και το σύνολο των υπηρεσιών που έχει ρυθμιστεί να παρέχει. Μια τυπική εγκατάσταση περιέχει «πίσω» από τον Web server μια μεγάλη ποικιλία εφαρμογών, οι οποίες στην πλειονότητά τους είναι

υπεύθυνες για τη συλλογή και την αναζήτηση δεδομένων από βάσεις δεδομένων ή άλλα εξωτερικά αρχεία, όπως counter, mailing lists, forms, fora κ.ά. Η επικοινωνία του browser με τον Web server πραγματοποιείται μέσα από το URL (Uniform Resource Locator), τη «διεύθυνση» που πληκτρολογούμε στην αντίστοιχη μπάρα. Με τον τρόπο αυτό ο server μπορεί να επεξεργαστεί το ερώτημα του πελάτη και να αντιληφθεί πληροφορίες τις οποίες θα επιστρέψει στον browser. Ένα τυπικό παράδειγμα ερωτήματος είναι το παρακάτω:

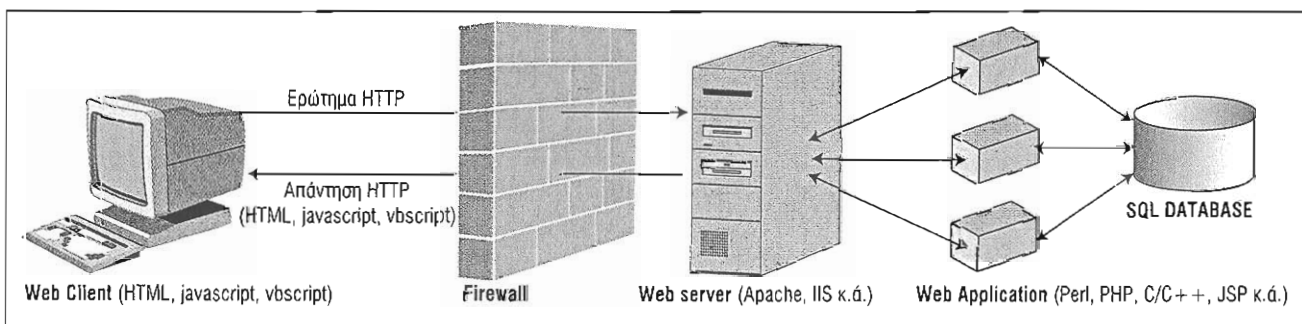
<http://10.0.0.1/books/display.asp?page=1&product=92>

Σε αυτό το ερώτημα διακρίνουμε το πρωτόκολλο (http), τη διεύθυνση του απομακρυσμένου server (10.0.0.1), τη διαδρομή ενός καταλόγου στο μηχανήμα που τον φιλοξενεί (/books), την εφαρμογή που πρόκειται να εκτελεστεί (display.asp) και την παράμετρο προς αυτή (?page=1&product=92).

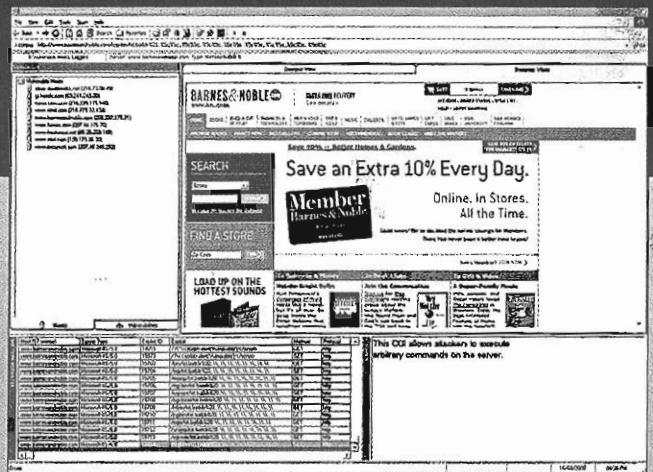
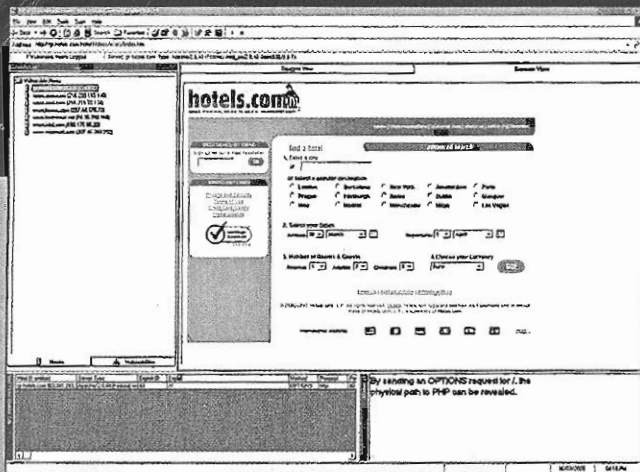
Το τρίτο βασικό μέρος ενός συστήματος εφαρμογών Web είναι η αριθμητική διεύθυνση IP (ή η μνημονική, από το DNS, που είναι το πιο σύνηθες), μαζί με τη διαδρομή (path) της εφαρμογής. Το τέταρτο συστατικό είναι οι παράμετροι που τροφοδοτούνται στην εφαρμογή.

ΚΙΝΔΥΝΟΙ. Κάθε τμήμα ενός URL κρύβει τις δικές του παγίδες. Το κομμάτι του IP και του path μπορεί να είναι ευάλωτο σε επιθέσεις unicode, double-decode και τροποποίησης των δικαιωμάτων χρήσης των αρχείων. Μια επίθεση αυτής της κατηγορίας μπορεί να μοιάζει με την επόμενη: www.example.com/scripts/%c0%af./winnt/system32/cmd.exe/?c+copy+winnt\system32\cmd.exe+inetpub\scripts

Μετά την πληκτρολόγηση ενός τέτοιου URL στην μπάρα διεύθυνσης του browser, το αρχείο cmd.exe –το κέλυφος γραμμής εντολών, command interpreter, των Windows 2000/2003/XP– θα αντιγραφεί αυτόματα μέσα στον κατάλογο inetpub\scripts, που είναι προσβάσιμος από το Web. Η εφαρμογή, στο



Σχηματική αναπαράσταση ενός σύγχρονου συστήματος εφαρμογών Web.



Το Web Hack Control Center είναι ένα εργαλείο για την αποκάλυψη δυνητικών προβλημάτων ασφαλείας διακομιστών ιστοσελίδων. Ακόμα και γνωστοί Web server ενδέχεται να έχουν σοβαρά προβλήματα, σε βαθμό που να επιτρέπουν την απομακρυσμένη εκτέλεση οποιασδήποτε εντολής.

Παράδειγμά μας το cmd.exe, εκτελείται από τον application server, ο οποίος ενδέχεται να αποδειχθεί ευάλωτος όσον αφορά στην εκτέλεση κώδικα που προέρχεται από φόρμες εισαγωγής δεδομένων ή από αρχεία που βρίσκονται στον server.

Σημειώστε, εξάλλου, ότι οι παράμετροι που περνούν σε μια εφαρμογή του application server, εάν δεν ελεγχθούν/επικυρωθούν κατάλληλα, είναι δυνατό να οδηγήσουν στην εκτέλεση παράτυπων λειτουργιών, παράλληλα με εκείνες που προβλέπονται. Μία επίθεση αυτής της κατηγορίας μπορεί να μοιάζει με την ακόλουθη: www.example2.com/cgi-in/news.cgi?story=10.txtlcp+/bin/sh+/usr/local/apache/cgi-bin/sh.cgi

Μετά την πληκτρολόγηση του URL το πρόγραμμα news.cgi θα δεχτεί την παράμετρο ?story=10.txtlcp+/bin/sh+/usr/local/apache/cgi-bin/sh.cgi. Επειδή το news.cgi δεν επικυρώνει σωστά τις παραμέτρους που του περνάμε, αφήνει το χαρακτήρα «|» να περάσει στην υπορουτίνα της Perl open(), με αποτέλεσμα την αντιγραφή του αρχείου /bin/sh (ο διερμηνευτής του κελύφους εντολών στα συστήματα Unix) στον κατάλογο /usr/local/apache/cgi-bin/ του απομακρυσμένου μηχανήματος. Έπειτα από αυτή την ενέργεια, το αρχείο sh.cgi θα είναι προσπελάσιμο από το Web, προσφέροντας στον επισκέπτη ένα παράθυρο γραμμής εντολών που δεν θα έπρεπε να έχει.

