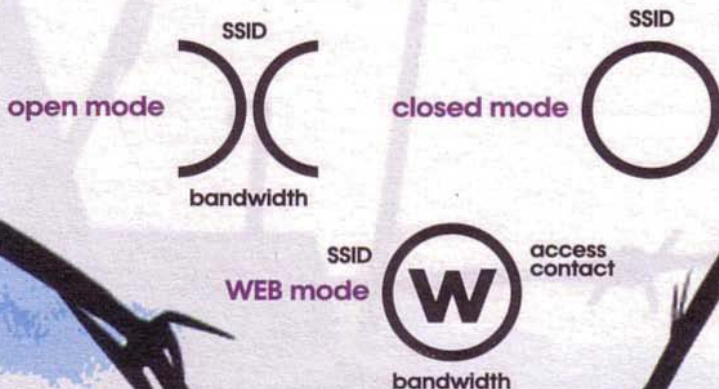


Όταν βρεθεί ένα ασύρματο δίκτυο, ο λεγόμενος warchalker σχεδιάζει ένα σύμβολο σε κάποιο εμφανές σημείο στην περιοχή και αναγράφει σε αυτό πληροφορίες σχετικά με τις ιδιότητες του ασύρματου δικτύου που ανακάλυψε.

Οι συσκευές ασύρματης δικτύωσης εκπέμπουν πακέτα δεδομένων μέσω των ραδιοσυχνοτήτων, τα οποία μπορούν με τη σειρά τους να τα μεταφέρουν σε μεγάλες αποστάσεις, με πάγια έξοδα και πολύ μικρό λειτουργικό κόστος. Με τη χρήση των ασύρματων δικτύων η επικοινωνία μεταξύ των πληροφοριακών συστημάτων ξεφεύγει από τα καθιερωμένα και γίνεται περισσότερο προσιτή για τον καθένα μας. Με αυτό το σκεπτικό, το 2000 δημιουργήθηκε στην Πάτρα μια μικρή εθελοντική ομάδα που απαρτιζόταν από ιδιώτες και κυρίως φοιτητές. Χωρίς καμία χρηματοδότηση, με δικά τους έξοδα, ξεκίνησαν να διαφημίζουν και να δημιουργούν τα γνωστά πια σήμερα μητροπολιτικά δίκτυα. Μέσα σε έξι χρόνια οι ομάδες που δημιουργήθηκαν μέσα από τα ασύρματα δίκτυα κατάφεραν να φέρουν την Ελλάδα στην πρώτη θέση στον κόσμο, με βάση τα στοιχεία από τη γνωστή nodedb.com. Η επιτυχία αυτή φυσικά δεν έμεινε ανεκμετάλλευτη. Το κράτος ξεκίνησε να δημιουργεί δράσεις ευρυζωνικής ανάπτυξης μέσα από την κοινωνία της πληροφορίας, ενθαρρύνοντας τις επιχειρήσεις και τους δημόσιους οργανισμούς να αναβαθμιστούν χρησιμοποιώντας την τεχνολογία των ασύρματων δικτύων. Η παραπάνω πρακτική ναι μεν είναι σωστή, αλλά έχει και κάποια μικρά αρνητικά, λόγω της άγνοιας ή της ελλιπούς/κακής ενημέρωσης στον τομέα της ασφάλειας.

Οι ιδιώτες έφτιαχναν τα ασύρματα δίκτυα για να μειώσουν το υψηλό κόστος των γρήγορων συνδέσεων που παρείχαν μέχρι πρότινος οι ιντερνετικοί φορείς. Έτσι, μπορούσαν να παίζουν παιχνίδια ή να ανταλλάσσουν αρχεία με πολύ μικρό κόστος, χωρίς να αναγκάζονται να πληρώνουν τέλη σύνδεσης. Αυτό είχε ως αποτέλεσμα να μην τους ενδιαφέρει ο τομέας της ασφάλειας, καθώς η κοινότητα αυτή δεν είχε και τίποτε να κρύψει.

Οι εταιρείες, από την άλλη, τον έκαναν για να μεταφέρουν δεδομένα από το ένα κτίριο στο άλλο και να γλιτώσουν το χαράτσι του πανάκριβου δημόσιου φορέα. Αυτή τη στιγμή υπάρχουν εκατοντάδες εταιρείες και δημόσιοι φορείς που δεν πληρούν τα βασικά στάνταρτ στον τομέα της ασφάλειας. Αυτό έχει ως συνέπεια αρκετές εταιρείες και δημόσιοι



οργανισμοί να διακινούν καθημερινά ευαίσθητες ή/και απόρρητες πληροφορίες για τη λειτουργία του οργανισμού ή της εταιρείας. Ακόμα, πιθανόν να μεταφέρονται προσωπικά δεδομένα, τα οποία είναι δυνατόν να διαβαστούν και να παραποιηθούν κατά βούληση.

Στα ασύρματα δίκτυα δεν υπάρχει η φυσική προστασία που υπάρχει στα ενσύρματα. Έτσι, κάποιος χρήστης που βρίσκεται στην εμβέλεια του ασύρματου δικτύου, με ένα φορητό υπολογιστή, με τις κατάλληλες γνώσεις και με μία κάρτα ασύρματου δικτύου (οι περισσότεροι φορητοί την έχουν ενσωματωμένη) μπορεί να συλλέξει διακινούμενα πακέτα, να παραγάγει νέα κατά βούληση, καθώς και να αποκρυπτογραφήσει τα δεδομένα που διακινούνται μέσα στο δίκτυο.

ΓΝΩΡΙΜΙΑ ΜΕ ΤΟ... ΘΥΜΑ

Ένα ασύρματο δίκτυο αποτελείται από μία ή περισσότερες ασύρματες συσκευές, τις οποίες μπορείτε να βρείτε στο εμπόριο με πολλές παραλλαγές. Κάθε τέτοια συσκευή αποτελεί ένα μοναδικό σταθμό και θα την ονομάζουμε station. Τα station αυτά στέλνουν τα δεδομένα τους μέσα από μια άλλη συσκευή, που ονομάζεται σημείο πρόσβασης ή Access Point — εν συντομία AP. Τα AP μοιράζουν τα δεδομένα στα station και είναι υπεύθυνα για τη σωστή δρομολόγηση των δεδομένων. Τα station και τα AP, όπως συμβαίνει και στις ενσύρματες συσκευές, έχουν μία μοναδική διεύθυνση που ονομάζεται Media Access Control (MAC). Πρόκειται για ένα 48μπιτο αριθμό που αντιστοιχίζεται από τον κατασκευαστή της συσκευής και έχει τη μορφή 00:10:1D:21:C1:F1. Είναι τυπωμένος πάνω στις συσκευές, όπως επίσης και στο κουτί της συσκευασίας, αλλά το σημαντικότερο είναι ότι μπορεί να παραποιηθεί μέσω λογισμικού. Αυτή η αδυναμία αξιοποιείται από τους cracker, προκειμένου να ξεγελάσουν το AP δίνοντας ψεύτικα στοιχεία για το station-θύμα ή απλώς για να το θέσουν εκτός λειτουργίας.

Ένα άλλο, απαραίτητο στοιχείο που θα πρέπει να γνωρίζει ο επιτιθέμενος είναι το Service Set Identifier (SSID). Έχει μήκος 32byte και ορίζει το όνομα του ασύρματου δικτύου. Πολλές φορές, οι διαχειριστές, για λόγους ασφάλειας, ρυθμίζουν το AP ώστε να μην εκπέμπει το όνομά του, με αποτέλεσμα να είναι αόρατο από τα station. Όμως και σε αυτή την περίπτωση υπάρχει τρόπος για τον επιτιθέμενο να βρει το όνομα του AP, με τη χρήση κατάλληλων προγραμμάτων παρακολούθησης.

Η όλη επικοινωνία μεταξύ των station και των AP γίνεται κρυπτογραφημένα, με τη χρήση ειδικών αλγόριθμων. Υπάρχουν αρκετοί αλγόριθμοι που διαφέρουν ως προς το επίπεδο προστασίας που παρέχουν. Ως πρό-

τυπα έχουν επικρατήσει τα WEP και WPA, τα οποία υλοποιούνται από όλες τις ασύρματες συσκευές που κυκλοφορούν σήμερα. Το Wired Equivalent Privacy (WEP) χρησιμοποιεί ένα κοινό κλειδί για να λειτουργήσει και πρέπει να υπάρχει τόσο στα station όσο και στο AP, όπου και γίνεται η ταυτοποίηση των χρηστών. Το WEP έχει μέγεθος 40 ή 104bit και για την κρυπτογράφηση των δεδομένων χρησιμοποιεί τον αλγόριθμο RC4. Ένα από τα αρνητικά στοιχεία του είναι ότι δεν κρυπτογραφεί όλα τα δεδομένα, αφήνοντας τα control και management frame να μεταφέρονται χωρίς κρυπτογράφηση!

