Τεχνολογικό Εκπαιδευτικό Ίδρυμα Δυτικής Ελλάδας (Τ.Ε.Ι)
Τμήμα Μηχανικών Πληροφορικής Τ.Ε.

Νομική και Πληροφορική: Παρουσίαση βασικών στοιχείων, μηχανισμών και case studies

Πτυχιακή εργασία της φοιτήτριας : Καλουδιώτη Νικολέττας
Εποπτεύων καθηγητής : Ασημακόπουλος Γεώργιος

Αντίρριο 07/06/2017

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1:
ΣΥΜΒΑΝΤΑ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΑΝΤΑΠΟΚΡΙΣΗ

ΚΕΦΑΛΑΙΟ 2:
ΑΡΧΙΚΗ ΦΑΣΗ ΑΝΤΑΠΟΚΡΙΣΗΣ ΚΑΙ ΒΟΗΘΗΤΙΚΑ ΕΡΓΑΛΕΙΑ

ΚΕΦΑΛΑΙΟ 3:
ΣΥΛΛΟΓΗ ΔΕΔΟΜΕΝΩΝ ΣΕ ΣΥΣΤΗΜΑΤΑ UNIX

ΚΕΦΑΛΑΙΟ 4:
ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΑ ΑΝΤΙΓΡΑΦΑ

ΚΕΦΑΛΑΙΟ 5:
ΣΥΛΛΟΓΗ NETWORK-BASED ΣΤΟΙΧΕΙΩΝ

ΚΕΦΑΛΑΙΟ 6:
ΧΕΙΡΙΣΜΟΣ ΑΠΟΔΕΙΚΤΙΚΩΝ ΣΤΟΙΧΕΙΩΝ

ΚΕΦΑΛΑΙΟ 7:
ΘΕΜΕΛΕΙΩΔΕΙΣ ΑΡΧΕΣ ΑΠΟΘΗΚΕΥΣΗΣ ΣΥΣΤΗΜΑΤΟΣ

ΚΕΦΑΛΑΙΟ 8:
ΤΕΧΝΙΚΕΣ ΑΝΑΛΥΣΗΣ ΔΕΔΟΜΕΝΩΝ

ΚΕΦΑΛΑΙΟ 9:
ΕΡΕΥΝΩΝΤΑΣ ΤΑ ΣΥΣΤΗΜΑΤΑ WINDOWS

ΚΕΦΑΛΑΙΟ 10:
ΕΡΕΥΝΩΝΤΑΣ ΤΑ ΣΥΣΤΗΜΑΤΑ UNIX

ΚΕΦΑΛΑΙΟ 11:
ΑΝΑΛΥΣΗ ΤΗΣ ΚΙΝΗΣΗΣ ΤΟΥ ΔΙΚΤΥΟΥ

ΚΕΦΑΛΑΙΟ 12:
ΕΡΕΥΝΩΝΤΑΣ ΤΑ ΕΡΓΑΛΕΙΑ ΤΩΝ HACKER

ΚΕΦΑΛΑΙΟ 13:
ΕΡΕΥΝΩΝΤΑΣ ΤΟΥΣ ROUTERS

ΕΙΣΑΓΩΓΗ

Η παρούσα πτυχιακή εργασία παρέχει βασικές γνώσεις που είναι απαραίτητες για την έρευνα και την εκτέλεση ανταπόκρισης σε περιστατικά εγκλήματος πληροφορικής. Αναφέρεται η συνολική διαδικασία αντιμετώπισης περιστατικών, η διαδικασία έρευνας και νομικές προσεγγίσεις ώστε να υπάρχουν επικυρωμένα πειστήρια για δικαστική χρήση. Με οποιονδήποτε τρόπο και σε οποιαδήποτε μορφή και αν βρεθούν αποδεικτικά στοιχεία σε έναν υπολογιστή αποτελούν αδιάψευστο τεκμήριο για οποιοδήποτε ηλεκτρονικό έγκλημα έχει διαπραχθεί. Επομένως θα αναλύσουμε τρόπους για συλλογή δεδομένων από συστήματα Unix και Windows. Για να υπάρξει γρήγορη ανταπόκριση σε ένα τέτοιο κρούσμα σαφώς επιστρατεύονται οι γνώσεις πολλών ανθρώπων χρησιμοποιώντας μια προκαθορισμένη μεθοδολογία. Στην συγκεκριμένη μεθοδολογία ανταπόκρισης που μελετάμε δίνεται έμφαση σε πολλά πράγματα καθώς, απαιτείται πολύπλευρη πειθαρχία επιστρατεύοντας μυριάδες ικανοτήτων από διαφορετικές λειτουργικές μονάδες καθώς και εξειδικευμένα εργαλεία. Συνεπώς στόχος είναι η ανάπτυξη και εφαρμογή μιας μεθοδολογίας που προάγει μια συντονισμένη συνεκτική απάντηση σε οποιοδήποτε συμβάν.

This graduation thesis establishes a baseline of knowledge necessary for performing incident response and computer forensics. We discuss the overall incident response and computer security investigation process, and how we can develop an incident response capability that successfully protects its assets. All investigations into computer security incidents require you to collect information. Specifically, you will collect host-based evidence, network-based evidence, and other, nontechnical evidence in order to determine what happened and how the incident might be resolved. Therefore, the chapters cover how to obtain host-based information from live computer systems, collecting the volatile data from Unix and Windows systems. We describe how to perform network monitoring with popular network packet-capturing programs in order to collect network-based evidence. We discuss how to obtain evidence by interviewing system administrators, managers,and other personnel when investigating a computer security incident. During the collection of all information, we never lose sight of the fact that the information must be retrieved and handled in a fashion that promotes authentication. Therefore,
we discuss how to document and maintain details about the evidence you collect

ΚΕΦΑΛΑΙΟ 1

ΤΙ ΚΑΛΕΙΤΑΙ ΣΥΜΒΑΝ ΑΣΦΑΛΕΙΑΣ

- Κλοπή ανταλλασσόμενων μυστικών σε ένα δίκτυο
- Ανεπιθύμητα e-mail και παρενόχληση
- Παράνομες ή αναρμόδιες εισβολές στο σύστημα
- Κατάχρηση/υπεξαίρεση
- Κατοχή ή διάδοση παιδικής πορνογραφίας
- Επιθέσεις άρνησης εξυπηρέτησης (DOS)
- Αδικήματα που αφορούν στην επί σκοπού καταστροφή επιχειρησιακών σχέσεων
- Εκβιασμοί
- Αποθηκευμένες αποδείξεις παράνομης δράσης όπως απάτη,απειλές κ παραδοσιακά εγκλήματα.

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΣΤΟΧΟΙ ΣΤΗΝ ΑΝΤΑΠΟΚΡΙΣΗ ΕΝΟΣ ΣΥΜΒΑΝΤΟΣ 1/2

- Επιβεβαιώνει ή διώχνει όποιο περιστατικό το απασχολεί
- Προωθεί τη συσσώρευση της ακριβούς πληροφορίας
- Καθιερώνει τους ελέγχους για την κατάλληλη ανάκτηση και χρήση των στοιχείων
- Προστατεύει τα δικαιώματα μυστικότητας που καθιερώνονται από τον νόμο και την πολιτική
- Αποτρέπει αποσπασματικές και ίσως καταστρεπτικές απαντήσεις
- Μειώνει τις διακοπές των διαδικασιών σε επιχειρήσεις και δίκτυα

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΣΤΟΧΟΙ ΣΤΗΝ ΑΝΤΑΠΟΚΡΙΣΗ ΕΝΟΣ ΣΥΜΒΑΝΤΟΣ 2/2

- Επιτρέπει την εγκληματική ή αστική δράση ενάντια στους δράστες
- Παρέχει τις ακριβείς εκθέσεις και χρήσιμες συστάσεις
- Παρέχει γρήγορες ανιχνεύσεις και αναχαιτίσεις
- Ελαχιστοποιεί την έκθεση των προσωπικών δεδομένων
- Προστατεύει την φήμη μιας επιχείρησης
- Προωθεί τις γρήγορες ανιχνεύσεις και την πρόληψη τέτοιων γεγονότων στο μέλλον

ΔΙΑΔΙΚΑΣΙΑ ΑΝΤΑΠΟΚΡΙΣΗΣ ΚΑΙ ΕΜΠΛΕΚΟΜΕΝΟΙ

Για την διαδικασία ανταπόκρισης ενός συμβάντος απαιτούνται δυνάμεις από διαφορετικούς τομείς όπως:

- Νομικοί σύμβουλοι
- Τεχνικοί εμπειρογνώμονες
- Επαγγελματίες ασφαλείας κ.α
- Οι περισσότερες οργανώσεις καθιερώνουν μια ομάδα ατόμων, συχνά καλούμενη ως Computer Security Incident Response Team (CSIRT)

ΜΕΘΟΔΟΛΟΓΙΑ ΑΝΤΑΠΟΚΡΙΣΗΣ

1. Προετοιμασία της ομάδας για την εμφάνιση του συμβάντος
2. Ανίχνευση/εντοπισμός περιστατικού

3. Αρχική ανταπόκριση
4. Δημιουργία στρατηγικής
5. Έρευνα περιστατικού
6. Αναφορά περιστατικού
7. Λύση

ΠΡΟΕΤΟΙΜΑΣΙΑ ΠΕΤΥΧΗΜΕΝΗΣ ΑΝΤΑΠΟΚΡΙΣΗΣ

- Εφαρμογή μέτρων ασφαλείας από το κεντρικό σύστημα/δίκτυο
- Εκπαίδευση χρηστών
- Χρήση ενός συστήματος ανίχνευσης εισβολών(IDS)
- Ισχυρός έλεγχος προσπέλασης
- Έγκαιρη εκτίμηση της ευπάθειας του συστήματος
- Εξασφάλιση αντιγράφων ασφαλείας

ΠΡΟΕΤΟΙΜΑΣΙΑ ΟΜΑΔΑΣ CSIRT

- Χρήση software/hardware για έρευνα γεγονότος ασφαλείας στον Η/Υ
- Επιτυχής τεκμηρίωση γεγονότος
- Κατάλληλες πολιτικές και λειτουργικές διαδικασίες για εφαρμογή στρατηγικής ανταπόκρισης
- Κατάρτιση του προσωπικού στις εγκληματολογικές έρευνες για επιτυχή ανταπόκριση και αποκατάσταση

ΕΝΤΟΠΙΣΜΟΣ ΣΥΜΒΑΝΤΟΣ

- Καταγραφή τρέχουσας ώρας και ημερομηνίας
- Φύση/προέλευση του συμβάντος
- Πότε εμφανίστηκε το συμβάν
- Τι υλικό/λογισμικό περιλαμβάνεται
- Σημεία επαφής για το προσωπικό που περιλαμβάνεται

ΑΡΧΙΚΗ ΑΝΤΑΠΟΚΡΙΣΗ

- Συζήτηση με τους διαχειριστές του συστήματος οι οποίοι έχουν άμεση επαφή με τις τεχνικές λεπτομέρειες
- Συζήτηση με τις μονάδες του προσωπικού
- Επανεξέταση των αναφορών της "εισβολής" για πιστοποίηση του γεγονότος
- Αναθεώρηση της τοπολογίας του δικτύου

ΔΗΜΙΟΥΡΓΙΑ ΣΤΡΑΤΗΓΙΚΗΣ

- Πόσο επηρεασμένη είναι η ασφάλεια του συστήματος;
- Πόσο ευαίσθητες είναι οι πληροφορίες που έχουν αποκαλυφθεί;
- Ποιοι είναι οι πιθανοί δράστες;
- Είναι το περιστατικό ευρέως γνωστό;
- Ποια είναι η προφανής ικανότητα του επιτιθέμενου
- Πόσος ήταν ο χρόνος διακοπής των χρηστών ή του συστήματος;
- Ποια η γενική απώλεια χρημάτων;

ΣΥΝΤΑΞΗ ΑΝΑΦΟΡΑΣ

- Γρήγορη καταγραφή δεδομένων με σαφήνεια και ακρίβεια
- Σαφής περιληπτική καταγραφή με πειθαρχία και οργάνωση
- Χρήση έτοιμης φόρμας αναφορών για εξασφάλιση χρόνου
- Απασχόληση τεχνικών συντακτών για έλεγχο και διόρθωση των αναφορών έτσι ώστε να είναι κατανοητές και από μη τεχνικό προσωπικό

ΑΝΑΛΥΣΗ ΠΡΟΒΛΗΜΑΤΟΣ

- Εντοπισμός της φύσης του περιστατικού έτσι ώστε να βρεθεί ο κατάλληλος τρόπος εξέτασης
- Καθορισμός των αιτιών που υποβόσκουν
- Αποκατάσταση επηρεασμένου συστήματος
- Εφαρμογή firewall κ.α
- Απόδοση ευθυνών για οποιοδήποτε ζήτημα αφορά στο σύστημα
- Παρακολούθηση της προόδου όλων των διορθώσεων
- Επικύρωση των διορθωτικών βημάτων
- Αναβάθμιση της πολιτικής ασφαλείας

ΠΡΟΕΤΟΙΜΑΣΙΑ ΕΓΚΑΙΡΗΣ ΑΝΤΑΠΟΚΡΙΣΗΣ

- Τι συνέβη ακριβώς;
- Ποιο σύστημα επηρεάστηκε;
- Ποιες πληροφορίες παραβιάστηκαν;
- Ποια αρχεία υπέστησαν αλλαγές;
- Ποιος μπορεί να ευθύνεται;
- Ποιος πρέπει να ειδοποιηθεί;

Η ΠΡΟΕΤΟΙΜΑΣΙΑ ΠΡΙΝ ΤΟ ΚΡΟΥΣΜΑ

- Προσδιορισμός των κινδύνων σε ένα δίκτυο
- Προετοιμασία των χρηστών
- Εφαρμογή μέτρων ασφαλείας στο δίκτυο
- Δημιουργία μιας καλής ομάδας CSIRT για την συγκέντρωση και τον χειρισμό των γεγονότων

ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΤΟΥ ΚΙΝΔΥΝΟΥ

- Επικινδυνότητα στον επαγγελματικό τομέα
- Πόσο προσωπική είναι η πληροφορία, τα στοιχεία που εκλάπησαν
- Υπήρξε κλοπή μη δημόσιων προσωπικών πληροφοριών

ΠΡΟΕΤΟΙΜΑΣΙΑ ΜΕΜΟΝΟΜΕΝΩΝ ΧΡΗΣΤΩΝ

- Καταγραφή κρυπτογραφημένων αρχείων από φακέλους
- Επιτρεπόμενη ασφαλή καταγραφή λογιστικών αρχείων

- Ενίσχυση της άμυνας κάθε υπολογιστή
- Δημιουργία αντιγράφων ασφαλείας δεδομένων
- Εκπαίδευση χρηστών σύμφωνα με το εγκατεστημένο σύστημα ασφαλείας

ΔΙΑΜΟΡΦΩΣΗ ΑΡΧΕΙΟΥ ΚΑΤΑΓΡΑΦΗΣ

- Καταγραφή αρχείων μηνυμάτων όπου μόνο ο διαχειριστής μπορεί να έχει πρόσβαση
- Αρχείο ασφαλείας σε απομακρυσμένο δέκτη
- Καταγραφή όσων περισσότερων χρήσιμων πληροφοριών γίνεται
- Καταγραφή IP διευθύνσεων

ΔΗΜΙΟΥΡΓΙΑ ΑΜΥΝΑΣ ΔΕΚΤΗ

- Σιγουρευτείτε ότι όλα τα προγράμματα λειτουργικών συστημάτων και εφαρμογών είναι εγκατεστημένα με την τελευταία έκδοση
- Θέστε εκτός λειτουργίας εφαρμογές και υπηρεσίες δικτύου που δεν χρησιμοποιείτε καθώς όταν τρέχουν περιττές εφαρμογές μπορούν να εισάγουν κινδύνους
- Όταν βρίσκεστε αντιμέτωπος με επιλογές διαμόρφωσης επιλέξτε σοφά καθώς πολλοί κίνδυνοι εισάγονται μέσω της επιπόλαιης διοίκησης του συστήματος

ΠΡΟΕΤΟΙΜΑΣΙΑ ΕΝΟΣ ΔΙΚΤΥΟΥ

- Εγκατάσταση συστήματος ανίχνευσης εισχώρησης κινδύνων
- Χρήση access control lists (λίστες ελέγχου προσπέλασης) στους δρομολογητές
- Δημιουργία τοπολογίας δικτύου που να συμβάλλει στον έλεγχο
- Κρυπτογράφηση της συμφόρησης σε ένα δίκτυο

ΠΕΡΙΠΤΩΣΕΙΣ ΕΙΣΒΟΛΗΣ

- Ο εισβολέας εγκαθιστά κάποιου είδους hardware/software υποκλοπής πακέτων που μεταφέρονται σε ένα δίκτυο
- Έτσι μπορεί να έχει πρόσβαση σε κωδικούς και προσωπικά δεδομένα όχι μόνο από έναν υπολογιστή αλλά από όλους τους υπολογιστές ενός δικτύου
- Για να να έχεις άμεση ανταπόκριση πρέπει να βρεις ποιος υπολογιστής έχει εκθέσει τα δεδομένα στον εισβολέα
- Το να απομακρύνεις τον προσβεβλημένο υπολογιστή είναι μάταιο καθώς ο εισβολέας θα έχει ήδη πρόσβαση σε όλο το σύστημα λόγω υποκλοπής κωδικών και ονομάτων χρηστών

ΚΡΥΠΤΟΓΡΑΦΩΝΤΑΣ ΤΗΝ ΚΥΚΛΟΦΟΡΙΑ ΣΕ ΕΝΑ ΔΙΚΤΥΟ

- Η κρυπτογράφηση του traffic ενός δικτύου βελτιώνει την ασφάλειά του
- Δυο δημοφιλείς εφαρμογές κρυπτογράφησης είναι οι SSL (Secure Sockets Layer) , SSH (Secure Shell)
- Η SSL χρησιμοποιείται για την κρυπτογράφηση των κινήσεων στον ιστό
- Η SSH χρησιμοποιείται για την κρυπτογράφηση των συνδέσεων των χρηστών και για την μεταφορά αρχείων στα ιδιωτικά δίκτυα (VPNs)

ΚΑΘΟΡΙΣΜΟΣ ΘΕΣΗΣ ΑΝΤΑΠΟΚΡΙΣΗΣ

- Αγνοήστε το γεγονός συνολικά
- Κρατήστε αμυντική στάση για τυχών νέες επιθέσεις
- Συλλογή και επιθεώρηση των αρχείων αντικατασκοπίας
- Καθορισμός επίδρασης του συμβάντος στον επαγγελματικό σας τομέα
- Έλεγχος των νομικών θεμάτων και περιορισμοί
- Τεχνικές ικανότητες της ομάδας ανταπόκρισης
- Χρηματοδότηση και διαθέσιμοι πόροι

ΝΟΜΙΚΑ ΘΕΜΑΤΑ

- Εγκατάσταση παγίδας περίεργων στοιχείων
- Πλήρη παρακολούθηση του δικτύου
- Έλεγχος των υπολογιστών ξεχωριστά