Αντίστοιχα, εάν μία παράμετρος χρησιμοποιηθεί κατάλληλα ως μέρος ενός ερωτήματος SQL και δεν επικυρωθεί σωστά από το διακομιστή, είναι δυνατόν να οδηγήσει σε εκτέλεση εντολών χρησιμοποιώντας εσωτερικές διαδικασίες της SQL, όπως η xp_cmdshell. Ιδού ένα παράδειγμα: www.example3.com/books/product.asp?id=5%01EXEC+master..xp_cmdshell+copy+\\winnt\system32\cmd.exe+inetpub\scripts

Μετά την εκτέλεση της εντολής το εκτελέσιμο αρχείο cmd.exe θα αντιγραφεί στον κατάλογο inetpub\scripts, που είναι προσβάσιμος από το Web.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ: WEB HACK CONTROL CENTER. Το Nikto είναι ένα από τα καλύτερα δωρεάν προγράμματα αναζήτησης κενών ασφαλείας σε έναν οποιονδήποτε Web server. Το πρόγραμμα τρέχει σε περιβάλλον Linux και Windows. Στα Windows θα πρέπει να υπάρχει εγκατεστημένη η γλώσσα προγραμματισμού Perl, την οποία μπορείτε να κατεβάσετε από το δικτυακό τόπο www.activestate.com/Products/ActivePerl

Το Nikto θεωρείται ένα από τα καλύτερα προγράμματα στην κατηγορία του. Είναι σε θέση να ελέγχει περισσότερα από 3.100 προβλήματα ασφαλείας, ενώ αναβαθμίζεται συχνά. Την εκδοχή Linux θα τη βρείτε και στη διανομή Operator, που συνοδεύει το περιοδικό. Επίσης μπορείτε να την κατεβάσετε από τη διεύθυνση <http://www.cirt.net/code/nikto.shtml>

Εναλλακτικά, εάν δεν θέσετε να μηλέξετε με τη γραμμή εντολών, μπορείτε να χρησιμοποιήσετε το εργαλείο Web Hack Control Center (www.ussysadmin.com/whcc/default.php, whcc-current.exe), προκειμένου να πραγματοποιήσετε ελέγχους ασφαλείας στο δικό σας δικτυακό τόπο.

ΕΓΩ, Ο
ΧΑΚΕΡ

ΑΦΙΕΡΩΜΑ | TROJAN HORSES & ROOTKITS

Φοβού τους Δοναούς!

Καθημερινά στο Internet γίνονται χιλιάδες επιθέσεις από cracker και «μολυσμένους» υπολογιστές, με θύματα τις περισσότερες φορές ανυποψίαστους χρήστες των chat room...

ΔΕΝ ΕΙΝΑΙ ΤΥΧΑΙΟ ΤΟ ΓΕΓΟΝΟΣ ότι οι cracker επιλέγουν τα θύματά τους από τα chat room. Όλα όσα ακολουθούν αποτελούν γνωστές πρακτικές για όλους όσοι δραστηριοποιούνται στο χώρο.

Κατ' αρχάς ο cracker φροντίζει ώστε να κερδίσει την εμπιστοσύνη του υποψήφιου θύματος, καταφεύγοντας σε τεχνικές social engineering. Για παράδειγμα, για να ανοίξει ευκολότερα συζήτηση, προσπαθεί να δείξει ότι έχει κάτι κοινό με το οιοινοί θύμα. Έτσι, προσποιείται ότι είναι του αντίθετου φύλλου ή μπαίνει σε δωμάτια με θέματα συζητήσεων τα αθλητικά ή τα βιβλία. Ίσως χρειαστεί αρκετός χρόνος για να κερδίσει την εμπιστοσύνη κάποιου, όταν όμως το πετύχει, έχει πετύχει την πρώτη σημαντική μάχη!

Αργότερα, σε φαινομενικά ανυποψίαστο χρόνο, ο cracker θα στείλει στο θύμα ένα αρχείο. Στην ερώτηση «τι είναι αυτό που μου στέλνεις;», θα δώσει ακριβώς την απάντηση που ο άλλος θέλει να ακούσει. Θα πει, για παράδειγμα, ότι πρόκειται για κάποιο screen saver με την αγαπημένη του ομάδα, ότι είναι ένας client του Amazon που κατεβάζει αυτόματα πληροφορίες για νέες κυκλοφορίες βιβλίων και κριτικές ή ότι πρόκειται για ένα εργαλείο Peer-to-Peer, με το οποίο μπορεί να κατεβάζει άνετα αρχεία MP3, χωρίς να είναι δυνατό να εντοπιστεί από τρίτους. Ο cracker στέλνει το αρχείο με e-mail, FTP, DCC¹ ή κάποιοι άλλοι τρόποι.

Όταν το θύμα λάβει το αρχείο και επιχειρήσει να το εκτελέσει, προς μεγάλη του απογοήτευση θα λάβει ένα μήνυμα λάθους: Το πρόγραμμα θα παραπονεθεί για κάποια βιβλιοθήκη που λείπει και θα ενημερώσει ότι η εγκατάσταση δεν μπορεί να προχωρήσει. Και όμως, κρυφίως θα έχει ήδη εγκατασταθεί. Ναι, είναι αυτό που μαντέψατε. Στην πραγματικότητα, το πρόγραμμα που ο cracker κατάφερε να «φυτέψει» στο μηχάνημα του θύματος είναι ένας δούρειος ίππος (trojan horse). Άλλη μια φορά, λοιπόν, ο δούρειος ίππος κατορθώνει να περάσει μέσα από τα τείχη της Τροίας, που στην περίπτωση μας «υλοποιούνται» από το application firewall. (Είναι εκπληκτικό το γεγονός ότι αρκετοί χρήστες δεν έχουν καν firewall στο μηχάνημά τους!)

Σκοπός κάθε trojan είναι ο απομακρυσμένος έλεγχος. Τα προγράμματα της κατηγορίας λειτουργούν ως διακομιστές, επιτρέποντας σε έναν απομακρυσμένο χρήστη (τον cracker) να ελέγξει τον υπολογιστή του θύματος. Θα σκεφτείτε εδώ ότι, παρουσία ενός firewall, οποιοδήποτε trojan θα αδυνατεί να επικοινωνήσει με τον έξω κόσμο, επομένως δεν θα μπορεί να προκαλέσει σοβαρή ζημιά. Αυτό είναι αληθές και ταυτόχρονα ψευδές και εξαρτάται αφενός από το firewall, αφετέρου από τον ίδιο το χρήστη. Για παράδειγμα, το firewall που έρχεται με το SP2 των Windows

Χτύπημα στη ρίζα!

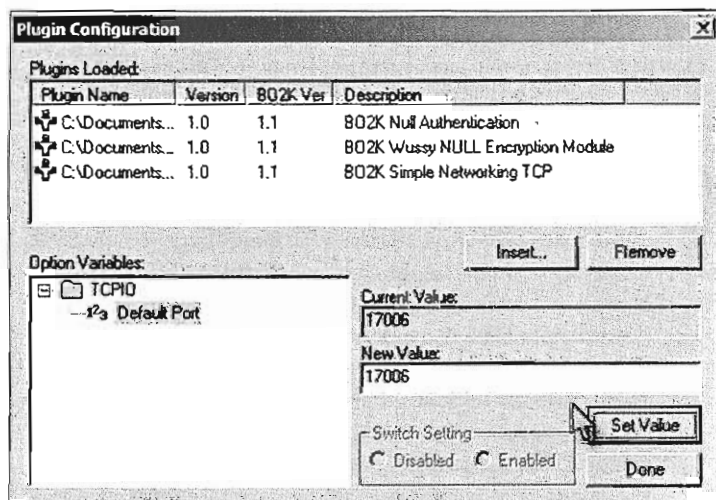
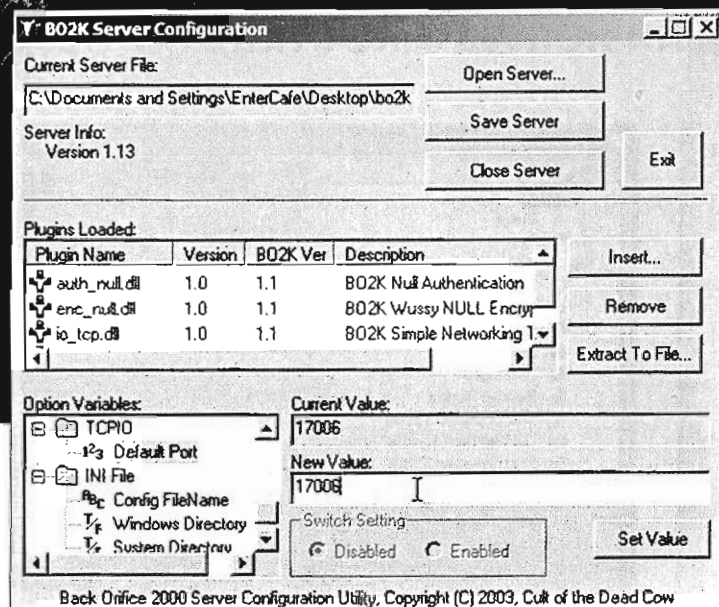
Μια εξελιγμένη μορφή Remote Administration Trojan αποτελούν τα λεγόμενα rootkit. Πρόκειται για ένα σετ εργαλείων που εκμεταλλεύεται ο εισβολέας, αφού αποκτήσει πρόσβαση στο μηχάνημα του θύματος. Ο σκοπός ενός rootkit είναι να βοηθήσει τον cracker ώστε να δρα ανενόχλητος, χωρίς να γίνεται αντιληπτός — ακόμα και από το διαχειριστή του συστήματος. Για παράδειγμα, τα πρώτα rootkit για Unix αντικαθιστούσαν τα εργαλεία «ps», «netstat» και «w». Τα νέα εργαλεία είχαν το ίδιο όνομα και την ίδια θέση στο σύστημα αρχείων, λειτουργούσαν όπως και τα αντίστοιχα νομότυπα, αλλά έκρυβαν την παρουσία του cracker (w), όπως και τις δραστηριότητές του (ps, netstat).