ΠΩΣ ΓΙΝΕΤΑΙ Η ΤΑΥΤΟΠΟΙΗΣΗ ΤΩΝ STATION;

Η ταυτοποίηση ενός station με κάποιο άλλο ή με κάποιο AP γίνεται ανάλογα με τον τρόπο σύνδεσής τους. Σε ένα ανοιχτό διαχειριστικό σύστημα, όλα τα station ταυτοποιούνται χωρίς κανέναν έλεγχο. Σε ένα άλλο διαχειριστικό σύστημα, το station A στέλνει ένα πακέτο που περιέχει την ταυτότητά του σε ένα station B, περιμένοντας από αυτό ένα άλλο πακέτο που φανερώνει ότι το station A αναγνωρίστηκε και έτσι εγκαθιδρύεται η μεταξύ τους επικοινωνία. Σε περίπτωση που το A δεν αναγνωριστεί, το station B επιστρέφει ένα πακέτο μη ταυτοποίησης. Ένα station μπορεί να κάνει ταυτοποίηση με όσα station θέλει, αλλά έχει το δικαίωμα να συνδεθεί μόνο με ένα από αυτά τη φορά. Το πρόβλημα εδώ είναι ότι ένας cracker μπορεί, με χρήση ειδικού

Το warchalking είναι ο σχεδιασμός συμβόλων σε δημόσιους χώρους, που γίνεται για την ενημέρωση των ενδιαφερομένων σχετικά με την ύπαρξη ασύρματων δικτύων στην περιοχή.



λογισμικού, να στέλνει κατάλληλα διαμορφωμένα πακέτα στο station B και να μαθαίνει για την πολιτική ασφάλειας και τις σχέσεις εμπιστοσύνης που υπάρχουν μεταξύ των station και των AP...

ΣΝΙΦΑΡΟΝΤΑΣ ΔΙΑΚΙΝΟΥΜΕΝΑ ΠΑΚΕΤΑ

Ο λόγος γίνεται για την τεχνική του λεγόμενου sniffing — η οποία μόνο καινούργια δεν είναι, παρεμπιπτόντως. Όπως στα ενσύρματα, έτσι και στα ασύρματα δίκτυα μπορούμε να παρακολουθούμε τα πακέτα που διακινούνται, και από εκεί και πέρα με διάφορους τρόπους να τα φιλτράρουμε με βάση τα κριτήρια που επιθυμούμε. Κατ' αυτό τον τρόπο μπορεί κάποιος να συλλέξει, π.χ., τους κωδικούς που διακινούνται εντός ενός δικτύου. Το sniffing στα ασύρματα δίκτυα είναι ακόμα πιο εύκολη διαδικασία. Αυτό διότι αφενός δεν χρειάζεται να είμαστε εντός του «φυσικού» χώρου στον οποίο εκτείνεται το δίκτυο, αφετέρου δεν είναι απαραίτητο να εγκαταστήσουμε στον υπολογιστή ενός υποψήφιου στόχου κάποιο λογισμικό καταγραφής δικτυακών πακέτων.

Από τη στιγμή που μιλάμε για ασύρματα δίκτυα, ο επιτιθέμενος μπορεί να έχει το φορητό του σε ένα αυτοκίνητο και να κόβει βόλτες στο τετράγωνο που είναι εγκατεστημένο το ασύρματο δίκτυο ή να έχει παρκάρει έως και 500 μέτρα μακριά και να αποθηκεύει τα δεδομένα που συλλέγει για περαιτέρω επεξεργασία. Ακόμα χειρότερα, μπορεί να πραγματοποιήσει τη διαδικασία απολαμβάνοντας ένα καφεδάκι ή μια παγωμένη μπίρα στο μπαλκόνι του σπιτιού του ; -)

Για να πραγματοποιηθεί σωστά η διαδικασία, πέρα από τον απαραίτητο εξοπλισμό, ο επίδοξος cracker θα πρέπει να έχει στη διάθεσή του το κατάλληλο λογισμικό. Ένα απαραίτητο εργαλείο είναι το Kismet (www.kismetwireless.net), για χρήση με μια κάρτα ασύρματης πρόσβασης που υποστηρίζει το mode λειτουργίας RF monitor. Σημειώστε ότι δυνατότητες καταγραφής δεν έχουν όλες οι ασύρματες κάρτες. Για να λειτουργήσουν σωστά κάποιες από αυτές θα πρέπει να αναβαθμιστεί το firmware τους ή να χρησιμοποιηθούν ειδικοί driver.

Η διαδικασία αυτή θα δώσει στον επιτιθέμενο πάρα πολλά στοιχεία — όπως, π.χ., αν το δίκτυο-στόχος είναι κρυφό και συνεπώς δεν εκπέμπει το SSID του. Με τα στοιχεία που θα συλλέξει ο επιτιθέμενος (Beacon, Probe Requests, Probe Responses, Association Requests και Reassociation Requests) έχει τη δυνατότητα να βρει το SSID, καταγράφοντας τα

Αν σκέφτεστε ότι η θεωρία δύσκολα εφαρμόζεται στην πράξη και ότι η ασφάλεια των ασύρματων δικτύων δεν παραβιάζεται τόσο εύκολα, γυρίστε στη σελίδα 114 και διαβάστε το χρονικό μιας αληθινής επίθεσης, που συνέβη κάπου στην Ελλάδα.



management frame που διακινούνται στο δίκτυο. Η όλη συλλογή είναι δυνατόν να γίνει ακόμα και αν είναι ενεργοποιημένη η κρυπτογράφηση μέσω WEP.

Παράλληλα, ο επιτιθέμενος συλλέγει τις διευθύνσεις MAC των station, έτσι ώστε αργότερα να είναι σε θέση να δημιουργεί κατάλληλα διαμορφωμένα πακέτα (spoofed frames) που εξαπατούν το AP. Ακόμα, γνωρίζοντας το MAC των συσκευών μπορεί κάποιος να βρει πληροφορίες για τον τύπο της συσκευής. Έτσι, όλα γίνονται ακόμα πιο εύκολα (βλ., π.χ., http://coffer.com/mac_find). Το επόμενο βήμα που θα κάνει είναι να επισκεφθεί το site του κατασκευαστή και να διαβάσει τα manual της συσκευής. Εκεί θα βρει τις προκαθορισμένες ρυθμίσεις και θα καταλάβει το επίπεδο προστασίας που παρέχει η συσκευή. Συνήθως, όταν στήνεται ένα ασύρματο δίκτυο από ιδιώτες, οι συσκευές μένουν με τις προκαθορισμένες ρυθμίσεις, οι οποίες είναι πολύ εύκολο να παραβιαστούν, ειδικά αν έχει κανείς στη διάθεσή του τις οδηγίες χρήσης της συσκευής.

ΚΡΥΠΤΟΓΡΑΦΗΜΕΝΑ ΠΑΚΕΤΑ; ΚΑΝΕΝΑ ΠΡΟΒΛΗΜΑ!

Ο σκοπός ενός επιτιθέμενου είναι να βρει το κλειδί με το οποίο κρυπτογραφούνται τα δεδομένα, έτσι ώστε να καταφέρει να αποκτήσει πρόσβαση στο ασύρματο δίκτυο. Το κλειδί μπορεί κανείς να το βρει με πάρα πολλούς τρόπους. Υπάρχουν drivers που το γράφουν στο μνήμιο των Windows ή μέσα σε script τα οποία μπορούν εύκολα να διαβαστούν, αρκεί βέβαια να έχει ο επιτιθέμενος πρόσβαση σε έναν υπολογιστή του τοπικού δικτύου. Ακόμα και με τεχνικές social engineering είναι δυνατόν να μαθευτεί το κλειδί, και μάλιστα χωρίς ιδιαίτερο κόπο :-). Σε περίπτωση που όλα αυτά αποτύχουν, ο επιτιθέμενος θα χρησιμοποιήσει κάποιο εξειδικευμένο λογισμικό καταγραφής κρυπτογραφημένων πακέτων, έτσι ώστε αργότερα, με τη βοήθεια κάποιου προγράμματος σπασίματος του WEP, να βρει το κλειδί. Ένα σχετικό πρόγραμμα είναι το Air Crack (www.aircrack-ng.org). Σε γενικές γραμμές, η «φύση» της κρυπτογραφίας είναι τέτοια,

ΠΑΝΟΜΟΙΟΤΥΠΑ AP

Ένας cracker μπορεί να στήσει ένα μηχανήμα πανομοιότυπο με κάποιο AP, με τη μόνη διαφορά ότι η εκπομπή του θα είναι ισχυρότερη από αυτή του κανονικού AP! Με αυτό τον τρόπο τα station θα συνδέονται σε αυτό, αντί για το προβλεπόμενο AP. Από εκεί και πέρα, ο επίδοξος cracker μπορεί να κλέψει κωδικούς πρόσβασης, να βρει πληροφορίες σχετικά με τα IP και γενικότερα να συλλέξει πληροφορίες που αργότερα θα χρησιμοποιήσει για να αποκτήσει περισσότερη πρόσβαση σε ένα δίκτυο.

Αυτή η μορφή επίθεσης ονομάζεται Evil Twin Attack.

