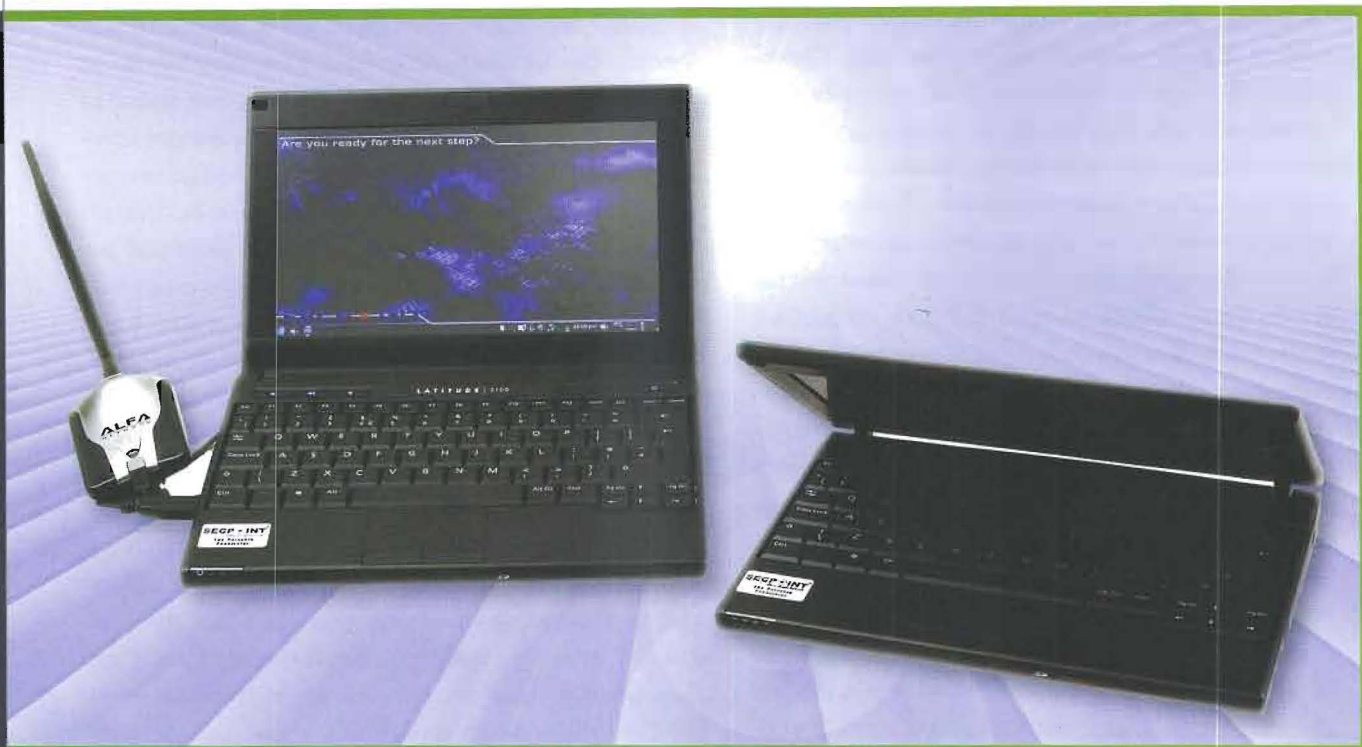


«Ηθικό» hacking



Ο φαινομενικά αντιφατικός όρος «ηθικό» hacking επινοήθηκε για να περιγράψει τη χρήση μεθόδων και εργαλείων των hackers, με σκοπό τη γνώση των ελλείψεων ενός συστήματος IT και την επακόλουθη θωράκισή του.