Τα σύγχρονα rootkit απευθύνονται τόσο στα Windows όσο και σε διάφορα «UNIXοειδή» λειτουργικά, όπως είναι το Linux και το Solaris. Συχνά περιλαμβάνουν κάποιο εργαλείο για την υποκλήση δεδομένων από τερματικά, δικτυακές συνδέσεις — ακόμη και από το πληκτρολόγιο. Επίσης, ένα rootkit περιέχει εργαλεία για τη διευκόλυνση της εισόδου του cracker στο σύστημα. Για παράδειγμα, με το που στείλεται ο τελευταίος σύνδεση σε συγκεκριμένη θύρα (port), το rootkit του προσφέρει απομακρυσμένη πρόσβαση σε ένα κέλυφος εντολών (command shell) του συστήματος.

Τα rootkit χωρίζονται σε δύο μεγάλες κατηγορίες: σε αυτά που λειτουργούν σε επίπεδο πυρήνα λειτουργικού συστήματος (kernel level) και σε εκείνα που λειτουργούν σε επίπεδο εφαρμογών (application level). Ένα kernel level rootkit αντικαθιστά μέρος του πυρήνα, με απώτερο σκοπό τη διευκόλυνση αλλήλ και την κάλυψη του cracker. Στο Linux, για παράδειγμα, ένα rootkit είναι πιθανό να έχει τη μορφή δυναμικού αρθρώματος (loadable kernel module). Μια κοινή πρακτική των rootkit του είδους είναι να αντικαθιστούν τις κλήσεις προς το σύστημα (system calls) με νέες, οι οποίες δεν φανερώνουν τις δραστηριότητες του επιτιθέμενου. Τα application level rootkit, από την άλλη, τροποποιούν ή αντικαθιστούν ήδη υπάρχοντα εκτελέσιμα αρχεία.

XP δεν ελέγχει καθόλου την εξερχόμενη (outbound) κυκλοφορία, επομένως το όποιο trojan θα δρα ανενόχλητο. Ένα καλύτερο firewall ελέγχει την εξερχόμενη κυκλοφορία. Επιπρόσθετα, με το που θα αντιληφθεί ότι κάποιο άγνωστο πρόγραμμα επιχειρεί να συνδεθεί στο δίκτυο, θα το εμποδίσει ενημερώνοντας

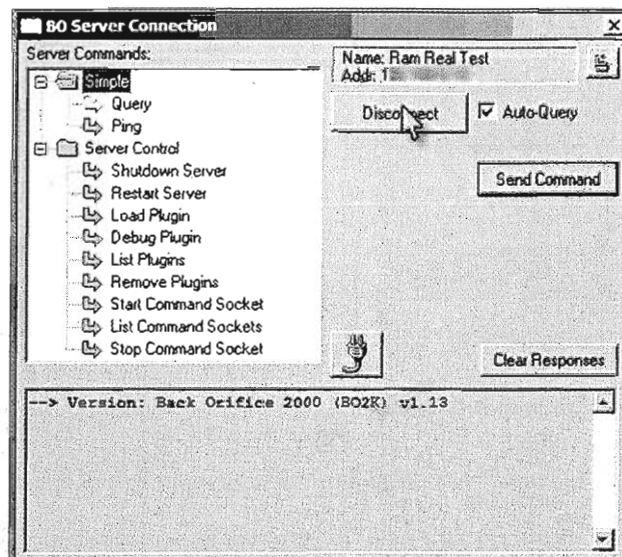
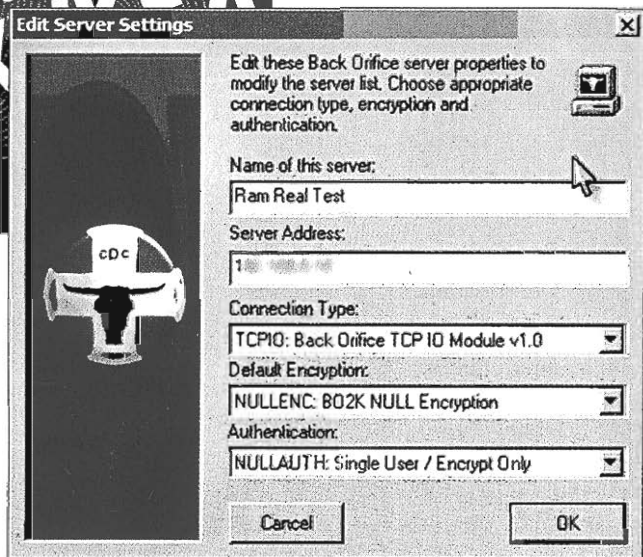
1. Πρόκειται για ένα πρωτόκολλο ανταλλαγής αρχείων στο δίκτυο IRC και από τους instant messenger, που χρησιμοποιεί απευθείας συνδέσεις TCP μεταξύ των μηχανημάτων.



Αφού φορτώσουμε τα απαραίτητα plug-in στον client και στον server του Back Office, ορίζουμε την προκαθορισμένη θύρα επικοινωνίας TCP, τόσο στον server όσο και στον client.

σχετικά το χρήστη, ο οποίος καλείται να αποφασίσει για το αν θα επιτρέψει στο πρόγραμμα τη σύνδεση ή όχι. Εάν είναι γνώστης ή/και υποψιασμένος θα του την απαγορεύσει. Τέλος, κάποιοι χρήστες βρίσκουν ενοχλητικά τα μηνύματα εν είδει pop up των firewall, οπότε σπεύδουν και απενεργοποιούν τους σχετικούς ελέγχους. Μέγα λάθος! Τα trojan horse μπορούν να χωριστούν σε πέντε μεγάλες κατηγορίες.

- **Remote Administration Trojans (RATs).** Πρόκειται για την πλέον διαδεδομένη κατηγορία trojan. Οι cracker τα προτιμούν, αφού προσφέρουν πληθώρα δυνατοτήτων και την ίδια στιγμή είναι πανεύκολα στη χρήση. Ένα RAT αποτελείται από δύο μέρη, τον client και τον server. Ο τελευταίος εγκαθίσταται στο μηχάνημα του θύματος και τον client τον χρησιμοποιεί ο cracker, προκειμένου να ελέγξει τον server. Άπαξ και εγκατασταθεί, ο server αντιγράφει εαυτόν σε έναν «αθώο» φάκελο του δίσκου και μετανομάζει το αντίστοιχο αρχείο, ώστε να μην κινεί υποψίες. Επίσης, πραγματοποιεί τροποποιήσεις στο μητρώο (registry) των Windows, ώστε να είναι δυνατή η αυτόματη και –το σημαντικότερο– σόρατη ενεργοποίησή του, κατά την εκκίνηση του λειτουργικού. Εξάλλου, η επικοινωνία του client με τον server είναι κρυπτογραφημένη, γεγονός που καθιστά εξαιρετικά δύσκολη την ανάλυση της επίθεσης, ακόμα και από έναν έμπειρο χρήστη. Τα πιο



Απαξ και εγκαθιδρυθεί η επικοινωνία μεταξύ πελάτη και εξυπηρέτη του Back Orifice, το απομακρυσμένο μηχανήμα είναι στο έλεος του επιτιθέμενου. Μετάξυ άλλων εντολών που μπορεί να εκτελέσει, συμπεριλαμβάνονται η επανεκκίνηση και ο τερματισμός (shutdown).

γνωστό RAT είναι τα NetBus, BO2K και το Sub7. Σημειώστε, τέλος, ότι ο server ενός RAT είναι δυνατόν να βρίσκεται προσαρμοσμένος σε κάποια τρίτη, καθ' όλα «νομότυπη» εφαρμογή, και να εγκατασταθεί μέσω αυτής. Τα περισσότερα προγράμματα antivirus θα αντιληφθούν έγκαιρα την παρουσία του trojan, θα εμποδίσουν την εγκατάστασή του και θα ενημερώσουν σχετικά το χρήστη. Αρκεί βέβαια εκείνος να μην έχει απενεργοποιήσει τη σχετική δυνατότητα...

- **Password Trojans.** Όταν εκτελείται ένα trojan αυτής της κατηγορίας αναζητά στον υπολογιστή συνθηματικά πάσης φύσεως (για λογαριασμούς e-mail, ISP κ.ά.), για λογαριασμούς πιστωτικών καρτών και άλλες «ευσταθές» πληροφορίες. Τα ευρήματά του τα αποστέλλει κρυφώς, με e-mail, στη διεύθυνση που έχει ορίσει ο cracker.