ΚΑΤΑΣΚΕΥΑΣΤΙΚΑ ΣΦΑΛΜΑΤΑ

Γνωρίζοντας το MAC address, τον τύπο και τη μάρκα της ασύρματης συσκευής, ένας cracker μπορεί να βρει στο Διαδίκτυο τα κατασκευαστικά σφάλματα που έχει το AP. Ακόμα χειρότερα, λόγω του ότι τα firmware είναι δυνατόν να κατεβούν στον υπολογιστή ενός χρήστη, δυνητικά έχει τη δυνατότητα να κάνει reverse engineering σε αυτά και να βρει όλες τις αδυναμίες. Για παράδειγμα,

ώστε θα πρέπει να συλλεχθούν πάνω από 1.000.000 πακέτα πριν σπάσει το κλειδί της κρυπτογράφησης. Η όλη διαδικασία της κρυπτογράφησης γίνεται μέσα στη συσκευή σε πραγματικό χρόνο. Η συσκευή δημιουργεί ένα αρχικό νούμερο μεγέθους 24bit, το λεγόμενο Initialization Vector (IV), το οποίο προστίθεται στο κοινό κλειδί που έχει ορίσει ο διαχειριστής. Τα δύο κλειδιά μάς δίνουν ένα τυχαίο, υποτίθεται, νούμερο 64 ή 128bit, ανάλογα με το χρησιμοποιούμενο αλγόριθμο κρυπτογράφησης. Ακολουθώντας τα δεδομένα κρυπτογραφούνται με αυτό το κλειδί και μεταφέρονται από station σε station, μέσω του AP. Τα AP και τα station, με τη σειρά τους, διαχωρίζουν το IV με το κλειδί που υπάρχει αποθηκευμένο μέσα στη συσκευή και αποκρυπτογραφούν τα δεδομένα. Ο RC4 είναι πολύ ισχυρός αλγόριθμος κρυπτογράφησης, αλλά το πρόβλημα εδώ είναι ότι αρκετές συσκευές που κυκλοφορούν στο εμπόριο ξεκινούν, πολύ απλά, τα IV τους από το 0 αντί από ένα τυχαίο νούμερο. Σαν να μην έφτανε αυτό, όταν χρειαστεί να μεταφέρουν κρυπτογραφημένα δεδομένα, αυξάνουν την τιμή του IV κατά 1, κάνοντας προβλέψιμα τα «τυχαία» νούμερα του IV. Συμπερασματικά, όσο περισσότερα δεδομένα συλλέξει ο επιτιθέμενος τόσο γρηγορότερα θα φτάσει στο στόχο του. Σε ένα αρχείο με 1.000.000 πακέτα IV, μόνο μερικές εκατοντάδες είναι προβληματικά. Αυτά όμως είναι αρκετά για να βρεθεί το κλειδί! Τα προγράμματα που σπάνε τα κλειδιά χρησιμοποιούν στατιστική ανάλυση και μέσα σε λίγα μόλις δευτερόλεπτα μπορούν να βρουν το ζητούμενο κλειδί. Υπό κανονικές συνθήκες τα πακέτα IV στέλνονται στο δίκτυο με πολύ αργούς ρυθμούς. Οι επιτιθέμενοι, προκειμένου να αυξήσουν την παραγωγή πακέτων IV, στέλνουν κατάλληλα διαμορφωμένα πακέτα στο AP παριστάνοντας ότι είναι τα station. Εναλλακτικά, ψάχνουν να βρουν στα πακέτα που διακινούνται ένα πακέτο IV και μετά το στέλνουν στο AP εκατοντάδες φορές γρηγορότερα. Τα πακέτα αυτά μπορεί να είναι οτιδήποτε. Για παράδειγμα, ένα απλό πακέτο arp αρκεί για να δημιουργήσει εκατοντάδες πακέτα IV.

Crow

ένα AP κολλάει όταν δεχτεί ένα πακέτο που έχει ως αρχικό MAC τον εαυτό του. Κάποιο άλλο, μέσα από την υπηρεσία TFTP (Trivial File Transfer Protocol), δίνει το αρχείο config.img, που περιέχει το αρχείο ρυθμίσεων, όταν αυτό του ζητηθεί. Περίττο να πούμε ότι αυτό περιέχει τους κωδικούς πρόσβασης της συσκευής, καθώς και το κλειδί WEP.

ΑΔΥΝΑΜΙΑ ΣΥΝΔΕΣΗΣ

Αυτή η μορφή επίθεσης μπορεί να βγάλει εκτός λειτουργίας ένα station για μερικά msec έως κάποιες ώρες. Πραγματοποιείται

με πάρα πολλούς τρόπους, π.χ., αν ο επιτιθέμενος συνδεθεί σε ένα AP περισσότερες από 2.007 φορές ή αν στέλνει πακέτα αποσύνδεσης στο AP, παριστάνοντας ότι είναι κάποιο από τα συνδεδεμένα station.

ΠΑΡΕΜΒΟΛΕΣ ΣΤΗ ΣΥΧΝΟΤΗΤΑ ΤΩΝ 2,4GHz

Στο εμπόριο υπάρχουν πάρα πολλές συσκευές που μπορούν να θέσουν εκτός λειτουργίας οποιαδήποτε συσκευή εκπέμπει στο φάσμα των ασύρματων δικτύων. Ονομάζονται WiFi Jammer και κοστίζουν κάτι λιγότερο από 200 ευρώ.

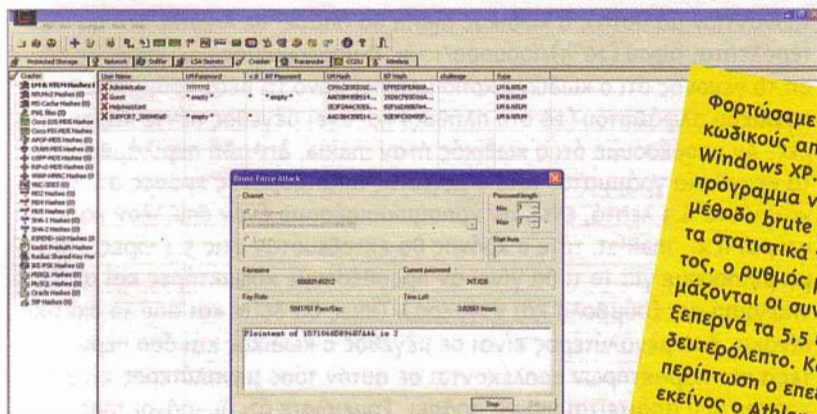
Είναι κοινό μυστικό ότι οι περισσότεροι από εμάς χρησιμοποιούμε ευκολομνημόνευτους κωδικούς, προφανώς για να μην τους ξεχάσουμε και μετά τρέχουμε και δεν φτάνουμε. Πολλοί, μάλιστα, για να είναι σίγουροι ότι δεν πρόκειται να χάσουν τον μπουσούλα, χρησιμοποιούν τον ίδιο κωδικό παντού, από το λογαριασμό στον υπολογιστή και το e-mail μέχρι τις κάθε λογής υπηρεσίες και sites στο Internet.

ΒΑΝΑΥΣΗ ΔΥΝΑΜΗ!

Δεν χρειάζεται να έχετε φοβερές γνώσεις για ν' αντιληφθείτε πόσο εύκολο είναι να σπάσουν κωδικοί όπως αυτοί που δώσαμε παραπάνω. Αρκεί μόνο να γνωρίζετε τον τρόπο με τον οποίο πραγματοποιείται το σπάσιμο. Η πιο διαδεδομένη μέθοδος για την αποκάλυψη κάθε λογής κωδικών είναι οι επιθέσεις brute force. Σε μια επίθεση του είδους δοκιμάζονται όλοι οι πιθανοί συνδυασμοί των χαρακτήρων που περιλαμβάνονται στο σετ το οποίο έχει επιλέξει ο επιτιθέμενος. Σημειώστε ότι, αν και οι δοκιμές είναι τυφλές, εξαιτίας

Το Zip Password Recovery δοκιμάζει πολύ περισσότερους από δύο εκατομμύρια συνδυασμούς λέξεων το δευτερόλεπτο, στα συμπίεσμένα, κλειδωμένα αρχεία ZIP. Αυτό σημαίνει ότι μικροί σε μέγεθος κωδικοί, οι οποίοι βασίζονται σε ένα μόνο σετ χαρακτήρων, θα σπάσουν σε ελάχιστο χρόνο. Στη συγκεκριμένη περίπτωση δοκιμάσαμε τον κωδικό Maria, ο οποίος έσπασε σε περίπου 40 δευτερόλεπτα, σε ένα μηχανήμα με επεξεργαστή Athlon 64 3000+ (single core).





Φορτώσαμε στο Cain & Abel κωδικούς από λογαριασμούς στα Windows XP. Ζητήσαμε από το πρόγραμμα να τους σπάσει με τη μέθοδο brute force. Σύμφωνα με τα στατιστικά του προγράμματος, ο ρυθμός με τον οποίο δοκιμάζονται οι συνδυασμοί λέξεων ξεπερνά τα 5,5 εκατομμύρια το δευτερόλεπτο. Και σε αυτή την περίπτωση ο επεξεργαστής ήταν εκείνος ο Athlon 64 3000+.

της μεγάλης ταχύτητας που χαρακτηρίζει ακόμα και έναν παλιό υπολογιστή, ένας ασθενής κωδικός είναι πιθανό να βρεθεί σε ελάχιστο χρόνο. Βασικά, για το σχηματισμό ενός κωδικού υπάρχουν τέσσερα σετ χαρακτήρων: α. τα πεζά μόνο γράμματα του αγγλικού αλφάβητου, β. τα κεφαλαία μόνο γράμματα, γ. τα νούμερα, από το 0 έως το 9 συμπεριλαμβανομένων και δ. τα κάθε λογής σύμβολα που είναι αποδεκτά σε έναν κωδικό (π.χ., * % & # !).