ΕΓΚΑΤΑΣΤΑΣΗ ΠΑΓΙΔΑΣ

- Διαφυλάσσει εν μέρει το προσωπικό απόρρητο του κάθε χρήστη σε ένα δίκτυο
- Επιτρέπει στον διαχειριστή του δικτύου να ανιχνεύσει τα λάθη και να προσδιορίσει την πηγή των τεχνικών βλαβών

ΣΥΝΟΨΗ ΕΦΑΡΜΟΓΗΣ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

- Συλλογή πληροφοριών από τους χρήστες του δικτύου
- Συναλλαγή πληροφοριών
- Καταγραφή των ηλεκτρονικών ανακοινώσεων που αποθηκεύονται σε έναν υπολογιστή
- Πλήρης παρακολούθηση του δικτύου

ΔΗΜΙΟΥΡΓΙΑ ΠΟΛΙΤΙΚΩΝ ΧΡΗΣΗΣ

- Σωστή επιλογή ανθρώπου για την δημιουργία των πολιτικών
- Χρήση του δικτύου μόνο από έμπιστα άτομα
- Ενημέρωση όλων των χρηστών για τις πολιτικές χρήσης του δικτύου
- Συνέπεια στις πολιτικές χρήσης και από τον διαχειριστή του δικτύου

ΤΕΧΝΙΚΟΣ ΣΧΕΔΙΑΣΜΟΣ 1/2

- Ποιος θα προσθέτει και θα αφαιρεί χρήστες στο δίκτυο;
- Ποιος θα έχει απομακρυσμένη πρόσβαση στα μηχανήματα;
- Ποιος θα ελέγχει τους υπολογιστές;
- Ποιος θα φυλάσσει τα αρχεία με τους κωδικούς;

ΤΕΧΝΙΚΟΣ ΣΧΕΔΙΑΣΜΟΣ 2/2

- Ποιος θα είναι διαχειριστής και σε τι;
- Επιτρέπετε η ταχυδρόμηση στις ομάδες πληροφόρησης;

- Ποιου είδους διαδικτυακών συνομιλιών επιτρέπονται;
- Θα παραβλέπατε την χρήση πειρατικού λογισμικού;

ΣΥΜΠΕΡΙΦΟΡΑ ΧΡΗΣΤΩΝ

- Ποια είναι η πρέπουσα χρήση του διαδικτύου;
- Πως θα αντιδρούσατε σε μια ενδεχόμενη σεξουαλική παρενόχληση ή μία απειλή;
- Ποιος μπορεί να σας παρακολουθεί και πότε;
- Ποιος θα μπορούσε να κατέχει μεθόδους hacking;

ΕΙΔΗ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

- Πολιτική αποδοχής χρήσης
- Πολιτική λογαριασμών χρηστών
- Πολιτική απομακρυσμένης πρόσβασης
-
- Πολιτική χρήσης διαδικτύου

ΠΡΟΔΙΑΓΡΑΦΕΣ ΓΙΑ ΤΟ HARDWARE ΑΝΤΑΠΟΚΡΙΣΗΣ

- Επεξεργαστή υψηλών αποδόσεων
- Το λιγότερο 256MB RAM
- Δίσκους υψηλής περιεκτικότητας
- Γρήγορο CD-RW drive

Η ΒΑΣΗ ΓΙΑ ΕΝΑ ΣΩΣΤΟ ΛΟΓΙΣΜΙΚΟ

- Εγκατάσταση 2-3 λειτουργικών συστημάτων (πχ LINUX) με δυνατότητα εκκίνησης μέσω CD-ROM
- Λογισμικό πακέτο εγκληματολογίας που χρησιμοποιείται για σκοπούς εγκληματολογικής – επεξεργασίας
- Κατοχή όλων των απαραίτητων drivers
- Εγκατάσταση λογισμικού που επιτρέπει το άνοιγμα σχεδόν όλων των τύπων αρχείων
- Αντίγραφα ασφαλείας σε DVD

ΣΚΟΠΟΣ ΤΗΣ ΟΜΑΔΑΣ ΑΝΤΑΠΟΚΡΙΣΗΣ 1/3

- Ανταπόκριση σε όλα τα γεγονότα ασφαλείας
- Να προβεί σε πλήρη έρευνα απαλλαγμένη από προκαταλήψεις
- Να επιβεβαιώσει άμεσα εάν όντως έχει πραγματοποιηθεί κάποια εισβολή
- Να εκτιμήσει τις ζημιές που προκλήθηκαν και το λόγο της εισβολής
- Καθιέρωση 24ωρης άμεσης επικοινωνίας κατά τη διάρκεια της έρευνας

ΣΚΟΠΟΣ ΤΗΣ ΟΜΑΔΑΣ ΑΝΤΑΠΟΚΡΙΣΗΣ 2/3

- Έλεγχος και περιορισμός του συμβάντος
- Συλλογή όλων των στοιχείων που σχετίζονται με το συμβάν
- Διατήρηση των αποδεικτικών στοιχείων μετά τη συλλογή
- Επιλογή πρόσθετης υποστήριξης όταν χρειάζεται
- Προστασία των δικαιωμάτων των προσωπικών δεδομένων που καθορίζονται από το νόμο

ΣΚΟΠΟΣ ΤΗΣ ΟΜΑΔΑΣ ΑΝΤΑΠΟΚΡΙΣΗΣ 3/3

- Καταγραφή μαρτυρίας εμπειρογνώμονα
- Παροχή συνδέσμου για την ορθή επιβολή του νόμου και των δικαστικών αρχών
- Διατήρηση της εμπιστευτικότητα του συμβάντος

ΕΡΩΤΗΣΕΙΣ

- Ποιοι οι βασικοί παράγοντες που χρησιμοποιούνται για τον προσδιορισμό του κινδύνου ;
- Ποια είναι τα πλεονεκτήματα των κρυπτογραφικών αθροισμάτων ελέγχου ;
- Πώς η τοπολογία του δικτύου επηρεάζει την ανταπόκρισή σε ένα περιστατικό ;
- Εάν σας ζητούσαν να παρακολουθήσετε το e-mail ενός φίλου ποιοι παράγοντες θα επηρέαζαν την απάντηση σας;

ΚΕΦΑΛΑΙΟ 2

ΕΠΙΣΚΟΠΗΣΗ ΤΗΣ ΑΡΧΙΚΗΣ ΦΑΣΗΣ ΑΝΤΑΠΟΚΡΙΣΗΣ

* Γρήγορη και αποτελεσματική λήψη αποφάσεων
* Γρήγορη συλλογή στοιχείων
* Σωστή κλιμάκωση του περιστατικού
* Γρήγορη ανάθεση αρμοδιοτήτων στα άτομα που αποτελούν την ομάδα ανταπόκρισης συμβάντων

ΑΠΟΚΤΗΣΗ ΠΡΟΚΑΤΑΡΚΤΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

* Λήψη της αρχικής ανακοίνωσης του συμβάντος
* Καταγραφή των πρώτων πληροφοριών σχετικά με το γεγονός
* Σύνταξη μιας συναφούς αναφοράς
* Συγκέντρωση της ομάδας ανταπόκρισης
* Εκτέλεση των εξεταστικών βημάτων
* Καθορίστε εάν το κρούσμα κλιμακώνεται ή όχι

ΠΡΩΤΟ ΜΕΡΟΣ ΤΗΣ ΑΡΧΙΚΗΣ ΑΝΤΑΠΟΚΡΙΣΗΣ 1/2

* Χρονολόγηση γεγονότος,πότε άρχισε;
* Ποια τα στοιχεία επικοινωνίας του προσώπου που συμπληρώνει το έντυπο;
* Ποια τα στοιχεία επικοινωνίας του προσώπου που ανίχνευσε το γεγονός;
* Τι είδους κρούσμα ανιχνεύτηκε;

ΠΡΩΤΟ ΜΕΡΟΣ ΤΗΣ ΑΡΧΙΚΗΣ ΑΝΤΑΠΟΚΡΙΣΗΣ 2/2

* Ποια η τοποθεσία των επηρεασμένων υπολογιστών
* Μια περιγραφή της φυσικής ασφάλειας στην τοποθεσία
* Ποια η ημερομηνία ανίχνευσης του περιστατικού
* Πως ανιχνεύθηκε το περιστατικό

ΔΕΥΤΕΡΟ ΜΕΡΟΣ ΤΗΣ ΑΡΧΙΚΗΣ ΑΝΤΑΠΟΚΡΙΣΗΣ 1/3
Λεπτομέρειες συστήματος

- Δημιουργία και διαμόρφωση των σχετικών συστημάτων
- Λειτουργικό σύστημα
- Βασικός χρήστης των συστημάτων
- Προγραμματισμένος διαχειριστής των συστημάτων
- Διαδικτυακή διεύθυνση ή IP για τα σχετικά συστήματα
- Διαδικτυακό όνομα των συστημάτων
- Αν υπάρχει η μόντεμ σύνδεση για τα συστήματα
- Κρίσιμες πληροφορίες που μπορεί να βρίσκονται στα συστήματα

ΔΕΥΤΕΡΟ ΜΕΡΟΣ ΤΗΣ ΑΡΧΙΚΗΣ ΑΝΤΑΠΟΚΡΙΣΗΣ 2/3
Περιορισμός του κρούσματος

- Αν το περιστατικό είναι σε εξέλιξη ή έχει διάρκεια
- Αν χρειάζεται η παρακολούθηση του δικτύου ή η διεξαγωγή του
- Αν το σύστημα είναι ακόμη συνδεδεμένο στο διαδίκτυο. Αν όχι ποιος είναι υπεύθυνος για την αφαίρεση του και πότε θα μπορεί να είναι πάλι ενεργό;
- Αν υπάρχουν κασέτες με αντίγραφα ασφαλείας των συστημάτων
- Αν είναι απαραίτητο να υπάρχουν στοιχεία για το περιστατικό σε μια βάση δεδομένων
- Αν υπάρχουν κάποια επανορθωτικά στάδια τα οποία έχουν παρθεί μέχρι τώρα(όπως νέες λίστες για τον έλεγχο πρόσβασης, φιλτράρισμα των πακέτων κ.α)

ΔΕΥΤΕΡΟ ΜΕΡΟΣ ΤΗΣ ΑΡΧΙΚΗΣ ΑΝΤΑΠΟΚΡΙΣΗΣ 3/3
Προκαταρκτική έρευνα

- Οι διευθύνσεις IP που συμμετέχουν στο περιστατικό
- Αν υπάρχουν κάποια στάδια έρευνας ή κάποιες ενέργειες τα οποία έχουν γίνει
- Αν υπάρχουν κάποια εγκληματολογικά αντίγραφα τα οποία πρέπει να δημιουργηθούν ή ένα λογικό αντίγραφο των σχετικών συστημάτων είναι αρκετό;

ΔΗΛΩΣΗ ΠΕΡΙΣΤΑΤΙΚΟΥ

- Υπήρξε εσκεμμένη ή τυχαία διακοπή του δικτύου κατά τη διάρκεια εμφάνισης του περιστατικού;
- Υπήρξε αναφορά διακοπής παροχής πόρων κατά την πιθανολογούμενη εμφάνιση του περιστατικού;
- Το σύστημα που επηρεάστηκε είχε υποστεί κάποια αναβάθμιση πρότινος;
- Για εσωτερικά περιστατικά υπάρχουν πιστοποιητικά που έχουν παρθεί για τις ενέργειες των χρηστών ώστε να περιοριστούν οι υποψίες;

ΣΥΓΚΕΝΤΡΩΣΗ ΤΗΣ ΟΜΑΔΑΣ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ 1/2

- Καθορισμός διαδικασιών κλιμάκωσης
- Εφαρμογή διαδικασίας γνωστοποίησης του περιστατικού
- Οριοθέτηση του γεγονότος και συγκέντρωση των κατάλληλων πόρων
- Διορισμός ενός ατόμου ως αρχηγού της ομάδας

ΣΥΓΚΕΝΤΡΩΣΗ ΤΗΣ ΟΜΑΔΑΣ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ 2/2

- Το κάθε μέλος της ομάδας θα πρέπει να μπορεί πραγματικά να βοηθήσει στη έρευνα
- Δεν θα πρέπει να προκαλεί σύγχυση,πανικό ή να παρεμποδίζει την έρευνα
- Να σιγουρέψετε πως δεν έχει φιλικές σχέσεις με υπόπτους

ΟΡΙΟΘΕΤΗΣΗ ΠΕΡΙΣΤΑΤΙΚΟΥ ΚΑΙ ΣΥΓΚΕΝΤΡΩΣΗ ΠΟΡΩΝ

- Ποιο το πλήθος των ατόμων που εμπλέκονται στο περιστατικό;
- Ποιο το πλήθος των συστημάτων;
- Ποιο το πλήθος των εμπλεκόμενων και ευάλωτων συστημάτων;
- Οριοθέτηση περιόδου κατά την οποία θα πρέπει η έρευνα να ολοκληρωθεί

ΟΡΙΣΜΟΣ ΑΡΧΗΓΟΥ ΟΜΑΔΑΣ 1/3

- Οργάνωσε την ομάδα σου κατά την διάρκεια ανταπόκρισης του περιστατικού
- Οργάνωσε την διαδικασία ανάκρισης καθώς μιλάς με τους μάρτυρες, τους διαχειριστές των συστημάτων, τον τελικό χρήστη, τον νομικό σύμβουλο, τον διευθυντή κ.α
- Να παρέχεις αναφορές της κατάστασης και να επικοινωνείς αποδοτικά με τη διεύθυνση κατά την διάρκεια ενός περιστατικού

ΟΡΙΣΜΟΣ ΑΡΧΗΓΟΥ ΟΜΑΔΑΣ 2/3

- Να παρέχεις μια ολοκληρωμένη ανάλυση του περιστατικού
- Να προστατεύεις τις αποδείξεις που συνέλεξες κατά την διάρκεια της έρευνας με συνέπεια μαζί με τις οδηγίες και τα αποδεικτικά στοιχεία
- Ανέλαβε την ευθύνη να επιβεβαιώσεις την αλληλουχία των αποδεικτικών στοιχείων
- Παρουσίασε εγκληματολογικά αντίγραφα και αναλύσεις αν είναι απαραίτητο

ΟΡΙΣΜΟΣ ΑΡΧΗΓΟΥ ΟΜΑΔΑΣ 3/3

- Να είσαι σίγουρος ότι έχουν χρησιμοποιηθεί οι καλύτερες πρακτικές και οι κατάλληλες τεχνικές ανταπόκρισης
- Σύνταξε, διαχειρήσου και παρουσίασε την αναφορά της έρευνας και δώσε προτάσεις στη διεύθυνση
- Κατάλαβε τα νομικά θέματα και τις πολιτικές της εταιρίας
- Να παρέχεις μια αμερόληπτη έρευνα χωρίς σύγκρουση συμφερόντων

ΟΡΙΣΜΟΣ ΤΕΧΝΙΚΟΥ ΠΡΟΣΩΠΙΚΟΥ 1/3

- Πλήρης γνώση των εμπλεκόμενων λειτουργικών συστημάτων από τα μέλη του τεχνικού προσωπικού
- Δυνατότητα εξέτασης αρχείων καταγραφής και στοιχείων για την σύνταξη αναφοράς πορίσματος
- Δυνατότητα σωστής εκτίμησης επιρροής στο σύστημα
- Κατανόηση των αποδεικτικών στοιχείων

ΟΡΙΣΜΟΣ ΤΕΧΝΙΚΟΥ ΠΡΟΣΩΠΙΚΟΥ 2/3

- Δυνατότητα να βοηθήσει στον καθορισμό του πεδίου ενός γεγονότος
- Δυνατότητα να καθοριστεί η φύση του περιστατικού και να εντοπιστούν οι τεχνικές λεπτομέρειες
- Δυνατότητα να κάνουν συστάσεις για το πώς θα διορθωθεί η κατάσταση
- Διατήρηση της προοπτικής οτι τα τεχνικά αποδεικτικά στοιχεία είναι ικανά να βοηθήσουν στην επίλυση του γεγονότος

ΟΡΙΣΜΟΣ ΤΕΧΝΙΚΟΥ ΠΡΟΣΩΠΙΚΟΥ 3/3

- Σύνταξη εγγράφου που να καταγράφει όλα τα στάδια διερεύνησης συνοπτικά και με σαφήνεια
- Δυνατότητα να παρέχουν στήριξη στον αρχηγό της ομάδας
- Δυνατότητα να πραγματοποιήσουν συνεντεύξεις όταν χρειάζεται

ΑΣΚΗΣΗ ΠΑΡΑΔΟΣΙΑΚΩΝ ΣΤΑΔΙΩΝ ΕΡΕΥΝΑΣ

- Αποδεικτικά στοιχεία σε κάθε υπολογιστή. Συλλέγονται ως συνήθως μέσω των Windows

- Αποδεικτικά στοιχεία στο δίκτυο. Συλλέγονται ως συνήθως μέσω των δρομολογητών ή κάποιου άλλου κόμβου
- Λοιπά αποδεικτικά στοιχεία που αφορούν το κίνητρο την πρόθεση κ.α

ΔΙΕΝΕΡΓΕΙΑ ΣΥΝΕΝΤΕΥΞΗΣ

- Τι έγινε;
- Πότε έγινε;
- Ποια συστήματα σχετίζονται;
- Ποιος μπορεί να το έκανε;
- Ποιος χρησιμοποιεί τα επηρεασμένα συστήματα;
- Τι ενέργειες έχουν ήδη γίνει;
- Ποια είναι η πολιτική για ένα τέτοιο περιστατικό;

ΚΑΤΑΓΡΑΦΗ ΠΛΗΡΟΦΟΡΙΩΝ ΕΠΙΚΟΙΝΩΝΙΑΣ ΧΡΗΣΤΩΝ

- Ονοματεπώνυμο
- Επάγγελμα
- Αριθμός τηλεφώνου
- E-mail διεύθυνση

ΣΥΝΕΝΤΕΥΞΗ ΜΕ ΤΟΥΣ ΔΙΑΧΕΙΡΙΣΤΕΣ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ

- Έχετε παρατηρήσει κάποια παράξενη δραστηριότητα;
- Πόσοι άνθρωποι έχουν πρόσβαση σαν διαχειριστές στο σύστημα;
- Ποιες εφαρμογές παρέχουν απομακρυσμένη πρόσβαση στο σύστημα;
- Ποιες είναι οι δυνατότητες πρόσβασης στο σύστημα και το διαδίκτυο;
- Τι προφυλάξεις έχουν παρθεί αυτή τη στιγμή για το σύστημα;

ΣΥΝΕΝΤΕΥΞΗ ΜΕ ΤΟΥΣ ΥΠΕΥΘΥΝΟΥΣ

- Υπάρχουν ιδιαίτερα ευαίσθητα δεδομένα ή εφαρμογές στο σύστημα;
- Υπάρχουν προσωπικά δεδομένα που θα πρέπει να ληφθούν υπόψιν;
- Υπήρχαν δοκιμές αδειοδότησης για πρόσβαση στο σύστημα;
- Ποιο είναι το χειρότερο σενάριο που σκεφτήκατε σχετικά με το περιστατικό;

ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΑΣΚΗΣΕΙΣ ΑΝΤΑΠΟΚΡΙΣΗΣ 1/2

- Διορισμός αρχηγού
- Καθιερώστε ένα ασφαλές κανάλι επικοινωνίας για τους χρήστες
- Εξετάστε όλες τις πιθανές πηγές των πληροφοριών

- Μάζεψε αρκετές πληροφορίες για να καθοριστεί αν το περιστατικό έχει στην πραγματικότητα συμβεί.
- Αξιολογήστε τις επαγγελματικές επιπτώσεις του περιστατικού

ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΑΣΚΗΣΕΙΣ ΑΝΤΑΠΟΚΡΙΣΗΣ 2/2

- Καθορίστε τον τύπο του περιστατικού που έχει συμβεί
- Εφαρμόστε άμυνες στο δίκτυο όπως το φιλτράρισμα πακέτων
- Αποφύγετε σπασμωδικές ενέργειες και πανικό
- Απομακρύνετε τον προσβεβλημένο υπολογιστή από το δίκτυο
- Δημιουργήστε αντίγραφα ασφαλείας

ΣΚΕΨΕΙΣ ΓΙΑ ΤΗΝ ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΑΠΟΚΡΙΣΗΣ 1/2

- Έχετε ορίσει μια συγκεκριμένη στάση για ανταπόκριση στις επιθέσεις η οποία πρέπει να τηρηθεί ώστε να βρίσκει σύμφωνους τους πελάτες και τα ΜΜΕ;
- Η επίθεση από το εξωτερικό το κάνει τεχνικά πιο δύσκολο να το καταδιώξετε νόμιμα;
- Αξίζει η εφαρμογή μιας στρατηγικής ως προς το κόστος/όφελος της;
- Υπάρχουν κάποιες νόμιμες σκέψεις οι οποίες μπορούν να επηρεάσουν την ανταπόκριση;

ΣΚΕΨΕΙΣ ΓΙΑ ΤΗΝ ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΑΠΟΚΡΙΣΗΣ 2/2

- Μπορείτε να ρισκάρετε την δημοσιοποίηση του περιστατικού;
- Πώς αντιμετωπίσατε παρόμοια περιστατικά στο παρελθόν;
- Ποιο είναι το παρελθόν εργασίας του καθενός από τους οποίους εμπλέκονται;
- Μήπως η έρευνα θα κοστίσει περισσότερο από το να αφήσεις το περιστατικό απλά να συνεχιστεί;

ΕΦΑΡΜΟΣΜΕΝΗ ΣΤΡΑΤΗΓΙΚΗ ΑΝΤΑΠΟΚΡΙΣΗΣ

- Να σιγουρέψετε πως θα συμμετάσχουν τα αρμόδια όργανα λήψης αποφάσεων
- Πλήρης κατανόηση της φύσης του περιστατικού,πιθανοί δράστες και επιπτώσεις
- Προσδιορίστε το άτομο που θα έχει την ευθύνη για τη λήψη αποφάσεων.
- Καθορίστε τους στόχους
- Επιλέξτε εναλλακτικές λύσεις ανάλογα με την κατάσταση

ΠΡΟΕΤΟΙΜΑΣΙΑ "ΕΡΓΑΛΕΙΟΘΗΚΗΣ"

- Δώστε όνομα στην εργαλειοθήκη σας και προσδιορίστε το περιεχόμενό της

α) Αριθμός υπόθεσης
β) Ημερομηνία
γ) Όνομα ερευνητή δημιουργίας των μέσων ενημέρωσης ανταπόκρισης
δ) Όνομα του ερευνητή που ασχολείται με την υπόθεση

- Δημιουργήστε ένα αρχείο ελέγχου της εργαλειοθήκης σας
- Προστατεύστε οποιαδήποτε δισκέτα ή CD περιέχει αποδεικτικά στοιχεία

ΑΡΧΕΙΟΘΕΤΗΣΗ ΠΛΗΡΟΦΟΡΙΩΝ

- Αρχειοθέτηση των πληροφοριών που ανακτήθηκαν από τον σκληρό δίσκο του προσβεβλημένου συστήματος

- Καταγράψτε τις πληροφορίες που ανακτήθηκαν σε ένα τετράδιο χειρόγραφα
- Αποθηκεύστε τις πληροφορίες που ανακτήθηκαν σε αποσπώμενο σκληρό δίσκο, CD ή USB
- Αποθηκεύστε τα στοιχεία σε ένα απομακρυσμένο ιατροδικαστικό σύστημα χρησιμοποιώντας κάποιου είδους κρυπτογράφηση (π.χ netcat, cryptcat tools)

ΜΕΤΑΦΟΡΑ ΔΕΔΟΜΕΝΩΝ ΜΕΣΩ NETCAT TOOL

- Το netcat tool επιτρέπει στον χρήστη να εισέλθει αλλά και να εξέλθει γρήγορα στο προσβεβλημένο σύστημα
- Σας επιτρέπει να εκτελέσετε μια επιτυχή offline ανασκόπηση στις πληροφορίες

ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΔΕΔΟΜΕΝΩΝ ΜΕ ΧΡΗΣΗ CRYPTCAT TOOL

- Ο επιτιθέμενος δεν μπορεί να ΄΄διαβάσει΄΄ τις πληροφορίες που έχετε αποκτήσει
- Η κρυπτογράφηση περιορίζει την πιθανότητα παραποίησης ή εισβολής στα δεδομένα

ΑΠΟΚΤΗΣΗ ΕΥΜΕΤΑΒΛΗΤΩΝ ΔΕΔΟΜΕΝΩΝ

- Καταγεγραμμένες ημερομηνίες συστήματος
- Λίστα ενεργών χρηστών στο σύστημα
- Ημερομηνίες και ώρες των αρχείων όλου του συστήματος
- Λίστα των διεργασιών που εκτελούνται
- Λίστα των ανοιχτών υποδοχών
- Λίστα των εφαρμογών που ακούνε σε ανοιχτές υποδοχές
- Λίστα των συστημάτων που αλληλεπίδρασαν πρόσφατα με το σύστημά μας

ΣΥΛΛΟΓΗ ΤΩΝ ΕΥΜΕΤΑΒΛΗΤΩΝ ΔΕΔΟΜΕΝΩΝ 1/2

- Εκτελέστε ένα αρχείο cmd (cmd.exe)
- Καταγράψτε ώρα και ημερομηνία
- Καθορίστε ποιος είναι συνδεδεμένος στο σύστημα ακόμη και απομακρυσμένα
- Καθορίστε ποια ports είναι ανοιχτά
- Καταγράψτε μετατροπές,δημιουργίες και τις ώρες πρόσβασης σε όλα τα αρχεία

ΣΥΛΛΟΓΗ ΤΩΝ ΕΥΜΕΤΑΒΛΗΤΩΝ ΔΕΔΟΜΕΝΩΝ 2/2

- Λίστα των εφαρμογών που σχετίζονται με ανοιχτές θύρες
- Λίστα των διεργασιών που εκτελούνται
- Λίστα των πρόσφατων συνδέσεων
- Καταγραφή των εντολών που εκτελούνται στο σύστημα κατά την αρχική ανταπόκριση

ΚΑΤΑΓΡΑΦΗ ΠΡΟΣΦΑΤΩΝ ΣΥΝΔΕΣΕΩΝ

- Netstat : πολλοί ειδικοί ασφαλείας χρησιμοποιούν το netstat για να ελέγξουν τις ανοιχτές πόρτες στο σύστημα. Μπορούν έτσι να εντοπίσουν ip διευθύνσεις που είχαν πρόσβαση.
- Arp : Αυτό το βοηθητικό πρόγραμμα έχει πρόσβαση στην cache ARP μνήμη και χαρτογραφώντας την ip διεύθυνση μας οδηγεί στην mac address που είχε πρόσβαση στο σύστημα το τελευταίο λεπτό
- Nbtstat : Απαριθμεί τις πρόσφατες NetBios συνδέσεις για περίπου τα τελευταία 10 λεπτά

ΣΥΛΛΟΓΗ ΔΕΔΟΜΕΝΩΝ ΖΩΝΤΑΝΗΣ ΑΠΟΚΡΙΣΗΣ

- Εξέταση των αρχείων καταγραφής συμβάντων
- Έλεγχος του Registry (μητρώο)
- Αποκτήστε τους κωδικούς πρόσβασης του συστήματος
- Απορρίψτε την μνήμη RAM του συστήματος

ΕΡΩΤΗΣΕΙΣ

- Σε ποια μέσα εγκαθιστάτε και χρησιμοποιείτε την ερευνητική σας εργαλειοθήκη;Γιατί;
- Πώς προσδιορίζεις ποιες θύρες είναι συνδεδεμένες με εφαρμογές που εκτελούνται;
- Γιατί είναι απαραίτητο να αποκτήσουμε αρχεία καταγραφής κατά τη διάρκεια ζωντανής ανταπόκρισης
- Γιατί δεν αποτελεί καλή τακτική ο απομακρυσμένος έλεγχος;

ΚΕΦΑΛΑΙΟ 3

ΣΥΛΛΟΓΗ ΔΕΔΟΜΕΝΩΝ ΑΠΟ ΣΥΣΤΗΜΑΤΑ UNIX

- Η διαδικασία ανταπόκρισης στα συστήματα Unix είναι παρόμοια με αυτή των Windows
- Στόχος είναι να αποκτήσουμε τα ευμετάβλητα δεδομένα του συστήματος πριν την δημιουργία αντιγράφων από την εγκληματολογική έρευνα
- Μπορείτε να επεκτείνετε την συλλογή δεδομένων καταγράφοντας αρχεία του συστήματος και ύποπτα προγράμματα για να επιβεβαιώσετε εάν υπάρχει όντως κάποιο κρούσμα

ΔΙΑΦΟΡΕΣ ΜΕΤΑΞΥ UNIX
ΚΑΙ WINDOWS

- Μια βασική διαφορά μεταξύ των Unix συστημάτων και των Windows είναι ότι σε κάποιες παραλλαγές των Unix δεν μπορείς να ανακτήσεις διαγραμμένα αρχεία
- Όταν εκτελείται μια διαδικασία σε περιβάλλον Windows δεν μπορείτε να διαγράψετε αρχεία που αντιστοιχούν και εκτελούνται στον σκληρό δίσκο
- Ωστόσο , το λειτουργικό σύστημα Unix σας επιτρέπει να διαγράψετε ένα πρόγραμμα που έχει εκτελεστεί, η διαδικασία βρίσκεται σε λειτουργία αλλά το πρόγραμμα έχει διαγραφεί από τον σκληρό δίσκο.

ΔΗΜΙΟΥΡΓΙΑ ΕΡΓΑΛΕΙΟΘΗΚΗΣ
ΑΝΤΑΠΟΚΤΡΙΣΗΣ

- Το να δημιουργήσεις μια σωστή εργαλειοθήκη ανταπόκρισης είναι δύσκολο καθώς κάθε παραλλαγή των Unix συστημάτων απαιτεί διαφορετικά πράγματα.
- Όταν αναφερόμαστε σε Unix συστήματα το μυαλό μας πάει στις παραλλαγές με τις οποίες είμαστε πιο εξοικειωμένοι όπως είναι οι Sun Solaris, Hewlett-Packard's HP-UX, FreeBSD, και φυσικά τα Linux
- Εάν για παράδειγμα η μηχανή του θύματος είναι ένας διακομιστής Sparc με λειτουργικό σύστημα Solaris 2.8 , θα πρέπει να συγκεντρωθούν τα εργαλεία σας σε ένα καθαρό αντίγραφο του Solaris 2.8 σε ένα σύστημα με την ίδια αρχιτεκτονική.

ΕΝΤΟΛΕΣ UNIX ΚΑΙ ΑΣΦΑΛΕΙΑ
ΑΡΧΕΙΟΘΕΤΗΣΗ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΤΑ ΤΗΝ ΑΝΤΑΠΟΚΡΙΣΗ

- Αποθηκεύστε τα δεδομένα στον τοπικό σκληρό δίσκο
- Αποθηκεύστε τα δεδομένα σε απομακρυσμένα μέσα όπως δισκέτες , USB drives και CD
- Καταγράψτε τις πληροφορίες με το χέρι
- Χρησιμοποιήστε το netcat (ή cryptcat) για να μεταφέρετε τα δεδομένα που ανακτήθηκαν με την ιατροδικαστική έρευνα μέσω του δικτύου.

ΣΥΛΛΟΓΗ ΔΕΔΟΜΕΝΩΝ

- Ημερομηνία και ώρα συστήματος
- Μια λίστα με τους χρήστες που είναι συνδεδεμένοι εκείνη τη στιγμή

- Ημερομηνία και ώρα για όλα τα αρχεία του συστήματος
- Μια λίστα των διεργασιών που εκτελούνται
- Μια λίστα των ανοικτών υποδοχών
- Μια λίστα με τα συστήματα που έχουν τρέχουσα ή πρόσφατη σύνδεση με το σύστημα

ΣΥΛΛΟΓΗ ΔΕΔΟΜΕΝΩΝ ΠΟΥ ΕΚΤΕΛΟΥΝΤΑΙ

- Χρησιμοποιείστε ένα αξιόπιστο κέλυφος
- Καταγράψτε την ώρα και την ημερομηνία συστήματος
- Καθορίστε ποιος είναι συνδεδεμένος στο σύστημα
- Καθορίστε ανοιχτές θύρες
- Λίστα εφαρμογών που σχετίζονται με ανοιχτές θύρες
- Προσδιορίστε τις διεργασίες που τρέχουν
- Κατάλογος των πρόσφατων συνδέσεων
- Καταγράψτε τα μέτρα που έχουν ληφθεί
- Εγγραφή των κρυπτογραφικών αθροισμάτων ελέγχου

ΕΚΤΕΛΕΣΗ ΕΝΟΣ ΑΞΙΟΠΙΣΤΟΥ ΚΕΛΥΦΟΥΣ

Όταν ανταποκριθείτε σε ένα συμβάν που τρέχει σε σύστημα Unix θα συναντήσετε ένα από τα δύο σενάρια :

- Το σύστημα τρέχει σε λειτουργία κονσόλας .
- Το σύστημα τρέχει σε ένα γραφικό περιβάλλον παρόμοιο με την επιφάνεια εργασίας των Windows

ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΣΥΝΔΕΔΕΜΕΝΩΝ ΧΡΗΣΤΩΝ

- Το να προσδιορίσετε ποιος είναι συνδεδεμένος στο σύστημα είναι απλό. Εκτελέστε απλά την εντολή w (what).
- Η w command εμφανίζει τα ID των συνδεδεμένων χρηστών καθώς και το τι εκτελούν στο σύστημα
- Παρέχει , επίσης, την ημερομηνία και την ώρα του συστήματος

ΠΑΡΑΔΕΙΓΜΑ ΧΡΗΣΗΣ W COMMAND

[root@conan /root]# w
11:39pm up 3:11, 3 users, load average: 1.27, 1.43, 1.84
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
nada ttyp0 jitter.rahul.net 8:30pm 3:02m 1:08 0.14s
telnet bothosti
bovine ttyp1 shell1.bothostin 8:35pm 3:02m 1:01 0.12s -bash
mandiak ttyp2 adsl-225-75.poto 11:38pm 0.00s 0.25s 0.11s w
[root@conan /root]#

ΑΝΑΛΥΣΗ ΠΕΔΙΩΝ W COMMAND

- Πεδίο USER: εμφανίζει τους συνδεδεμένους χρήστες
- Πεδίο TTY: δείχνει το τερματικό ελέγχου
- Πεδίο FROM: δείχνει το domain name και την IP

- Πεδίο LOGIN@: δείχνει την τοπική ώρα έναρξης της σύνδεσης
- Πεδίο IDLE: δείχνει το χρονικό διάστημα από την τελευταία διαδικασία που είχε τρέξει
- Πεδίο JCPU: δείχνει τον χρόνο των διαδικασιών που συνδέονται με την συγκεκριμένη κονσόλα
- Πεδίο PCPU:δείχνει τον χρόνο που απασχολείται ο επεξεργαστής
- Πεδίο WHAT: δείχνει τις διαδικασίες που ο χρήστης ήδη εκτελεί

ΣΦΡΑΓΙΔΕΣ ΧΡΟΝΟΛΟΓΗΣΗΣ

Όπως και στα Windows έτσι και στα Unix συστήματα έχουμε 3 σφραγίδες χρονολόγησης για συλλογή στοιχείων από τα αρχεία

- Access time(atime)
- Modification time(mtime)
- Inode change time(ctime)
- Για την απόκτηση αυτών των σφαγίδων χρονολόγησης μπορείτε να χρησιμοποιήσετε την εντολή ls.

ls -alRu / > /floppy/atime
ls -alRc / > /floppy/ctime
ls -alR / > /floppy/mtime

ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΑΝΟΙΧΤΩΝ ΘΥΡΩΝ

[root@conan /root]# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 176 66.192.0.66:22 66.192.0.26:20819
ESTABLISHED
Tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN
Tcp 0 0 0.0.0.0:21 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN
Udp 0 0 0.0.0.0:69 0.0.0.0:*
Η εντολή netstat κυριαρχεί όταν πρόκειται να απαριθμήσουμε τις ανοιχτές θύρες

ΕΦΑΡΜΟΓΕΣ ΠΟΥ ΣΥΝΔΕΟΝΤΑΙ ΜΕ ΑΝΟΙΧΤΕΣ ΘΥΡΕΣ

[root@conan /root]# netstat -anp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
PID/Program name
1) tcp 0 0 0.0.0.0:143 0.0.0.0:* LISTEN 385/inetd
2) tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 395/sshd
3) tcp 0 0 0.0.0.0:512 0.0.0.0:* LISTEN 385/inetd
4) tcp 0 0 0.0.0.0:513 0.0.0.0:* LISTEN 385/inetd
5) tcp 0 0 0.0.0.0:514 0.0.0.0:* LISTEN 385/inetd
6) tcp 0 0 0.0.0.0:23 0.0.0.0:* LISTEN 385/inetd
7) tcp 0 0 0.0.0.0:21 0.0.0.0:* LISTEN 385/inetd
8) udp 0 0 0.0.0.0:69 0.0.0.0:* 385/inetd
9) raw 0 0 0.0.0.0:1 0.0.0.0:* 7
-
10)raw 0 0 0.0.0.0:6 0.0.0.0:* 7
Στα συστήματα Unix χρησιμοποιούμε την εντολή netastat-anp για την χαρτογράφηση της αντιστοίχισης των εφαρμογών που εκτελούνται στις ανοιχτές θύρες

ΕΥΡΕΣΗ ΣΤΟΙΧΕΙΩΝ ΜΕ ΧΡΗΣΗ ΤΗΣ ΕΝΤΟΛΗΣ LSOF 1/2

1) lpq 647 root cwd VDIR 118,0 7680 27008
/usr/lib
2) lpq 647 root txt VREG 118,0 99792 27120
/usr (/dev/dsk/c0t2d0s0)
3) lpq 647 root txt VREG 118,0 16932 41023
/usr/platform/sun4u/lib/libc_psr.so.1
4) lpq 647 root txt VREG 118,0 1015636 28179
/usr/lib/libc.so.1
5) lpq 647 root txt VREG 118,0 19304 27118
/usr/lib/libmp.so.2
6) lpq 647 root txt VREG 118,0 53656 27130
/usr/lib/libsocket.so.1