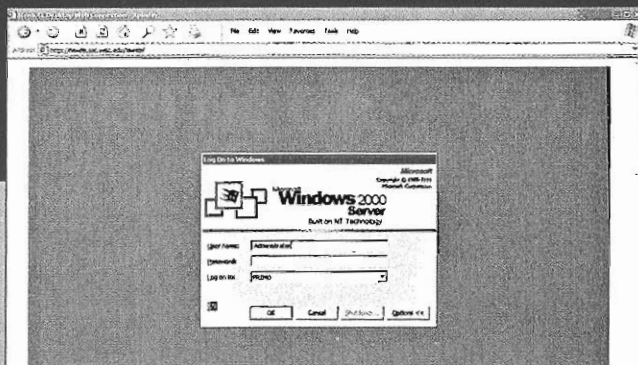
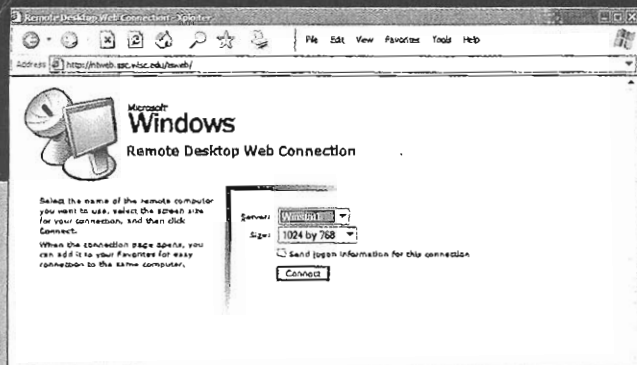
- **Privileges-Elevating Trojans.** Σκοπός ενός τέτοιου trojan είναι να ξεγελάσει το διαχειριστή ενός συστήματος που θα το εκτελέσει, επιδεικνύοντας αναμενόμενη συμπεριφορά. Στον κόσμο των Windows, τα trojan της κατηγορίας έχουν την κατάληξη .com, ώστε να έχουν μεγαλύτερη προτεραιότητα εκτέλεσης από το αντίστοιχο, νομότυπο .exe. Απαξ και εκτελεστεί ένα privileges-elevating trojan, δίνει αυτομάτως περισσότερα δικαιώματα χρήσης στον cracker ή προετοιμάζει κατάλληλα το έδαφος για μια επικείμενη επίθεση.

- **Keylogger Trojan.** Σκοπός ενός τέτοιου trojan είναι να καταγράφει οτιδήποτε πληκτρολογεί το θύμα, συμπεριλαμβανομένων, φυσικά, και των password που δεν φαίνονται στην οθόνη. Όλα αυτά τα στοιχεία αποθηκεύονται σε ένα κρυφό αρχείο. Ορισμένα keylogger «διαβάζουν» τους τίτλους των παραθύρων, ψάχνοντας για φράσεις όπως «Enter password», «Authorization required» κ.ά. Εάν εντοπίσουν κάτι σχετικό, αρχίζουν την καταγραφή της πληκτρολόγησης. Αργότερα αποστέλλουν στον cracker τα ευρήματά τους, π.χ., μέσω e-mail.

- **Destructive Trojans ή Logic Bombs.** Πρόκειται για τα πλέον καταστροφικά trojan, τα οποία μάλιστα δεν αφήνουν

κανένα περιθώριο αντίδρασης στο άτυχό θύμα. Με την εκτέλεσή τους διαγράφουν τα πάντα από το σκληρό δίσκο, μέσα σε ελάχιστα δευτερόλεπτα. Οι ρουτίνες τους είναι έτσι σχεδιασμένες, ώστε να καταστρέφουν τα δεδομένα όσο το δυνατόν ταχύτερα και αποτελεσματικότερα. Συνήθως έχουν στόχο κρίσιμα αρχεία, την καταστροφή boot record, καταμήσεων (partitions) και πινάκων εκχώρησης αρχείων (file allocation tables). Ορισμένα άλλα trojan της κατηγορίας δεν διαγράφουν, αλλά προκαλούν τρομερή αναστάτωση. Για παράδειγμα, μετονομάζουν μαζικά υπάρχοντα αρχεία, δημιουργούν νέα με τυχαίο περιεχόμενο, φτιάχνουν φακέλους και υποφάκελους με μεγάλο «βάθος», γεμίζουν καταμήσεις και μνήμη με άχρηστες πληροφορίες κ.ο.κ. Ως αποτέλεσμα, το σύστημα οδηγείται σύντομα σε πλήρη κατάρρευση.

72



Επιλογή μηχανήματος ενός LAN και εισαγωγή στα Windows 2000, μέσα από τον Web browser! Ευτυχώς, στην περίπτωση αυτή ο άγνωστος διαχειριστής ήταν προσεκτικός και δεν άφησε το προκαθορισμένο password του υπερχρήστη.

και «site:borland.com Delphi».

filetype: Το Google ψάχνει για κείμενα με την κατάληξη που ακολουθεί το συγκεκριμένο τελεστή, π.χ., «filetype:doc reykjavik».

link: Το Google αναζητεί συνδέσεις υπερκειμένου που περιέχουν ένα συγκεκριμένο όρο, π.χ., «link:hack».

cache: Όταν το site που ψάχνουμε δεν είναι διαθέσιμο για κάποιο λόγο, με τη χρήση του συγκεκριμένου τελεστή το Google ψάχνει στη βάση δεδομένων όπου καταχωρίζει τις σελίδες από πρόσφατες αναζητήσεις.

intitle: Καθοδηγεί το Google να αναζητήσει σελίδες με συγκεκριμένη λέξη στον τίτλο τους, π.χ., «intitle:warp».

allintitle: Εάν ψάχνουμε σελίδες με περισσότερες από μία συγκεκριμένες λέξεις στον τίτλο τους, χρησιμοποιούμε τον εν λόγω χειριστή, π.χ., «allintitle: warp nacelle».

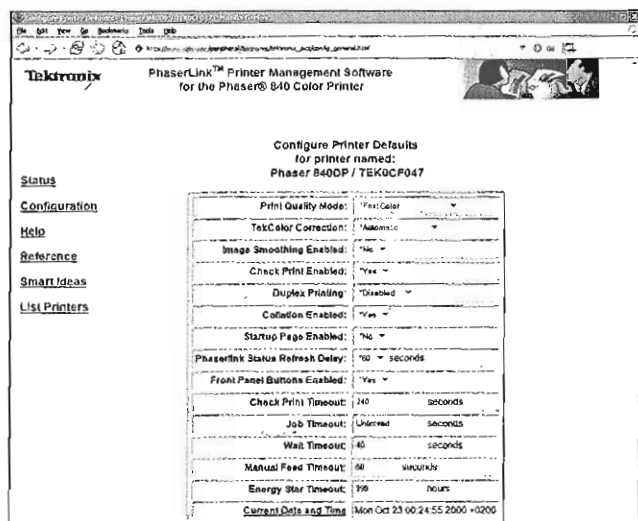
inurl: Καθοδηγεί το Google να επιστρέψει site με συγκεκριμένη λέξη στο URL τους.

allinurl: Όμοια, όταν ψάχνουμε site με περισσότερες από μία συγκεκριμένες λέξεις στο URL τους, χρησιμοποιούμε το χειριστή allinurl, π.χ., «allinurl:system hack».

ΕΚΜΕΤΑΛΛΕΥΣΗ. Όλοι οι προηγούμενοι χειριστές, σε συνδυασμό με τις βασικές τεχνικές αναζήτησης, καθιστούν το Google ένα πανίσχυρο εργαλείο συλλογής πληροφοριών και αναζήτησης ευπαθειών ασφαλείας. Πολλά site, για παράδειγμα, επιτρέπουν σε οποιονδήποτε να βλέπει τα περιεχόμενα του βασικού καταλόγου του σχετικού διακομιστή ιστοσελίδων. Αυτό συμβαίνει αλλιώς ηθελημένα, αλλιώς εξαιτίας φτωχής ρύθμισης του Web server. Έτσι, πληκτρολογώντας «intitle:index.of "parent directory"» στη θυρίδα αναζήτησης του Google, παίρνουμε πάνω από 15 εκατομμύρια αποτελέσματα. Επίσης, δίνοντας «intitle:index.of name last modified size» το Google επιστρέφει γύρω στα 13 εκατομμύρια αποτελέσματα.

Προφανώς, με τους κατάλληλους συνδυασμούς, το Google μπορεί να δώσει συγκεκριμένα αρχεία που περιέχονται σε καταλόγους ή λίστες καταλόγων. Έτσι, διαπιστώνουμε, π.χ., ότι ακόμα και ένας τόπος που χρησιμοποιεί ασφαλείς συνδέσεις (HTTPS), δεν σημαίνει ότι είναι πραγματικά ασφαλής!

Ακολουθώντας παρόμοιες τεχνικές, πληκτρολογώντας «VNC inurl:5800» το Google επιστρέφει URL που καταλήγουν σε διακομιστές οι οποίοι τρέχουν τη γνωστή εφαρμογή απομακρυσμένου ελέγχου VNC (βλ., π.χ., www.tightvnc.com). Στο ίδιο μοτίβο, γράφοντας «intitle:Remote.Desktop.Web.Connection



Ένας άλλος, περισσότερο απρόσεκτος διαχειριστής, έχει εκτεθειμένη την ιστοσελίδα ρυθμίσεων ενός δικτυακού εκτυπωτή σε όλους τους χρήστες του Internet!

inurl:tsweb» παίρνουμε μία λίστα με server που έχουν ενεργοποιημένη την υπηρεσία απομακρυσμένης σύνδεσης στο desktop των Windows. Ευτυχώς, στις περισσότερες των περιπτώσεων ο διαχειριστής του απομακρυσμένου συστήματος μεριμνά ώστε να ζητείται όνομα χρήστη και συνθηματικό για τη σύνδεση ή έστω έχει αλλάξει τις προκαθορισμένες τιμές.