Ένας κωδικός που περιλαμβάνει χαρακτήρες από ένα μόνο σετ, αντιλαμβάνεστε ότι είναι περισσότερο εύαλωτος από έναν άλλο, ο οποίος έχει το ίδιο μήκος ή μέγεθος αλλά συνδυάζει χαρακτήρες από δύο σετ. Ο λόγος είναι προφανής: στην πρώτη περίπτωση θα χρειαστεί να δοκιμαστούν όλοι οι πιθανοί συνδυασμοί χαρακτήρων από ένα μόνο σετ, ενώ στη δεύτερη όλοι οι συνδυασμοί χαρακτήρων που προέρχονται από δύο σετ. Ας υποθέσουμε, για παράδειγμα, ότι έχουμε έναν κωδικό μεγέθους πέντε χαρακτήρων, π.χ., τον κωδικό maria (ευφάνταστος, ε;). Η συγκεκριμένη λέξη μπορεί να εντοπιστεί με τη μέθοδο του brute force σε ελάχιστα δευτερόλεπτα. Αν ο κωδικός είχε μικρότερο μέγεθος (π.χ., τρεις ή τέσσερις χαρακτήρες), θα εντοπιζόταν σχεδόν ακαριαία. Ασφαλώς, ο χρόνος που απαιτείται εξαρτάται από την ισχύ του επεξεργαστή, τον αριθμό των υπολογιστών που συμμετέχουν στην επίθεση brute force και από τον αριθμό των πιθανών συνδυασμών που το ίδιο το σπαστήρι μπορεί να δοκιμάζει ανά δευτερόλεπτο. Για να συνεκτιμοποιήσετε όλα τα προηγούμενα καλύτερα, ας μιλήσουμε με αριθμούς.

Η ΑΛΗΘΕΙΑ ΜΕ ΑΡΙΘΜΟΥΣ

Ο μέγιστος απαιτούμενος χρόνος (σε δευτερόλεπτα) για να σπάσει ένας κωδικός ισούται με $(x^y)/m/k$, όπου x είναι το μέγεθος του σετ χαρακτήρων, y το μέγεθος του password, m ο αριθμός των συνδυασμών που μπορεί το σπαστήρι να δοκιμάζει ανά δευτερόλεπτο και k ο αριθμός των υπολογιστών που χρησιμοποιούνται. Έτσι, αν υποθέσουμε ότι χρησιμοποιείται ένας υπολογιστής και το σπαστήρι μπορεί να δοκιμάζει ένα εκατομμύριο συνδυασμούς το δευτερόλεπτο (νούμερο διόλου υπερβολικό —

τουναντίον μάλιστα), ο κωδικός maria θα σπάσει σε λιγότερο από 11 δευτερόλεπτα, αφού $(26^5)/1000000/1 = 11$. Ο υπολογισμός μας έγινε με βάση το γεγονός ότι ο κωδικός χρησιμοποιεί μόνο τα πεζά γράμματα του αγγλικού αλφαβήτου (26 στο πλήθος) και έχει μέγεθος πέντε χαρακτήρες. Αν υποθέσουμε ότι ο κωδικός ήταν maria, δηλαδή περιλάμβανε και τα κεφαλαία γράμματα, τότε ο μέγιστος απαιτούμενος χρόνος θα αυξανόταν στα 6,3 λεπτά, ενώ, αν χρησιμοποιούσαμε έναν επιπλέον χαρακτήρα, π.χ., maria!, τότε ο χρόνος θα εκτοξευόταν στις 5,4 ώρες. Για να μη μιλήσουμε για το τι θα γίνει αν προσθέσουμε χαρακτήρες και από τα υπόλοιπα σετ (σύμβολα και νούμερα). Όπως θα δείτε και από το σχετικό πίνακα, όσο μεγαλύτερος είναι σε μέγεθος ο κωδικός και όσο περισσότερα σετ χαρακτήρων εμπλέκονται σε αυτόν τόσο μεγαλύτερος είναι ο χρόνος που απαιτείται για να σπάσει. Σημειώστε ότι οι χρόνοι τους οποίους προαναφέραμε —αλλά και εκείνοι που δίνουμε στον πίνακα— είναι οι μέγιστοι που απαιτούνται ανά περίπτωση. Ανάλογα με τον κωδικό, ο χρόνος που χρειάζεται το πρόγραμμα για να τον σπάσει ενδέχεται να είναι από λίγο έως πολύ μικρότερος.

ΔΗΜΙΟΥΡΓΙΑ ΑΝΘΕΚΤΙΚΩΝ ΚΩΔΙΚΩΝ

Όλα τα παραπάνω μας οδηγούν στο προφανές συμπέρασμα ότι πρέπει να έχουμε έναν κωδικό με όσο το δυνατόν μεγαλύτερο μέγεθος, ο οποίος θα περιλαμβάνει γράμματα (πεζά και κεφαλαία), νούμερα και σύμβολα. Εννοείται ότι δεν έχει σχεδόν καμία αξία να δημιουργήσουμε ένα μακροσκελές password με χαρακτήρες που ανήκουν μόνο σε ένα σετ χαρακτήρων.

Για τους περισσότερους από εμάς είναι αρκετά δύσκολο να δημιουργήσουμε έναν κωδικό ο οποίος να είναι ταυτόχρονα και ισχυρός και ευκολομνημόνευτος. Για παράδειγμα, ο κωδικός 8Z9%χ\$ρ8ib7Wrt είναι, το

Μέγεθος Password	Ένα σετ χαρακτήρων (26) Όλα πεζά ή όλα κεφαλαία	Δύο σετ χαρακτήρων (52) Πεζά και κεφαλαία	Τρία σετ χαρακτήρων (62) Πεζά, κεφαλαία και νούμερα	Όλα τα σετ χαρακτήρων (92) Πεζά, κεφαλαία, νούμερα και σύμβολα
3 χαρακτήρες	0,01 δευτερόλεπτα	0,14 δευτερόλεπτα	0,22 δευτερόλεπτα	0,77 δευτερόλεπτα
4 χαρακτήρες	0,45 δευτερόλεπτα	7,3 δευτερόλεπτα	14,7 δευτερόλεπτα	71 δευτερόλεπτα
5 χαρακτήρες	11,8 δευτερόλεπτα	6,3 λεπτά	15,2 λεπτά	1,8 ώρες
6 χαρακτήρες	5,1 λεπτά	5,4 ώρες	15,7 ώρες	1 εβδομάδα
7 χαρακτήρες	2,2 ώρες	11 μέρες	40 μέρες	1,7 χρόνια
8 χαρακτήρες	2,4 μέρες	1,6 χρόνια	6,9 χρόνια	1,62 αιώνες
9 χαρακτήρες	2 μήνες	88 χρόνια	4,29 αιώνες	14,9 χιλιετηρίδες
10 χαρακτήρες	4,4 χρόνια	4,5 χιλιετηρίδες	26,6 χιλιετηρίδες	1.377 χιλιετηρίδες

Τα νούμερα που παραθέτουμε στον πίνακα έχουν προκύψει από την παραδοχή ότι ένα σπαστήρι δοκιμάζει ένα εκατομμύριο συνδυασμούς το δευτερόλεπτο, σε ένα τυπικό σύστημα. Ο αριθμός των συνδυασμών που δοκιμάζονται ανά δευτερόλεπτο εξαρτάται κυρίως από το πρόγραμμα-σπαστήρι και την ισχύ του κεντρικού επεξεργαστή, με έναν πυρήνα. Επίσης, οι χρόνοι αφορούν στη χρήση ενός μόνο υπολογιστή. Ο αριθμός μέσα στις παρενθέσεις, στα ονόματα των στηλών, αντιπροσωπεύει το πλήθος των χαρακτήρων.

δίχως άλλο, πανίσχυρος! Για του λόγου το αληθές, ανατρέξτε στη διεύθυνση www.microsoft.com/athome/security/privacy/password_checker.mspx ή στη www.securitystats.com/tools/password.php και δοκιμάστε τον (παρεμπιπτόντως, κάντε το ίδιο και για τους δικούς σας κωδικούς). Τα συγκεκριμένα sites αξιολογούν (ουσιαστικά σύμφωνα με όσα περιγράψαμε παραπάνω) έναν κωδικό και σας λένε αν και κατά πόσο είναι ισχυρός ή αδύναμος. Παρ' όλα αυτά, είναι εξαιρετικά δύσκολο να απομνημονεύσει κανείς δύο, τρεις ή και περισσότερους κωδικούς όπως αυτός. Λέμε δύο ή τρεις, καθώς είμαστε της άποψης ότι πρέπει να χρησιμοποιείτε διαφορετικούς κωδικούς για κάθε περίπτωση. Η χρήση ενός μόνο κωδικού προσφέρει, προφανώς, τεράστια ευχρηστία. Από την άλλη, όμως, αν σπάσει, θα βρεθείτε τελείως εκτεθειμένοι – και μάλιστα σε πολλά μέτωπα. Πώς λοιπόν θα καταφέρετε να δημιουργήσετε τόσο ισχυρά και διαφορετικά passwords, τα οποία θα θυμάστε όπως θυμάστε το όνομά σας ή την ημερομηνία γέννησής σας;

