ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Ακαδημαϊκό Έτος 1999-2000
Εξάμηνο Σπουδών Η

Μάθημα : Ασφάλεια Πληροφοριακών Συστημάτων
Διδάσκων : κ. Δημήτρης Γκρίτζαλης

Εργαστηριακή Άσκηση SM-5/TL-UG : Ανίχνευση προσβολών στην πράξη

Μέλη ομάδας εκπόνησης :
Οικονομίδης Δημήτριος 3960070
Παπαϊωάννου Μιχαήλ 3960004

Αθήνα, Μάιος 2000

Πίνακας Περιεχομένων

1. Εισαγωγή στα Συστήματα Ανίχνευσης Εισβολών 3
2. Tripwire 5
Σκοπός 5
Αρχιτεκτονική και χαρακτηριστικά 6
Διαδικασίες εγκατάστασης και διαχείρισης 6
Λειτουργία σε επίπεδο τελικού χρηστή (end-user) 7
Περιορισμοί από την χρήση 8
3. COPS 9
Σκοπός 9
Αρχιτεκτονική και χαρακτηριστικά 9
Διαδικασίες εγκατάστασης και διαχείρισης 10
Λειτουργία σε επίπεδο τελικού χρηστή (end-user) 11
Περιορισμοί από την χρήση 11
4. SATAN 12
Σκοπός 12
Αρχιτεκτονική και χαρακτηριστικά 13
Διαδικασίες εγκατάστασης και διαχείρισης 13
Λειτουργία σε επίπεδο τελικού χρηστή (end-user) 15
Περιορισμοί από την χρήση 16
Σχόλια για το SATAN 16
5. Crack 17
Σκοπός 17
Αρχιτεκτονική και χαρακτηριστικά 17
Διαδικασίες εγκατάστασης και διαχείρισης 18
Λειτουργία σε επίπεδο τελικού χρηστή (end-user) 18
Περιορισμοί από την χρήση 19
Ββιβλιογραφία – References 20

1.Εισαγωγή στα Συστήματα Ανίχνευσης Εισβολών (Intrusion Detection Systems)

Μια εισβολή (intrusion) πραγματοποιείται όταν κάποιος "hacker" ή "cracker" προσπαθεί να εισέλθει παράνομα και να κάνει κακή χρήση (misuse) ενός συστήματος. Η λέξη "misuse" είναι ευρεία και μπορεί να σημαίνει κάτι σοβαρό όπως κλοπή εμπιστευτικών δεδομένων ή κάτι πιο ελαφρύ όπως η κατάχρηση του email συστήματος για Spam-mails.

Ενα Σύστημα Ανίχνευσης Εισβολών ("Intrusion Detection System (IDS)") είναι ένα Σύστημα που ανιχνεύει τέτοιες εισβολές. Τα IDS μπορούν να χωριστούν στις εξής κατηγορίες :

Network intrusion detection systems (NIDS) : Παρακολουθούν πακέτα στο δίκτυο και προσπαθούν να ανακαλύψουν εάν κάποιος hacker/cracker προσπαθεί να μπει στο Σύστημα, ή να προκαλέσει μια επίθεση άρνησης υπηρεσίας (denial of service). Ένα NIDS μπορεί να τρέχει είτε στην μηχανή-target που παρακολουθεί την δική της κίνηση, είτε σε μια ανεξάρτητη μηχανή που παρακολουθεί όλη την κίνηση του δικτύου(hub, router, probe). Ένα "network" IDS παρακολουθεί πολλές μηχανές, ενώ τα άλλα παρακολουθούν μόνο την μηχανή στην οποία είναι εγκατεστημένα.

System integrity verifiers (SIV) : Παρακολουθούν τα αρχεία συστήματος για να βρουν πότε ένας εισβολέας τα μεταβάλλει. Το πιο γνωστό προϊόν από αυτά είναι το "Tripwire". Ένα SIV μπορεί να επιτηρεί και αλλά μέρη του συστήματος, όπως το Windows registry. Μπορεί επίσης να ανιχνεύσει πότε ένας κανονικός χρήστης αποκτά δικαιώματα επιπέδου root/administrator.

Log file monitors (LFM) : Παρακολουθούν log files που δημιουργούνται από υπηρεσίες δικτύου. Με παρόμοιο τρόπο προς τα NIDS, αυτά τα συστήματα ψάχνουν για πρότυπα (patterns) στα log files που συνιστούν ότι κάποιος εισβολέας επιτίθεται. Ένα τυπικό παράδειγμα θα μπορούσε να είναι ένας parser για log files ενός HTTP server, ο οποίος ψάχνει για εισβολείς που προσπαθούν να εκμεταλλευθούν γνωστές (well-known) τρύπες ασφάλειας, όπως η επίθεση "phf".

Deception systems : Περιέχουν ψευδό-υπηρεσίες των οποίων ο σκοπός είναι να προσομοιώσουν γνωστά (well-known) ρήγματα ασφάλειας ώστε να παγιδέψουν τους επίδοξους εισβολείς.

Πώς ανιχνεύονται οι εισβολές ;

- **Ανίχνευση ανωμαλίας (Anomaly detection)**
  Ο πιο κοινός τρόπος με τον οποίο προσεγγίζεται η ανίχνευση Εισβολών σε δίκτυα είναι με την ανίχνευση στατιστικών ανωμαλιών. Η ιδέα πίσω από αυτή την προσέγγιση είναι να υπολογισθεί ένας μέσος όρος (baseline) τέτοιων στατιστικών μεγεθών , όπως η χρησιμοποίηση της CPU, η δραστηριότητα του δίσκου, τα logins των χρηστών, η δραστηριότητα σε αρχεία κτλ. Το Σύστημα μετά μπορεί να ανιχνεύσει πότε υπάρχει απόκλιση από τον μέσο όρο.

  Το πλεονέκτημα αυτής της μεθόδου είναι ότι μπορεί να ανιχνεύσει ανωμαλίες χωρίς να είναι απαραίτητο να κατανοηθεί η αιτία που κρύβεται πίσω από αυτές τις ανωμαλίες

- **Αναγνώριση υπογραφής (Signature recognition**)
  Η πλειοψηφία των εμπορικών προϊόντων βασίζεται στην εξέταση της κίνησης ψάχνοντας για γνωστά πρότυπα (well-known patterns) επίθεσης. Αυτό σημαίνει ότι για κάθε τεχνική εισβολής, κάποιο είδος κώδικα εμφυτεύεται μέσα στο Σύστημα.

  Αυτό μπορεί να είναι τόσο εύκολο σαν μια αντιστοίχιση προτύπου. Το κλασσικό παράδειγμα είναι η εξέταση κάθε πακέτου στο δίκτυο για το πρότυπο "/cgi-bin/phf?", το οποίο μπορεί να υπονοεί ότι κάποιος προσπαθεί να αποκτήσει πρόσβαση σε αυτό το ευάλωτο CGI script σε έναν web-server. Μερικά IDS είναι χτισμένα πάνω σε μεγάλες βάσεις δεδομένων οι οποίες Περιέχουν εκατοντάδες (ή και χιλιάδες) τέτοιων συμβολοσειρών. Απλώς συνδέονται στο δίκτυο και ελέγχουν κάθε πακέτο εάν περιέχει κάποια από αυτές τις συμβολοσειρές.

Μέσα στα πλαίσια της εργασίας αυτής ασχοληθήκαμε συγκεκριμένα με τα εργαλεία Tripwire, COPS, Satan και Crack. Ακολουθεί μια αναλυτική παρουσίαση τους όπου επικεντρωνόμαστε στα ακόλουθα σημεία για κάθε εργαλείο :
1. Ο *σκοπός* που εξυπηρετεί το κάθε εργαλείο
2. Η *αρχιτεκτονική* και τα χαρακτηριστικά του
3. Οι *διαδικασίες εγκατάστασης* και *διαχείρισης* του σχετικού λογισμικού
4. Η *λειτουργία* του εργαλείου σε επίπεδο τελικής χρήσης
5. Οι *περιορισμοί* που εισάγονται από τη χρήση του συγκεκριμένου συστήματος.