Εξάλλου, στο Internet δεν βρίσκονται «συνδεδεμένοι» μόνο υπολογιστές αλλά και πλήθος δικτυακών συσκευών. Όπως σωστά θα μαντέψατε, πολλές από αυτές είναι αφελώς ρυθμισμένες, με αποτέλεσμα να έχει πρόσβαση σε αυτές οποιοσδήποτε, από οποιοδήποτε μέρος του πλανήτη. Είναι δυνατόν, για παράδειγμα, να βλέπουμε μέσα από μία κάμερα «ασφαλείας» ενός ιδιόκτητου χώρου, ακόμα και να την ελέγχουμε. Όμοια, ένας διαχειριστής δικτύου που δεν λαμβάνει υπόψη βασικές αρχές ασφαλείας, χωρίς να το γνωρίζει ενδέχεται να έχει δώσει ανεπιόριστη πρόσβαση στο δικτυακό εκτυπωτή ενός γραφείου. Ψάξτε για τους αντίστοιχους κωδικούς πρόσβασης; Συχνά δεν ζητούνται καν! Για του λόγου το αληθές, δοκιμάστε τις επόμενες αναζητήσεις στο Google:

```
inurl:"view/index.shtml"
inurl:"axis-cgi/mjpg"
inurl:"axis-cgi/jpg"
inurl:"ViewerFrame?Mode=Refresh"
```


ΕΓΩ, Ο
ΧΥΚΕΡ

ΑΦΙΕΡΩΜΑ | ΑΝΩΝΥΜΙΑ

Αόρατο surfing & e-mailing

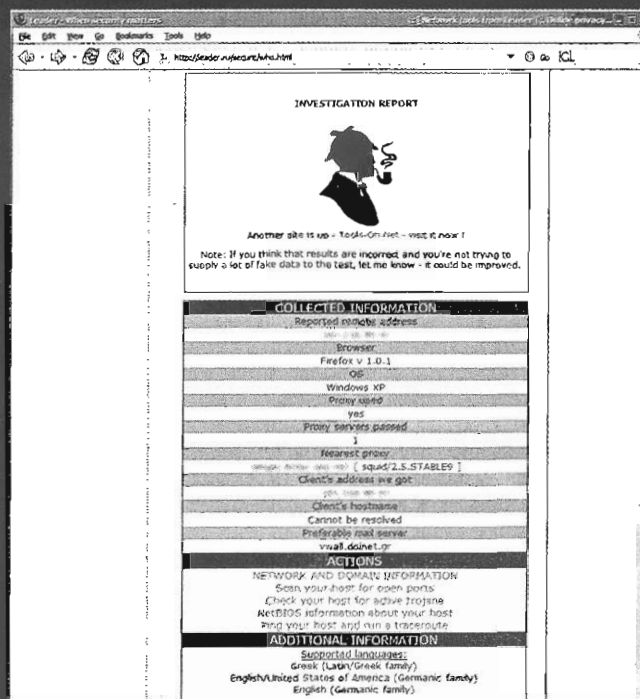
Αναρωτηθήκατε ποτέ, καθώς περιδιαβαίνετε ανυποψίαστοι το Διαδίκτυο, τι είδους πληροφορίες συλλέγουν για εσάς οι δικτυακοί τόποι που επισκέπτεστε; Αλήθεια, θελήσατε ποτέ να στείλετε ένα πραγματικά ανώνυμο e-mail;

ΕΝΑΣ ΤΥΠΙΚΟΣ ΔΙΚΤΥΑΚΟΣ ΤΟΠΟΣ συγκεντρώνει βασικές πληροφορίες, όπως η έκδοση και ο τύπος του browser που χρησιμοποιούμε, η προεπιλεγμένη γλώσσα, οι τύποι MIME (Multipurpose Internet Mail Extensions) που χρησιμοποιεί ο browser κ.ά. Τα στοιχεία αυτά συχνά αποθηκεύονται για στατιστικούς λόγους. Με βάση αυτά, ο διαχειριστής του εκάστοτε τόπου είναι σε θέση να παίρνει αποφάσεις που σχετίζονται με τον κώδικα των ιστοσελίδων και τις υπηρεσίες που θα μπορούσε να προσφέρει σε σχέση με το διαθέσιμο bandwidth. Δυστυχώς, υπάρχουν δικτυακοί τόποι που συλλέγουν και άλλες πληροφορίες, όπως η διεύθυνση IP του μηχανήματός μας, η οποία προσδιορίζει την τοποθεσία από όπου έχουμε συνδεθεί. Άλλες φορές, διάφοροι τόποι εκμεταλλεύονται γνωστές αδυναμίες των browser, προκειμένου να συγκεντρώσουν και άλλες πολύτιμες πληροφορίες, πάντα χωρίς τη συγκατάθεσή μας και ενίοτε εις βάρος μας.

Εξάλλου, το δημοφιλές IRC (Internet Relay Chat) και τα πλείστα όσα προγράμματα άμεσης επικοινωνίας (messenger) που κυκλοφορούν ευρέως, επίσης προδίδουν το IP μας. Στο IRC, συγκεκριμένα, εάν γνωστοποιηθεί σε κάποιον κακόβουλο χρήστη το IP μας, είναι πολύ πιθανόν να πέσουμε θύμα επίθεσης «διδασκασίας». Ακόμα χειρότερα, το μηχανήμα μας ενδέχεται να χρησιμοποιηθεί ως εφαλτήριο για τη διάπραξη παράνομων ενεργειών. Εκτός από τις επιθέσεις αυτής της μορφής, είναι πιθανόν να «τσιπηθούμε» κάποιο virus ή worm, είτε μέσα από το IRC είτε από κάποια σελίδα Web.

Η χρήση ενός κολληρυθμισμένου firewall προσφέρει αρκετή ασφάλεια απέναντι σε επιθέσεις του είδους, ωστόσο το firewall, εκτός από ότι δεν μας παρέχουν ανωνυμία, συχνά δεν επαρκούν ούτε για να μας προστατεύσουν από επιθέσεις ανίχνευσης «ανοιχτών» υπηρεσιών. Επιπρόσθετα, αρκετά software firewall έχουν αδυναμίες. Εάν κάποιος γνωρίζει το IP μας, χρησιμοποιώντας εργαλεία όπως τα hping2 και nmap (έρχονται με τη διανομή Operator Linux που θα βρείτε στο CD μας), θα είναι σε θέση να εντοπίσει τέτοιες αδυναμίες, να «διαπεράσει» το firewall και να συλλέξει πληροφορίες, που αργότερα θα αξιοποιήσει προκειμένου να διεισδύσει στο μηχανήμα μας.

Στις παραπάνω περιπτώσεις, ο επιτιθέμενος πρέπει να γνωρίζει το IP μας. Επομένως, εμείς από την πλευρά μας οφείλουμε να το κρύβουμε. Το ίδιο προτείνεται να κάνουμε και με άλλες πληροφορίες που μας αφορούν, αφού, αν πέσουν σε λάθος χέρια, είναι δυνατόν να πουληθούν σε τρίτους (π.χ., spammer) ή να χρησιμοποιηθούν από κάποιον που

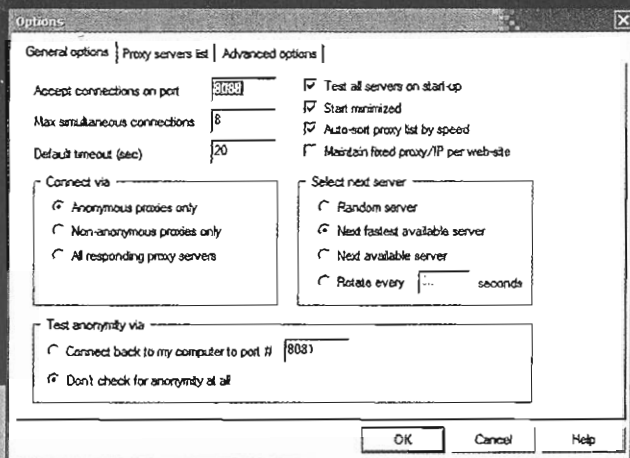


Κατά τις δικτυακές μας περιηγήσεις, πολλοί δικτυακοί τόποι αποθηκεύουν πλήθος στοιχείων που μαρτυρούν την πραγματική μας ταυτότητα, τον browser που χρησιμοποιούμε, ακόμα και τις συνήθειές μας.

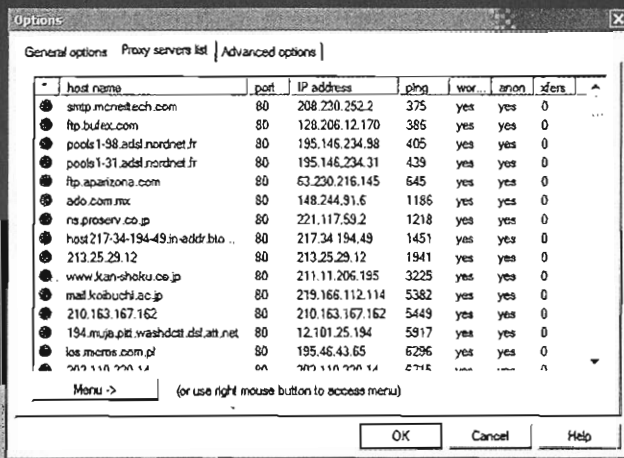
θα οικειοποιηθεί την ταυτότητά μας (identity theft).