ΕΥΡΕΣΗ ΣΤΟΙΧΕΙΩΝ ΜΕ ΧΡΗΣΗ ΤΗΣ ΕΝΤΟΛΗΣ LSOF 2/2

7) lpq 647 root txt VREG 118,0 726968 27189
/usr/lib/libnsl.so.1
8) lpq 647 root txt VREG 118,0 4308 28208
/usr/lib/libdl.so.1
9) lpq 647 root txt VREG 118,0 181820 27223
/usr/lib/ld.so.1
10) lpq 647 root 0u inet 0x64221050 0t2144
ICMP
11) lpq 647 root 3u inet 0x6438aa80 0x1477689c
ICMP
12) lpq 647 root 4r DOOR 0x641881a0
(FA:->0x641b5878)

ΚΑΘΟΡΙΣΜΟΣ ΤΩΝ ΔΙΕΡΓΑΣΙΩΝ ΠΟΥ ΕΚΤΕΛΟΥΝΤΑΙ

- Είναι ζωτικής σημασίας να πάρετε ένα στιγμιότυπο από όλες τις διεργασίες που τρέχουν κατά την αρχική ανταπόκριση . Αυτό μπορεί να επιτευχθεί χρησιμοποιώντας την εντολή ps (process status).
- Η έξοδος της εντολής διαφέρει λίγο ανάλογα με το είδος του Unix συστήματός μας.
- Χρησιμοποιούμε την εντολή ps-eaf για τα συστήματα Solaris και ps-aux για τα Linux και FreeBSD συστήματα

ΧΡΗΣΗ ΤΗΣ ΕΝΤΟΛΗΣ PS-AUX 1/2

[root@conan]# ps –aux

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	1	0.1	0.7	1060	480	?	S	17:52	0:03	init [3]
root	2	0.0	0.0	0	0	?	SW	17:52	0:00	[kflushd]
root	3	0.0	0.0	0	0	?	SW	17:52	0:00	[kupdate]
root	4	0.0	0.0	0	0	?	SW	17:52	0:00	[kpiod]
root	5	0.0	0.0	0	0	?	SW	17:52	0:00	[kswapd]

root 6 0.0 0.0 0 0 ? SW< 17:52 0:00 [mdrecoveryd]
root 259 0.0 0.2 348 136 ? S 17:52 0:00 /sbin/dhcpcd eth0
root 316 0.0 0.8 1112 556 ? S 17:52 0:00 syslogd -m 0
root 326 0.0 1.1 1360 756 ? S 17:52 0:00 klogd
daemon 341 0.0 0.7 1084 492 ? S 17:52 0:00 /usr/sbin/atd
root 356 0.0 0.9 1272 608 ? S 17:53 0:00 crond

ΧΡΗΣΗ ΤΗΣ ΕΝΤΟΛΗΣ PS-AUX 2/2

root 385 0.0 0.7 1080 488 ? S 17:53 0:00 inetd
root 395 0.0 1.5 2032 980 ? S 17:53 0:00 /usr/sbin/sshd
xfs 422 0.0 5.0 4292 3172 ? S 17:53 0:00 xfs -port -1 –dae
root 438 0.0 1.7 2188 1072 tty1 S 17:53 0:00 login root
root 439 0.0 0.6 1028 404 tty2 S 17:53 0:00 /sbin/mingetty tt
root 440 0.0 0.6 1028 404 tty3 S 17:53 0:00 /sbin/mingetty tt
root 441 0.0 0.6 1028 404 tty4 S 17:53 0:00 /sbin/mingetty tt
root 442 0.0 0.6 1028 404 tty5 S 17:53 0:00 /sbin/mingetty tt
root 443 0.0 0.6 1028 404 tty6 S 17:53 0:00 /sbin/mingetty tt
root 446 0.0 2.1 2108 1328 tty1 S 17:55 0:00 bash
root 499 0.0 0.7 1112 480 tty1 S 18:41 0:00 script
root 500 0.5 0.8 1116 508 tty1 S 18:41 0:00 script
root 501 1.7 2.0 2084 1292 pts/0 S 18:41 0:00 bash I
root 513 0.0 1.5 2636 984 pts/0 R 18:42 0:00 ps aux

ΤΙ ΣΥΜΒΑΙΝΕΙ ΚΑΙ ΤΙ ΑΠΟΤΕΛΕΣΜΑΤΑ ΕΜΦΑΝΙΖΟΝΤΑΙ 1/2

- Εκτελείτε μια εντολή -ps και παρατηρείτε κάποια πολύ παράξενη διαδικασία στο σύστημά σας. Είστε σίγουροι ότι δεν έχετε ξεκινήσει τη διαδικασία εσείς, και αναρωτιέστε ποιος το έκανε.
- Ένα σύντομο παράδειγμα εμφάνισης συναγερμού είναι το εξής:

[root@conan /root]# ps –aux
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 461 0.0 1.2 1164 780 p0 S 10:21 0:00 bash
root 5911 0.0 0.7 808 468 ? S 13:58 0:00 /sbin/cardmgr
root 6011 0.0 0.6 776 444 ? S 14:04 0:00 inetd

ΤΙ ΣΥΜΒΑΙΝΕΙ ΚΑΙ ΤΙ ΑΠΟΤΕΛΕΣΜΑΤΑ ΕΜΦΑΝΙΖΟΝΤΑΙ 1/2

root 6244 0.0 0.9 1120 624 ? S 14:46 0:00
9\37777777761\37777777777\37777777677
root 6277 99.9 0.8 1164 564 ? S 14:50 0:03 xterm
root 6278 0.0 0.7 816 484 ? R 14:50 0:00 ps -aux

- Τι ακριβώς είναι η διαδικασία 6244;Φαίνεται να είναι μια διαδικασία με το όνομα: 9\37777777761\37777777777\37777777677
- Τι είδους επίθεση θα μπορούσε να δημιουργήσει μια τέτοια παράξενη εγγραφή στην λίστα;

ΚΑΤΑΓΡΑΦΗ ΒΗΜΑΤΩΝ ΕΚΤΕΛΕΣΗΣ ΕΝΤΟΛΩΝ

- Καταγράψτε όλες τις εντολές που έχουν εκδοθεί στο σύστημα

- Χρησιμοποιείστε τις εντολές script,history ή vi για καταγραφή, αν εκτελείται ζωντανά η απάντησή σας από τον επεξεργαστή
- Η χρήση της εντολής history θα εμφανίσει όλες τις εντολές που έχετε εκτελέσει
- Η καλύτερη επιλογή είναι η χρήση της εντολής script που καταγράφει όλα όσα έχουν πληκτρολογηθεί και τα αποτελέσματα τους
- **π.χ**[root@conan/root]#script/mnt/floppy/command_log.txt
- Script started, file is command_log.txt

ΑΠΟΚΤΗΣΗ ΑΡΧΕΙΟΥ ΚΑΤΑΓΡΑΦΗΣ ΚΑΤΑ ΤΗΝ ΑΝΤΑΠΟΚΡΙΣΗ

- Στο αρχείο utmp έχεις πρόσβαση με το w
- Στο αρχείο wtmp έχεις πρόσβαση με το last
- Στο αρχείο lastlog έχεις πρόσβαση με το lastlog
- Στους ενεργούς λογαριασμούς χρηστών έχεις πρόσβαση με το lastcomm

ΑΠΟΚΤΗΣΗ ΣΗΜΑΝΤΙΚΩΝ ΠΑΡΑΜΕΤΡΩΝ ΤΩΝ ΑΡΧΕΙΩΝ

- **/etc/psswd** για μη εξουσιοδοτημένους λογαριασμούς χρηστών
- **/etc/shadow** για την εξασφάλιση κάθε λογαριασμού απαιτείται έλεγχος ταυτότητας μέσω κωδικού
- **/etc/groups** για κλιμάκωση των προνομίων και το λόγο της πρόσβασης
- **/etc/hosts** για καταγραφή των DNS(DOMAIN NAME SYSTEM)
- **/etc/hosts.equiv** για έλεγχο της εμπιστοσύνης των σχέσεων
- **~/.rhosts** για να αναθεωρήσει όλες τις τυχόν σχέσεις εμπιστοσύνης με βάση το χρήστη
- **/etc/hosts.allow και /etc/hosts.deny** για έλεγχο των κανόνων του tcp
- **/etc/syslog.conf** για καθορισμό της τοποθεσίας των αρχείων
- **/etc/rc** για να εξετάσει τα αρχεία εκκίνησης
- **/etc/inetd.conf και /etc/xinetd.confequiv** για καταγραφή λίστας υπηρεσιών

ΕΞΕΤΑΣΗ ΑΡΧΕΙΩΝ PROC

- Το σύστημα /proc είναι ένα σύστημα ψευδοαρχείων που χρησιμοποιείται ως διεπαφή με τον πυρήνα δεδομένων(Kernel) σε ορισμένα είδη των συστημάτων Unix
- Κάθε διεργασία έχει έναν κατάλογο στο /proc που αντιστοιχεί στο κάθε PID.
- Κάθε διεργασία που εκτελείται θα έχει αριθμητική υποδομή στον κατάλογο
- Μέσα σε αυτόν τον κατάλογο είναι ζωτικής σημασίας πληροφορίες της διαδικασίας που κάθε ερευνητής θα ήθελε να επεξεργαστεί
- Τα ακόλουθα επεξηγούν τα περιεχόμενα καταλόγου για μια διεργασία που ονομάζεται / root / ir / lo και εκτελείται σε ένα σύστημα Linux :

ΠΑΡΑΔΕΙΓΜΑ /PROC ΑΡΧΕΙΩΝ 1/2

- Έχουμε εκτελέσει την διαδικασία που ονομάζεται / root / ir / lo . Στη συνέχεια θα εκτελέσουμε μια εντολή ps για να αποκτήσουμε το PID για το / root / ir / lo :

[root@conan]# ps -aux | grep /root/ir/lo
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
Root 970 0.0 0.4 872 312 ? S 20:12 0:00 /root/ir/lo
Root 972 0.0 1.6 2668 1016 pts/4 R 20:12 0:00 grep

Το /root/ir/lo έχει PID 970 αλλάζουμε λοιπόν τους καταλόγους στο /proc/970 για να αναθεωρήσουμε τα περιεχόμενα

ΠΑΡΑΔΕΙΓΜΑ /PROC ΑΡΧΕΙΩΝ 2/2

```
[root@conan]# cd /proc/970
[root@conan 970]# ls –al
total 0
dr-xr-xr-x    3 root   root  0 Apr   5 20:12 .
dr-xr-xr-x    61root   root  0 Apr   5 13:52 ..
-r--r--r--    1 root   root  0 Apr   5 20:12 cmdline
lrwx------    1 root   root  0 Apr   5 20:12 cwd -> /tmp
-r--------    1 root   root  0 Apr   5 20:12 environ
lrwx------    1 root   root  0 Apr   5 20:12 exe -> /root/ir/lo
dr-x------    2 root   root  0 Apr   5 20:12 fd
pr--r--r--    1 root   root  0 Apr   5 20:12 maps
-rw-------    1 root   root  0 Apr   5 20:12 mem
lrwx------    1 root   root  0 Apr   5 20:12 root -> /
-r--r--r--    1 root   root  0 Apr   5 20:12 stat
-r--r--r--    1 root   root  0 Apr   5 20:12 statm
-r--r--r--    1 root   root  0 Apr   5 20:12 status
```

Exe Link ΣΤΑ ΑΡΧΕΙΑ Proc ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ 1/2

Ο σύνδεσμος exe επιτρέπει στους ερευνητές να ανακτήσουν τα διαγραμμένα αρχεία για όσο διάστημα βρίσκονται σε εξέλιξη.Για παράδειγμα , ας υποθέσουμε ότι έχετε τις ακόλουθες εντολές :

```
[root@conan 970]# rm /root/ir/lo
rm: remove `/root/ir/lo'? Y
```

Το /root/ir/lo πρόγραμμα αποσυνδέεται από το σύστημα αρχείων. Η εντολή ls στο /root / ir κατάλογο δεν θα δείξει το πρόγραμμα lo στο σύστημα αρχείων.Ωστόσο,όταν εξετάστε τα περιεχόμενα του / proc / 970 καταλόγου,μπορείτε να δείτε την εξής έξοδο:

Exe Link ΣΤΑ ΑΡΧΕΙΑ Proc ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ 2/2

Ωστόσο,όταν εξετάστε τα περιεχόμενα του / proc / 970 καταλόγου,μπορείτε να δείτε την εξής έξοδο:

```
[root@conan 970]# ls -al
1) total 0
2) dr-xr-xr-x   3 root   root  0 Apr    5 20:12 .
3) dr-xr-xr-x   60root   root  0 Apr    5 13:52 ..
4) -r--r--r--   1 root   root  0 Apr    5 20:13 cmdline
5) lrwx------   1 root   root  0 Apr    5 20:13 cwd -> /tmp
6) -r--------   1 root   root  0 Apr    5 20:13 environ
7) lrwx------   1 root   root  0 Apr    5 20:13 exe -> /root/ir/lo(deleted)
8) dr-x------   2 root   root  0 Apr    5 20:13 fd
9) pr--r--r--   1 root   root  0 Apr    5 20:13 maps
10) -rw-------  1 root   root  0 Apr    5 20:13 mem
11) lrwx------  1 root   root  0 Apr    5 20:13 root -> /
12) -r--r--r--  1 root   root  0 Apr    5 20:13 stat
13) -r--r--r--  1 root   root  0 Apr    5 20:13 statm
14) -r--r--r--  1 root   root  0 Apr    5 20:13 status
```

Ο FD ΣΤΑ Proc/File ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ 1/2

- Με την εξέταση του fd(file descriptor) μπορούμε να εντοπίσουμε όλους τους φακέλους που έχουν ανοίξει λόγω μιας διαδικασίας.
- Όταν ο Kernel του Unix ανοίγει , διαβάζει , γράφει , ή δημιουργεί ένα αρχείο ή ένα socket του δικτύου, επιστρέφει ένα αρχείο περιγραφής(ένας θετικός ακέραιος αριθμός) που χρησιμοποιείτε ως αναφορά του αρχείου.
- Συνήθως, μπορείτε να αγνοήσετε τους αριθμούς περιγραφής αρχείων 0 , 1 , και 2 , οι οποίοι είναι προκαθορισμένοι για την κανονική είσοδο , κανονική έξοδο , και το τυπικό σφάλμα , αντίστοιχα .
- Στις γραμμές 6 και 7 του παρακάτω παραδείγματος , μπορείτε να δείτε ότι το πρόγραμμα lo χρησιμοποιεί τους αριθμούς περιγραφής 3 και 4 για την αναφορά στα socket του δικτύου

Ο FD ΣΤΑ Proc/File ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ 2/2

```
[root@conan 970]# cd fd
[root@conan fd]# ls –al
1) total 0
2) dr-x ------ 2 root  root    0 Apr  5  20:12 .
3) dr-xr-xr-x  3 root  root    0 Apr  5  20:12 ..
4) lrwx------  1 root  root    64 Apr 5  20:12 1 -> /dev/pts/4
5) lrwx------  1 root  root    64 Apr 5  20:12 2 -> /dev/pts/4
6) lrwx------  1 root  root    64 Apr 5  20:12 3 -> socket:[1358]
7) lrwx------  1 root  root    64 Apr 5  20:12 4 -> socket:[1359]
```

ΤΟ ΑΡΧΕΙΟ Cmdline ΣΤΑ ΑΡΧΕΙΑ PROC

- Το αρχείο cmdline εμφανίζει τις ακριβείς εντολές που χρησιμοποιήθηκαν για να τρέξει μια εφαρμογή. Κανονικά , αυτό εμφανίζεται όταν ένας χρήστης εκτελεί μια εντολή ps .
- Εδώ είναι ένα παράδειγμα των περιεχομένων του αρχείου Cmdline :

```
[root@conan 970]# cat cmdline
/root/ir/lo
```

ΕΝΤΟΠΙΣΜΟΣ ΣΤΟΙΧΕΙΩΝ

- Ας υποθέσουμε πως βλέπουμε την ακόλουθη διαδικασία :

```
[root@conan /proc]# /root/ir/s & [1] 827
```

- Ένας εισβολέας έτρεξε ένα πρόγραμμα που ονομάζεται s στο παρασκήνιο (εξ ου και το σύμβολο &) . Ο επιτιθέμενος έλαβε το PID με τον αριθμό 827.
- Είναι ένας αδίστακτος διακομιστής που άνοιξε κάποιο socket στο δίκτυο, είναι κάποιο πρόγραμμα ή απλά κάποιος ανιχνευτής του συστήματος εντόπισε δεδομένα στο δίκτυό σας.
- Μπορείτε αμέσως να εξετάσετε το /proc/827 για να ελέγξετε ποια αρχεία ανοίχτηκαν

ΑΛΛΑΓΗ ΓΡΑΜΜΗΣ ΕΝΤΟΛΩΝ ΚΑΤΑ ΤΗΝ ΕΚΤΕΛΕΣΗ 1/2

- Πολλές φορές οι επιτιθέμενοι με χρήση της γλώσσας προγραμματισμού C μπορούν και παραποιούν τις γραμμές εντολών κατά την εκτέλεση ενός προγράμματος αποκρύπτοντας την επίθεσή τους.
- Κάθε πρόγραμμα C έχει μια λειτουργία που ονομάζεται main ως σημείο εκκίνησης. Η main μπορεί να δεχτεί δύο παραμέτρους : argv και argc
- Ας υποθέσουμε πως έχουμε το εξής παράδειγμα εντολής: tcpdump -x -v –n
- Επομένως τα argv και argc είναι τα εξής:

argv[0] = tcpdump
argv[1] = -x
argv[2] = -v
argv[3] = -n
argc = 4

ΑΛΛΑΓΗ ΓΡΑΜΜΗΣ ΕΝΤΟΛΩΝ ΚΑΤΑ ΤΗΝ ΕΚΤΕΛΕΣΗ 2/2

- Ο επιτιθέμενος μπορεί να αλλάξει τις τιμές των παραμέτρων στην main παραποιώντας το argv πεδίο
- Για παράδειγμα με την χρήση της γλώσσας C μπορεί να αλλάξει το όνομα του προγράμματος:

strcpy(argv[0], “xterm”);

Τώρα το argv[0] ονομάζεται “xterm” και όχι “tcpdump”
Αυτή είναι μια απλή τεχνική που χρησιμοποιούν οι επιτιθέμενοι για να αποκρύψουν τις ενέργειές τους.