2. Tripwire

Σκοπός

Το Tripwire κυκλοφόρησε για πρώτη φορά το 1992 από τον Gene Kim (Tripwire's CTO) και τον Dr. Eugene Spafford (από το εργαστήριο COAST του πανεπιστημίου Perdue). Ο σκοπός του λογισμικού Tripwire είναι η εξακρίβωση της ακεραιότητας των συστημάτων αρχείων (file-systems), καταλόγων ή κλειδιών μητρώου σε προστατευόμενα μηχανήματα. Παρέχει ένα θεμελιώδες επίπεδο ασφάλειας για κάθε οργανισμό που ενδιαφέρεται για την ακεραιότητα του συστήματος δεδομένων του. Αυτό επιτυγχάνεται από το Tripwire με την ανίχνευση οποιωνδήποτε μεταβολών, είτε από εσωτερικές ή εξωτερικές επιθέσεις στην ακεραιότητα των δεδομένων.
Το Tripwire είναι το πλέον ευρέως διαδεδομένο εργαλείο ανάλυσης ακεραιότητας αρχείων σε πλατφόρμες UNIX, χρησιμοποιούμενο από χιλιάδες εμπορικές εταιρείες, κυβερνητικούς και εκπαιδευτικούς οργανισμούς παγκοσμίως.
Η τεχνολογία ανάλυσης ακεραιότητας που χρησιμοποιεί το Tripwire επιτρέπει στο χρήστη να ελέγξει επακριβώς τι έχει αλλάξει σε ένα Σύστημα μέσα στο χρόνο. Το Tripwire σαν ανιχνευτής Εισβολών σε συγκεκριμένες μηχανές-στόχους, μπορεί να προστατεύσει αποτελεσματικά από απειλές τους εξυπηρετητές και τους σταθμούς εργασίας που αποτελούν ένα εταιρικό δίκτυο. Μπορεί επίσης να καθοριστεί ένα μοναδικό αρχείο πολιτικής για την ασφάλεια μίας ομάδας μηχανημάτων επιτρέποντας έτσι την ανάπτυξη διοίκησης σε κλιμακωτά επίπεδα.
Παραδείγματα συγκεκριμένων εφαρμογών για τις οποίες μπορεί να χρησιμοποιηθεί το Tripwire είναι τα ακόλουθα :

- **Ανίχνευση Εισβολών** – Το Tripwire σχεδιάστηκε ως το πλέον αξιόπιστο εργαλείο Ανίχνευσης Εισβολών σε υπολογιστικά συστήματα. Το Tripwire ανιχνεύει εισβολείς ή μη – εξουσιοδοτημένες αλλαγές σε βασικά αρχεία του συστήματος και κατάλογους.
- **Συμμόρφωση Συστήματος και πολιτικής** – Το Tripwire επιβεβαιώνει ότι το Σύστημα είναι σύμφωνο με τα πρότυπα της Τεχνολογίας Πληροφορικής παρακολουθώντας τα αρχεία του συστήματος για αλλαγές. Βοηθά τον διαχειριστή να δημιουργήσει μια *baseline* βάση δεδομένων του ιδανικού συστήματος για λόγους σύγκρισης με αλλά συστήματα που πρέπει να βρίσκονται στην ίδια κατάσταση.
- **Κλείδωμα Συστήματος** – Το Tripwire μπορεί επίσης να χρησιμοποιηθεί για την εξασφάλιση ότι δεν έχει εγκατασταθεί νέο μη-εξουσιοδοτημένο λογισμικό στο Σύστημα. Εφόσον το Σύστημα έχει κλειδωθεί, το Tripwire ελέγχει οποιαδήποτε εγκατάσταση μη-εξουσιοδοτημένου λογισμικού ή εφαρμογών.
- **Εκτίμηση Ζημίας και Ανάνηψη** – Το Tripwire μπορεί να χρησιμοποιηθεί επίσης και μετά από μια επίθεση για να προσδιορισθεί το μέγεθος της Ζημίας και ποια αρχεία πρέπει να επιδιορθωθούν ή να αντικατασταθούν.
- **Ιατροδικαστική (Forensics)** – Οι αναφορές του Tripwire μπορούν να χρησιμοποιηθούν για τη συλλογή ντοκουμέντων που στοιχειοθετούν μια εισβολή.

Αρχιτεκτονική και χαρακτηριστικά

Το Tripwire διαφέρει από αλλά Συστήματα Ανίχνευσης Εισβολών (Intrusion Detection Systems) στο ότι δεν βασίζεται στην διαρκή ενημέρωσή του με τις «γνωστές» μεθόδους (υπογραφές επίθεσης) των Εισβολών, αλλά επικεντρώνεται στην παρακολούθηση του προσδιορισμένου συστήματος. Το Tripwire δεν ενδιαφέρεται για το «πώς» συνέβη μια συγκεκριμένη επίθεση, αλλά για το ότι πραγματικά έλαβε χώρα. Το Tripwire ανιχνεύει όλους τους τύπους των ανωμαλιών, από κακοήθεις εξωτερικές επιθέσεις έως την καταστροφή αρχείων. Έτσι , εφόσον το Tripwire ανιχνεύει κάθε μετατροπή σε αρχείο, κατάλογο, κλειδί μητρώου, θα αναγνωρίσει και νέες άγνωστες επιθέσεις ή ιούς και τεχνολογία που δεν ανιχνεύονται από firewalls ή αλλά συστήματα ανίχνευσης εισβολών.
Το Tripwire χρησιμοποιεί ένα συνδυασμό 3 αλγόριθμων *message-digest* και ενός αλγόριθμου έλεγχου αθροίσματος (checksum) για να επαληθεύσει την ακεραιότητα των επιλεγμένων αρχείων σε ένα αρχείο πολιτικής (*policy file*). Οι συγκεκριμένοι αλγόριθμοι περιλαμβάνουν τους MD5, SHA, Haval, οι οποίοι όλοι κάνουν χρήση 128-bit ή μεγαλύτερων υπογραφών. Επιπρόσθετα, χρησιμοποιείται και ο αλγόριθμος CRC-32 που έχει 32-bit υπογραφή. Ένας αλγόριθμος ή ένας συνδυασμός τους μπορεί να χρησιμοποιηθεί για τον κατακερματισμό αρχείων δηλωμένων σε ένα αρχείο πολιτικής του Tripwire. Αν ένα αρχείο δεδομένων εισόδου (input file) μεταβληθεί, και ο αλγόριθμος ομοίως για αυτό το αρχείο θα μεταβληθεί, οπότε μικρές μεταβολές σε ένα αρχείο θα παρήγαγαν μεταβολές στο αρχείο εξόδου (output file).
Το Tripwire λαμβάνει μέριμνα επίσης για την προστασία των δικών του αρχείων. Πιο συγκεκριμένα κωδικοποιεί και υπογράφει τα αρχεία πολιτικής, διαρρύθμισης, βάσης δεδομένων και προαιρετικά αρχεία αναφορών χρησιμοποιώντας τον συμμετρικό κρυπτογραφικό αλγόριθμο El Gamal με 1024-bit κλειδιά. Υπογράφοντας έτσι ένα αρχείο κατά αυτό τον τρόπο το κάνει υπολογιστικά ανέφικτο για έναν εισβολέα να μεταβάλλει το αρχείο χωρίς να αναγνωρισθεί το αρχείο ως άκυρο από το Tripwire.