Πριν εξετάσουμε το θέμα της ανωνυμίας από την πρακτική του σκοπιά —θα ασχοληθούμε με το ανώνυμο surfing—, καλό είναι να έχουμε υπόψη ότι η απόλυτη ανωνυμία σε ένα μέσο όπως το Διαδίκτυο αποτελεί ουτοπία.

ΑΝΩΝΥΜΟΙ ΔΙΑΚΟΜΙΣΤΕΣ ΜΕΣΟΛΑΒΗΣΗΣ. Ένας διακομιστής μεσολάβησης (proxy server) είναι ένα μηχανήμα που ενεργεί ως μεσάζοντας μεταξύ ενός υπολογιστή και άλλων μηχανημάτων στο Διαδίκτυο, εξασφαλίζοντας έως ένα βαθμό την ασφάλεια και τον έλεγχο της πρόσβασης, μέσω κατάλληλων φίλτρων. Επιπρόσθετα, ένας proxy αποθηκεύει προσωρινά τα δεδομένα που ζήτησε ένας πελάτης (client, π.χ., ο browser ενός PC που χρησιμοποιεί τον εν λόγω proxy) από κάποιο δικτυακό τόπο, έτσι ώστε την επόμενη φορά που θα ζητηθούν τα ίδια δεδομένα από κάποιον άλλο πελάτη να του επιστραφούν ταχύτερα από τον ίδιο τον proxy. Κάθε ISP συνήθως προσφέρει τουλάχιστον έναν proxy, αλλά μόνο στους συνδρομητές του. Επιπρόσθετα, οι proxy των ISP δεν εξασφαλίζουν



Αφ'όντας την επιλογή «Maintain fixed proxy/IP per web-site» άευκή, το Multiproxy αλλάζει τους διακομιστές μεσολάβησης ακόμα και κατά το φόρτωμα διαφορετικών στοιχείων του ίδιου δικτυακού τόπου.



Λίστα με ανώνυμους διακομιστές μεσολάβησης που χρησιμοποιεί το Multiproxy. Κατά τις περιηγήσεις μας στο Web τους εναλλάσσει διαρκώς, προσφέροντάς μας μέγιστη ανωνυμία.

ανωνυμία. Στο Internet, όμως, υπάρχουν λίστες με δεκάδες ή και εκατοντάδες ανώνυμους proxy, που μπορούν να χρησιμοποιηθούν από οποιοδήποτε μηχανήμα, από οποιοδήποτε μέρος του πλανήτη. Υπάρχουν μάλιστα και δικτυακοί τόποι τους οποίους μπορεί οποιοσδήποτε να επισκεφθεί και να κατεβάσει τη δική του λίστα με proxy server.

Ενδεικτικά μπορείτε να ξεκινήσετε την ανασήτηση ανώνυμου proxy από τις ακόλουθες διευθύνσεις:

www.proxyblind.org/list.shtml#1

www.publicproxyservers.com/index.html

www.proxys4all.com

Καλό θα ήταν, για να μη καθείτε σε κατεβαστά με proxy, να αφιερώσετε λίγο χρόνο στη δημιουργία της προσωπικής σας λίστας, που θα συμπεριλαμβάνει γρήγορους proxy με όσο το δυνατόν χαμηλότερες τιμές στην απόκριση (ping time). Ένα άλλο χαρακτηριστικό που θα πρέπει να προσέξετε είναι να μην παρέχουν οι proxy σας ευαίσθητα δεδομένα στους δικτυακούς τόπους που επισκέπτεστε, μέσω των επικεφαλίδων των αιτήσεων (requests). Ένας καλός ανώνυμος proxy θα πρέπει να φιλτράρει τουλάχιστον τα παρακάτω πεδία:

REMOTE HOST: Το IP του υπολογιστή ή του proxy που χρησιμοποιούμε.

HTTP_X_FORWARDED_FOR: Μερικές φορές ο proxy μεταφέρει τη διεύθυνσή μας μέσα από αυτό το πεδίο.

HTTP_USER_AGENT: Αν και δεν κρίνεται ιδιαίτερα επικίνδυνο, αυτό το πεδίο φέρει την έκδοση του browser.

FORWARDED: Αυτό το πεδίο αποκαλύπτει το γεγονός ότι χρησιμοποιούμε proxy server.

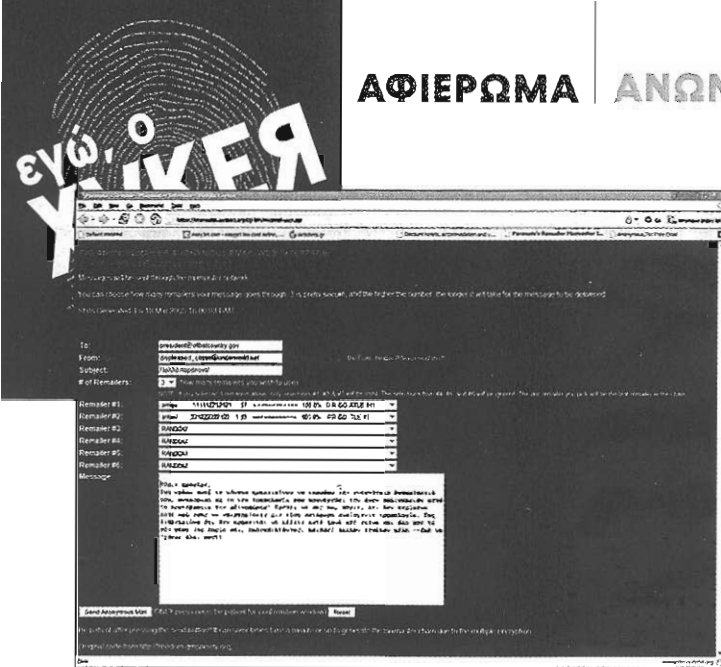
HTTP_VIA: Όμοιο με το προηγούμενο πεδίο.

HTTP_FROM: Μέσω από αυτό το πεδίο είναι δυνατόν να γίνει γνωστή η ηλεκτρονική σας διεύθυνση.

Ο καθορισμός ενός proxy server γίνεται ξεχωριστά σε καθένα από τα προγράμματα-πελάτες που χρησιμοποιούμε (π.χ., browser, FTP ή P2P client κ.λπ.). Για παράδειγμα, στο Mozilla Firefox δίνουμε <Tools→Options→General→Connection Settings...→Manual proxy configuration> και πληκτρολογούμε τη διεύθυνση IP και τη θύρα (port) του επιθυμητού proxy τουλάχιστον στη θυρίδα ονόματι «HTTP Proxy». Εάν επιθυμούμε τη χρήση του proxy για κάθε πρωτόκολλο, πληκτρολο-

γούμε τη διεύθυνσή του, σε ένα οποιοδήποτε πεδίο, και μετά τσεκάρουμε το «Use the same proxy for all protocols». Εξάλλου, εάν για έναν ή περισσότερους δικτυακούς τόπους δεν επιθυμούμε τη μεσολάβηση του proxy, καθορίζουμε τις σχετικές εξαιρέσεις στη θυρίδα «No Proxy for». Τέλος, επικυρώνουμε τις αλλαγές με κλικ στο «OK» (δεν απαιτείται επανεκκίνηση του προγράμματος).

Στο URL <http://leader.ru/secure/who.html> έχετε την ευκαιρία να κάνετε έναν έλεγχο, έτσι ώστε να δείτε μερικές από τις πληροφορίες που είναι δυνατόν να συλλέξει ένας τόπος κατά την επίσκεψή σας. Παράλληλα, μπορείτε να ελέγξετε και τις δυνατότητες που σας παρέχει ο proxy server που έχετε ήδη επιλέξει.



Αποστολή ανώνυμου μηνύματος από web based remailer. Για περισσότερη ασφάλεια χρησιμοποιούνται περισσότεροι του ενός remailer.

ΑΝΩΝΥΜΟ E-MAILING. Όποτε στέλνουμε μία επιστολή με το παραδοσιακό ταχυδρομείο, στην πραγματικότητα δεν υπάρχει κάτι που θα μπορούσε να αποτρέψει έναν αδιάκριτο υπόδηλο κάποιου ταχυδρομείου να ανοίξει την αλληλογραφία μας, να τη διαβάσει, να βάλει την επιστολή σε έναν άλλο φάκελο και να τη στείλει στον προορισμό της σαν να μην συνέβη τίποτα. Με το ηλεκτρονικό ταχυδρομείο τα πράγματα είναι ακόμα χειρότερα, αφού συχνά διατηρείται ένα αντίγραφο του e-mail