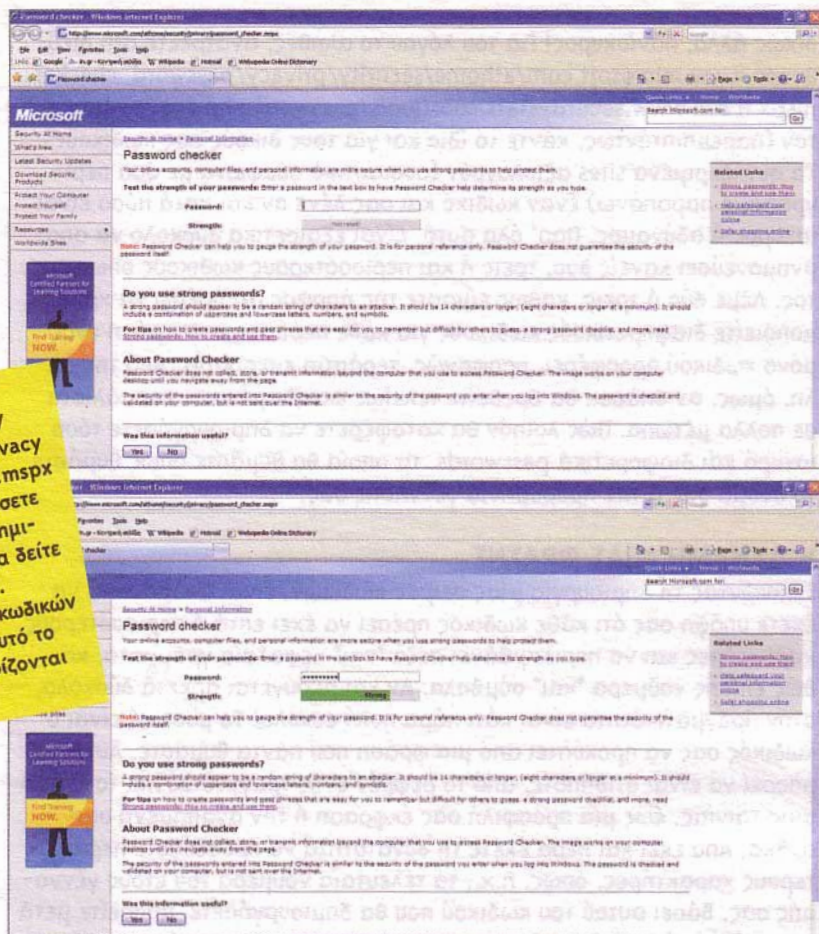
Η ΔΥΝΑΜΗ ΜΙΑΣ ΦΡΑΣΗΣ

Ξεκινώντας τη δημιουργία μιας σειράς κωδικών, είναι απαραίτητο να έχετε υπόψη σας ότι κάθε κωδικός πρέπει να έχει επτά ή περισσότερους χαρακτήρες και να περιλαμβάνει πεζά *και* κεφαλαία γράμματα, καθώς επίσης νούμερα *και* σύμβολα. Αν και ακούγεται αρκετά δύσκολο, στην πραγματικότητα είναι κάτι πάρα πολύ εύκολο! Το μυστικό είναι ο κωδικός σας να προκύπτει από μια φράση που πάντα θυμάστε. Αυτή μπορεί να είναι οτιδήποτε, από το ρεφρέν ενός τραγουδιού και τον τίτλο μιας ταινίας, έως μια προσφιλή σας έκφραση ή την αγαπημένη σας ατάκα. Από εκεί και πέρα έχετε τη δυνατότητα να προσθέσετε περισσότερους χαρακτήρες, όπως, π.χ., τα τελευταία νούμερα του έτους γέννησής σας. Βάσει αυτού του κωδικού που θα δημιουργήσετε, μπορείτε μετά να φτιάξετε ένα πλήθος άλλων, οι οποίοι θα διαφοροποιούνται σε ένα μόνο αριθμό, ο οποίος θα έχει το ρόλο του αύξοντα αριθμού. Για παράδειγμα, παίρνετε τα πρώτα γράμματα του γνωστού τραγουδιού «i love rock and roll». Επιλέγετε κάποια από τα γράμματα να είναι κεφαλαία και στο τέλος βάζετε ένα σύμβολο ακολουθούμενο από το έτος γέννησής σας. Έτσι, δημιουργείτε τον κωδικό iLRAR-80, όπου το 80 αντιπροσωπεύει το έτος γέννησής σας. Την λέξη and μπορείτε να την αντικαταστήσετε με το σύμβολο &, οπότε θα έχετε iLR&R-80. Επειδή αυτός θα είναι ο πρώτος κωδικός σας, κοτσάρετε στο τέλος και το 1. Το αποτέλεσμα, λοιπόν, είναι iLR&R-801. Αν ανησυχείτε μήπως το 1 σας προδώσει και ξεσκεπαστούν και οι υπόλοιποι κωδικοί σας, είτε το βάζετε σε ένα ξεκάρφωτο σημείο, όπως, π.χ., μετά το τελευταίο γράμμα (iLR&R1-80, iLR&R2-80, iLR&R3-80 κ.ο.κ.) είτε αντ' αυτού χρησιμοποιείτε γράμματα (iLR&Ra-80, iLR&Rb-80, iLR&Rc-80). Ο συγκεκριμένος κωδικός, εκτός του ότι είναι πραγματικά ισχυρός (μια δοκιμή θα σας πείσει), ακόμα και αν υποθέσετε ότι κάποιος θα τον βρει, θα είναι πολύ δύσκολο να φανταστεί ότι ο αριθμός 1 ή το γράμμα a αντιπροσωπεύουν τον αύξοντα αριθμό σας.

Τα πανίσχυρα password είναι άχρηστα όταν μεταδίδονται σε επισφαλή κανάλια επικοινωνίας. Δείτε γιατί – και διασκεδάστε με όσους περφανεύονται για την ασφάλεια των συστημάτων τους – στο άρθρο της σελίδας 92.



Στη διεύθυνση
www.microsoft.com/
athome/security/privacy/
password_checker.mspx
μπορείτε να δοκιμάσετε
το password που δημι-
ουργήσατε ώστε να δείτε
πόσο ισχυρό είναι.
Τα παραδείγματα κωδικών
που δώσαμε σ' αυτό το
άρθρο χαρακτηρίζονται
ως ισχυρά :)



Θέλετε άλλο παράδειγμα; Πάρτε τη ρήση «ουκ εν τω πολλώ το ευ». Σημειώστε τα πρώτα γράμματα κάθε λέξης και επιλέξτε ένα ή περισσότερα να είναι κεφαλαία. Μπορείτε, για παράδειγμα, να φτιάξετε τις λέξεις οε7pTe και οE7pTe. Τέλος, προσθέστε ανάμεσα στα γράμματα ή στο τέλος της λέξης το έτος γέννησής σας και τον αύξοντα αριθμό, διαχωρίζοντάς τες με σύμβολα, όπως, π.χ., οε7pTe/i/8o ή οE7pTe-i/8o. Όσο περίπλοκος και αλλόκοτος και αν φαίνεται αυτός ο κωδικός, δεν πρόκειται να τον ξεχάσετε ποτέ, αφού ουσιαστικά έχει προκύψει από την αγαπημένη σας φράση και το έτος γέννησής σας. Αν εφαρμόσετε αυτή τη λογική, θα δημιουργήσετε πραγματικά πανίσχυρα password, τα οποία θα είναι πολύ δύσκολο να σπάσουν. Τέλος, θα πρέπει να επισημάνουμε ότι όσο ισχυρός και αν είναι ένας κωδικός, όταν μεταδίδεται μέσα από ένα επισφαλές κανάλι επικοινωνίας, χωρίς κανενός είδους κρυπτογράφηση, τότε γίνεται το ίδιο ανίσχυρος με τον κωδικό που αποτελείται από ένα μόλις ψηφίο (βλ. άρθρο σελ. 92).

NaZ

Τώρα που μάθαμε πόσο εύκολα πραγματοποιείται το σνιφάρισμα σε ένα τοπικό δίκτυο (βλ. σελίδα 92), ήρθε η ώρα να δούμε τα μέτρα προστασίας που μπορούμε να πάρουμε. Η αλήθεια είναι ότι το anti-sniffing είναι μια εξαιρετικά δύσκολη υπόθεση, κυρίως γιατί από τη φύση του το πρωτόκολλο ARP είναι ευάλωτο σε επιθέσεις τύπου ARP poisoning. Αν και υπάρχουν διάφορες τεχνικές/μέθοδοι προστασίας, οι πλέον αποτελεσματικές άμυνες είναι δύο: η διαρκής (αυτοματοποιημένη) παρακολούθηση του ARP table για τον εντοπισμό αλλαγών στις διευθύνσεις MAC των συστημάτων, καθώς και η χρήση στατικών καταχωρίσεων. Ας πάρουμε όμως τα πράγματα από την αρχή...