Διαδικασίες εγκατάστασης και διαχείρισης

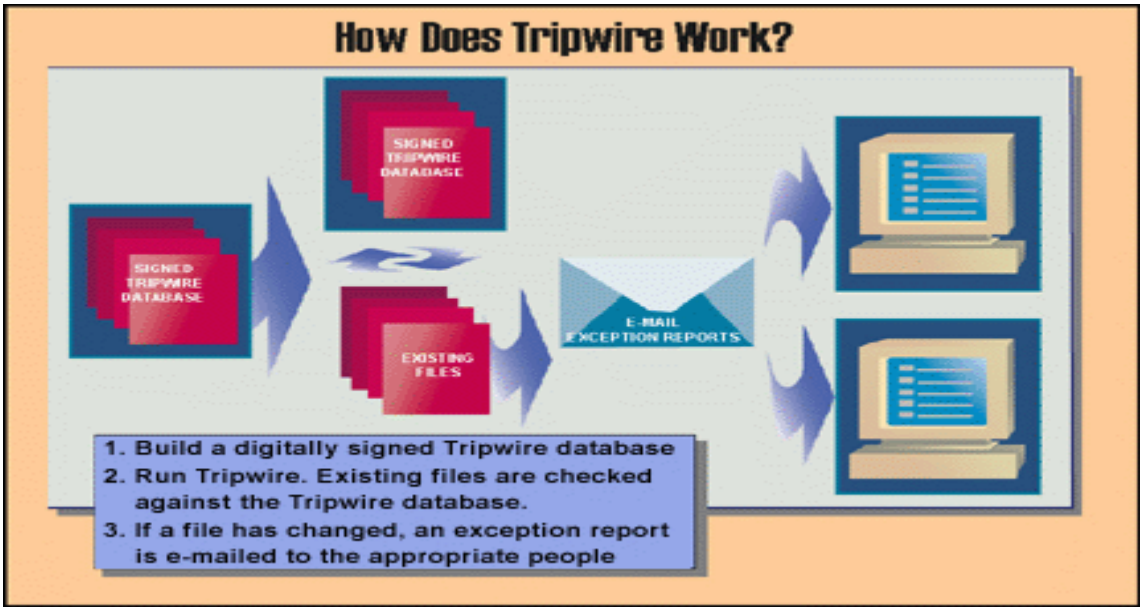
Το Tripwire τρέχει τοπικά σε κάθε υπολογιστή που παρακολουθείται. Το Tripwire είναι σχετικά ελαφρύ πρόγραμμα και έχει ελάχιστες απαιτήσεις απόδοσης συστήματος. Π.χ. η έκδοση για τα Windows NT απαιτεί χώρο στο δίσκο 5 MB (χώρια την βάση δεδομένων που διατηρεί), και απαιτεί μνήμη 32 MB RAM για να λειτουργήσει αποδοτικά. Η τρέχουσα έκδοση 2.2.1 του Tripwire υποστηρίζει τις ακόλουθες πλατφόρμες :

- Windows NT, version 4.0
- Solaris (SPARC), versions 2.6, 7.0
- Solaris (Intel), version 2.6, 7.0
- HP-UX, versions 10.20, 11.00
- IBM AIX, versions 4.2, 4.3
- SGI Irix, version 6.5
- Compaq TRU64 UNIX, version 4.0
- Red Hat Linux, versions 5.1, 5.2

Αξίζει να σημειωθεί ότι η έκδοση 2.2.1 είναι εμπορική και χρειάζεται η αγορά της άδειας χρήσης της. Από το Internet και από το δικτυακό site της εταιρείας (http://www.tripwire.com) ελεύθερη για download είναι μόνο η παλαιότερη έκδοση 1.3 Academic Source Release η οποία είναι διαθέσιμη μόνο για Unix πλατφόρμες και έχει αρκετούς περιορισμούς στην χρήση της και την εγκατάσταση σε σχέση με την 2.x. Τα πιο

σημαντικά μειονεκτήματα είναι ότι δεν διαθέτει γραφικό περιβάλλον (GUI) και καθώς επίσης ότι η εγκατάσταση είναι αρκετά περίπλοκη καθώς ο χρήστης πρέπει να μεταγλωττίσει τον πηγαίο κώδικα και να κάνει εκτεταμένες διαρρυθμίσεις (configurations) του εργαλείου.
Η διαδικασία εγκατάστασης από την έκδοση 2.x και στις μεταγενέστερες είναι σχετικά εύκολη. Για τις πλατφόρμες Unix το Tripwire έρχεται με *install scripts* ενώ για τα Windows NT υπάρχει ειδική εφαρμογή εγκατάστασης. Επίσης και για τα άλλα Λειτουργικά Συστήματα που υποστηρίζονται υπάρχουν έτοιμα προς εκτέλεση δυαδικά αρχεία, οπότε δεν υπάρχει ανάγκη για make files και μεταγλώττιση.

Λειτουργία σε επίπεδο τελικού χρηστή (end-user)



Το Tripwire πρώτα εξετάζει (scans) τον υπολογιστή και κατόπιν δημιουργεί μια *baseline* βάση δεδομένων του συστήματος αρχείων, ένα δηλαδή περιεκτικό ψηφιακό στιγμιότυπο του συστήματος σε μια γνωστή ασφαλή κατάσταση. Ο χρήστης μπορεί να κάνει μια πολύ ακριβή διαρρύθμιση του εργαλείου, υποδεικνύοντας μεμονωμένα αρχεία και καταλόγους προς παρακολούθηση σε συγκεκριμένα μηχανήματα. Το Tripwire μπορεί εν συνεχεία να καθορίσει χωρίς αμφιβολία εάν ένα προστατευμένο αρχείο έχει μεταβληθεί κατά τρόπο που παραβιάζει την πολιτική ασφάλειας που έχει καταστρωθεί από τον διαχειριστή του συστήματος.
Το Tripwire έρχεται με ένα default αρχείο πολιτικής (policy file) για κάθε συγκεκριμένη λειτουργική πλατφόρμα. Αυτό το αρχείο πολιτικής είναι σχεδιασμένο να παρακολουθεί συγκεκριμένα αρχεία ανάλογα με το λειτουργικό σύστημα. Παρόλα αυτά ο χρήστης μπορεί εύκολα να επιλέξει αυτός ποια αρχεία θέλει να παρακολουθεί στον συγκεκριμένο υπολογιστή.
Μετά από ένα έλεγχο ακεραιότητας, το Tripwire θα συγκρίνει τα ευρήματα του με την *baseline* βάση δεδομένων που έχει ήδη δημιουργήσει, και αν τυχόν υπάρχουν διαφορές, παράγεται μια αναφορά παραβίασης (violation report) που αναλύει λεπτομερειακά τις συγκεκριμένες αλλαγές που επιφέρει κάθε παραβίαση. Αυτές οι αναφορές μπορούν να σταλούν με e-mail στο διαχειριστή του συστήματος για επισκόπηση ή μπορούν να παρατηρηθούν τοπικά στη μηχανή-στόχο.

Εάν όμως η παραβίαση στην ουσία ήταν μια εξουσιοδοτημένη αλλαγή, όπως η εγκατάσταση μίας νέας εφαρμογής ή μίας αναβάθμισης, τότε το Tripwire ενημερώνει τις αλλαγές στην βάση δεδομένων έτσι ώστε να μην εμφανίζονται στις αναφορές ως παραβιάσεις.
Οι χρήστες έχουν επιλογή να εκτελούν το πρόγραμμα μια φορά την ημέρα σε ώρες μη αιχμής για να ολοκληρώσουν ένα πλήρη έλεγχο ακεραιότητας, ή μπορούν να το εκτελούν σε επιλεγμένα «σημαντικά» αρχεία κάθε λίγες ώρες για επιβεβαίωση της ακεραιότητας των δεδομένων και κατόπιν να εκτελέσουν ένα πλήρη έλεγχο του αρχείου συστήματος μια φορά την ημέρα.

Περιορισμοί από την χρήση

Οι περιορισμοί από την χρήση του Tripwire σε ένα σύστημα είναι κυρίως ότι δεν μπορεί να γίνει οποιαδήποτε εγκατάσταση νέου λογισμικού ή αναβάθμιση υπάρχοντος λογισμικού, ή μεταβολή σε κάποιο κρίσιμο αρχείο του συστήματος χωρίς εξουσιοδότηση από τον διαχειριστή του συστήματος.

3. COPS

Σκοπός

Το πακέτο λογισμικού COPS (Computer Oracle and Password System) προέρχεται από το Πανεπιστήμιο του Perdue, όπως εξάλλου και το Tripwire. Εξετάζει ένα σύστημα για έναν αριθμό γνωστών αδυναμιών του συστήματος και τις κοινοποιεί στον διαχειριστή του συστήματος. (Σε ορισμένες περιπτώσεις μπορεί να διορθώσει αυτόματα τα προβλήματα αυτά.)