σε κάθε διακομιστή που παρεμβάλλεται μεταξύ του μηχανήματός μας και εκείνου του τελικού παραλήπτη. Ακόμα και η κρυπτογραφία —υποθέτουμε ότι έχουμε πείσει τους ανθρώπους με τους οποίους αλληλογραφούμε για την αξία της— δεν προσφέρει απόλυτη προστασία. Ένας άλλος κίνδυνος είναι οι spammer ή όλοι όσοι τους πωλούν στοιχεία. Κανείς δεν μπορεί να μας διαβεβαιώσει ότι κάποιος διαχειριστής ενός mail server δεν συλλέγει έγκυρες ηλεκτρονικές διευθύνσεις, τις οποίες... μοσχοπουλά σε κάθε ενδιαφερόμενο. Εδώ που τα λέμε, βέβαια, όλα τα προηγούμενα μάλλον αγγίζουν τα όρια της παράνοιας. Πράγματι, πολλές φορές δεν αξίζει να μπαίνουμε σε κόπο και μπελάδες, μόνο και μόνο για να διασκεδάσουμε τις όποιες (κρυφές) ανησυχίες μας. Σκεφτείτε, όμως, ότι από καιρού εις καιρόν έχουμε πάντα ανάγκη για ένα πραγματικά ανώνυμο σύστημα ηλεκτρονικής αλληλογραφίας. Κάτι τέτοιο συμβαίνει, π.χ., όταν θέλουμε να γράψουμε μία οξεία κριτική προς κάποιο φορέα, αλλά ταυτόχρονα επιθυμούμε να προστατέψουμε το —για πολλούς δημοκρατικό— δικαίωμα της ανωνυμίας. Πολλοί άνθρωποι πιστεύουν ότι τα δωρεάν web mail τους εξασφαλίζουν την ανωνυμία που χρειάζονται. Αυτό είναι αληθές και ταυτόχρονα ψευδές. Είναι αληθές, όταν, π.χ., γράφουμε σε μία δικτυακή υπηρεσία που απαιτεί ένα πραγματικό e-mail. Είναι όμως και ψευδές, αφού σχεδόν σε όλους τους διακομιστές web mail τηρούνται λεπτομερή αρχεία καταγραφής (log file) με τις δραστηριότητες των χρηστών, καθώς και άλλοι στοιχεία που μαρτυρούν, π.χ., από πού συνδέθηκαν και πότε έστειλαν κάθε μήνυμα. Έτσι, αν κάποιος ενοχληθεί αρκετά από μια κριτική ή ένα σχόλιό μας, είναι σε θέση —έστω και αν κινήσει γη και ουρανό— να φτάσει σε εμάς!

Φάρμακο στις παραπάνω ανησυχίες αποτελούν οι λεγόμενοι remailers. Όπως φανερώνει και το όνομα, πρόκειται για συστήματα αλληλογραφίας που λαμβάνουν το αρχικό e-mail, και αφού το τροποποιήσουν, το αποστέλλουν στον προορισμό του. Συγκεκριμένα, το περιεχόμενό του παραμένει αναλλοίωτο, αλλά οι νέοι header είναι απογυμνωμένοι από πληροφορίες που μαρτυρούν την ταυτότητα του αποστολέα. Αμέσως αμέσως, αυτό σημαίνει ότι δεν πρέπει να περιμένουμε απάντηση όταν στέλνουμε ανώνυμο e-mail μέσω remailer, όμως σε τέτοιες περιπτώσεις η απάντηση είναι το τελευταίο πράγμα στο μυαλό μας. Σημειώστε, εξάλλου, ότι μετά τον πρώτο remailer το μήνυμα είναι δυνατόν να περάσει και από άλλους remailer, σε μια (παρανοϊκή;) απόπειρα ενίσχυσης της ανωνυμίας.

Τρεις web based remailer παρέχονται στους ακόλουθους τόπους: <https://mixmaster.autistici.org/cgi-bin/mixemail-user.cgi>, www.gilc.org/speech/anonymous/remailer.html και <http://anonymouse.to>. Πριν από την 11η Σεπτεμβρίου του 2001, κυκλοφορούσαν και αρκετά αυτόνομα προγράμματα remailer, τα οποία πρόσφεραν ακόμα περισσότερη ανωνυμία από τα αντίστοιχα συστήματα web based, αφού το μήνυμα κρυπτογραφούνταν πριν ακόμα φύγει από το μηχανήμα του αποστολέα (και όχι σε κάποιον απομακρυσμένο διακομιστή). Μετά την 11η Σεπτεμβρίου, τα προγράμματα της κατηγορίας αποτελούν είδος προς εξαφάνιση, αφού οι Αρχές θεώρησαν ότι χρησιμοποιούνται για παράνομους σκοπούς ή σκόπη και για τρομοκρατικές ενέργειες.



Εσωτερικός κίνδυνος!

Όσο καλά προστατευμένο και αν είναι ένα τοπικό δίκτυο από τον έξω κόσμο, η πιθανότητα μιας επιτυχημένης επίθεσης παραμένει υψηλή. Διαπιστώστε του λόγου το αληθές παρακολουθώντας ένα αληθινό παράδειγμα.

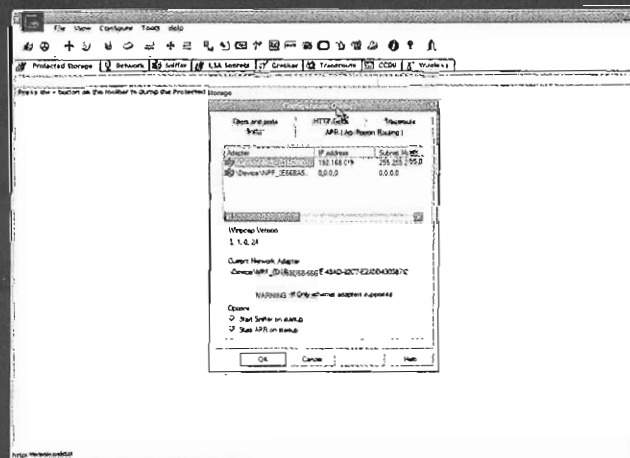
ΤΑ ΤΕΛΕΥΤΑΙΑ ΧΡΟΝΙΑ οι τεχνολογίες ασφάλειας προσφέρουν τη δυνατότητα στις εταιρείες να περιορίσουν σημαντικά τους κινδύνους που διατρέχουν τα τοπικά τους δίκτυα. Η αύξηση της ασφάλειας σε εφαρμογές client και server είναι αισθητή, χωρίς να απαιτούνται από τους χρήστες πολύπλοκες διαδικασίες κατά την εγκατάσταση και τη χρήση τους. Σε πολλές περιπτώσεις, για παράδειγμα, εταιρείες όπως οι τράπεζες χρησιμοποιούν βιομετρικά συστήματα για την επικύρωση της ταυτότητας των εργαζομένων σε «ευαίσθητα» πόστα.

Μολαταύτα, η ανάγκη για περισσότερη ασφάλεια εντείνεται διαρκώς. Κατά καιρούς, μεγάλες εταιρείες του χώρου της πληροφορικής έχουν πέσει θύματα επιθέσεων από cracker, που κατόρθωσαν να εισβάλουν στα εταιρικά Intranet. Το αποτέλεσμα ήταν να πέσουν στα χέρια των cracker εφαρμογές λογισμικού υψηλής αξίας, οι οποίοι είτε τις διακινούσαν δωρεάν στο Διαδίκτυο είτε ζητούσαν λύτρα από τις θιγόμενες πλευρές προκειμένου να τους επιστρέψουν την πνευματική τους ιδιοκτησία. Χαρακτηριστικό παράδειγμα αποτελεί η αμερικανική εταιρεία κατασκευής παιχνιδιών Valve. Χρησιμοποιώντας μια επίθεση DDoS (Distributed Denial of Service), οι cracker κατάφεραν να αποκρύψουν την υποκλοπή του πηγαίου κώδικα του παιχνιδιού Half Life 2 από το Intranet της εταιρείας.

ΚΟΙΝΕΣ ΠΡΑΚΤΙΚΕΣ. Σε ένα τυπικό Intranet υπάρχουν ένας ή περισσότεροι server με ένα σύστημα ERP (Enterprise Resource Planning) ή ένα Intranet Portal για τη διαχείριση εγγράφων. Το εσωτερικό δίκτυο επικοινωνεί με το Internet μέσω σύνδεσης DSL ή κάποιου άλλου μισθωμένου κυκλώματος.

Στην περίπτωση που υπάρχουν υποκαταστήματα, η σύνδεση μεταξύ τους και με τα κεντρικά γίνεται από το Internet, αλλά με χρήση τεχνολογιών VPN (Virtual Private Networks). Όταν υπάρχει οπτική επαφή, συχνά επιστρατεύονται ασύρματες ζεύξεις τύπου 802.11a, b ή g. Σε πολλές περιπτώσεις, προκειμένου να ελαττωθούν τα τηλεπικοινωνιακά κόστη, οι τηλεφωνικές κλήσεις πραγματοποιούνται «πάνω» από το ενσύρματο ή ασύρματο δίκτυο, με τη χρήση τεχνολογιών VoIP (Voice over IP).

Για την προστασία του Intranet από ιντερνετικές επιβουλές, όπως ιοί, worm, επιθέσεις (D)DoS κ.ο.κ., στα σημεία σύνδεσης με τον έξω κόσμο εγκαθίστανται συστήματα firewall. Επιπρόσθετα, οι διακομιστές αλληλογραφίας είναι εξοπλισμένοι με εφαρμογές anti-spam και AntiVirus, ούτως ώστε η παρείσρφηση ιών και worm στο εσωτερικό δίκτυο να δυσχεραίνεται. Η παραπάνω εταιρεία μπορεί να είναι η δική σας ή έστω να μοιάζει αρκετά με αυτή.



Επιλογή της κάρτας δικτύου μέσω της οποίας το πρόγραμμα Cain & Abel θα παρακολουθεί τη διακίνηση πακέτων.