ΕΡΩΤΗΣΕΙΣ ΓΙΑ ΔΙΑΒΑΣΜΕΝΟΥΣ

- Ποιο βήμα επαναλαμβάνεται δύο φορές στη ζωντανή διαδικασία συλλογής των δεδομένων ; Γιατί είναι σημαντικό;
- Γιατί είναι σημαντικό να καταγράψετε την ώρα / ημερομηνία κατά την αρχική ανταπόκριση;
- Γιατί να εκτελέσουμε μια ζωντανή ανταπόκριση σε ένα σύστημα Unix και όχι απλά να κλείσουμε το σύστημα και να εκτελέσουμε μια αντιγραφή δεδομένων από το δίσκο;
- Τι είναι το netstat και τι το lsof ; Γιατί αυτά τα εργαλεία είναι τόσο σημαντικά κατά την αρχική απάντηση ;

ΚΕΦΑΛΑΙΟ 4

ΑΝΤΙΓΡΑΦΑ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΗΣ ΕΡΕΥΝΑΣ

Στα προηγούμενα κεφάλαια, εξηγήσαμε πώς μπορούμε να αποκτήσουμε δεδομένα από συστήματα Windows και Unix. Σε πολλές περιπτώσεις, η διαδικασία συλλογής δεδομένων είναι ένα προοίμιο της εκτέλεσης μιας εγκληματολογικής έρευνας, η οποία αποτελεί το αντικείμενο αυτού του κεφαλαίου. Η απόφαση για το πότε πρέπει να εκτελεστεί μια έρευνα θα πρέπει να βασίζεται στη στρατηγική απόκρισης που έχει ήδη αναφερθεί.
Πριν να εξηγήσουμε τις πραγματικές διαδικασίες για μια εγκληματολογική έρευνα, θα εξετάσουμε τον τρόπο με τον οποίο μπορούν να χρησιμοποιηθούν τα δεδομένα της έρευνας ως νομικά αποδεικτικά στοιχεία. Στη συνέχεια, θα εξετάσουμε ορισμένα γενικά αποδεκτά εργαλεία και τεχνικές που χρησιμοποιούνται για την απόκτηση μιας έγκυρης διπλής εικόνας.

ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΑ ΑΝΤΙΓΡΑΦΑ ΩΣ ΑΠΟΔΕΚΤΑ ΣΤΟΙΧΕΙΑ

Ένα εργαλείο ή μια διαδικασία πρέπει να παρέχει κάποιες αποδείξεις που θα χρησιμοποιηθούν στην δίκη όμως υπάρχουν κάποια κριτήρια που πρέπει να πληρούνται ώστε να θεωρηθεί μια πληροφορία ως στοιχείο. Εδώ λαμβάνουν χώρο τα εγκληματολογικά αντίγραφα τα οποία εφαρμόζονται σε κάθε πληροφορία που έχουμε για την υπόθεση. Βάση νόμου ένα αντικείμενο ή μια πληροφορία που θα κατατεθεί στο δικαστήριο πρέπει να είναι αυθεντική. Πολλές φορές όμως τα αυθεντικά πειστήρια δεν μπορούν να παρευρίσκονται γι αυτό υπάρχουν κ εξαιρέσεις οι οποίες είναι:

- ορισμοί και αντίγραφα:Αν τα δεδομένα αποθηκεύτηκαν από υπολογιστή ή παρόμοια συσκευή , οποιαδήποτε εκτύπωση η οποία διαβάζεται δια γυμνού οφθαλμού και φαίνεται να αντικατοπτρίζει τα δεδομένα θεωρείται αυθεντική.
- Αποδοχή του αντιγράφου:΄Ένα αντίγραφο είναι αποδεκτό στον ίδιο βαθμό σαν αυθεντικό εκτός αν 1)μια γνήσια ερώτηση εναντιώνεται ως προς την αυθεντικότητα του αρχικού 2)Στις περιπτώσεις που έχουμε και το αυθεντικό θα ήταν άδικο να μην το προτιμήσουμε σε σχέση με το αντίγραφο.

ΤΙ ΕΙΝΑΙ ΤΑ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΑ ΑΝΤΙΓΡΑΦΑ

Ένα εγκληματολογικό αντίγραφο είναι ένα αρχείο που περιέχει οποιαδήποτε πληροφορία από την πηγή με ένα ακατέργαστο σχήμα. Στο αρχείο δεν αποθηκεύονται παραπάνω δεδομένα πέρα από τα αρχικά με εξαίρεση τα λάθη που προκύψουν στην διαδικασία ανάγνωσης από το αρχικό. Σε αυτή την περίπτωση ένα υποκατάστατο συλλέγει όλα τα "βλαβερά" δεδομένα που υπάρχουν. Ένα εγκληματολογικό αντίγραφο μπορεί να συμπιεστεί μετά την διαδικασία αντιγραφής.

ΠΟΙΑ ΑΝΤΙΓΡΑΦΑ ΘΕΩΡΟΥΝΤΑΙ ΕΞΕΙΔΙΚΕΥΜΕΝΑ

Ένα εξειδικευμένο εγκληματολογικό αντίγραφο είναι ένα αρχείο που περιέχει οποιαδήποτε πληροφορία από την πηγή το οποίο έχει αποθηκευτεί με διαφορετική μορφή. Δυο παραδείγματα διαφορετικής μορφής είναι το in-band hashes και το empty sector compression. Κάποια εργαλεία διαβάζουν έναν αριθμό πεδίων από την πηγή, δημιουργούν έναν κατακερματισμό από μια ομάδα πεδίων και γράφουν την ομάδα του πεδίου ακολουθούμενη από την κατακερματισμένη τιμή στο αρχείο εξόδου. Η μέθοδος αυτή είναι πολύ αποδοτική αν κάτι πάει στραβά κατά την διάρκεια της αναπαραγωγής ή της αποκατάστασης του αντιγράφου. Το empty sector compression είναι μια συνηθισμένη μέθοδος ελαχιστοποίησης του αρχείου εξόδου. Αν ένα αρχείο συναντήσει 500 τομείς όλους με μηδενικά θα δημιουργήσει μια ειδική είσοδο μέσα στο αρχείο εξόδου όπου το πρόγραμμα αποκατάστασης θα αναγνωρίσει.

ΤΙ ΕΙΝΑΙ Η ΑΠΟΚΑΤΕΣΤΗΜΕΝΗ ΕΙΚΟΝΑ ΕΙΚΟΝΑ

Μια αποκατεστημένη εικόνα είναι αυτό που παίρνεις αποκαθιστάς ένα εγκληματολογικό αντίγραφο ή ένα εξειδικευμένο εγκληματολογικό αντίγραφο σε ένα άλλο μέσο απομνημόνευσης. Η διαδικασία αποκατάστασης είναι πιο περίπλοκη απ ότι ακούγεται. Για παράδειγμα μια μια μέθοδος περιέχει ένα τυφλό αντίγραφο στον σκληρό δίσκο του προορισμού. Αν ο σκληρός δίσκος του προορισμού μας είναι ίδιος με τον αυθεντικό όλα θα δουλεύουν καλά και η πληροφορία στον πίνακα χωρισμάτων θα αντιστοιχίζει την γεωμετρία του σκληρού δίσκου. Τι γίνεται όμως αν ο σκληρός δίσκος προορισμού δεν είναι ίδιος με τον αρχικό; Αν αποκαταστήσεις ένα εγκληματολογικό αντίγραφο ενός δίσκου 2.1 GB σε έναν 20 GB οι γεωμετρίες δεν θα ταιριάζουν. Στην πραγματικότητα όλα τα δεδομένα από τον αρχικό δίσκο θα απασχολούν μόνο τους 3 κυλίνδρους από τα 20 GB του δίσκου προορισμού με αποτέλεσμα το λογισμικό να το κατατάξει σε λάθος τοποθεσία και να δώσει ανακριβή αποτελέσματα. Πως το σύστημα αποκατάστασης το αντισταθμίζει αυτό; Καθώς το εγκληματολογικό αντίγραφο αποκαθίσταται στον σκληρό δίσκο προορισμού οι πίνακες χωρισμάτων αναβαθμίζονται με νέες τιμές.

ΤΙ ΕΙΝΑΙ ΜΙΑ ΚΑΤΟΠΤΡΙΚΗ ΕΙΚΟΝΑ-ΕΙΔΩΛΟ (Mirror Image)

Ένα είδωλο δημιουργείται από το hardware που κάνει αντιγραφή bit προς bit από τον ένα σκληρό δίσκο στον άλλο. Οι ερευνητές μπορεί να μην δημιουργούν συχνά είδωλα γιατί δημιουργείται ακόμη ένα στάδιο στην εγκληματολογική ανάλυση απαιτώντας από τον εξεταστή να δημιουργήσει ένα αντίγραφο με έναν εγκληματολογικό αλλά κ υγιή τρόπο. Αν έχουμε την δυνατότητα να κρατήσουμε τον αρχικό δίσκο μπορούμε άνετα να δημιουργήσουμε αντίγραφα. Αν ο αρχικός δίσκος πρέπει να επιστραφεί, ο αναλυτής θα εξακολουθεί να χρειάζεται την δημιουργία ενός αντιγράφου από ένα είδωλο για ανάλυση. Το μικρό ποσοστό χρόνου που γλιτώνουμε επιτόπου επικαλύπτεται από τα γενικά έξοδα παραγωγής ενός δεύτερου αντιγράφου. Αυτό που πρέπει να επιβεβαιωθεί είναι ότι ο πολύγραφος του hardware πραγματικά δημιουργεί ένα είδωλο. Πολλές μηχανές αντιγράφων στην αγορά έχουν δημιουργηθεί για την ολοκλήρωση συστημάτων εταιριών που θα τις χρησιμοποιούν για να εγκαταστήσουν λειτουργικά συστήματα σε μεγάλο αριθμό σκληρών δίσκων.

ΕΡΓΑΛΕΙΑ ΔΗΜΙΟΥΡΓΙΑΣ ΑΝΤΙΓΡΑΦΩΝ

Το εργαλείο πρέπει να μπορεί να σχεδιάζει κάθε Bit απο τα δεδομένα στο μέσο απομνημόνευσης:

- Πρέπει να δημιουργεί ένα εγκληματολογικό αντίγραφο ή ένα είδωλο του αρχικού μέσου απομνημόνευσης.
- Πρέπει να διαχειρίζεται τα λάθη με σθεναρό και κομψό/διακριτικό τρόπο. Αν μια διαδικασία αποτύχει ύστερα από επανειλημμένες προσπάθειες, τότε το σφάλμα καταγράφεται και η διαδικασία απεικόνισης συνεχίζεται.
- Δεν πρέπει να κάνει καμία αλλαγή στο μέσο απομνημόνευσης.
- Πρέπει να έχει την ικανότητα να κρατιέται στην κορυφή των επιστημονικών αξιολογήσεων. Τα αποτελέσματα πρέπει να είναι επαναλαμβανόμενα και πιστοποιημένα από κάποιον τρίτο αν είναι απαραίτητο.

ΝΟΜΙΚΑ ΘΕΜΑΤΑ 1/2

Τα εργαλεία που χρησιμοποιούμε για το εγκληματολογικό αντίγραφο πρέπει να περάσουν τα νόμιμα τεστ για αξιοπιστία. Πολύ σημαντικό επίσης είναι πως μπορούμε πολύ πιο εύκολα να αποδείξουμε την αξιοπιστία κ την ακρίβεια των πληροφοριών μας όταν τα εργαλεία μας είναι αποδεκτά από το δικαστήριο. Και αυτό μας φέρνει στον τρόπο που εξετάζουν την αξιοπιστία των τεχνικών που χρησιμοποιούνται στα δικαστήρια.

Υπάρχουν 4 παράγοντες που χρησιμοποιούνται για να αποφασιστεί η αξιοπιστία των επιστημονικών τεχνικών:

- Αν η επιστημονική θεωρία έχει τεσταριστεί εμπειρικά
- Αν η επιστημονική θεωρία ή τεχνική υποβλήθηκε σε αξιολόγηση ή εκδόθηκε στο κοινό.
- Υπάρχει κάποιος γνωστός ή πιθανός δείκτης λαθών;
- Υπάρχει μια γενική αποδοχή της μεθοδολογίας ή τεχνικής από την σχετική επιστημονική κοινότητα;

ΝΟΜΙΚΑ ΘΕΜΑΤΑ 2/2

Σύμφωνα με κάποιες μεθόδους που έχουν δοκιμαστεί αν και έγκυρες, δεν ήταν τόσο αποδοτικές. Επομένως πρόσθεσαν κάποια καινούρια τεστ για να αντιμετωπίσουν αυτές τις ατέλειες:

- Η τεχνική αυτή δημιουργήθηκε για κάποιον άλλο σκοπό εκτός από την δίκη;
- Ο εμπειρογνώμονας εξηγεί αρκετά τα σημαντικά εμπειρικά στοιχεία;
- Είναι η τεχνική βασισμένη σε ικανοποιητικά/ποιοτικά στοιχεία;
- Υπάρχει ένα μέτρο συνέπειας στην διαδικασία της τεχνικής;
- Υπάρχει ένα μέτρο συνέπειας στην διαδικασία της τεχνικής όπως εφαρμόζεται στην παρούσα υπόθεση;
- Η τεχνική αντιπροσωπεύεται από όγκο βιβλιογραφίας;
- Ο εμπειρογνώμονας κατέχει τα επαρκή πιστοποιητικά στον τομέα;
- Πως η τεχνική αυτή διαφέρει από άλλες παρόμοιες προσεγγίσεις;

ΔΗΜΙΟΥΡΓΙΑ ΑΝΤΙΓΡΑΦΟΥ ΑΠΟ ΣΚΛΗΡΟ ΔΙΣΚΟ

Τα πιο συνηθισμένα εργαλεία που χρησιμοποιούνται για την απόκτηση ενός πραγματικού εγκληματολογικού διπλότυπου είναι κατασκευασμένα για να τρέχουν σε ένα λειτουργικό περιβάλλον Unix. Ένα εργαλείο, dd, είναι μέρος του λογισμικού GNU. Αυτό βελτιώθηκε από προγραμματιστές στο εργαστήριο DoD Computer Forensics Lab και επανεκδόθηκε ως dcfldd. Οι παράμετροι της γραμμής εντολών για dd και dcfldd είναι σχεδόν πανομοιότυπες και ο βασικός κώδικας μεταφοράς δεδομένων δεν έχει αλλάξει. Ένα άλλο εργαλείο που θα εξετάσουμε εδώ είναι το Open Data Duplicator από το Openforensics.org. Ένα από τα ισχυρά σημεία αυτού του εργαλείου Unix είναι ότι επιτρέπει σε έναν ερευνητή να εκτελεί πολλαπλές λειτουργίες καθώς δημιουργείται η εικόνα.

ΔΗΜΙΟΥΡΓΙΑ ΜΕΣΩΝ ΕΚΚΙΝΗΣΗΣ Linux

Από όλες τις μεθόδους που συζητάμε σε αυτή την ενότητα,η προετοιμασία δημιουργίας αντιγράφων με Linux είναι η πιο δύσκολη. Η προσπάθεια αξίζει τον κόπο, επειδή μπορεί να είναι το πιο ευέλικτο περιβάλλον εκκίνησης στην εργαλειοθήκη σας. Η εύκολη διαδρομή είναι να ξεκινήσετε με μια προ συμπιεσμένη έκδοση του Linux, όπως το Tomsrtbt, το Trinux ή το FIRE (Forensic and Incident Response Environment). Αφού βάλετε το βασικό πακέτο σε λειτουργία μπορείτε να προσθέσετε τα δικά σας δυαδικά αρχεία, όπως το dcfldd.

ΔΗΜΙΟΥΡΓΙΑ ΑΝΤΙΓΡΑΦΩΝ ΜΕ dd 1/2

Σε ορισμένες περιπτώσεις, τα εγκληματολογικά αντίγραφα αποθηκεύονται σε μια σειρά αρχείων που έχουν μέγεθος τέτοιο ώστε να ταιριάζουν σε συγκεκριμένο τύπο μέσου (όπως CD ή DVD) ή σε τύπο αρχείου (όπως αρχεία κάτω από 2.1GB). Αυτό είναι που καλούμε κατατμημένη εικόνα. Παρακάτω υπάρχει ένα

script shell bash που θα δημιουργήσει ένα αληθινό δικαστικό αντίγραφο ενός σκληρού δίσκου και αποθηκεύει την εικόνα σε έναν σκληρό δίσκο τοπικής αποθήκευσης.

```
#!/bin/bash
# Bash script for duplicating hard drives with dd
# Set source device name here
source=/dev/hdc
# Set output file name here
output_name=/mnt/RAID_1/dd_Image
# Set output file size here
output_size=2048k;
####
count=1
while (dd if=$source of=$output_name.$count bs=$output_size \
count=1 skip=$(($count-1)) conv=noerror,notrunc);
do printf "#"; count=$((count+1)); done
####
echo "Done. Verify the image with md5sum."
```

ΔΗΜΙΟΥΡΓΙΑ ΑΝΤΙΓΡΑΦΩΝ ΜΕ dd 2/2

Τα περισσότερα εμπορικά εγκληματολογικά πακέτα θα έχουν τη δυνατότητα επεξεργασίας μιας διαχωρισμένης εικόνας. Εάν επεξεργάζεστε σε Linux, μπορείτε να συγκολλήσετε τα τμήματα ή να ρυθμίσετε μια συσκευή RAID λογισμικού για να επεξεργαστείτε τα τμήματα σαν να ήταν μια μεγάλη συσκευή. Εάν δεν έχετε λόγο να χωρίσετε το αρχείο εξόδου, είναι πολύ πιο εύκολο να εκτελέσετε πολλαπλές λειτουργίες σε ένα πέρασμα. Το ακόλουθο σενάριο θα δημιουργήσει ένα πραγματικό αντίγραφο και θα υπολογίσει ένα άθροισμα MD5 ολόκληρης της μονάδας δίσκου σε ένα πέρασμα πάνω από τον σκληρό δίσκο προέλευσης.

```
#!/bin/bash
# Bash script for duplicating hard drives with dd
# Set source device name here
source=/dev/hdc
# Set output file name here
output_name=/mnt/RAID_1/dd_Image
####
dd if=$source bs=16384 conv=noerror,notrunc | tee $output_name | md5
####
echo "Done. Verify the image with md5sum."
```

ΧΡΗΣΗ ΤΟΥ ΠΡΟΓΡΑΜΜΑΤΟΣ ODD (Open Data Duplicator) ½

Ο ανοικτός αντιγραφέας δεδομένων (ODD) είναι ένα εργαλείο ανοικτού κώδικα. Αυτό το εργαλείο ακολουθεί ένα μοντέλο client / server που επιτρέπει στον ερευνητή να πραγματοποιεί εγκληματολογικές αντιγραφές σε διάφορα συστήματα υπολογιστών ταυτόχρονα μέσω τοπικού LAN. Φυσικά, και τα δύο μισά μπορούν να τρέξουν στο ίδιο σύστημα υπολογιστών, ώστε να μπορείτε να χρησιμοποιήσετε το λογισμικό σε έναν ενιαίο σταθμό εργασίας εγκληματολογίας. Ένα άλλο χαρακτηριστικό του ODD είναι η ικανότητά του να εκτελεί πρόσθετες λειτουργίες στα δεδομένα όση ώρα εκτελείται η επεξεργασία. Το ODD περιλαμβάνει ενότητες (plug-ins) που θα υπολογίζουν τα αθροίσματα ελέγχου και τα hashes, θα πραγματοποιούν αναζητήσεις συμβολοσειρών και θα εξάγουν αρχεία βάσει των headers των αρχείων.