Το COPS είναι ένα ελεύθερα διαθέσιμο σύνολο προγραμμάτων τα οποία ελέγχουν ποικίλες προβληματικές περιοχές της ασφάλειας ενός συστήματος UNIX. Το COPS δεν διορθώνει αλλά απλά αναφέρει πιθανά ρήγματα ασφαλείας (security holes). Το COPS μπορεί να χρησιμοποιηθεί για να επιτελέσει έλεγχο στις παρακάτω περιοχές, μεταξύ άλλων :

- Άδειες και τρόποι λειτουργίας (modes) αρχείων, καταλόγων, συσκευών
- Αδύναμα συνθηματικά (passwords)
- Περιεχόμενο, μορφότυπο και ασφάλεια των αρχείων των συνθηματικών και της πολιτικής (policy) του συστήματος
- Τα προγράμματα και τα αρχεία που τρέχουν στο /etc/rc* και τα αρχεία cron(tab)
- Ύπαρξη των αρχείων root-SUID (Set User ID), το δικαίωμα επανεγγραφής τους και το αν είναι ή όχι shell-scripts.
- Έναν έλεγχο CRC σε σημαντικά δυαδικά (binary) αρχεία για την αναφορά τυχόν αλλαγών σε αυτά.
- Δυνατότητα έγγραφης στους αρχικούς καταλόγους των χρηστών και στα αρχεία εκκίνησης (.profile, .cshrc κλπ.)
- Ρύθμιση ανώνυμου ftp

Αρχιτεκτονική και χαρακτηριστικά

Τα προγράμματα που συνιστούν το COPS ήταν αρχικά γραμμένα σε φλοιό Bourne (με την χρήση awk, sed, grep, κτλ) για μέγιστη μεταφερσιμότητα σε αλλά συστήματα, υελιξια και αναγνωσιμοτητα, με λιγες γραμμες κωδικα σε C για μεγαλυτερη ταχυτητα. Το ολοκληρο συστημα τρεχει παντως στις περισσότερες, μηχανες με BSD και System V. Επιπρόσθετα, περιλαμβάνεται και μια έκδοση σε Perl, η οποία μπορεί να μην είναι τόσο φορητή όσο η έκδοση Bourne/C, αλλά έχει κάποια πλεονεκτήματα.
Το COPS κατασκευάστηκε με τέτοιο τρόπο ώστε νέα εργαλεία να μπορούν να προστεθούν ή υπάρχοντα εργαλεία να μεταβληθούν ώστε να ανταποκρίνονται στις ανάγκες ασφάλειας του συστήματος στο οποίο έχει εγκατασταθεί.
Το COPS περιλαμβάνει επίσης κάποια προγράμματα υποστήριξης. Το κυριότερο είναι το CARP (COPS Analysis and Report Program). Το CARP είναι ένας διερμηνευτής αποτελεσμάτων που είναι σχεδιασμένος να αναλύει και να παράγει μια περίληψη για τις διαφορές αναφορές του COPS από ένα πλήρες δίκτυο ή σύνολο υπολογιστών.
Το COPS είναι έτσι σχεδιασμένο ώστε να μην μπορεί να χρησιμοποιηθεί από κακόβουλους χρήστες και εισβολείς με σκοπό να εκμεταλλευθούν (exploit) τις αδυναμίες του συστήματος. Για αυτό τον σκοπό δεν προχωρά στην εκτέλεση μετατροπών στο σύστημα προσπαθώντας να διορθώσει προβλήματα, ούτε περιγράφει την πιθανή αιτία των

αδυναμιών του συστήματος, πληροφορίες οι οποίες θα μπορούσαν να χρησιμοποιηθούν για κάποια επίθεση στο σύστημα. Επίσης, δεν περιλαμβάνει εργαλεία τα οποία θα μπορούσαν να δώσουν κάποιο στρατηγικό πλεονέκτημα σε επίδοξους εισβολείς. Το εργαλείο έλεγχου συνθηματικών που διαθέτει π.χ. έχει έναν τόσο απλό αλγόριθμο, ο οποίος ήδη βρίσκεται στις βιβλιοθήκες του συστήματος.

Τα συγκεκριμένα προγράμματα που αποτελούν το COPS είναι τα ακόλουθα:

dir.check, file.chk : Ελέγχουν μια λίστα καταλογών και αρχείων για να επαληθεύσουν ότι δεν έχουν δικαίωμα έγγραφης στα αρχεία αυτά όλοι οι χρήστες. Τυπικά, τα αρχεία που εξετάζονται είναι τα */etc/passwd, /.profile, /etc/rc* και αλλά σημαντικά αρχεία, ενώ κατάλογοι μπορεί να είναι οι */, /bin, /usr/adm, /etc*.

pass.chk : Ελέγχει και ανιχνεύει αδύναμα συνθηματικά, όπως αυτά που είναι όμοια με το login του χρηστή ή το όνομα του, ή βρίσκονται εύκολα σε ένα λεξικό κτλ. Χρησιμοποιεί την ρουτίνα crypt της πρότυπης βιβλιοθήκης του συστήματος.

group.chk, passwd.chk : Ελέγχουν το αρχείο των συνθηματικών (*/etc/passwd*) και το αρχείο των ομαδων (*/etc/group*) για την ανίχνευση διάφορων προβλημάτων, όπως κενές γραμμές, null συνθηματικά, λογαριασμοί με uid=0 (user id) που δεν ανήκουν στον root.

cron.chk, rc.chk : Επιβεβαιώνουν ότι κανένα από τα αρχεία ή τα προγράμματα που τρέχουν από το `cron` ή αναφέρονται στο */etc/rc** δεν είναι εγγράψιμα από όλους τους χρήστες. Αυτό αποθαρρύνει έναν εισβολέα να μεταβάλλει προγράμματα η αρχεία δεδομένων που τρέχουν με δικαιώματα root κατά την εκκίνηση του συστήματος

dev.chk : εξετάζει τα */dev/kmem, /dev/mem*, και τα αρχεία συστήματος που αναγράφονται στο */etc/fstab* για το αν έχουν δικαίωμα έγγραφης σε αυτά όλοι οι χρήστες. Αυτό εμποδίζει κάποιον εισβολέα από το να αποκτήσει άδειες σε αρχεία και να διαβάσει / γράψει απευθείας σε συσκευή ή στην μνήμη του συστήματος.

home.chk, user.chk: Ελέγχουν τους αρχικούς καταλόγους κάθε χρηστή και τα αρχεία εκκίνησης (*.login, .profile*, etc) για δικαιώματα έγγραφης.

root.chk : Ελέγχει τα start-up αρχεία (e.g., */.login, /.profile*) του root για λανθασμένες ρυθμίσεις umask

suid.chk : Ελέγχει για αλλαγές στα SUID (Set User ID) αρχεία του συστήματος. χρειάζεται να εκτελεστεί από τον root για καλύτερα αποτελέσματα. Χρησιμοποιεί τα αποτελέσματα της προηγούμενης εκτέλεσης του σαν αναφορά για την ανίχνευση νέων, διαγραμμένων, ή μεταβλημένων SUID αρχείων.

Διαδικασίες εγκατάστασης και διαχείρισης

Το COPS έχει δοκιμαστεί επιτυχημένα σε ένα μεγάλο αριθμό υπολογιστικών μηχανών, συμπεριλαμβανόμενων των UNIX συστημάτων των εταιρειών Sun, DEC, HP, IBM, AT&T, Sequent, Gould, NeXT, και MIPS.
Η εγκατάσταση και η εκτέλεση του COPS σε ένα σύστημα συνήθως διαρκεί λιγότερο από μια ώρα, ανάλογα στην εμπειρία του διαχειριστή, την ταχύτητα του επεξεργαστή και τις επιλογές του χρηστή. Μετά την αρχική εγκατάσταση, κάθε εκτέλεση του COPS χρειάζεται λίγα λεπτά. Ο χρόνος αυτός εξαρτάται από την ταχύτητα του επεξεργαστή, τις

επιλογές στον έλεγχο των συνθηματικών και στον αριθμό των λογαριασμών που υπάρχουν στο σύστημα.
Ο καλύτερος τρόπος για την χρήση του COPS είναι η εκτέλεση του σε τακτική βάση, διάμεσου του a**t** ή του **cron**.

Λειτουργία σε επίπεδο τελικού χρηστή (end-user)

Το COPS είναι δομημένο σαν μια συλλογή από υποπρογράμματα τα οποία καλούνται από κάποιο script του φλοιού. Το script του ανώτερου επιπέδου (toplevel script) συλλέγει τις εξόδους από τα υποπρογράμματα και είτε στέλνει ένα mail με τις σχετικές πληροφορίες στον διαχειριστή του συστήματος είτε δημιουργεί ένα αρχείο (επιλεγμένο από τον χρηστή) με τα προβλήματα που βρήκε κατά την λειτουργία του στο σύστημα. Όλα τα προγράμματα του COPS μονάχα ενημερώνουν τον χρηστή για κάποιο πιθανό πρόβλημα. Δεν προσπαθούν να διορθώσουν και σε καμία περίπτωση να εκμεταλλευτούν οποιοδήποτε από τα προβλήματα που ανιχνευουν. Επειδή το COPS δεν διορθώνει πιθανούς κινδύνους που βρίσκει, δεν χρειάζεται να εκτελεστεί από κάποιον λογαριασμό με αυξημένα δικαιώματα(privileges), οπως από τον root για παράδειγμα. Ο μόνος έλεγχος ασφάλειας που πρέπει να γίνεται από το root για βέλτιστα αποτελέσματα και επειδή απαιτεί αρκετό χρόνο, είναι ο έλεγχος των αρχείων SUID, προκειμένου να βρεθούν όλα τα παρόμοια αρχεία στο σύστημα.