ΜΕΘΟΔΟΙ ΠΡΟΣΤΑΣΙΑΣ ΑΠΟ ΤΗ ΔΗΛΗΤΗΡΙΑΣΗ

Ανάλογα με το αν είμαστε διαχειριστές του δικτύου ή απλοί χρήστες, θα στραφούμε σε διαφορετικές μεθόδους προστασίας. Οι διαχειριστές έχουν πρόσβαση στον router και δυνατότητα εποπτείας του συνολικού (τοπικού) δικτύου. Είναι σαφώς ευκολότερο για ένα διαχειριστή να εντοπίσει ή ακόμα και να αποτρέψει μια επίθεση ARP poisoning, απ' ό,τι για έναν απλό χρήστη, ενός απλού μηχανήματος, ο οποίος κάνει απλώς τη δουλειά του χωρίς να πειράζει κανέναν. Εδώ που τα λέμε, ο απλός χρήστης¹ μπορεί να αντιληφθεί μόνο τις επιθέσεις που γίνονται στο δικό του σύστημα χωρίς να γνωρίζει τι συμβαίνει στο υπόλοιπο δίκτυο.

Ο διαχειριστής είναι σε θέση να ανακαλύψει την παρουσία ή τη δράση, αν θέλετε, ενός sniffer από τη διακίνηση και μόνο των δικτυακών πακέτων. Και αυτό γιατί ο υπολογιστής μέσω του οποίου θα εξαπολυθεί μια επίθεση ARP poisoning είναι αρκετά πιθανό να παρουσιάζει μεγάλη κίνηση, αφού θα λαμβάνει όλα τα πακέτα που ανταλλάσσουν οι υπολογιστές που παρακολουθεί. Στην περίπτωση μάλιστα που ο άνθρωπος ο οποίος βρίσκεται πίσω από την επίθεση σνιφάρει ανεξέλεγκτα, ο υπολογιστής του θα παρουσιάζει ανεξήγητα υψηλή δικτυακή κίνηση, κάτι που ενδέχεται να τραβήξει εύκολα την προσοχή του διαχειριστή. Ένα ακόμα μεγάλο πλεονέκτημα του διαχειριστή έναντι του απλού χρήστη είναι ότι μπορεί ακόμα και να αποτρέψει μια επίθεση ARP poisoning. Αυτό που χρειάζεται να κάνει είναι να χρησιμοποιήσει στατικές καταχωρίσεις



Το Xarp είναι ένα καλό εργαλείο για να αντιληφθούμε αν κάποιος σνιφάρει τα πακέτα που μπεινοβαίνουν στο σύστημά μας. Το πρόγραμμα είναι πολύ μικρό σε μέγεθος και δεν χρειάζεται ούτε καν εγκατάσταση!

Xarp									
File	Action	?							
IP	MAC		in bytes	chance	last changed	vendor	network order IP	host order IP	type
✓ 192.168.1.46.2	00-0F-34-9C-24-00	yes			12:59:03	CiscoSystemsC	43452888	3232272088	dynamic
✓ 192.168.1.46.10	00-0C-F1-8A-FC-CA	yes			-	IntelCorporationC	177263615	3232272088	dynamic
✓ 192.168.1.46.11	00-0C-F1-8A-FC-CA	yes			-	IntelCorporationC	19160032	3232272088	dynamic
✓ 192.168.1.46.21	00-16-17-1A-00-34	no			-		36192992	3232272088	dynamic
✓ 192.168.1.46.46	00-00-87-62-62-60	no			-	INTEL CORPORATIONC	78126392	3232272088	dynamic
✓ 192.168.1.46.47	00-0F-EA-P0-9C-A2	no			12:55:33	Giga-ByteTechnologyC	79814568	3232272088	dynamic
✓ 192.168.1.46.56	00-00-87-6B-3C-3A	no			-	INTEL CORPORATIONC	94912992	3232272088	dynamic



1. Ξέρετε, ο ίδιος που κάθεται μπροστά από ένα απλό μηχάνημα και κάνει απλά τη δουλειά του χωρίς να πειράζει κανέναν.

IP	Selected selected entries	from system cache	vendor	network order IP	host order IP	type	adapter
✓	Clear output list						
✓	Discover using broadcast ping						
✓	192.168.146.11	00-0C-F1-6D-80-86	IntelCorporationC	17228166	323227296	dynamic	0-2 Bluetooth PAN Network Adapter...
✓	192.168.146.15	00-00-07-05-0F-F1	IntelCorporationC	19460832	323227267	dynamic	0-2 Bluetooth PAN Network Adapter...
✓	192.168.146.21	00-10-18-3A-00-24	IntelCorporationC	36126666	323227291	dynamic	0-2 Bluetooth PAN Network Adapter...
✓	192.168.146.26	00-10-26-CD-3D-C3		36102292	323227297	dynamic	0-2 Bluetooth PAN Network Adapter...
✓	192.168.146.27	00-14-00-00-0F-6E		40819072	323227262	dynamic	0-2 Bluetooth PAN Network Adapter...
✓	192.168.146.27	00-0E-46-43-65-6A		40287638	323227263	dynamic	0-2 Bluetooth PAN Network Adapter...
✓	192.168.146.36	00-0E-46-0C-06-06	ASUSTeKComputerIn	63808448	323227293	dynamic	0-2 Bluetooth PAN Network Adapter...
✓	192.168.146.36	00-0E-46-0C-06-06	ASUSTeKComputerIn	64745664	323227294	dynamic	0-2 Bluetooth PAN Network Adapter...
✓	192.168.146.49	00-11-39-05-82-86	IntelCorporationC	15343117	323227295	dynamic	0-2 Bluetooth PAN Network Adapter...
✓	192.168.146.53	00-60-85-26-CD-80	IntelCorporationC	82199540	323227296	dynamic	0-2 Bluetooth PAN Network Adapter...
✓	192.168.146.55	00-00-07-00-49-6F	IntelCorporationC	88883394	323227299	dynamic	0-2 Bluetooth PAN Network Adapter...
✓	192.168.146.55	00-00-07-00-49-6F	IntelCorporationC	93206136	323227261	dynamic	0-2 Bluetooth PAN Network Adapter...
✓	192.168.146.65	00-11-39-05-82-86	ASUSTeKComputerIn	1106130496	323227291	dynamic	0-2 Bluetooth PAN Network Adapter...
✓	192.168.146.71	00-00-07-00-49-6F	IntelCorporationC	11111111	323227262	dynamic	0-2 Bluetooth PAN Network Adapter...
✓	192.168.146.81	00-00-07-00-49-6F	IntelCorporationC	134860902	323227267	dynamic	0-2 Bluetooth PAN Network Adapter...
✓	192.168.146.85	00-00-07-0A-A7-4C	IntelCorporationC	1459374816	323227261	dynamic	0-2 Bluetooth PAN Network Adapter...
✓	192.168.146.86	00-10-0C-0C-02-33	HEICO-STARKORPORA	1459374816	323227262	dynamic	0-2 Bluetooth PAN Network Adapter...
✓	192.168.146.93	00-00-07-00-49-6F	IntelCorporationC	1459374816	323227262	dynamic	0-2 Bluetooth PAN Network Adapter...
✓	192.168.146.93	00-0F-6A-6A-6A-6A	Giga-ByteTechnologyC	173964704	323227299	dynamic	0-2 Bluetooth PAN Network Adapter...
✓	192.168.146.122	00-10-70-70-00-00		208443888	323227263	dynamic	0-2 Bluetooth PAN Network Adapter...



Μέσα από το Xarp μπορούμε να διαγράψουμε μεμονωμένες καταχωρίσεις ή ολόκληρο τον πίνακα ARP. Όποτε υπάρχουν πολλές καταχωρίσεις στον εν λόγω πίνακα, καλό είναι να χρησιμοποιούμε τη δυνατότητα αυτή, αφού διαφορετικά γίνεται δύσκολος ο έλεγχος των ύποπτων συνδέσεων.

στον πίνακα ARP. Βλέπετε, σε ένα στατικό πίνακα ARP η διεύθυνση IP κάθε υπολογιστή του δικτύου είναι αντιστοιχισμένη μονοσήμαντα σε μια διεύθυνση MAC – προφανώς σε αυτή της κάρτας δικτύου του. Έτσι, είναι πρακτικά αδύνατον κάποιος να σνιφάρει αλλάζοντας τις διευθύνσεις MAC! Βέβαια, οι στατικοί πίνακες εξασφαλίζουν μεν ασφάλεια, ωστόσο προϋποθέτουν ότι σε κάθε υπολογιστή του δικτύου θα προστεθούν όλες οι αντιστοιχίσεις διευθύνσεων IP και MAC. Σε μικρά δίκτυα οι στατικές καταχωρίσεις αποτελούν άριστη λύση, καθώς μπορούν να υλοποιηθούν και να συντηρηθούν χωρίς μεγάλο κόπο. Όμως σε μεγάλα δίκτυα, π.χ., των 20 και πλέον υπολογιστών, είναι κάτι πρακτικά ανέφικτο, αφού σε κάθε υπολογιστή θα πρέπει να δηλωθούν όλες οι αντιστοιχίσεις διευθύνσεων IP και MAC και σε οποιαδήποτε αλλαγή, όπως, π.χ., αντικατάσταση μιας κάρτας δικτύου, είναι απαραίτητο να επαναλαμβάνεται η ίδια διαδικασία. Εξετάζοντας το θέμα από την πλευρά του απλού χρήστη, γρήγορα διαπιστώνουμε ότι τα πράγματα είναι πολύ πιο ζόρικα, αφού δεν υπάρχει κανένα ουσιαστικό μέτρο αποτροπής του σνιφάρισματος. Το μόνο που μπορούμε να κάνουμε ως απλοί χρήστες, όταν υποψιαζόμαστε ότι μας παρακολουθούν, είναι να εγκαταστήσουμε ένα... συναγερμό, ο οποίος θα χτυπάει κάθε φορά που κάποιος θα επιχειρεί να σνιφάρει πακέτα που μπαίνουν και βγαίνουν από το μηχανήμα μας. Έχοντας πλέον βεβαιωθεί ότι είμαστε υπό παρακολούθηση, μπορούμε μόνοι μας ή με τη βοήθεια του διαχειριστή να ξετρυπώσουμε-ξεντροπιάσουμε τον άνθρωπο που μας παρακολουθεί².