ΑΔΥΝΑΜΙΕΣ. Όλα τα Intranet έχουν αδυναμίες και μπορούν να γίνουν στόχοι επιθέσεων, καθώς η ιστορία δείχνει ότι ακόμα και τα πιο ασφαλή δίκτυα είναι δυνατόν να παραβιαστούν. Εκτός από τις επιθέσεις αποδυναμωμένων ή δυσχερατισμένων υψηλής-λειτουργίας, υπάρχει πάντα η δυνατότητα πληροφόρησης εκ των έσω. Ένας μόνο ή μία ολόκληρη ομάδα από cracker είναι σε θέση να χρησιμοποιήσει έντεχνα και αποτελεσματικά τέτοιες πληροφορίες, ώστε τελικά να «διεισδύσει» στο εταιρικό δίκτυο. Εκτός από τις εταιρείες δεν θα πρέπει να ξεχνάμε τα net cafe με προβληματικές ή ελλιπείς ρυθμίσεις ασφάλειας, όπου καθημερινά δεκάδες ή και εκατοντάδες άνθρωποι χρησιμοποιούν τους υπολογιστές τους.

Η αρχιτεκτονική ενός τυπικού Intranet που χρησιμοποιεί το πρωτόκολλο TCP/IP είναι τοπολογικά ισοδύναμη με την αρχιτεκτονική του Internet, του μεγαλύτερου δικτύου TCP/IP στον πλανήτη. Έτσι, όπως διακινούνται οι πληροφορίες στο παγκόσμιο Διαδίκτυο, παρόμοια διακινούνται και στο εσωτερικό δίκτυο μιας εταιρείας, ενός σχολείου ή ενός net café. Το τελευταίο έχει σχεδιαστεί έτσι ώστε να παρέχει τη μέγιστη δυνατή ανοιχτή αρχιτεκτονική και ταυτόχρονα να επιτρέπει τη βέλτιστη επικοινωνία μεταξύ των υπολογιστών-κόμβων που το απορτίζουν ανά πάσα στιγμή. Όπως και το Internet έτσι και ένα Intranet είναι ευπαθές σε επιθέσεις, όταν δεν έχουν ληφθεί επαρκή μέτρα ασφαλείας.

Η πλέον επικίνδυνη επίθεση μπορεί να πραγματοποιηθεί από έναν υπολογιστή που συμμετέχει σε ένα ασύρματο ή ενσύρματο τοπικό δίκτυο. Η κάρτα δικτύου που φέρει ο υπολογιστής του επιτιθέμενου θα πρέπει να λειτουργήσει σε Promiscuous Mode,



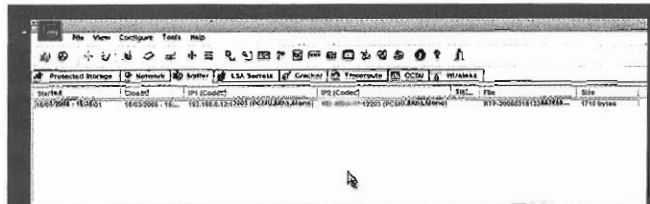
ΑΦΙΕΡΩΜΑ SNIFFING & ARP POISONING

με άλλα λόγια να δέχεται όλα τα διακινούμενα στο δίκτυο πακέτα και όχι μόνο εκείνα που προορίζονται για το δικό της MAC address. Όταν η κάρτα δικτύου λειτουργεί κατ' αυτό τον τρόπο, ο αντίστοιχος υπολογιστής είναι ικανός για sniffing. Επίσης, στο μηχανήμα του υπολογιστή

θα πρέπει να υπάρχει εγκατεστημένο κάποιο πρόγραμμα που να εφαρμόζει τεχνικές ARP poisoning, δηλαδή τροποποιήσης συγκεκριμένων κεφαλίδων (header) ενός πακέτου ARP.

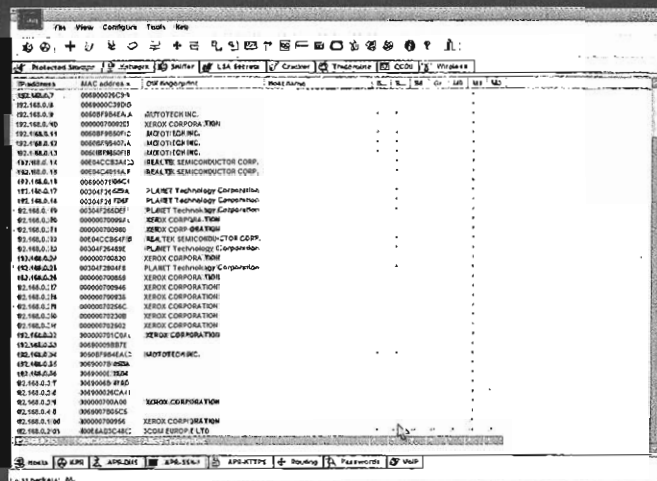
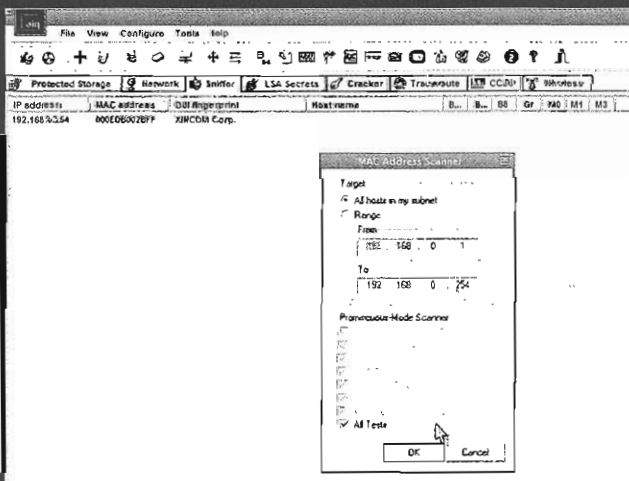
ΔΗΛΗΤΗΡΙΑΣΗ! Τα λεγόμενα πακέτα ARP χρησιμοποιούνται σε κάθε δίκτυο IP για την αντιστοίχιση της φυσικής διεύθυνσης (MAC address) μιας κάρτας δικτύου Ethernet με την αριθμητική διεύθυνση IP που της έχει αντιστοιχιστεί από το λειτουργικό σύστημα ή κάποια άλλη εφαρμογή. Το ενδιαφέρον είναι ότι η διακίνηση πακέτων ARP δεν εμπεριέχει κάποιο μηχανισμό πιστοποίησης, με αποτέλεσμα να είναι δυνατή η τροποποίηση ενός πακέτου ARP τη στιγμή που αυτό ταξιδεύει. Ακριβώς σε αυτό το γεγονός βασίζονται οι επιθέσεις «man in the middle», όπως χαρακτηριστικά ονομάζονται.

Για παράδειγμα, ας υποθέσουμε ότι σε ένα τοπικό δίκτυο υπάρχουν οι host A, B και C. Έστω ότι οι A και B ανταλλάσσουν πακέτα μέσω ενός switch και ότι ο C είναι ικανός για sniffing. Αυτό το τελευταίο σημαίνει ότι ο C μπορεί να συλλέγει πακέτα unicast, μεταξύ των A και B, καθώς και πακέτα multicast και broadcast. Με χρήση της τεχνικής ARP poisoning, ο host C θα μπορεί να αλλοδώει τη διεύθυνση (source MAC) ενός πακέτου ARP, πληροφορώντας τον host A ότι η διεύθυνση IP του B αντιστοιχεί στο MAC address του C. Ταυτόχρονα κάνει το ίδιο και για τον host B, λέγοντάς του ότι η διεύθυνση IP του A αντιστοιχεί στο δικό του MAC address. Αυτό θα έχει ως αποτέλεσμα να τα δρομολογούνται πακέτα των A και B μέσω του C, χωρίς να παρεμβαίνει το switch. Αφού ο C επεξεργαστεί κατάλληλα τα διακινούμενα πακέτα, δρομολογεί τα πακέτα προς τους σωστούς αποδέκτες



Το Cain & Abel έχει τη δυνατότητα παρακολούθησης τηλεφωνικών συνδιαλέξεων και τη μετέπειτα αποθήκευσή τους σε αρχείο WAV.

αποκαθιστώντας την τάξη. Εάν όμως δεν το κάνει, τότε το αποτέλεσμα θα είναι μια επίθεση DoS που θα θέσει εκτός δικτύου τόσο τον host A όσο και τον B. Αξίζει να σημειωθεί, τέλος, ότι υπάρχουν κάποιοι περιορισμοί στην εφαρμογή του ARP poisoning. Συγκεκριμένα, η τεχνική εφαρμόζεται μόνο σε υπολογιστές που βρίσκονται στο ίδιο subnet. Επίσης, κατά την εφαρμογή του ARP poisoning η συνολική απόδοση του δικτύου μειώνεται, αφού πλέον δρομολογούνται πρόσθετα πακέτα.



Αριστερά: Επιλογή όλων των μηχανημάτων του subnet προς παρακολούθηση.

Δεξιά: Το Cain & Abel έχει πιάσει δουλειά. Στη λίστα φαίνεται μέρος των υπό παρακολούθηση υπολογιστών.