Περιορισμοί από την χρήση

Το COPS δεν μπορεί να χρησιμοποιηθεί ώστε να ελέγχει έναν υπολογιστή από μακριά, καθώς όλα τα τεστ και οι έλεγχοι που γίνονται απαιτούν ένα φλοιό που πρέπει να βρίσκεται πάνω στον υπολογιστή που εξετάζεται.
Επιπλέον, αναφέρεται ξανά ότι το COPS δεν διορθώνει τα λάθη και τα προβλήματα που ανιχνεύει στην ασφάλεια του συστήματος. Αυτό συμβαίνει για διάφορους λόγους, ο κυριότερος εκ των οποίων είναι ότι η ασφάλεια των υπολογιστικών συστημάτων δεν είναι κάτι το σταθερά και παγιοποιημένα ορισμένο. κάτι που είναι σημαντικό ρήγμα στην ασφάλεια ενός συστήματος, σε κάποιο άλλο σύστημα μπορεί να πάγια ανοικτή (open) και ελεύθερη πολιτική.
Παρότι όμως το COPS δεν προχωρά στην διόρθωση των σφαλμάτων για να μην χρησιμοποιηθεί από πιθανούς εισβολείς, έχουν αναφερθεί περιπτώσεις όπου συνείσφερε σε πράξεις βανδαλισμού με το να εκθέσει απλώς τις αδυναμίες του συγκεκριμένου συστήματος. Σε μια περίπτωση, ο εισβολέας το χρησιμοποίησε για να βρει έναν κατάλογο χρηστή ο οποίος είχε δικαιώματα προστασίας 777 (υπήρχε δηλ. δικαίωμα παν-έγγραφης). Σε μια άλλη υπόθεση, το COPS είχε χρησιμοποιηθεί για την εύρεση ενός κατάλογου συστήματος στον οποίον υπήρχαν δικαιώματα έγγραφης.

4. SATAN

Σκοπός

Το SATAN (Security Analysis Tool for Auditing Networks) σχεδιάστηκε και κατασκευάστηκε το 1995από τους **Dan Farmer και Wietse Venema**. Η διάφορα του από το COPS είναι ότι το COPS είναι ένα host-based Unix εργαλείο έλεγχου ασφάλειας, δηλαδή τρέχει πάνω στον υπολογιστή του οποίου εξετάζεται η ασφάλεια. Το SATAN είναι ένα εργαλείο έλεγχου ασφάλειας απομακρυσμένου δικτύου (remote network), δηλαδή μπορεί να κάνει αναφορά για την ασφάλεια οποιουδήποτε υπολογιστή ή δικτύου στον οποίο έχει IP πρόσβαση το μηχάνημα στο οποίο εκτελείται το SATAN. Δεν χρειάζεται κάποιος λογαριασμός ή δικαιώματα στις απομακρυσμένες μηχανές στις οποίες γίνεται έλεγχος.
Στην πιο απλή (και default) μορφή του το SATAN συλλέγει όσες το δυνατόν περισσότερες πληροφορίες για απομακρυσμένους υπολογιστές και δίκτυα εξετάζοντας υπηρεσίες δικτύων όπως είναι οι finger, NFS, NIS, ftp και tftp, rexd κλπ. Η πληροφορία που συγκεντρώνεται περιέχει την παρουσία διάφορων υπηρεσιών πληροφοριών για δίκτυα καθώς και πιθανά ελαττώματα στην ασφάλεια – συνήθως λανθασμένη εγκατάσταση ή διαρρύθμιση υπηρεσιών δικτύου, γνωστά bugs σε utilities του συστήματος ή του δικτύου, ή φτωχές και αδύναμες αποφάσεις πολιτικής του συστήματος.
Μπορεί κατόπιν είτε να αναφέρει τα δεδομένα αυτά ή να χρησιμοποιήσει ένα rule-based σύστημα για να ανακαλύψει πιθανά προβλήματα ασφάλειας. Οι χρήστες μπορούν να εξετάσουν, να ερευνήσουν και να αναλύσουν τα την έξοδο του προγράμματος μέσα από κάποιον HTML browser, όπως τον Mosaic, Netscape, ή Lynx.
Ενώ το πρόγραμμα είναι κυρίως προσανατολισμένο προς την ανάλυση των θεμάτων ασφάλειας μέσω των αποτελεσμάτων, ένα μεγάλο ποσό γενικής πληροφορίας για το δίκτυο μπορεί να αντληθεί με την χρήση του εργαλείου – όπως τοπολογία δικτύου, ποιες υπηρεσίες δικτύου τρέχουν, τύπος λογισμικού και υλικού που χρησιμοποιείται στο δίκτυο κλπ.
Το SATAN είναι πλέον χρήσιμο όταν χρησιμοποιείται από τους διαχειριστές συστήματος η ασφάλειας που είναι υπεύθυνοι για την ασφάλεια του συγκεκριμένου συστήματος. Πάντως, καθώς είναι ελευθέρα διαθέσιμο μέσα στο Διαδίκτυο, μπορεί να χρησιμοποιηθεί από οποιονδήποτε ανησυχεί για την ασφάλεια του συστήματος του, αφού πιθανοί εισβολείς θα μπορούν να έχουν πρόσβαση στις ίδιες πληροφορίες αδυναμίας του συστήματος και εφόσον είναι πιθανόν να αποκαλυφθούν προβλήματα ασφάλειας που πρώτα ήταν άγνωστα.

Αρχιτεκτονική και χαρακτηριστικά

Το SATAN έχει μια έκτατη αρχιτεκτονική. Στο κέντρο βρίσκεται ένας σχετικά μικρός γενικός πυρήνας ο οποίος γνωρίζει ελάχιστα έως καθόλου για τύπους συστημάτων, ονόματα υπηρεσιών δικτύου, αδυναμίες, ή άλλες λεπτομέρειες. Η γνώση για τις λεπτομέρειες των υπηρεσιών δικτύου, των τύπων συστημάτων κτλ. είναι δομημένη σε μικρά αφιερωμένα εργαλεία συλλογής δεδομένων και βάσεις κανόνων (rule bases). Η συμπεριφορά του SATAN ελέγχεται από ένα configuration file. Οι ρυθμίσεις μπορούν να αλλάξουν είτε μέσω επιλογών της γραμμής εντολών είτε μέσα από ένα *hypertext-type* σύστημα διεπαφής με τον χρηστή.

Ο πυρήνας του SATAN αποτελείται από τα ακόλουθα κύρια μέρη:

Magic cookie generator

Κάθε φορά που ξεκινά το SATAN σε interactive mode, παράγει μια ψευδοτυχαία συμβολοσειρά που ο HTML browser πρέπει να στείλει στο SATAN custom http server σαν μέρος όλων των εντολών.

Policy engine

Σύμφωνα με τους περιορισμούς στο configuration file του SATAN, αποφασίζει εάν ένας υπολογιστής θα ελεγχθεί και ποιο επίπεδο εξετάσεως είναι κατάλληλο για αυτόν τον υπολογιστή.

Target acquisition

παράγει ένα κατάλογο από τεστ που πρέπει να τρέξουν σε μια λίστα υπολογιστών που δέχεται ως είσοδο. Η λίστα των τεστ είναι είσοδος για το υποσύστημα data acquisition

Data acquisition

Δοθείσης μίας λίστας από τεστ, τρέχει τα αντίστοιχα εργαλεία συλλογής δεδομένων στους υπολογιστές και δημιουργεί νέα γεγονότα (facts), τα οποία είναι είσοδος στο υποσύστημα inference engine.

Inference engine

Έχοντας σαν είσοδο μια λίστα από facts, παράγει νέους target-hosts, νέα τεστ , και νέα facts. Οι νέοι target-hosts είναι είσοδος στο υποσύστημα target acquisition, τα νέα τεστ χειρίζονται από το υποσύστημα data acquisition, και τα νέα facts επεξεργάζονται από το υποσύστημα inference engine.

Report and analysis

Παίρνει τα δεδομένα που έχουν συλλεχθεί και χτίζει έναν εικονικό υπέρ-χώρο στον οποίο μπορεί ο χρηστής να πλοηγηθεί διάμεσου του αγαπημένου του HTML browser.