Ο πυρήνας της φιλοσοφίας του «ηθικού» hacking μεταφέρεται αυτούσια και σε έννοιες όπως το penetration testing και το vulnerability testing, που δικαίως θεωρούνται και ταυτόσημες. Ένας από τους πιο έμπειρους και καταρτισμένους γνώστες της παραπάνω ορολογίας είναι η εταιρεία SecPoint®, η οποία συνδυάζοντας την τεχνογνωσία και την επιστημονική επάρκεια, έχει συγκεντρώσει τους μηχανισμούς του τρόπου δράσης των hackers σε μία συσκευή, το Portable Penetrator. Η καινοτομία του συγκεκριμένου συστήματος έγκειται στη δυνατότητα που παρέχει στους χρήστες πραγματοποίησης penetration testing ΚΑΙ σε ασύρματα δίκτυα, τα οποία απο-

δεικνύονται ιδιαίτερα ευπαθή και χρήζουν προστασίας. Επικρατεί η αντίληψη ότι η θωράκιση ενός ασύρματου δικτύου δεν θα έπρεπε να αποτελεί προτεραιότητα των χρηστών, μιας και η ασφάλεια του δικτύου εξασφαλίζεται επαρκώς με ένα κλειδί. Η διάψευση της συγκεκριμένης αντίληψης βρίσκεται στη μάλλον απογοητευτική αλήθεια της τρωτής φύσης των δικτύων σε επιθέσεις, ακόμα και με απουσία ασύρματης σύνδεσης. Η κατανόηση της αναγκαιότητας προστασίας των ασύρματων δικτύων γίνεται εμφανής μετά την κατανόηση των μειονεκτικών σημείων των Wi-Fi δικτύων, καθώς και την ενδελεχή μελέτη των μεθόδων επίθεσης που υφίστανται.

Το encryption μπορεί ίσως να θεωρηθεί ως πρωτεύουσα πηγή ευπάθειας του συστήματος. Αρχικά χρησιμοποιήθηκε το WEP (Wired Equivalent Privacy), το οποίο αν και θεωρείται πλέον ξεπερασμένο, χρησιμοποιείται ακόμα σε μεγάλη κλίμακα. Το βασικό του πρόβλημα είναι ότι αν ο επίδοξος hacker μπορεί να λαμβάνει πακέτα, είναι θέμα χρόνου μέχρι να βρει το κλειδί. Και ο χρόνος αυτός είναι εξαιρετικά περιορισμένος, μια και τα κλειδιά είναι 128-bit ή 256-bit. Το WEP encryption αδυνατεί να χειριστεί το θέμα διαχείρισης των κλειδιών (όλοι οι χρήστες έχουν το ίδιο) και όταν τελικά σπάσει, ο hacker αποκτά πρόσβαση σε όλους τους χρήστες.

Η αναγνώριση των αδυναμιών του WEP encryption οδήγησε αναπόφευκτα στην κυκλοφορία των διαδόχων του, του WPA και του WPA2 (Wi-Fi Protected Access) encryption, τα οποία χρησιμοποιούν TKIP και AES-CCMP αλγόριθμους. Αν και πολύ πιο ασφαλή, εμφανίζουν και αυτά αδυναμίες σε dictionary attacks. Το Hole 196 είναι ένα vulnerability στο πρωτόκολλο ασφαλείας του WPA2. Μέσω αυτού δεν μπορεί κάποιος να σπάσει το encryption, μπορεί όμως να μολύνει κάθε εξουσιοδοτημένο χρήστη στο ασύρματο δίκτυο.

Συγκεκριμένα, τα WPA2 πρωτόκολλα ασφαλείας χρησιμοποιούν ένα group temporal key (GTK), το οποίο μοιράζονται όλοι οι χρήστες. Έτσι, ένας εξουσιοδοτημένος χρήστης έχει τη δυνατότητα να στείλει παραποιημένα αρχεία και μάλιστα encrypted, σε οποιονδήποτε άλλο χρήστη του ασύρματου δικτύου. Έχει επίσης τη δυνατότητα να βρει δεδομένα και ευπάθειες οποιουδήποτε συστήματος βρίσκεται συνδεδεμένο στο ασύρματο δίκτυο και να εξαπολύσει man-in-the-middle και Denial of Service (DoS) attacks, περνώντας επιβλαβείς κώδικες και σε άλλες ασύρματες συσκευές. Αφού όλα αυτά ολοκληρωθούν, το traffic μπορεί ξανά να προωθηθεί στο πραγματικό gateway του δικτύου. Το Hole 196 vulnerability αποτελεί θεμελιώδες σφάλμα στο σχεδιασμό του WPA2 και ανεξάρτητα με το authentication (PSK ή 802.1x) και το encryption (AES), όλα τα δίκτυα είναι τρωτά στο exploit αυτό.

