

REVIEW

Secpoint Portable Penetrator

Φορητός Έλεγχος Διεισδύσεων

Μια φορητή λύση για αξιολόγηση της ευπάθειας σε ασύρματα και ενσύρματα δίκτυα, αποτελεί το Portable Penetrator της Secpoint, η χρήση του οποίου είναι σίγουρο ότι θα ενισχύει το επίπεδο ασφάλειας σε μια εταιρική υποδομή πληροφορικής.

SECPPOINT
www.secpoint.com



τα πλαίσια των ολοκληρωμένων λύσεων ασφάλειας που διαθέτει η προερχόμενη από τη Δανία εταιρεία Secpoint, η οποία αντιπροσωπεύεται στη χώρα μας από την εταιρεία **K & G Digital Service**, συναντάμε και το Portable Penetrator. Αποτελεί μια φορητή λύση που επιτρέπει να κά-νουμε security audit σε ασύρματα και ενσύρματα δίκτυα, εκτελώντας παράλληλα διεισδύσεις σε όλα τα πρωτόκολλα WEP, WPA και WPA2. Οι λειτουργίες αυτές αποσκοπούν στη διαχείριση και αξιολόγηση ευπάθειας σε όλα τα δίκτυα μιας επιχείρησης, κάτι που αποτελεί προτεραιότητα σε οποιαδήποτε πολιτική εταιρείας ασφάλειας, ιδιαίτερα σήμερα όπου οι κίνδυνοι που ελλοχεύουν είναι ποσοτικά αρκετοί και μπορούν να προκαλέσουν σημαντικές ζημιές. Το Portable Penetrator δεν διαφέρει σχεδιαστικά από ένα φορητό υπολογιστή, κάτι που θεωρείται πλεονέκτημα, μιας και οι χρήστες του συστήματος εξοικειώνονται άμεσα με το χειρισμό του. Στην ουσία όμως, αυτό που επιφανειακά θυμίζει ένα απλό laptop, είναι ένα σύστημα το οποίο συνδυάζει τα πλέον σύγχρονα εργαλεία hacking και cracking, αποτελώντας έτσι μια πλήρη λύση δοκιμής διείσδυσης. Για το λόγο αυτό, εκτός από Windows XP ή Vista Business, υποστηρίζει και σύστημα Linux. Όσον αφορά τις δυνατότητές του και συγκεκριμένα το auditing σε ασύρματα δίκτυα, το Portable Penetrator υποστηρίζει όπως προαναφέραμε, τα πρότυπα WEP, WPA και WPA2, αναδεικνύοντας κάθε ευπάθεια των δικτύων και λειτουργώντας έτσι όπως κάθε επιτιθέμενος θα ενεργούσε. Με αυτόν τον τρόπο, προβάλλει ταυτόχρονα πώς μπορεί να εξαλειφθεί κάθε αδυναμία του δικτύου, έτσι ώστε να το προστατεύσει πιο αποτελεσματικά. Η Data Base του Penetrator βασίζεται σε έρευνες άνω των δέκα ετών και διαθέτει πάνω 10.000 μοναδικές υπογραφές ευπάθειας, ενώ η βάση δεδομένων ανανεώνεται συνεχώς και κάθε μέρα. Ο διαχειριστής του δικτύου μπορεί να προωθήσει πραγματικά exploits (επιθέσεις) προκειμένου να ελέγξει ότι μια προσδιορισμένη ευπάθεια είναι εκμεταλλεύσιμη. Είναι επίσης δυνατό να προωθηθεί πραγματική Denial of Service επίθεση σε συστήματα προ-παραγωγής, για έλεγχο και δοκιμή της σταθερότητάς τους. Η έκδοση αναφορών, αλλά και το μαρκάρισμα των εκθέσεων και η προσωποποίηση για κάθε χρήστη ξεχωριστά, αποδεικνύονται αρκετά χρήσιμες για ένα πλήθος εφαρμογών, ενώ αξίζει να σημειωθεί ότι ο φορητός Penetrator υποστηρίζει security audit για κάθε λειτουργικό σύστημα. Παράλληλα, παρέχει λεπτομερείς θεραπείες για προσδιορισμένες ευπάθειες, κάτι που επιτρέπει στο διαχειριστή δικτύων να διορθώσει ταχύτατα τις αναγνωρισμένες τρωτότητες. Επίσης έχει τη δυνατότητα αυτόματων προσαρμογών της βάσης δεδομένων, συνεχώς, στις απαιτήσεις κάθε εφαρμογής.

Διάθεση: **K & G Digital Service**, τηλ.: 210-6641362 **ITSecurity**