Διαδικασίες εγκατάστασης και διαχείρισης

Για την εγκατάσταση του SATAN χρειάζεται το ακόλουθο πρόσθετο λογισμικό:
PERL 5.000 ή ανώτερη έκδοση, ένας compiler της C και ένας web-browser (Netscape, Mosaic, or Lynx). Το SATAN εμφανίζεται καλύτερα σε έγχρωμες οθόνες.
Το SATAN λειτουργεί στα ακόλουθα λειτουργικά συστήματα:

- SunOS 4.1.3_U1
- SunOS 5.3
- Irix 5.3

Το SATAN έχει δοκιμαστεί στις ακόλουθες πλατφόρμες από πλευράς υλικού:

- SPARCstation 4/75
- SPARCstation 5
- Indigo 2

Άλλες πλατφόρμες στις οποίες ενδέχεται να δουλεύει είναι οι AIX, BSD types, IRIX5, HP-UX 9.x, SunOS 4 & 5, SYSV-R4, Ultrix 4.x, και ίσως Linux..

Το SATAN από μόνο του καταλαμβάνει 2 MB χώρο στο δίσκο. Παρόλα αυτά χρειάζεται να ληφθούν υπόψη και τα συμπληρωματικά πακέτα που είναι απαραίτητα για την λειτουργία του (PERL, web browser)

Η μνήμη που απαιτεί το SATAN για την λειτουργία του εξαρτάται από τον αριθμό των υπολογιστών που πρόκειται να ελεγχθούν. Ενα ελάχιστο ποσό μνήμης πάντως θα ήταν τα 32MB RAM.
Για την αποσυμπιέσει του αρχείου του SATAN που διατίθεται ελευθέρα στο Διαδικτυο η ακόλουθη εντολή πρέπει να δοθεί:
compress -d <satan-X.X.tar.Z | tar xvf -
Τα επόμενα βήματα για την εγκατάσταση του είναι τα ακόλουθα :

- εκτέλεση του `reconfig' script.
- εκτέλεση της εντολής `make', η οποία θα χτίσει ένα εκτελέσιμο αρχείο για την αυθεντικοποίηση μεταξύ του SATAN και του Web browser.
- εκτέλεση του `satan' script. Εάν τρέξει χωρίς παραμέτρους θα ξεκινήσει έναν Web browser για την HTML διεπαφή με τον χρήστη. Για να τρέξει το SATAN από την γραμμή εντολών θα πρέπει να δοθεί μια εντολή σαν satan victim.com (δηλ. satan target_hostname).

Για την εκτέλεση του SATAN απαιτούνται δικαιώματα υπέρ-χρήστη (root).
Μπορούν επίσης να εκτελούνται παράλληλες διεργασίες του SATAN για την επιτάχυνση της διαδικασίας συλλογής δεδομένων. Σε κάθε διαδικασία πάντως πρέπει να δοθεί η δική της βάση δεδομένων (μέσω της επιλογής "-d" της γραμμής εντολών.

Τα αρχεία του SATAN χωρίζονται στις ακόλουθες κατηγορίες:

1. *bin/** Τα προγράμματα με τα οποία το SATAN αποκτά τα δεδομένα.

2. *config/** αρχεία διαρρυθμίσεων που χρησιμοποιεί το SATAN για να βρει αλλά προγράμματα, και για default ρυθμίσεις.

3. *html/** *html* σελίδες ή *perl* προγράμματα για την παραγωγή σελίδων για την διεπαφή με το χρηστή.

4. *perl/** Ενότητες κώδικα που χρησιμοποιούνται είτε από το SATAN είτε από τα εργαλεία απόκτησης δεδομένων

5. *results/database-name*. Ββάσεις δεδομένων του SATAN. Κάθε βάση δεδομένων αποτελείται από 3 αρχεία:

    1. *all-hosts*. Μια λίστα όλων των υπολογιστών που βρήκε το SATAN κατά την λειτουργία του, ακόμα και αυτούς που δεν εξέτασε.

    2. *facts*. Μια λίστα όλων των εγγράφων εξόδου που δημιουργούν τα εργαλεία **.satan*. Αυτές οι εγγραφές επεξεργάζονται από το SATAN για την παραγωγή των αναφορών.

3. *todo*. λίστα των υπολογιστών και των τεστ που έτρεξε το SATAN σε αυτούς. Με αυτόν τον τρόπο το SATAN γνωρίζει ποια τεστ να παραλείψει όταν ξαναελέγξει τους υπολογιστές αυτούς.

6. *rules/**. Οι κανόνες που χρησιμοποιεί το SATAN για να εκτιμήσει την κατάσταση και να βγάλει συμπεράσματα από την υπάρχουσα πληροφορία. Εξαιρετικά ευέλικτο (απλός perl κώδικας που διερμηνεύεται) είναι ένα από τα πιο δυνατά χαρακτηριστικά το SATAN.

7. *src/** Ο πηγαίος κώδικας για ορισμένα από τα προγράμματα υποστήριξης του SATAN.

Το πιο σημαντικό αρχείο του SATAN Πάντως είναι το αρχείο των διαμορφώσεων (configuration file) του (*config/satan.cf*). Ο,τιδήποτε κάνει το SATAN όταν εξετάζει υπολογιστές και δίκτυα ελέγχεται μέσω αυτού του αρχείου, ποσό σκληρά να εξετάσει τις μηχανές – στόχους, ποσό μακριά να δράσει από την αρχική μηχανή, ποια τεστ να τρέξει κτλ. Ενώ ένας περιορισμένος αριθμός επιλογών μπορεί να γίνει μέσω της HTML διεπαφής με τον χρηστή, οι χαμηλού-επιπέδου μεταβλητές πρέπει να οριστούν με επεξεργασία αυτού του αρχείου, το οποίο είναι γραμμένο σε γλώσσα PERL. Ο κώδικας αυτού του αρχείου αρχίζει να τρέχει μόλις όταν αρχικοποιείται το πρόγραμμα.

Λειτουργία σε επίπεδο τελικού χρηστή (end-user)

Το SATAN έχει ένα πρόγραμμα απόκτησης πληροφοριών για ένα στόχο (target) το οποίο χρησιμοποιεί την εντολή fping για να προσδιορίσει εάν ένας υπολογιστής ή ένα σύνολο υπολογιστών σε ένα υπό-δίκτυο είναι ζωντανοί (alive). Κατόπιν περνάει την λίστα με τους υπολογιστές σε μια μηχανή η οποία οδηγεί την συλλογή δεδομένων και τον κύριο βρόγχο επανατροφοδότησης. Κάθε υπολογιστής εξετάζεται εάν έχει ελεγχθεί νωρίτερα, και αν όχι, ένα σύνολο από τεστ τρέχει πάνω του (το σετ των τεστ εξαρτάται από την απόσταση στην οποία βρίσκεται ο υπολογιστής από την αρχική μηχανή και το επίπεδο εξέτασης που έχει ορισθεί). Τα τεστ δημιουργούν μια εγγραφή δεδομένων που περιλαμβάνει το όνομα του υπολογιστή, τα τεστ που έτρεξαν σε αυτόν, και τα αποτελέσματα που προέκυψαν από τον έλεγχο. Τα δεδομένα αυτά κατόπιν σώζονται σε ένα αρχείο για περαιτέρω ανάλυση. Το υποσύστημα της διεπαφής με τον χρηστή χρησιμοποιεί HTML για να συνδέσει και να παρουσιάσει με τρόπο κατανοητό και ευανάγνωστο προς τον χρηστή τα τεράστια ποσά δεδομένων σαν αποτελέσματα.

Το SATAN μπορεί να εκτελεστεί όπως προαναφέρθηκε μόνο σε επίπεδο υπέρ-χρηστή. Από τον πίνακα έλεγχου στην HTML διεπαφή, πρέπει να επιλέγει *Run SATAN*. κατόπιν ζητείται να δοθεί το όνομα του υπολογιστή στον οποίο τρέχει το SATAN(*Primary target selection).* κατόπιν μπορεί να επιλέξει ο χρήστης να ελέγξει μόνο τον υπολογιστή στον οποίο βρίσκεται (*Scan the target host only),* ή εάν έχει την εξουσιοδότηση και τον χρόνο να επιλέξει να εξετάσει όλους τους υπολογιστές στο υποδίκτυο (*Scan all hosts in the primary (i.e. the target's) subnet)*.