Ένα φαινόμενο που παρατηρείται τελευταία και που συχνά καταλήγει στη μόλυνση υπολογιστών ασύρματων δικτύων, είναι η σύνδεση χρηστών σε μη εξουσιοδοτημένα δίκτυα από το χώρο εργασίας, λόγω κακής ή παντελούς έλλειψης του το-

πικού εταιρικού δικτύου. Στο ίδιο αποτέλεσμα μπορεί να καταλήξουν και οι ενέργειες ενός επίδοξου hacker, ο οποίος στήνοντας ένα ασύρματο δίκτυο με το όνομα της στοχευόμενης εταιρείας και με δυνατό σήμα, «ξεγελάει» τους χρήστες. Τα τρωτά σημεία των ασύρματων δικτύων γίνονται εξαιρετικά εμφανή και στους χώρους κοινής χρήσης ασύρματων δικτύων (hotspot), όπου οι υπολογιστές εκτίθενται απροστάτευτοι στους κινδύνους του hacking.

Το εύρος του προβλήματος διογκώνεται, αναλογιζόμενοι ότι για να μολυνθεί ένας φορητός υπολογιστής δεν χρειάζεται να βρίσκεται στα στενά όρια του χώρου εργασίας. Η

δε μόλυνσή του έχει ως συνέπεια την πιθανή υποκλοπή αρχείων μείζονος σημασίας και τη μόλυνση μιας ευρύτερης ομάδας υπολογιστών που οδηγούν αναπόφευκτα στη μείωση της αξιοπιστίας του παρόχου της ασύρματης σύνδεσης αλλά και του επιπέδου ασφαλείας της εταιρείας. Συμπολογίζοντας την ευρύτητα χρήσης των Wi-Fi δικτύων και των συσκευών που συνδέονται σε αυτά (laptops smartphones, PDAs, iPADS), ο κίνδυνος μόλυνσης γίνεται σαφώς πιο πραγματικός.

Συνοψίζοντας, η πολιτική της μη-χρήσεως ασύρματου δικτύου δεν παρέχει καμία απολύτως ασφάλεια λόγω της ελεύθερης διακίνησης και συνεχούς εξέλιξης των μεθόδων,

εργαλείων και οδηγών hacking, που έχει ως αποτέλεσμα την αύξηση του αριθμού των επιτυχών επιθέσεων. Τι μπορεί λοιπόν να κάνει κάποιος για να προστατέψει το δίκτυο της εταιρείας που εργάζεται;

Η SecPoint® κατανοώντας την έλλειψη χρόνου των IT Managers (υπευθύνων) και την ελλιπή εκπαίδευση των χρηστών στους εργασιακούς χώρους, καλύπτει επιτυχώς τις ανάγκες ασφαλείας IT κάθε δυναμικής εταιρείας. Γνωρίζοντας καλά τη νοοτροπία των hackers και χρησιμοποιώντας τις ίδιες μεθόδους, εντοπίζει κάθε ευπάθεια του δικτύου σας και προστατεύει μέχρι και Layer 7. Το ρίσκο είναι αρκετά υψηλό και ο hacker θα χτυπήσει πάντα εκεί που είναι πιο εύκολο. Και μην ανησυχείτε για την έλλειψη χρόνου, το Portable Penetrator είναι πάντα ενημερωμένο και μπορεί να στοχεύσει μέχρι και τα zero-day threats. **ITSecurity**

Επικοινωνία:

SecPoint Hellas • Τηλ.: 210 6108000
www.secpoint.co.gr • info@secpoint.co.gr