ΧΡΗΣΗ ΤΟΥ ΠΡΟΓΡΑΜΜΑΤΟΣ ODD (Open Data Duplicator) 2/2

Το ODD είναι το τμήμα δημιουργίας αντιγράφων δεδομένων του πλαισίου Open Digital Evidence Search and Seizure Architecture (ODESSA). Ο στόχος του έργου ODESSA είναι να παρέχει μια ανοικτή και επεκτάσιμη σειρά εργαλείων επεξεργασίας αποδεικτικών στοιχείων και ανάλυσης δεδομένων στην εγκληματολογική κοινότητα των υπολογιστών. Το πακέτο ODD αποτελείται από 3 τμήματα:

- Bootable CD-ROMs
- Server-side application: Ο διακομιστής θα εκτελέσει το μεγαλύτερο μέρος της επεξεργασίας του αντιγράφου της εικόνας, συμπεριλαμβανομένου του υπολογισμού των hashes, των αναζητήσεων συμβολοσειρών και την αποθήκευση της πραγματικής εγκληματολογικής έρευνας
- Client-side application :Αυτό το τμήμα μπορεί να εκτελείται τοπικά αν αντιγράφετε δίσκους σε ιατροδικαστικό σταθμό εργασίας

ΔΗΜΙΟΥΡΓΙΑ ΕΞΕΙΔΙΚΕΥΜΕΝΩΝ ΑΝΤΙΓΡΑΦΩΝ ΑΠΟ ΣΚΛΗΡΟ ΔΙΣΚΟ

Ένα από τα πρώτα πράγματα που πρέπει να μάθει ένας εξεταστής της πρώτης φάσης είναι να μην κάνει boot ποτέ από τον ύποπτο σκληρό δίσκο. Πολλά στοιχεία στα μέσα αποδείξεων μπορούν να τροποποιηθούν, ξεκινώντας από τη στιγμή που το BIOS εκτελεί το boot block στο σκληρό δίσκο. Κατά την αρχική διαδικασία εκκίνησης, τα χρονικά σήματα πρόσβασης αρχείων, οι πληροφορίες για τα partition, το Registry , τα αρχεία ρυθμίσεων και τα βασικά αρχεία καταγραφής μπορούν να αλλάξουν σε λίγα δευτερόλεπτα.

ΔΗΜΙΟΥΡΓΙΑ ΕΞΕΙΔΙΚΕΥΜΕΝΩΝ ΑΝΤΙΓΡΑΦΩΝ ΜΕ SafeBack

Το SafeBack είναι μια μικρή εφαρμογή που έχει σχεδιαστεί για να τρέχει από μια δισκέτα εκκίνησης του DOS, επομένως θα χρειαστεί να έχετε έτοιμο περιβάλλον DOS σε μια δισκέτα εκκίνησης. Η δημιουργία διπλότυπου συστήματος υπολογιστή με SafeBack είναι αρκετά απλή και προσφέρει 4 λειτουργίες :

- Backup :δημιουργεί ένα αρχείο από τα αρχεία προέλευσης.
- Restore: αποκαθιστά τα αρχεία εγκληματολογικών εικόνων .
- Verify :επαληθεύει τις τιμές ελέγχου αθροίσματος εντός ενός αρχείου εικόνας.
- Copy: εκτελεί τις λειτουργίες δημιουργίας αντιγράφων ασφαλείας και επαναφοράς σε μία ενέργεια.

ΔΗΜΙΟΥΡΓΙΑ ΕΞΕΙΔΙΚΕΥΜΕΝΩΝ ΑΝΤΙΓΡΑΦΩΝ ΜΕ EnCase ½

Το EnCase από το Guidance Software είναι η πιο δημοφιλής εργαλειοθήκη που διατίθεται στο εμπόριο. Η δημοτικότητά του βασίζεται κυρίως στην εύκολη πλοήγηση στο περιβάλλον GUI. Περιλαμβάνεται μια ευέλικτη γλώσσα δέσμης ενεργειών, η οποία επιτρέπει στον εξεταστή να προσαρμόζει τους τύπους των πραγματοποιηθεισών αναζητήσεων. Ίσως το πιο πολύτιμο χαρακτηριστικό είναι η επιλογή προεπισκόπησης. Κατά τη διάρκεια των πρώτων σταδίων μιας έρευνας, μπορείτε να χρησιμοποιήσετε τη λειτουργία προεπισκόπησης για να εξακριβώσετε γρήγορα εάν ένα συγκρότημα ηλεκτρονικών υπολογιστών αποτελεί υλικό στο ζήτημα που ερευνάται. Για να χρησιμοποιήσετε την επιλογή προεπισκόπησης, εκκινήστε το ύποπτο σύστημα υπολογιστή με μια δισκέτα εκκίνησης EnCase. Αντί να αποκτήσετε μια εικόνα, συνδέεστε

στον ύποπτο υπολογιστή μέσω ενός παράλληλου καλωδίου ή μιας σύνδεσης δικτύου με ένα αντίγραφο του EnCase που τρέχει στον εγκληματολογικό σταθμό εργασίας σας. Μόλις δημιουργηθεί η σύνδεση, η διαδικασία ανάλυσης είναι ίδια με την περίπτωση που εργάζεστε σε ένα αρχείο εικόνας EnCase.

ΔΗΜΙΟΥΡΓΙΑ ΕΞΕΙΔΙΚΕΥΜΕΝΩΝ ΜΕ EnCase 2/2

Το EnCase θα σας παρουσιάσει μια σειρά από επιλογές και πεδία εισαγωγής κειμένου που θα τοποθετηθούν στην επικεφαλίδα του κατάλληλου εγκληματολογικού διπλότυπου. Θα σας ζητηθούν οι ακόλουθες πληροφορίες:

- Τοποθεσία του αντιγράφου
- Αριθμός υπόθεσης
- Ονοματεπώνυμο του ερευνητή
- Αριθμός αποδεικτικών στοιχείων
- Περιγραφή των αποδεικτικών στοιχείων που αποκτώνται
- Επαλήθευση της τρέχουσας ημερομηνίας και ώρας
- Οποιεσδήποτε άλλες σημειώσεις ή σχόλια που θέλετε να κάνετε

ΣΥΜΠΕΡΑΣΜΑΤΙΚΑ

Σε αυτό το κεφάλαιο, έχουμε ορίσει τους τύπους αντιγράφων που πιθανόν να δημιουργήσετε ή να αποκτήσετε. Ένα πραγματικό εγκληματολογικό αντίγραφο θα σας επιτρέψει να έχετε μεγαλύτερη ευελιξία κατά την ανάλυση των φάσεων της έρευνας σας. Εάν ο σκληρός δίσκος έχει καταστραφεί κακόβουλα ή όχι μια επιτυχημένη ανάκτηση εγκληματολογικού αντιγράφου είναι πιθανότερη από την ανάκτηση από ειδικευμένο εγκληματολογικό αντίγραφο. Ανεξάρτητα από το διπλότυπο που έχετε επιλέξει, πρέπει να είστε εξοικειωμένοι με όλα τα εργαλεία απεικόνισης και αναπαραγωγής που είναι διαθέσιμα για την έρευνά σας. Δεν αρκεί απλώς να έχουμε μια εργασιακή γνώση ενός εργαλείου εγκληματολογικής έρευνας. Θα πρέπει να μπορείτε να επιλέξετε το εργαλείο έρευνας που είναι κατάλληλο για την κατάσταση και τη διατήρηση των αποδεικτικών στοιχείων με τρόπο που διασφαλίζει την εγκυρότητά του σε περίπτωση που χρησιμοποιηθεί στο δικαστήριο.

ΕΡΩΤΗΣΕΙΣ

- Ποια η διαφορά ενός απλού εγκληματολογικού αντιγράφου από ένα εξειδικευμένο εγκληματολογικό αντίγραφο;
- Έχετε ένα εγκληματολογικό αντίγραφο που δημιουργήθηκε κατά τη διάρκεια μιας έρευνας. Μετά την ανάλυση της εικόνας και την εξάντληση όλων των διαδικασιών, αποφασίζετε να δημιουργήσετε μια αποκατεστημένη εικόνα και αφήνετε το σύστημα να κάνει boot για να εξετάσει τον υπολογιστή του ύποπτου όπως τον είδε για τελευταία φορά. Δημιουργείτε την κατοπτρική εικόνα, αλλά το λειτουργικό σύστημα δεν εκκινεί. Πως το διορθώνετε αυτό;
- Το τμήμα πληροφορικής σας ανακαλύπτει ένα νέο βοηθητικό πρόγραμμα που ισχυρίζεται ότι μπορεί να χρησιμοποιηθεί για εγκληματολογικά αντίγραφα ασφαλείας. Ποιες οδηγίες θα χρησιμοποιούσατε για την επικύρωση αυτού του εργαλείου προτού το προσθέσετε στο σύνολο εργαλείων σας;

ΚΕΦΑΛΑΙΟ 5

ΣΥΛΛΟΓΗ ΑΠΟΔΕΙΚΤΙΚΩΝ ΣΤΟΙΧΕΙΩΝ ΜΕΣΩ ΔΙΚΤΥΟΥ

Εάν υποψιαστείτε πως το σύστημά σας έχει δεχθεί επίθεση ή κάποιος που έχει παρεισφρήσει στέλνει ή συλλέγει προσωπικά σας δεδομένα τι θα κάνατε; Η πιο εύστοχη κίνηση που μπορείτε να κάνετε είναι να αναπτύξετε ένα σύστημα παρακολούθησης και συλλογής της επικοινωνίας του δικτύου σας. Η συλλογή των δικτυακών επικοινωνιών είναι αναγκαία κατά την διερεύνηση υποτιθέμενων διαδικτυακών επιθέσεων.

ΤΙ ΘΕΩΡΟΥΜΕ ΑΠΟΔΕΙΚΤΙΚΟ ΣΤΟΙΧΕΙΟ ΣΕ ΕΝΑ ΔΙΚΤΥΟ

Αναφερόμαστε στα αποτελέσματα μιας πλήρους παρακολούθησης του δικτύου ή την παρακολούθηση των ηλεκτρονικών επικοινωνιών που βασίζονται στο δίκτυο ως αποδεικτικά στοιχεία. Η συλλογή στοιχείων απαιτεί την εγκατάσταση ενός συστήματος που :

- Να εκτελεί την παρακολούθηση του δικτύου
- Να αναπτύσσει την παρακολούθηση και καταγραφή του δικτύου
- Να αξιολογεί την αποτελεσματικότητα της εποπτείας
- Η συλλογή των πληροφοριών κίνησης του δικτύου είναι μόνο ένα κομμάτι της εργασίας η πραγματική πρόκληση είναι η εξαγωγή των σημαντικών στοιχείων, καθώς οτιδήποτε έχει συλλεχθεί αποτελεί ακατέργαστο υλικό.

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΣΤΟΧΟΙ ΕΛΕΓΧΟΥ ΤΟΥ ΔΙΚΤΥΟΥ

Τα ηλεκτρονικά εγκλήματα αντιμετωπίζονται όπως τα κοινά εγκλήματα. Για παράδειγμα, εάν η αστυνομία θέλει να πιάσει κάποιον που κάνει διακίνηση ναρκωτικών θα πρέπει να θέσει τον ύποπτο και όσους συναναστρέφονται μαζί του υπό επιτήρηση. Η ίδια προσέγγιση πραγματοποιείται και στα πιθανά διαδικτυακά εγκλήματα. Ο έλεγχος σε ένα δίκτυο δεν πραγματοποιείτε για να αποτρέψει ένα έγκλημα αλλά για να επιτρέψει στους ερευνητές να ολοκληρώσουν έναν αριθμό εργασιών :

- Επιβεβαίωση ή διάλυση των υποψιών που περιβάλλουν ένα υποτιθέμενο γεγονός ασφαλείας
- Συγκέντρωση πρόσθετων αποδεικτικών στοιχείων
- Επαλήθευση του πεδίου ενός συμβιβασμού
- Προσδιορισμός πρόσθετων εμπλεκόμενων πεδίων
- Καθορισμός χρονοδιαγράμματος των γεγονότων
- Διασφάλιση συμμόρφωσης σε μια ανεπιθύμητη δραστηριότητα

ΕΙΔΗ ΕΛΕΓΧΟΥ ΔΙΚΤΥΟΥ

Η παρακολούθηση ενός δικτύου μπορεί να περιλαμβάνει διαφορετικούς τύπους συλλογής δεδομένων :

- Έλεγχο γεγονότων
- Σχεδιασμό παγίδων στοιχείων
- Παρακολούθηση πλήρους περιεχομένου
- Ένα από τα εργαλεία συλλογής που χρησιμοποιούνται είναι το tcpdump

ΕΛΕΓΧΟΣ ΣΥΜΒΑΝΤΟΣ

Ο έλεγχος των γεγονότων είναι βασισμένος σε κανόνες. Τα γεγονότα δεν είναι τίποτε άλλο παρά ένας συναγερμός ότι κάτι δεν πάει καλά στο δίκτυο σας. Είθισται τα γεγονότα να παράγονται από ένα δίκτυο IDS. Γεγονότα μπορούν επίσης να δημιουργηθούν από λογισμικά παρακολούθησης όπως το MRTG (Multi Router Traffic Grapher). Το ακόλουθο είναι παράδειγμα από Snort, μια γεννήτρια στοιχείων.
[**] [1:0:0] Outbound connection attempt from web server [**]
[Priority: 0]
02/10-14:21:34.668747 172.16.1.7:49159 -> 66.192.0.70:22
TCP TTL:64 TOS:0x0 ID:42487 IpLen:20 DgmLen:60 DF
******S* Seq: 0x3B0BF3E1 Ack: 0x0 Win: 0xFFFF TcpLen: 40
TCP Options (6) => MSS: 1460 NOP WS: 1 NOP NOP TS: 5255946 0

ΠΑΓΙΔΕΥΣΗ ΚΑΙ ΑΝΙΧΝΕΥΣΗ

(trap and trace)
Η χωρίς περιεχόμενο παρακολούθηση καταγράφει την ανταλλαγή δεδομένων συνοψίζοντας έτσι όλη τη δραστηριότητα του δικτύου. Η επιβολή του νόμου αποκαλεί αυτή τη δραστηριότητα trap-and-trace (παγίδευση και ανίχνευση). Εάν υπάρχουν TCP πακέτα στα πρόσθετα στοιχεία μπορούν να συμπεριληφθούν και τα flags που υπάρχουν κατά τη διάρκεια μιας συνομιλίας, την καταμέτρηση δηλαδή των bytes που στέλνονται από τη μία πλευρά στη άλλη καθώς και το σύνολο των πακέτων γενικότερα.

ΕΛΕΓΧΟΣ ΠΛΗΡΟΥΣ ΠΕΡΙΕΧΟΜΕΝΟΥ

Ο πλήρης έλεγχος των πεδίων δεδομένων περιλαμβάνει τα ακατέργαστα πακέτα που συλλέχθηκαν μέσω του καλωδίου. Τα στοιχεία αυτά προσφέρουν την ύψιστη ακρίβεια καθώς αντιπροσωπεύουν την πραγματική επικοινωνία μεταξύ των υπολογιστών σε ένα δίκτυο. Τα πλήρως ικανοποιητικά στοιχεία περιλαμβάνουν τα headers και τα payloads των πακέτων. Τα ακόλουθα πακέτα αποτελούν παράδειγμα χρήσης tcpdump :

ΠΑΡΑΔΕΙΓΜΑ TCPDUMP

```
02/10/2003 19:18:53.938315 172.16.1.128.1640 > 172.16.1.7.80: P 1:324(323)
ack 1 win 65520 (DF)
0x0000   4500 016b a090 4000 7f06 ff54 ac10 0180        E..k..@....T....
0x0010   ac10 0107 0668 0050 6b0a eccc 0ea7 ae9d        .....h.Pk.......
0x0020   5018 fff0 18f9 0000 4745 5420 2f20 4854        P.......GET./.HT
0x0030   5450 2f31 2e31 0d0a 4163 6365 7074 3a20        TP/1.1..Accept:.
0x0040   696d 6167 652f 6769 662c 2069 6d61 6765        image/gif,.image
0x0050   2f78 2d78 6269 746d 6170 2c20 696d 6167        /x-xbitmap,.imag
0x0060   652f 6a70 6567 2c20 696d 6167 652f 706a        e/jpeg,.image/pj
0x0070   7065 672c 2061 7070 6c69 6361 7469 6f6e        peg,.application
0x0080   2f76 6e64 2e6d 732d 6578 6365 6c2c 2061        /vnd.ms-excel,.a
0x0090   7070 6c69 6361 7469 6f6e 2f76 6e64 2e6d        pplication/vnd.m
0x00a0   732d 706f 7765 7270 6f69 6e74 2c20 6170        s-powerpoint,.ap
0x00b0   706c 6963 6174 696f 6e2f 6d73 776f 7264        plication/msword
0x00c0   2c20 2a2f 2a0d 0a41 6363 6570 742d 4c61        ,.*/*..Accept-La
0x00d0   6e67 7561 6765 3a20 656e 2d75 730d 0a41        nguage:.en-us..A
0x00e0   6363 6570 742d 456e 636f 6469 6e67 3a20        ccept-Encoding:.
0x00f0   677a 6970 2c20 6465 666c 6174 650d 0a55        gzip,.deflate..U
0x0100   7365 722d 4167 656e 743a 204d 6f7a 696c        ser-Agent:.Mozil
0x0110   6c61 2f34 2e30 2028 636f 6d70 6174 6962        la/4.0.(compatib
0x0120   6c65 3b20 4d53 4945 2036 2e30 3b20 5769        le;.MSIE.6.0;.Wi
0x0130   6e64 6f77 7320 4e54 2035 2e31 290d 0a48        ndows.NT.5.1)..H
0x0140   6f73 743a 2031 3732 2e31 362e 312e 370d        ost:.172.16.1.7.
0x0150   0a43 6f6e 6e65 6374 696f 6e3a 204b 6565        .Connection:.Kee
0x0160   702d 416c 6976 650d 0a0d 0a                    p-Alive....
```

ΔΗΜΙΟΥΡΓΙΑ ΣΥΣΤΗΜΑΤΟΣ ΕΛΕΓΧΟΥ ΔΙΚΤΥΟΥ

Το λογισμικό διάγνωσης και επίλυσης προβλημάτων ενός δικτύου μπορούν να συλλέξουν σοβαρά στοιχεία τα οποία είναι και τα σημαντικότερα σε έναν πλήρη έλεγχο. Η δημιουργία ενός επιτυχούς συστήματος παρακολούθησης δικτύων περιλαμβάνει τα ακόλουθα βήματα :

- Καθορίστε τους στόχους σας για την εκτέλεση της επιτήρησης δικτύου
- Βεβαιωθείτε ότι έχετε την κατάλληλη νομική υπόσταση για την εκτέλεση της παρακολούθησης
- Αποκτήστε και εφαρμόστε το κατάλληλο harware και software
- Διασφαλίστε την ασφάλεια της πλατφόρμας τόσο σε ηλεκτρονικό όσο και σε φυσικό επίπεδο
- Εξασφαλίστε την κατάλληλη τοποθέτηση του οργάνου ελέγχου στο δίκτυο.
- Αξιολογήστε τον έλεγχο

ΚΑΘΟΡΙΣΜΟΣ ΣΤΟΧΩΝ

Το πρώτο βήμα για την επιτήρηση ενός δικτύου είναι να καθορίσουμε τους λόγους που μας οδήγησαν σε αυτόν τον έλεγχο. Έτσι θα βοηθήσετε το hardware και το software να συλλέξουν τα σωστά στοιχεία, όπως :

- Την κίνηση δεδομένων από και προς ένα συγκεκριμένο host
- Την κίνηση δεδομένων σε ένα συγκεκριμένο δίκτυο
- Τις ενέργειες ενός συγκεκριμένου ανθρώπου
- Τις προσπάθειες παρείσφρησης κάποιου
- Εστίαση στη χρήση ενός συγκεκριμένου πρωτοκόλλου
- Υ.Σ : Μόλις έχετε δημιουργήσει τους στόχους σας για την επιτήρηση του δικτύου , βεβαιωθείτε ότι οι πολιτικές που έχετε εγκαταστήσει υποστηρίζουν αυτούς τους στόχους.