Στις αναφορές που παράγει το SATAN, εάν υπάρχει μια κόκκινη τελεία δίπλα από έναν υπολογιστή (), αυτό σημαίνει ότι ανιχνεύθηκε κάποια αδυναμία στην ασφάλεια του υπολογιστή. Μια μαύρη τελεία () δίπλα σε έναν υπολογιστή στη λίστα σημαίνει ότι δεν βρέθηκαν αδυναμίες στον συγκεκριμένο υπολογιστή. Ακολουθώντας τους

υπερσυνδέσμους μπορεί ο χρήστης να βρει περισσότερες πληροφορίες για τον υπολογιστή, το δίκτυο και τις αδυναμίες του.

Περιορισμοί από την χρήση

Οι hacker συστημάτων, πιθανοί εισβολείς, ή οποιοιδήποτε τυχαίοι χρήστες του Διαδικτύου θα μπορούσαν να τρέξουν το SATAN εναντίον υπολογιστών στους οποίους δεν έχουν καμία εξουσιοδότηση. Αυτό είναι ένα πρόβλημα από την στιγμή μερικά από τα τεστ που εκτελεί το SATAN είναι παρόμοια με τεχνικές επίθεσης που χρησιμοποιούν οι cracker συστημάτων. Επίσης , ακόμα και ένας διαχειριστής συστήματος με καλούς σκοπούς θα μπορούσε να τρέξει το SATAN στο δικό του σύστημα και θα μπορούσε να ακολουθήσει αυτό οδούς εμπιστοσύνης ή πιθανής αδυναμίας μακριά από τα αναγνωρισμένα ηλεκτρονικά του σύνορα και να προκαλέσει θυμό και ανησυχία στους γείτονες του.
Ο πιο ασφαλής τρόπος για να τρέξει το SATAN είναι πίσω από ένα firewall, εφόσον σε αυτήν την περίπτωση το SATAN θα εξετάσει μόνο συστήματα στα οποία έχει πρόσβαση μέσω της IP διεύθυνσης, και δεν θα ξεπεράσει τον υπολογιστή στον οποίο είναι εγκατεστημένος ο firewall.
Το SATAN έχει τρεις προστατευτικές δικλείδες ασφάλειας μέσα στο πρόγραμμα του. Πρώτον, δεν θα προσπαθήσει να εξετάσει υπολογιστές οι οποίοι είναι μακρύτερα από το επίπεδο εγγύτητας (*proximity level)* , που έχει οριστεί, από το αρχικό μηχάνημα ή υποδίκτυο. Κάθε υπολογιστής ή δακτύλιος υπολογιστών που είναι γειτονικοί στην αρχική μηχανή είναι ένα επίπεδο εγγύτητας μακριά. Οπότε εάν το επίπεδο εγγύτητας έχει οριστεί σε 2, το SATAN δεν θα εξετάσει υπολογιστές που βρίσκονται δυο hops μακριά από την αρχική μηχανή. Δυο άλλοι μέθοδοι που περιορίζουν την δράση του SATAN είναι οι μεταβλητές εξαίρεσης επίθεσης *"$only_attack_these"* και *"$don't_attack_these"*. Η πρώτη περιορίζει το SATAN να εξετάσει υπολογιστές που βρίσκονται σε ένα συγκεκριμένο σύνολο υπολογιστών, ενώ η δεύτερη πληροφορεί το SATAN ότι δεν πρέπει να εξετάσει υπολογιστές με κάποιο ορισμένο όνομα, για παράδειγμα όλα τα στρατιωτικά (*".mil"*) ή κυβερνητικά (*".gov"*) sites.

Σχόλια για το SATAN

Πριν την κυκλοφορία του…

"It's like randomly mailing automatic rifles to 5,000 addresses. I hope some crazy teen doesn't get a hold of one." (Oakland tribune.)

"SATAN is like a gun, and this is like handing a gun to a 12-year-old." (LA times.)

"It's like distributing high-powered rocket launchers throughout the world, free of charge, available at your local library or school, and inviting people to try them out by shooting at somebody." (San Jose mercury.)

"It discovers vulnerabilities for which we have no solutions." (The New York Times.)

"...people could die." (vikr@aol.com (VikR))

…Μετά την κυκλοφορία του

"...there is no obscuring its presence. It announces itself like a rock concert to the scanned machine's log file." (Nick Christenson, npc@minotaur.jpl.nasa.gov)

5. Crack

Σκοπός

Το Crack έχει αναπτυχθεί από τον Alec D.E. Muffett και η πιο πρόσφατη έκδοση του ελευθέρα διαθέσιμη στο Διαδικτυο είναι η 4.1, με ημερομηνία κυκλοφορίας 3/3/1992. Το Crack είναι ένας αναλυτής συνθηματικών για συστήματα UNIX. Είναι σχεδιασμένο να βρίσκει συνθηματικά 8-χαρακτηρων κρυπτογραφημένα σε DES χρησιμοποιώντας ορισμένες τεχνικές πρόβλεψης. Έχει γραφτεί έτσι ώστε να είναι ευέλικτο, διαμορφώσιμο, και γρήγορο.

Αρχιτεκτονική και χαρακτηριστικά

Η έκδοση της πρότυπης βιβλιοθήκης (stdlib) της υπορουτινάς crypt() που χρησιμοποιείται στα συστήματα UNIX για την κρυπτογράφηση των συνθηματικών είναι υπερβολικά αργή και θα προκαλούσε μια μαζική συμφόρηση (bottleneck) κατά την εκτέλεση του Crack. Στο Διαδικτυο υπάρχουν πολλές υλοποιήσεις γρηγορότερων εκδόσεων της crypt(). Αυτή που χρησιμοποιείται στο Crack από την έκδοση 3.2 και στις μεταγενέστερες ονομάζεται fcrypt(). Γράφτηκε το Μάιο του 1986 από τον Robert Baldwin στο MIT. Σε ένα DecStation 5000/200 η fcrypt() είναι περίπου 16 φορές γρηγορότερη από την πρότυπη (crypt)
Ανάμεσα στις άλλες διαθέσιμες υλοποιήσεις της crypt() είναι και η UFC από τον Michael Glad. Η UFC-crypt είναι μια έκδοση της crypt η οποία είναι βελτιστοποιημένη για πλατφόρμες με 32-bit long integers. Το Crack είναι γραμμένο έτσι ώστε αυτόματα να κάνει χρήση της UFC εάν την βρει. Αυτό που πρέπει να κάνει ο χρήστης που θέλει να χρησιμοποιήσει την UFC είναι, αφού την κατεβάσει, να την αποσυμπιέσει σε ένα κατάλογο ufc-crypt στο $CRACK_HOME, και κατόπιν να σβήσει τα παλιά binaries. Η UFC θα αναγνωρισθεί, μεταγλωττισθεί, ελεγχθεί και χρησιμοποιηθεί κατά προτίμηση σε σχέση με την fcrypt()από το Crack, όπου είναι δυνατόν.

Διαδικασίες εγκατάστασης και διαχείρισης

Το Crack είναι ένα αυτό-εγκαθιστάμενο (self-installed) πρόγραμμα σε περιβάλλον UNIX, δεν χρειάζεται δηλαδή να μεταγλωττίσει ο χρήστης τα αρχεία πηγαίου κώδικα προκειμένου να φτιάξει binaries. Το πρώτο βήμα μετά το κατέβασμα του αρχείου Crack41.tgz από το Διαδίκτυο είναι η αποσυμπίεσή του σε έναν κατάλογο με την εντολή :

```
tar -xvzf Crack41.tgz
```

Κατόπιν πρέπει να γίνουν κάποιες ρυθμίσεις του προγράμματος. Τα αρχεία των ρυθμίσεων του Crack είναι δυο, το script του φλοιού Crack, το οποίο περιέχει όλα τα δεδομένα ρυθμίσεων σχετικά με την εγκατάσταση, και το αρχείο Sources/conf.h, το οποίο περιέχει επιλογές ρυθμίσεων συγκεκριμένες για διαφορές πλατφόρμες. Στο shell-script Crack ο χρήστης πρέπει πρώτα να εκχωρήσει στην μεταβλητή CRACK_HOME την σωστή τιμή, που είναι η απόλυτη διαδρομή του κατάλογου στον οποίο έχει αποσυμπιεσθεί το πρόγραμμα. Υπάρχει επίσης και η μεταβλητή CRACK_OUT, η οποία καθορίζει τον κατάλογο που πρέπει να τοποθετηθούν τα αρχεία εξόδου (δηλ. τα σπασμένα συνθηματικά)- εξ ορισμού έχει την ίδια τιμή με την μεταβλητή $CRACK_HOME.