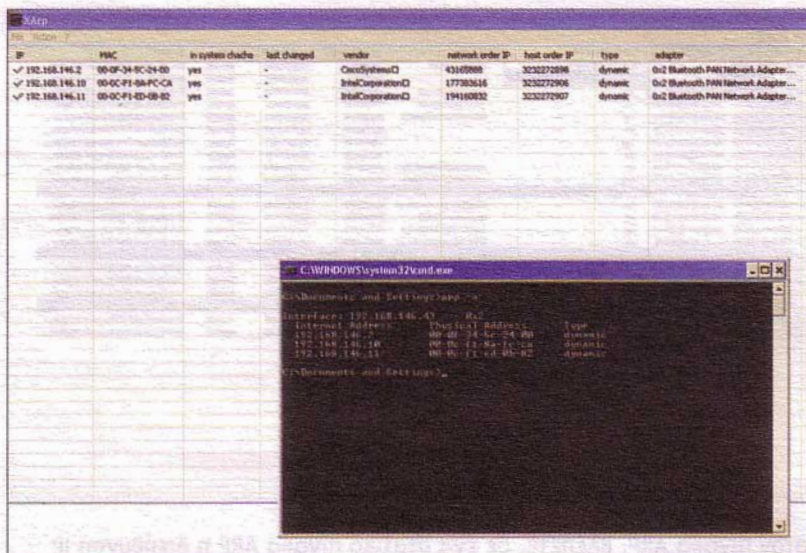


2. Αρκεί βέβαια εκείνος που σνιφάρει να μην το κάνει με τις ευλογίες του διαχειριστή ή/και του διευθυντή, π.χ., στο πλαίσιο της προετοιμασίας ενός σχετικού άρθρου για το total XakeR :-)





Στα Windows
θα δούμε τον
πίνακα ARP
ηλεκτρολογώντας
την εντολή
arp -a σε ένα
Command
Prompt.



ΝΤΕΤΕΚΤΙΒ Χαρπ ΣΤΙΣ ΨΗΗΡΕΣΙΕΣ ΣΑΣ!

Το πόσο εύκολο είναι να ανακαλύψουμε αν σνιφάρουν τα πακέτα μας εξαρτάται κυρίως από το λειτουργικό σύστημα το οποίο χρησιμοποιούμε, τα εργαλεία που έχουμε στη διάθεσή μας, αλλά και από τις ικανότητες απόκρυψης του προγράμματος-sniffer. (Όπως λέει και ο λαός μας, δεν αρκεί να ξέρεις να κλέβεις· πρέπει να ξέρεις και να κρύβεσαι, γιατί αλλιώς δεν κάνεις για κλέφτης!) Ένα από τα εργαλεία που ξεχωρίζει στην πλατφόρμα των Windows είναι το Χαρπ. Το πρόγραμμα διατίθεται δωρεάν, είναι πολύ απλό στη χρήση και δεν χρειάζεται ούτε καν εγκατάσταση. Το σημαντικότερο όπλο του, ωστόσο, είναι ότι αντιλαμβάνεται σχεδόν οποιαδήποτε απόπειρα ARP poisoning ενάντια στο PC στο οποίο τρέχει. Έχει μέγεθος περί τα 800kb και μπορείτε να το κατεβάσετε από τη διεύθυνση www.chrismc.de. Κυκλοφορεί σε δύο εκδόσεις: τη 0.1.5 και τη 2. Η πρώτη είναι τελική έκδοση (stable) και λειτουργεί χωρίς κανένα πρόβλημα, ενώ η δεύτερη είναι ακόμα σε φάση beta (παρ' όλα αυτά, έχετε τη δυνατότητα να την κατεβάσετε και να τη δοκιμάσετε). Θα σταθούμε στη 0.1.5, η οποία είναι λιτή, απλή στη χρήση και πλήρως λειτουργική.

Το πρόγραμμα δεν κάνει τίποτε περισσότερο από το να παρακολουθεί και να καταγράφει τις καταχωρίσεις και τις αλλαγές που γίνονται στο (δυναμικό) πίνακα ARP του συστήματος στο οποίο τρέχει. Αυτή η απλή δουλειά είναι αρκετή για να γίνει αντιληπτή μια απόπειρα σνιφαρίσματος πακέτων. Σημειώστε ότι ο πίνακας ARP πρακτικά μας δείχνει τα συστήματα με τα οποία είχε συνδεθεί ο υπολογιστής μας το τελευταίο χρονικό διάστημα, από τη στιγμή που τον ανοίξαμε. Σε ένα μεγάλο τοπικό δίκτυο με domain server και πρόσβαση στο Internet, αν δεν έχουμε κά- νει τίποτε άλλο από το να επισκεφθούμε μερικά site, στις καταχωρίσεις

Εντάξει, σουχάσατε από τους αδιάκριτους χρήστες του LAN. Ωρα για χαλάρωση και παιχνίδι - γιατί όχι με το Lineage; Ελάτε, μην το σκέπτεστε, έχουμε και cheats! (σελ. 132)



του ARP θα περιλαμβάνονται οι διευθύνσεις IP του συστήματος που εκτελεί χρέη gateway (dedicated router ή υπολογιστής), καθώς και των συστημάτων που εκτελούν χρέη DNS και domain server. Κάθε φορά που πραγματοποιείται μια σύνδεση με έναν υπολογιστή του δικτύου (έστω και αν αυτή προέκυψε από ένα απλό ping το οποίο έκανε κάποιος στο σύστημά μας ή από πρόσβαση σε ένα μοιραζόμενο πόρο), αυτόματα ο υπολογιστής αυτός προστίθεται στον πίνακα ARP. Πώς, λοιπόν, θα ξεχωρίσουμε μέσα από το Χαρπ ποιος είναι αθώος και ποιος ένοχος ή έστω ποιος είναι ύποπτος και ποιος όχι; Απλούστατα, ελέγχοντας τις διευθύνσεις MAC των υπολογιστών που μας δείχνει το Χαρπ. Αν κάποιος πράγματι σνιφάρει τα πακέτα μας, θα δούμε στο Χαρπ δύο διαφορετικές διευθύνσεις IP να αντιστοιχούν σε μία μόνο διεύθυνση MAC! Στην περίπτωση μάλιστα που ο υπολογιστής στον οποίο θα μεταμφιεστεί ο sniffer περιλαμβάνεται ήδη στον πίνακα ARP, το πρόγραμμα θα αντιληφθεί την αλλαγή διεύθυνσης MAC και θα μας ενημερώσει.

Ας δούμε ένα παράδειγμα στην πράξη. Υποθέτουμε ότι κάποιος θέλει να κατασκοπεύσει τα site που επισκεπτεύετε (πάντα με τη μέθοδο του ARP poisoning). Αυτό που θα κάνει είναι να μπει ανάμεσα στον υπολογιστή σας και τον router, δηλώνοντας στον μεν router ότι είναι εσείς, στο δε υπολογιστή σας ότι είναι ο router. Μόλις συνδεθεί ο κατάσκοπος στον υπολογιστή σας παριστάνοντας τον router, το Χαρπ αμέσως θα τον

Μόλις το Χαρπ αντιληφθεί αλλαγή μιας διεύθυνσης MAC, θα καταγράψει το γεγονός στο πλαίσιο αναφορών που βρίσκεται ακριβώς κάτω από τη λίστα καταχωρίσεων. Όταν σας σνιφάρουν πακέτα, θα δείτε, λογικά, έναν υπολογιστή (αυτόν με τον οποίο ανταλλάσσετε δεδομένα) να αλλάζει διεύθυνση MAC δύο φορές. Μία στην αρχή, όταν θα μπει ανάμεσά σας ο sniffer, και μία αφού αποχωρήσει.