ΕΠΙΛΟΓΗ ΚΑΤΑΛΛΗΛΟΥ HARDWARE

Μπορείτε να αγοράσετε ένα εμπορικό σύστημα ή να δημιουργήσετε το δικό σας σύστημα ελέγχου. Το βασικό ζήτημα είναι να εξασφαλίσετε οτι το σύστημά σας έχει τις δυνατότητες που απαιτούνται για να εκτελέσουν τη λειτουργία παρακολούθησης. Οι δυνατότητες συλλογής δεδομένων στηρίζονται σε 3 παράγοντες

- Τις προδιαγραφές της CPU
- Τη μνήμη RAM
- Τον σκληρό δίσκο

ΣΚΛΗΡΟΣ ΔΙΣΚΟΣ

Το μέγεθος της χωρητικότητας του σκληρού δίσκου εξαρτάται από την ιδιαιτερότητα των φίλτρων που έχετε τοποθετήσει καθώς και απο την κίνηση στο δίκτυο. Οι σκληροί δίσκοι είναι πλέον φτηνοί επομένως είναι καλό να ξοδέψετε ένα ποσό ώστε να έχετε ας πούμε τουλάχιστον 40GB σκληρό σε ένα laptop και τουλάχιστον 80GB σε έναν πύργο. Το ζητούμενο είναι να έχετε έναν επαρκή αποθηκευτικό χώρο στο δίσκο σας. Από τη συνεχή μεταφορά δεδομένων και αρχείων μπορεί να ξεπεράσετε τον χώρο αποθήκευσης γιαυτό είναι καλό να κρατάτε backup τα αρχεία σας σε εξωτερικό δίσκο για κάθε ενδεχόμενο.

ΕΠΙΛΟΓΗ ΚΑΤΑΛΛΗΛΟΥ SOFTWARE ½

Ίσως η πιο δύσκολη πρόκληση είναι η εγκατάσταση ενός σωστού λογισμικού για την παρακολούθηση του δικτύου. Τα εργαλεία παρακολούθησης έχουν μεγάλο κόστος και ίσως χρειαστείτε διαφορετικά εργαλεία

που να ανταποκρίνονται σε διαφορετικές ανάγκες. Πολλά από τα δωρεάν εργαλεία ωστόσο είναι εξίσου καλά όσο και του εμπορίου. Ωστόσο, τα εμπορικά εργαλεία γενικά ξεπερνούν τις υπηρεσίες που παρέχουν τα δωρεάν, όταν πρόκειται για την ανάλυση και την ερμηνεία της ληφθείσας κυκλοφορίας του δικτύου. Κάθε βοηθητικό πρόγραμμα προσφέρει διαφορετικές υπηρεσίες έτσι θα πρέπει να γνωρίζεται τι επιθυμείτε να σας προσφέρει το λογισμικό επιτήρησης προτού το αποκτήσετε. Μερικοί παράγοντες που επηρεάζουν την επιλογή του λογισμικού επιτήρησης είναι οι εξής:

ΕΠΙΛΟΓΗ ΚΑΤΑΛΛΗΛΟΥ SOFTWARE 2/2

- Ποιο λειτουργικό σύστημα υποδοχής θα χρησιμοποιήσετε;
- Θέλετε να επιτρέψετε την εξ' αποστάσεως πρόσβαση στο όργανο ελέγχου σας ή να έχετε πρόσβαση στο όργανο ελέγχου σας μόνο απευθείας;
- Θέλετε να εγκαταστήσετε ένα "σιωπηλό" λογισμικό ανίχνευσης στο δίκτυο;
- Μήπως θα πρέπει να έχετε τη δυνατότητα μεταφοράς των αρχείων καταγραφής;
- Ποιες είναι οι τεχνικές δεξιότητες των υπευθύνων για την παρακολούθηση ;
- Πόσα δεδομένα διασχίζουν το δίκτυο ;
- Η επιλογή του κατάλληλου λειτουργικού συστήματος είναι εξίσου σημαντική με την επιλογή του κατάλληλου λογισμικού ανίχνευσης που θα αποφασίσετε να χρησιμοποιηθεί για την επιτήρηση του δικτύου.

ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ

Ορισμένα λειτουργικά συστήματα προσφέρουν από μόνα τους καλή ανίχνευση του δικτύου. Προφανώς, όσο περισσότερος χρόνος CPU και I/O διατίθεται προς παρακολούθηση τόσο το καλύτερο καθώς θα υπάρχει μεγάλος όγκος δεδομένων προς έλεγχο. Όταν δημιουργείτε την πλατφόρμα ελέγχου, να είστε βέβαιοι ότι θα διακόψετε όλες τις εφαρμογές και διαδικασίες που δεν είναι ουσιαστικές στη λειτουργία του λειτουργικού συστήματος.Αυτό περιλαμβάνει την αφαίρεση οποιονδήποτε περιττών γραφικών περιβαλλόντων χρηστών καθώς δεν θέλετε η CPU να απασχολείτε με ασήμαντες διεργασίες όπως το να κινήσει ένα εικονίδιο στη οθόνη. Μετά απο χρήση πολλών συστημάτων καταλήξαμε ότι μια σταθερή πλατφόρμα Unix εχει τα καλύτερα αποτελέσματα. Ειδικότερα, το λειτουργικό σύστημα FreeBSD έχει προσφέρει την πιο αποτελεσματική σύλληψη περιβάλλοντος επειδή οι προγραμματιστές έχουν εκσυγχρονίσει την κίνηση των frames του δικτύου απο το χώρο μνήμης του πυρήνα(το σημείο σύλληψης) στο χώρο μνήμης του χρήστη (σημείο αποθήκευσης).

ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ FreeBSD

Επιλέξαμε το FreeBSD λειτουργικό σύστημα καθώς προσφέρει τα εξής:

- Ισχυρή στοίβα TCP/IP δικτύου.
- Ασφαλή, απομακρυσμένη πρόσβαση μέσω Secure Shell (SSH).
- Απλούς μηχανισμούς για την απενεργοποίηση των περιττών υπηρεσιών και την εφαρμογή ενός τοπικού τείχους προστασίας.
- Δυνατότητα να τρέξει σε πολλούς τύπους hardware, με ελάχιστη μνήμη και απαιτήσεις επεξεργαστή.
- Χαμηλό κόστος καθώς είναι δωρεάν

ΑΠΟΜΑΚΡΥΣΜΕΝΗ ΠΡΟΣΒΑΣΗ

Εάν χρειάζεστε απομακρυσμένη πρόσβαση στην οθόνη, μπορείτε να χρησιμοποιήσετε μια σύνδεση δικτύου ή ένα μόντεμ. Μία προσέγγιση είναι να εγκαταστήσετε ένα δεύτερο προσαρμογέα δικτύου, συνδέστε το με ένα ξεχωριστό δίκτυο ή εικονικό LAN (VLAN), και στη συνέχεια, εγκαταστήστε λογισμικό

απομακρυσμένου ελέγχου όπως είναι το OpenSSH. Θα πρέπει να περιορίσετε τις εισερχόμενες διευθύνσεις IP στις περιοχές που βρίσκονται υπό τον έλεγχό σας. Μια άλλη επιλογή είναι να προσεγγιστεί το σύστημα μέσω modem για τις «εκτός ζώνης» επικοινωνίες,ή επικοινωνίες που δεν μπορούν να υποκλαπούν εύκολα από έναν επιτιθέμενο. Βεβαιωθείτε ότι η απομακρυσμένη πρόσβαση μέσω modem είναι ασφαλής απαιτώντας ένα ελάχιστο έλεγχο ταυτότητας χρήστη ID / κωδικού πρόσβασης. Ίσως επίσης να θέλετε να ρυθμίσετε την απομακρυσμένη πρόσβαση μέσω της γραμμής modem, έτσι ώστε να δέχεται μόνο τις κλήσεις που προέρχονται από συγκεκριμένους αριθμούς τηλεφώνου.

ΚΡΥΦΗ ΑΝΙΧΝΕΥΣΗ

Είναι δύσκολο για τους εισβολείς να διαγράψουν στοιχεία τα οποία δεν γνωρίζουν. Η εφαρμογή ενός κρυφού ανιχνευτή είναι ο πιο αλάνθαστος τρόπος αποτροπής του εισβολέα να λάβει γνώση για το σύστημα παρακολούθησης σας. Ένα κρυφό σύστημα δεν θα αποκριθεί σε οποιαδήποτε πακέτα λαμβάνει όπως κατευθυνόμενα διαγράμματα δεδομένων IP, broadcast,multicast. Πολλοί κρυφοί εμπορικοί ανιχνευτές διαμορφώνουν το δίκτυο σας θέτοντας τα ενεργά interface σε λειτουργία απόκρυψης (stealth mode). Για να επιτύχετε τη μέγιστη απόκρυψη θα πρέπει να διαμορφώσετε τα interface ώστε να επικοινωνούν μόνο με TCP/IP. Κάποια άλλα πρωτόκολλα, όπως το NetBIOS, δημιουργούν μεγάλη κίνηση που θα έθετε σε κίνδυνο την παρακολούθηση.
Τα συστήματα Unix διαμορφώνονται έτσι ώστε να επικοινωνούν μόνο με πρωτόκολλα TCP/IP. Σε συστήματα Windows, θα πρέπει να βεβαιωθείτε ότι έχετε αποσυνδέσει όλα τα πρωτόκολλα (NetBIOS και IPX), εκτός από το πρωτόκολλο TCP / IP. Θα πρέπει επίσης να αποτρέψετε στο σύστημά σας τα Address Resolution Protocol (ARP) πακέτα, αλλιώς η παρακολούθηση σας μπορεί να ανιχνευθεί από τον εισβολέα. Τα συστήματα Unix υποστηρίζουν τις εντολές ipconfig και έτσι μπορείτε να αποτρέψετε τα πακέτα ARP. Ένας άλλος τρόπος κρυφής ανίχνευσης είναι απευθείας με τη χρήση μονόδρομου καλωδίου Ethernet. Η χρήση μονόδρομου καλωδίου προστατεύει από τυχόν διαδραστικές επιθέσεις. Πολλές εταιρείες αποσυνδέουν τα καλώδια μετάδοσης στο δίκτυο τους προσφέροντας έτσι μια αξιόπιστη και φτηνή λύση να αποκαλυφθεί η ανίχνευση του δικτύου τους.

ΜΟΡΦΗ ΑΡΧΕΙΩΝ ΔΕΔΟΜΕΝΩΝ

Όταν επιλέγετε ένα εργαλείο για την παρακολούθηση πλήρους περιεχομένου, είναι φρόνιμο να ελέγξετε πώς οι πληροφορίες που συλλαμβάνονται στο σύστημά σας αποθηκεύονται. Οι περισσότερες εμπορικές εφαρμογές έχουν ιδιόκτητες μορφές αρχείων κάτι που μπορεί να κάνει την προετοιμασία του περιστατικού δύσκολη όταν άλλες διαφημίσεις ή φορείς επιβολής του νόμου συμμετάσχουν. Το να επιλέξετε λογισμικό που δημιουργεί αρχεία ανοιχτού τύπου μπορεί να σας σώσει ή να σας δυσκολέψει αρκετά. Εδώ είναι μερικά παραδείγματα λογισμικών ανίχνευσης τόσο εμπορικά όσο και ελεύθερα διαθέσιμα που χρησιμοποιούν ιδιόκτητη μορφή σύλληψης δυαδικής μορφής αρχείων :

- Lawrence Livermore National Labs (LLNL) libpcap-based sniffers (tcpdump,Ethereal, and Snort)
- Sun Solaris Snoop
- IBM AIX’s iptrace
- RADCOM’s WAN/LAN Analyzer
- Cisco Secure Intrusion Detection System (CSIDS)

ΑΝΑΠΤΥΞΗ ΠΡΟΓΡΑΜΜΑΤΟΣ ΕΠΟΠΤΕΙΑΣ ΔΙΚΤΥΟΥ 1/2

Η θέση του οργάνου ελέγχου του δικτύου είναι ενδεχομένως ο πιο σοβαρός παράγοντας στην δημιουργία ενός συστήματος παρακολούθησης. Νεότερες συσκευές και τεχνολογίες δικτύου, όπως διακόπτες του δικτύου, VLANs, και πολλαπλά δίκτυα δεδομένων-ρυθμού (10/100 Mb / second Ethernet) έχουν δημιουργήσει ορισμένες νέες προκλήσεις για τους ερευνητές. Ο συνηθισμένος στόχος της επιτήρησης δικτύων είναι να συλληφθεί όλη η δραστηριότητα σχετικά με ένα συγκεκριμένο στοχοποιημένο σύστημα.

Τα switches θα χωρίσουν το δίκτυο σε τμήματα εντοπίζοντας την παρουσία των σταθμών εργασίας βασιζόμενοι στις MAC διευθύνσεις τους. Μόλις λοιπόν ένα switch δημιουργήσει μια θύρα (port) βασισμένη στις MAC διευθύνσεις, θα απελευθερώσει τα πακέτα από μια θύρα μόνο αν το σύστημα που λαμβάνει είναι παρόν. Αυτό σημαίνει, για παράδειγμα, ότι μια παρακολούθηση δικτύου που πραγματοποιείται στη θύρα 4 του switch δεν θα δει ποτέ πακέτα που προορίζονται για τη θύρα 2 εκτός και αν περιλαμβάνεται στη παρακολούθηση.

ΑΝΑΠΤΥΞΗ ΠΡΟΓΡΑΜΜΑΤΟΣ ΕΠΟΠΤΕΙΑΣ ΔΙΚΤΥΟΥ 2/2

Τα σύγχρονα switch έχουν ένα χαρακτηριστικό γνώρισμα γνωστό ως μεταστρεφόμενη ανάλυση θυρών ή SPAN το οποίο επιτρέπει σε μια θύρα του switch να διαβιβάσει όλα τα frames ανεξαρτήτως από το αν το switch έχει εντοπίσει τη παρουσία της διεύθυνσης προορισμού στη συγκεκριμένη θύρα. Είναι επίσης σημαντικό το σύστημα παρακολούθησης να τοποθετηθεί σε μια φυσικά ασφαλή θέση. Καθώς καθένας που μπορεί φυσικά να έχει πρόσβαση στη μηχανή επιτήρησης σας μπορεί να παρακάμψει οποιουσδήποτε ελέγχους λογισμικού έχετε (κωδικοί πρόσβασης, άδειες πρόσβασης αρχείων, κτλ). Όταν αναπτύσσεις ένα σύστημα για την εκτέλεση επιτήρησης του δικτύου θα πρέπει να ασφαλίσεις το σύστημα αυτό σε ένα κλειστό χώρο στον οποίο θα έχουν πρόσβαση μόνο εξουσιοδοτημένα άτομα.

ΑΞΙΟΛΟΓΗΣΗ ΤΗΣ ΕΠΟΠΤΕΙΑΣ ΔΙΚΤΥΟΥ 1/3

Κατά την εκτέλεση της παρακολούθησης του δικτύου, δεν μπορείτε απλώς να κάνετε εκκίνηση στο tcpdump και να απομακρυνθείτε. Θα θελήσετε να ελέγξετε για να βεβαιωθείτε ότι ο δίσκος δεν γεμίζει γρήγορα, βεβαιωθείτε επίσης ότι το πρόγραμμα συλλογής πακέτων εκτελείται σωστά και τι είδους φορτίο μεταφέρετε στο δίκτυο. Πρώτα, χρησιμοποιήστε την εντολή df για να ελέγξετε την κατάσταση του υπάρχοντος διαχωρισμού:

```
monitor# df -h
Filesystem    Size     Used   Avail Capacity  Mounted on
/dev/ad0s1a   650M    452M    145M    76%     /
/dev/ad0s1f   31M     4.0K     29M    0%      /tmp
/dev/ad0s1e   6.9G    66M      6.6G    2%      /var
procfs        4.0K    4.0K     0B     100%    /proc
```

Η έξοδος της εντολής df μας δείχνει πως υπάρχουν 66MB δεδομένων και 6.6GB ελεύθερου χώρου.

ΑΞΙΟΛΟΓΗΣΗ ΤΗΣ ΕΠΟΠΤΕΙΑΣ ΔΙΚΤΥΟΥ 2/3

Στη συνέχεια, χρησιμοποιούμε την εντολή top για να ελέγξουμε το φορτίο του δικτύου:

```
last pid: 68409; load averages: 0.00, 0.00, 0.00 up 26+20:28:09 09:29:13
18 processes: 1 running, 17 sleeping
CPU states: % user, % nice, % system, % interrupt, % idle
Mem: 3584K Active, 6756K Inact, 11M Wired, 3500K Cache, 6080K Buf, 1996K Free
Swap: 96M Total, 2028K Used, 94M Free, 2% Inuse
```

ΑΞΙΟΛΟΓΗΣΗ ΤΗΣ ΕΠΟΠΤΕΙΑΣ ΔΙΚΤΥΟΥ 3/3

```
PID  USERNAME PRI NICE SIZE RES STATE TIME WCPU CPU COMMAND
68    root 2 0 944K 328K select 11:44 0.00% 0.00% syslogd
75    root 10 0 996K 220K nanslp 0:34 0.00% 0.00% cron
62570 root 4 0 3016K 180K bpf 0:20 0.00% 0.00% tcpdump
77    root 2 0 2740K 292K select 0:06 0.00% 0.00% sshd
```

68371 root 2 0 2880K 1552K select 0:00 0.00% 0.00% sshd
68373 root 18 0 1556K 1024K pause 0:00 0.00% 0.00% csh
68409 root 29 0 1896K 1032K RUN 0:00 0.00% 0.00% top
68372 username 10 0 1056K 836K wait 0:00 0.00% 0.00% bash
Αυτή η έξοδος μας δείχνει ότι το πρόγραμμα ελέγχου δεν δυσκολεύετε κάπου. Οι υψηλοί αριθμοί των μέσων όρων των φορτίων υποδηλώνουν κύνδυνο, εμείς εδώ όμως βλέπουμε μηδενικά επομένως δεν υπάρχει φορτίο. Ωστόσο, αν ο δίσκος σας γεμίζει γρήγορα, πέρα από το hardware,μπορεί να χρειαστεί να αλλάξει το είδος των δεδομένων που συλλέγετε, όπως θα περιγράψουμε παρακάτω.