Εφόσον ο χρήστης έχει ολοκληρώσει την επεξεργασία του shell-script Crack, είναι έτοιμος να τρέξει το πρόγραμμα για πρώτη φορά. Η εντολή που πρέπει να δώσει είναι η ακόλουθη:

Crack [options] [bindir] /etc/passwd [...άλλα αρχεία συνθηματικών]

Όπου bindir είναι το προαιρετικό όνομα του κατάλογου στον οποίο ο χρήστης θα ήθελε να εγκατασταθούν τα δυαδικά αρχεία, σε περίπτωση που θα ήθελε να τρέξει το Crack σε κάποια άλλη αρχιτεκτονική.

Το Crack έχει πολλές επιλογές λειτουργίας, όπως για παράδειγμα :

–f : το Crack εκτελείται στο προσκήνιο αντί του παρασκηνίου, όπως είναι το default, και όλα τα μηνύματα εμφανίζονται κανονικά στο stdout και stderr

-m: στέλνει mail στους χρήστες των οποίων το συνθηματικό αναλύθηκε από το Crack.

Ο κατάλογος των Scripts περιέχει έναν μικρό αριθμό από script για υποστήριξη και γενικότερα utilities. Μερικά από τα πιο χρήσιμα είναι γι παράδειγμα τα εξής:

shadmrg : Το script αυτό συνενώνει τα αρχεία /etc/passwd και /etc/shadow σε συστήματα System V. Η έξοδος του κατευθύνεται στο stdout και πρέπει να ανακατευθυνθεί σε ένα αρχείο προκειμένου να μπορέσει το Crack να δουλέψει πάνω του.

nastygram : Αυτό το script καλείται από τον αναλυτή συνθηματικών για να στείλει mail σε χρήστες με αδύναμα και εύκολα προβλέψιμα συνθηματικά, εάν χρησιμοποιείται η παράμετρος –m.

Λειτουργία σε επίπεδο τελικού χρηστή (end-user)

Το Crack δέχεται ως είσοδο μια σειρά από αρχεία συνθηματικών και λεξικά (dictionaries). Ενώνει τα λεξικά μεταξύ τους, ταξινομεί τα αρχεία των συνθηματικών και παράγει μια λίστα από πιθανά συνθηματικά από τα συνενωμένα λεξικά ή από πληροφορίες που προέρχονται για τους χρήστες από το αρχείο των συνθηματικών. Δεν προσπαθεί να θεραπεύσει το πρόβλημα του να έχουν οι χρήστες εύκολα και προβλέψιμα συνθηματικά και γι αυτό δεν ενδείκνυται στην θέση κάποιου εργαλείου αντικατάστασης αδύνατων συνθηματικών.

Το Crack εργάζεται κάνοντας διαδοχικά περάσματα από τα συνθηματικά που του έχουν εισαχθεί. Σε κάθε πέρασμα προσπαθεί να μαντέψει τα συνθηματικά βασιζόμενο σε μια ακολουθία κανόνων οι οποίοι δίνονται από τον χρήστη στα αρχεία gecos.rules και dicts.rules στον κατάλογο των Scripts. Οι κανόνες αυτοί είναι απλές συμβολοσειρές χαρακτήρων με έναν κανόνα σε κάθε σειρά. Οι εντολές του κάθε κανόνα ακολουθούνται από αριστερά προς τα δεξιά και εφαρμόζονται στις λέξεις του λεξικού μια προς μια, καθώς οι λέξεις φορτώνονται.

Οι κανόνες αποθηκεύονται σε δυο διαφορετικά αρχεία για δυο διαφορετικούς σκοπούς. Οι κανόνες στο αρχείο Scripts/gecos.rules εφαρμόζονται σε δεδομένα τα οποία παράγει το Crack από την καταχώρηση (entry) του χρηστή στο αρχείο των συνθηματικών του συστήματος. Π.χ. για τον χρηστή dimoiko ο οποίος είναι ο Dimitris Pantelis Oikonomidis, τα δεδομένα που θα χρησιμοποιούσαν οι κανόνες gecos για την εύρεση του συνθηματικού του χρηστή θα ήταν : dimoiko, Dimitris, Pantelis, Oikonomidis, καθώς και μια σειρά από αναγραμματισμούς και συνδυασμούς αυτών των λέξεων (για παράδειγμα DPOikonomidis). Το σύνολο των κανόνων του αρχείου gecos.rules εφαρμόζεται σε καθεμία τέτοια λέξη, οπότε δημιουργούνται πολλοί περισσότεροι συνδυασμοί, οι οποίοι όλοι ελέγχονται.

αφού έχει ολοκληρωθεί το πέρασμα πάνω από τα δεδομένα που βασίζονται στην πληροφορία από το αρχείο των συνθηματικών, έρχεται η ώρα για την λεξικογραφική ανάλυση. Το Crack κάνει επιπλέον περάσματα πάνω από τα συνθηματικά χρησιμοποιώντας κανόνες από το αρχείο Scripts/dicts.rules. Φορτώνει το συνενωμένο λεξικό (το οποίο έχει δημιουργηθεί από τα λεξικά που βρίσκονται στο κατάλογο DictSrc) στην μνήμη και εφαρμόζει τον τρέχοντα κανόνα σε κάθε λέξη από αυτό το αρχείο. αφού ολοκληρωθεί κάθε πέρασμα, η μνήμη ελευθερώνεται από το λεξικό για να ξαναχρησιμοποιηθεί από το επόμενο. Ο χρήστης επίσης μπορεί να παρέχει στο πρόγραμμα το δικό του λεξικό, το οποίο απλώς αντιγράφει στον κατάλογο DictSrc. Το λεξικό αυτό θα συνενωθεί κατόπιν με τα υπόλοιπα στην επόμενη εκτέλεση του προγράμματος.
Εάν το Crack μαντέψει ορθά ένα συνθηματικό, τότε σημειώνει τον χρηστή ώστε να μην ξαναπροσπαθήσει να σπάσει το συνθηματικό του. μόλις τελειώσει ένα πέρασμα με το λεξικό, το πρόγραμμα σβήνει από την λίστα όσους χρήστες των οποίων βρήκε το συνθηματικό. Το Crack αποθηκεύει τα σπασμένα συνθηματικά και σε μορφή plaintext και σε κρυπτογραφημένη μέσα σε ένα feedback αρχείο στον κατάλογο Runtime. Ο σκοπός αυτού είναι όταν το Crack κληθεί ξανά, να μπορεί να αναγνωρίσει συνθηματικά τα οποία έχει επιτυχημένα αναλύσει παλαιότερα, και να τα φιλτράρει από την είσοδο στον αναλυτή συνθηματικών. Έτσι παρέχεται άμεσα μια λίστα χρηστών των οποίων το συνθηματικό είναι εύκολο να σπάσει και οι οποίοι δεν το έχουν αλλάξει από τότε που εκτελέστηκε για τελευταία φορά το Crack.

Περιορισμοί από την χρήση

Αυτό το πρόγραμμα λογισμικού έχει σχεδιαστεί σαν εργαλείο για τους διαχειριστές να βρίσκουν αδύναμα συνθηματικά τα οποία αποτελούν πηγή κίνδυνων για την ασφάλεια του συστήματος, και δεν είναι φρόνιμο να εκτελείται από άτομα τα οποία δεν έχουν την σχετική εξουσιοδότηση από τους διαχειριστές των συστημάτων. Ο λόγος είναι ότι πρόκειται για ένα ισχυρό εργαλείο το οποίο αν βρεθεί στα χέρια λάθος ατόμων θα μπορούσε να προξενήσει μεγάλες καταστροφές στην ασφάλεια ενός πληροφοριακού συστήματος ενός οργανισμού.

Βιβλιογραφία - References:

ftp://ftp.cert.dfn.de/pub/tools/admin/Cops/01-README
ftp://ftp.bath.ac.uk/pub/security
http://www.bath.ac.uk/BUCS/
http://tripwire.com
http://tripwiresecurity.com
http://www.cs.purdue.edu/coast/ids (*COAST Intrusion Detection System Resources page)*
ftp://coast.cs.purdue.edu/pub/tools/unix/
http://www.robertgraham.com/pubs/network-intrusion-detection.html