Χαρπ									
File	Action	?							
IP	MAC	in system cache	last changed	vendor	network order IP	host order IP	type	adapter	
✓ 192.168.146.2	00-0F-34-5C-24-00	yes	12:50:20	CiscoSystemsC	43165808	3232272898	dynamic	Dn2 Bluetooth PAN Network Adapter...	
✓ 192.168.146.5	00-11-06-C2-6E-0C	no	-	-	93497936	3232272901	dynamic	Dn2 Bluetooth PAN Network Adapter...	
✓ 192.168.146.19	00-0C-F1-6A-F0-CA	yes	-	IntelCorporationC	177303616	3232272906	dynamic	Dn2 Bluetooth PAN Network Adapter...	
✓ 192.168.146.11	00-0C-F1-6D-08-82	yes	-	IntelCorporationC	194168832	3232272907	dynamic	Dn2 Bluetooth PAN Network Adapter...	
✓ 192.168.146.15	00-00-87-15-0F-F1	yes	-	INTELCORPORATIONC	261265966	3232272911	dynamic	Dn2 Bluetooth PAN Network Adapter...	
✓ 192.168.146.21	00-16-17-1A-0A-03	yes	-	-	36192992	3232272917	dynamic	Dn2 Bluetooth PAN Network Adapter...	
✓ 192.168.146.26	00-16-36-C2-3C-05	no	-	-	445819072	3232272922	dynamic	Dn2 Bluetooth PAN Network Adapter...	
✓ 192.168.146.27	00-14-89-05-0F-E0	no	-	-	462596288	3232272923	dynamic	Dn2 Bluetooth PAN Network Adapter...	
✓ 192.168.146.37	00-0E-46-A1-95-6A	no	-	ASUSTeKComputerInc	63026940	3232272923	dynamic	Dn2 Bluetooth PAN Network Adapter...	
✓ 192.168.146.38	00-0E-A6-9C-0A-36	no	-	ASUSTeKComputerInc	647145664	3232272924	dynamic	Dn2 Bluetooth PAN Network Adapter...	
✓ 192.168.146.41	00-00-87-C0-97-62	no	-	INTELCORPORATIONC	662477312	3232272937	dynamic	Dn2 Bluetooth PAN Network Adapter...	
✓ 192.168.146.46	00-00-87-82-82-60	yes	-	INTELCORPORATIONC	781363392	3232272942	dynamic	Dn2 Bluetooth PAN Network Adapter...	
✓ 192.168.146.47	00-00-87-82-82-60	yes	12:50:36	INTELCORPORATIONC	798140608	3232272943	dynamic	Dn2 Bluetooth PAN Network Adapter...	
✓ 192.168.146.49	00-11-0F-95-82-80	no	-	ASUSTeKComputerInc	831895960	3232272945	dynamic	Dn2 Bluetooth PAN Network Adapter...	
✓ 192.168.146.53	00-02-83-28-C2-80	no	-	IntelCorporationC	898803904	3232272949	dynamic	Dn2 Bluetooth PAN Network Adapter...	
✓ 192.168.146.55	00-00-87-90-49-0F	no	-	INTELCORPORATIONC	932358336	3232272951	dynamic	Dn2 Bluetooth PAN Network Adapter...	
✓ 192.168.146.65	00-11-2F-95-82-8E	no	-	ASUSTeKComputerInc	1108130496	3232272961	dynamic	Dn2 Bluetooth PAN Network Adapter...	
✓ 192.168.146.70	00-02-49-58-02-02	no	-	IntelCorporationC	1194516576	3232272966	dynamic	Dn2 Bluetooth PAN Network Adapter...	
✓ 192.168.146.81	00-00-87-40-94-C2	no	-	INTELCORPORATIONC	136668992	3232272977	dynamic	Dn2 Bluetooth PAN Network Adapter...	
✓ 192.168.146.85	00-00-87-5A-47-4C	no	-	INTELCORPORATIONC	1425648816	3232272981	dynamic	Dn2 Bluetooth PAN Network Adapter...	
✓ 192.168.146.96	00-10-0C-4C-08-31	no	-	MICRO-STARINTERNA...	1452462032	3232272982	dynamic	Dn2 Bluetooth PAN Network Adapter...	
✓ 192.168.146.98	00-00-87-60-38-27	no	-	INTELCORPORATIONC	1480090464	3232272984	dynamic	Dn2 Bluetooth PAN Network Adapter...	
✓ 192.168.146.103	00-0F-EA-66-A8-C3	no	-	Giga-ByteTechnologyC...	1737664704	3232272999	dynamic	Dn2 Bluetooth PAN Network Adapter...	
✓ 192.168.146.112	00-15-F2-78-16-05	no	-	-	2056431808	3232273018	dynamic	Dn2 Bluetooth PAN Network Adapter...	

1 : 12:49:47: Mapping changed: 192.168.146.2 changed from 00-0F-34-5C-24-00 to 00-00-87-82-82-60
 2 : 12:50:20: Mapping changed: 192.168.146.2 changed from 00-00-87-82-82-60 to 00-0F-34-5C-24-00
 3 : 12:50:36: Mapping changed: 192.168.146.47 changed from 00-0F-EA-66-A8-C3 to 00-00-87-82-82-60



Το Χαρρ κάθεται στο notification bar των ΧΡ και σιωπηρά παρακολουθεί τον πίνακα ARP. Σε περίπτωση αλλαγής θα δείτε να σας εμφανίζει σχετικό μήνυμα στο notification bar.

IP	MAC	In network interface	Last changed	Vendor	Network order ID	Host name ID	Type	Address
✓ 192.168.1.42.2	00-00-00-00-00-00	yes	12-05-05	NETELCORP/AT/0302	439-00001	0012070000	dynamic	612 Bluetooth-Fake Network Adapter...
✓ 192.168.1.42.3	00-00-00-00-00-00	yes	12-05-05	NETELCORP/AT/0302	439-00001	0012070000	dynamic	612 Bluetooth-Fake Network Adapter...
✓ 192.168.1.42.4	00-00-00-00-00-00	yes	12-05-05	NETELCORP/AT/0302	439-00001	0012070000	dynamic	612 Bluetooth-Fake Network Adapter...
✓ 192.168.1.42.5	00-00-00-00-00-00	yes	12-05-05	NETELCORP/AT/0302	439-00001	0012070000	dynamic	612 Bluetooth-Fake Network Adapter...
✓ 192.168.1.42.6	00-00-00-00-00-00	yes	12-05-05	NETELCORP/AT/0302	439-00001	0012070000	dynamic	612 Bluetooth-Fake Network Adapter...
✓ 192.168.1.42.7	00-00-00-00-00-00	yes	12-05-05	NETELCORP/AT/0302	439-00001	0012070000	dynamic	612 Bluetooth-Fake Network Adapter...
✓ 192.168.1.42.8	00-00-00-00-00-00	yes	12-05-05	NETELCORP/AT/0302	439-00001	0012070000	dynamic	612 Bluetooth-Fake Network Adapter...
✓ 192.168.1.42.9	00-00-00-00-00-00	yes	12-05-05	NETELCORP/AT/0302	439-00001	0012070000	dynamic	612 Bluetooth-Fake Network Adapter...
✓ 192.168.1.42.10	00-00-00-00-00-00	yes	12-05-05	NETELCORP/AT/0302	439-00001	0012070000	dynamic	612 Bluetooth-Fake Network Adapter...

εμφανίσει στη λίστα του. Ωστόσο, το γεγονός αυτό από μόνο του δεν έχει να πει τίποτε, καθώς δεν θα ξέρετε ποιος ήταν ο πραγματικός λόγος που εμφανίστηκε στη λίστα του Χαρρ. Θα μπορούσε, για παράδειγμα, να σας έχει κάνει ένα ring ή να έχει ρίξει μια ματιά σε κάποιον κοινό-χρηστο φάκελό σας. Αν όμως ελέγξετε τη διεύθυνση MAC του, θα παρατηρήσετε ότι είναι ακριβώς ίδια με εκείνη του router. Ακόμα και αν ο sniffer κρύψει την πραγματική του διεύθυνση, κάνοντας IP spoofing, όταν θα αλλάξει η διεύθυνση MAC του router, το Χαρρ θα το αντιληφθεί και θα σας ενημερώσει. Συνεπώς, στη χειρότερη των περιπτώσεων μπορεί να μην εντοπίσετε ποιος χρήστης χειρίζεται τον sniffer, θα αντιληφθείτε όμως ότι κάποιος σνιφάρει τα πακέτα σας. Σε πολλές περιπτώσεις αυτό είναι αρκετό για να προστατευτείτε.

Η ΕΝΤΟΛΗ ARP

Τον πίνακα ARP του συστήματός μας μπορούμε να τον δούμε και πληκτρολογώντας την εντολή `arp -a` σε Command Prompt. Πρακτικά θα δούμε τις ίδιες ακριβώς πληροφορίες που μας δείχνει και το Χαρρ. Επειδή όμως η συγκεκριμένη εντολή δεν δείχνει τις μεταβολές του πίνακα σε πραγματικό χρόνο, αλλά μόνο τις καταχωρίσεις που περιλάμβανε μόλις πατήσαμε [Enter], δεν μπορεί να αποτελέσει αξιόπιστο όπλο κατά του ARP poisoning. Επίσης, ανάλογα με το πρόγραμμα-sniffer, το `arp` ενδέχεται να μη μας δείξει το σύστημα που σνιφάρει τον υπολογιστή μας. Η εντολή `arp` μπορεί να μας δώσει μια ιδέα για το αν συμβαίνει κάτι ύποπτο μόνο αν την εκτελέσουμε πριν και μετά την επίθεση και συγκρίνουμε τις καταχωρίσεις. Μέσω της ίδιας εντολής θα διαγράψουμε καταχωρίσεις, θα δημιουργήσουμε στατικές αντιστοιχίσεις διευθύνσεων IP σε MAC κ.λπ. Δώστε `arp /?` προκειμένου να πάρετε περισσότερες πληροφορίες για τη χρήση της εντολής.