ΕΚΤΕΛΕΣΗ ΠΑΓΙΔΑΣ ΣΤΟΙΧΕΙΩΝ
(trap-and-trace)

Όπως προαναφέρθηκε στο κεφάλαιο, για να συλλάβετε πληροφορίες χωρίς περιεχόμενο από ένα δίκτυο, μπορείτε να χρησιμοποιήσετε ό,τι επιβάλλει ο νόμος ακόμη και μια παγίδα στοιχείων (trap and trace). Στα δίκτυα που είναι βασισμένα στο διαδύκτιο η εφαρμογή μιας παγίδας trap and trace περιλαμβάνει έλεγχο των ip και tcp επικεφαλίδων χωρίς παρακολούθηση οποιουδήποτε περιεχομένου μέσα στα ίδια τα πακέτα. Αυτός είναι ένας διακριτικός τρόπος προσδιορισμού της πηγής μιας επίθεσης που βασίζεται στο δίκτυο. Μπορεί επίσης να χρησιμοποιηθεί για την ανίχνευση ανωμαλιών του δικτύου. Η παρακολούθηση αυτή ειναι εξαιρετικά χρήσιμη σε περιπτώσεις DoS. Αν το δίκτυο σας έχει IDS, router ή web server και μυστυριωδώς σταματήσει να δουλεύει σε μια απλή περίπτωση ρουτίνας η παρακολούθηση trap and trace δεν βοηθά μόνο στο να βρεθεί η πηγή του προβλήματος αλλά πιθανόν να μπορεί να βοηθήσει και στην τεχνική επιδιόρθωση. Μπορείτε να εκτελέσετε μια τέτοια παρακολούθηση χρησιμοποιώντας ελεύθερα εργαλεία όπως το tcpdump, υπάρχει επίσης ένα βοηθητικό πρόγραμμα για Windows που ονομάζεται WinDump και είναι πλήρως συμβατό με το tcpdump και ακολουθεί ίδιους κανόνες. Το WinDump χρησιμοποιεί μια βιβλιοθήκη για τα Windows που ονομάζεται WinPcap. Έτσι το tcpdump και το WinDump καταγράφουν αρχεία με ίδια δυαδική μορφή έτσι ώστε να καταγράφετε τα στοιχεία με tcpdump και να τα διαβάζετε με WinDump.

ΕΝΑΡΞΗ ΑΝΙΧΝΕΥΣΗΣ ΜΕ TCPDUMP 1/2

Η ακόλουθη γραμμή εντολών εκκινεί μια ανίχνευση και παγίδευση χρησιμοποιώντας το tcpdump χωρίς φιλτράρισμα και εκτυπώνει την έξοδο στην οθόνη:
[root@linux taps]# tcpdump
tcpdump: listening on eth0

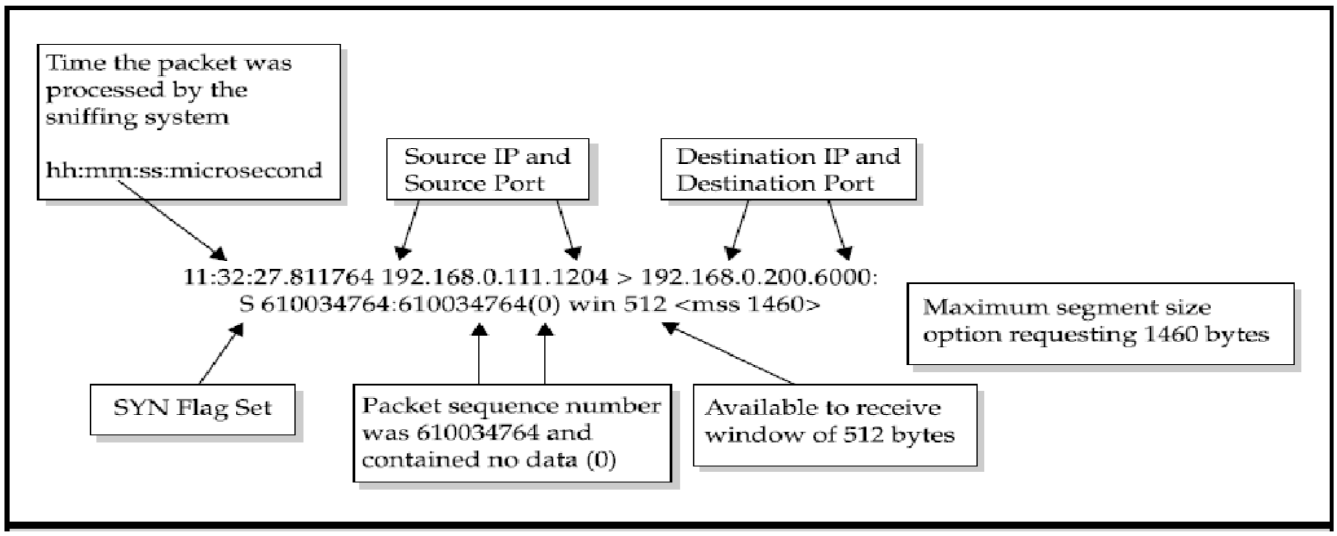
Αν βρίσκεστε σε πολυάσχολο δίκτυο, θα δείτε κάτι σαν header(επικεφαλίδα). Το πρόγραμμα tcpdump δημιουργεί μια επικεφαλίδα με πολυάριθμα πεδία που μεταφράζονται από τα IP και TCP headers , πράγμα που παρέχει γρηγορότερες απαντήσεις.

ΕΝΑΡΞΗ ΑΝΙΧΝΕΥΣΗΣ ΜΕ TCPDUMP 2/2

Όταν εξετάζετε την έξοδο παγίδευσης και ανίχνευσης (trap and trace output) καλό είναι να εξετάσετε τις εξής ερωτήσεις:

- Υπάρχει κάτι ύποπτο στην επικεφαλίδα ip; Είναι η πηγή προέλευσης της ip ύποπτη; Υπάρχει κατακερματισμός ή περίεργο μέγεθος στο πακέτο;
- Υπάρχει κάτι ύποπτο στη επικεφαλίδα tcp; Είναι η θύρα προορισμού έγκυρη;
- Η κυκλοφορία του δικτύου ακολουθεί τα πρότυπα RFC;
- Ποιες είναι οι χρονικές σημάνσεις (timestamps) της κυκλοφορίας; Αυτό βοηθάει στον καθορισμό της αυτοματοποιημένης κυκλοφορίας (πλημμύρα) έναντι της κυκλοφορίας που απαιτεί αλληλεπίδραση χρηστών.

ΣΧΕΔΙΑΓΡΑΜΜΑ TCPDUMP



ΕΝΑΡΞΗ ΑΝΙΧΝΕΥΣΗΣ ΜΕ WinDump

Όπως σημειώθηκε παραπάνω, μπορείτε επίσης να χρησιμοποιήσετε το WinDump, ένα εργαλείο που μοιάζει με το tcpdump και βοηθάει στην προβολή της κυκλοφορίας του δικτύου και είναι για τα Windows.

```
cmd.exe
E:\taps>windump -x -v -r traptrace6.bin | more
17:19:53.846068 192.168.0.200 > 192.168.0.210: icmp: echo request (ttl 55, id 58
11)
                        4500 001c 16b3 0000 3701 ea43 c0a8 00c8
                        c0a8 00d2 0800 ffd7 f827 0000 0000 0000
                        0000 0000 0000 0000 0000 0000 0000
17:19:53.846145 192.168.0.200.49628 > 192.168.0.210.80: . ack 354351313 win 3072
 (ttl 46, id 23371)
                        4500 0028 5b4b 0000 2e06 ae9a c0a8 00c8
                        c0a8 00d2 c1dc 0050 ffc8 0003 151e f8d1
                        5010 0c00 5101 0000 0000 0000 0000
17:19:53.847097 192.168.0.210 > 192.168.0.200: icmp: echo reply (ttl 255, id 525
1)
                        4500 001c 1483 0000 ff01 2473 c0a8 00d2
                        c0a8 00c8 0000 07d8 f827 0000
17:19:53.847632 192.168.0.210.80 > 192.168.0.200.49628: R 354351313:354351313(0)
 win 0 (ttl 255, id 5252)
                        4500 0028 1484 0000 ff06 2461 c0a8 00d2
                        c0a8 00c8 0050 c1dc 151e f8d1 0000 0000
                        5004 0000 5cd9 0000
17:19:54.148497 192.168.0.200.49608 > 192.168.0.210.139: FP 0:0(0) win 3072 urg
0 (ttl 46, id 44112)
                        4500 0028 ac50 0000 2e06 5d95 c0a8 00c8
                        c0a8 00d2 c1c8 008b 0000 0000 0000 0000
                        5029 0c00 5e7d 0000 0000 0000 0000
```

ΔΗΜΙΟΥΡΓΙΑ ΕΞΩΤΕΡΙΚΟΥ ΑΡΧΕΙΟΥ ΠΑΓΙΔΕΥΜΕΝΩΝ ΣΤΟΙΧΕΙΩΝ

Όταν εκτελείτε μια παγίδα και ανίχνευση, είναι πιο εύκολο να δημιουργήσετε ένα μόνιμο αρχείο εξόδου από το να βλέπετε τα αποτελέσματα ζωντανά. Χωρίς αρχείο εξόδου τα στοιχεία χάνονται τη στιγμή που

τερματίζετε τη διαδικασία. Η ακόλουθη γραμμή εντολών θα ξεκινήσει να συλλαμβάνει πληροφορίες επικεφαλίδας για όλη την κίνηση (χωρίς φίλτρα)

```
[root@homer /root]# tcpdump > traptrace1
```

ΧΡΗΣΗ TCPDUMP ΓΙΑ ΠΛΗΡΟΥΣ ΠΕΡΙΕΧΟΜΕΝΟΥ ΣΤΟΙΧΕΙΩΝ ΕΛΕΓΧΟΥ

Συνήθως, για την αντιμετώπιση περιστατικών ασφάλειας υπολογιστών, θα πραγματοποιήσετε παρακολούθηση πλήρους περιεχομένου. Εάν υποπτεύεστε ότι κάποιος υπάλληλος μεταφέρει εμπορικά μυστικά ή κάποιος έχει επιτεθεί σε κάποιον κεντρικό server σας θέλετε να ξέρετε ποιες ακριβώς πληροφορίες μεταφέρει ή θέλετε να παρεμποδίσετε τη διαβίβαση; Αφού ρυθμίσετε το σύστημα παρακολούθησης δικτύου, είστε έτοιμοι να ξεκινήσετε τη πλήρη παρακολούθηση των στοιχείων και να συλλέξετε τα ακατέργαστα πακέτα από το δίκτυο. Η ακόλουθη εντολή καταγράφει στο δίσκο τα πακέτα με τη βοήθεια tcpdump:
tcpdump -n -i dc0 -s 1514 -w /var/log/tcpdump/emergency_capture.lpc &

ΦΙΛΤΡΑΡΙΣΜΑ ΠΛΗΡΟΥΣ ΠΕΡΙΕΧΟΜΕΝΟΥ ΔΕΔΟΜΕΝΩΝ 1/3

Σε καταστάσεις όπου συλλέγετε υπερβολική κυκλοφορία για να χειριστείτε το σύστημα παρακολούθησης, θα πρέπει να φιλτράρετε πλήρως το περιεχόμενο των δεδομένων. Ο απλούστερος τρόπος για την εφαρμογή φιλτραρίσματος στο tcpdump βασίζεται στην κατασκευή Berkeley Packet Filters. Το εγχειρίδιο προσφέρει πολλές επιλογές για την επισήμανση της προσοχής του εργαλείου προς συγκεκριμένα πακέτα. Κατά τη διάρκεια περιστατικών ασφάλειας βασιζόμαστε στην κυκλοφορία ενδιαφέροντος από και προς διάφορα hosts. Παραδείγματος χάριν για να καταγράψετε την κυκλοφορία του network block 12.44.56.0/24 θα ακολουθήσετε την ακόλουθη γραμμή εντολών:
tcpdump -n -i dc0 -s 1514 -w /var/log/tcpdump/emergency_capture.lpc
net 12.44.56 &

ΦΙΛΤΡΑΡΙΣΜΑ ΠΛΗΡΟΥΣ ΠΕΡΙΕΧΟΜΕΝΟΥ ΔΕΔΟΜΕΝΩΝ 2/3

Η ακόλουθη γραμμή εντολής μπορεί να χρησιμοποιηθεί για να συλλέξει όλη την κυκλοφορία σε και από έναν συγκεκριμένο οικοδεσπότη (ip address 172.16.1.7):
tcpdump -n -i dc0 -s 1514 -w /var/log/tcpdump/emergency_capture.lpc
host 172.16.1.7 &
Για να συλλέξετε όλη την κυκλοφορία δικτύου από ένα μπλοκ δικτύου 12.44.56 και να συγκεντρώσετε όλα τα πακέτα προς και από το σύστημα με διεύθυνση IP 172.16.1.7, μπορείτε να χρησιμοποιήσετε τη παρακάτω γραμμή εντολών:
tcpdump -n -i dc0 -s 1514 -w /var/log/tcpdump/emergency_capture.lpc
net 12.44.56 or host 172.16.1.7 &

ΦΙΛΤΡΑΡΙΣΜΑ ΠΛΗΡΟΥΣ ΠΕΡΙΕΧΟΜΕΝΟΥ ΔΕΔΟΜΕΝΩΝ 3/3

Όταν τα φίλτρα σας αρχίσουν να γίνονται πολύπλοκα, μπορείτε να τα βάλετε σε ένα αρχείο και να παραπέμπεστε εκεί με μια γραμμή εντολών .Το παρακάτω αρχείο θα μπορούσε να χρησιμοποιηθεί για την υλοποίηση του προηγούμενου παραδείγματος σε αμεσότερη μορφή. Για παράδειγμα, μπορείτε να δημιουργήσετε ένα αρχείο που ονομάζεται tcpdump.ips (αυτό το όνομα αρχείου είναι αυθαίρετο) με αυτά τα περιεχόμενα.
net 12.44.56 or host 172.16.1.7
Τώρα μπορείτε να παραπεμφθείτε στο tcpdump.ips από τη γραμμή εντολών χρησιμοποιώντας το -F:

tcpdump -n -i dc0 -s 1514 -w /var/log/tcpdump/emergency_capture.lpc
–F tcpdump.ips &

ΔΙΑΤΗΡΗΣΗ ΑΡΧΕΙΩΝ ΔΕΔΟΜΕΝΩΝ ½

Δύο άλλες πτυχές της συλλογής πλήρους περιεχομένου που αξίζουν την προσοχή μας:

- Ονοματοδοσία φακέλων
- Εξασφάλιση της ακεραιότητας των αρχείων
- Τα συλληφθέντα ονόματα φακέλων πρέπει να είναι μοναδικά καθώς έτσι μας βοηθάνε να εντοπίζουμε την προέλευση τους και τον σκοπό τους. Μας αρέσει τα ονόματα να περιλαμβάνουν μια χρονική σήμανση και διασύνδεση στο όνομα του αρχείου καταγραφής. Ένα παράδειγμα είναι το εξής :
  tcpdump -n -i dc0 -s 1514 -w /var/log/tcpdump/`/bin/date "
+DMY_%d-%m-%Y_HMS_%H%M%S"`.`hostname`.dc0.lpc net 12.44.56 &

ΔΙΑΤΗΡΗΣΗ ΑΡΧΕΙΩΝ ΔΕΔΟΜΕΝΩΝ 2/2

Αυτή η εντολή θα παράγει ένα αρχείο με το ακόλουθο όνομα, αν άρχισε στις10 Φλεβάρη 2003, στις 15:18:50, σε ένα σύστημα που ονομάζεται archangel, ακούγοντας στο interface dc0.
DMY_10_02_2003_HMS_151850.archangel.dc0.lpc
Συμπεριλάβαμε το DMY για να μας υπενθυμίσει ότι οι χαρακτήρες που ακολουθούν είναι η ημέρα, ο μήνας και το έτος. Το HMS διευκρινίζει οτι ακολουθούν η ώρα τα λεπτά και τα δευτερόλεπτα.

ΣΥΛΛΟΓΗ ΑΡΧΕΙΟΥ ΚΑΤΑΓΡΑΦΗΣ ½

Μην παραβλέπουμε όλες τις πιθανές πηγές των αποδεικτικών στοιχείων κατά την απάντηση σε ένα περιστατικό! Οι περισσότερες κινήσεις στο δίκτυο αφήνουν μια διαδρομή ελέγχου κάπου κατά μήκος της διαδρομής που διανύθηκε. Εδώ είναι μερικά παραδείγματα:

- Routers, firewalls, servers, IDS sensors και άλλες συσκευές του δικτύου μπορεί να έχουν καταγράψει γεγονότα
- Οι διακομιστές DHCP κατά την διάρκεια που ένα pc ζητά ip διεύθυνση
- Τα σύγχρονα firewalls επιτρέπουν στους διαχειριστές να έχουν μεγάλο ποσοστό λεπτομερειών κατά τη δημιουργία αρχείων καταγραφής ελέγχου

ΣΥΛΛΟΓΗ ΑΡΧΕΙΟΥ ΚΑΤΑΓΡΑΦΗΣ 2/2

- Οι αισθητήρες IDS μπορεί να ανιχνεύσουν ένα τμήμα μιας επίθεσης που οφείλεται στην αναγνώριση μιας υπογραφής ή σε μια ανωμαλία στο φίλτρο ανίχνευσης
- Αισθητήρες κεντρικού υπολογιστή μπορεί να ανιχνεύσουν την αλλαγή μιας βιβλιοθήκης συστήματος ή την προσθήκη ενός αρχείου σε μια ευαίσθητη περιοχή
- Όταν συνδυάσετε όλα τα υπάρχοντα κομμάτια του δικτύου στα οποία υπάρχουν αποδείξεις, μπορεί να είναι δυνατή η επανασύσταση συγκεκριμένων γεγονότων του δικτύου, όπως η μεταφορά αρχείων, μία επίθεση buffer overflow, ή ένας κλεμμένος λογαριασμός χρήστη και κωδικός πρόσβασης που χρησιμοποιείται στο δίκτυό σας.

ΣΥΜΠΕΡΑΣΜΑΤΙΚΑ

Οι κακοποιοί γίνονται όλο και πιο ικανοί. Πολλές φορές, οι επιτιθέμενοι έχουν πρόσβαση root-level και μπορούν να αλλάξουν ή να καταστρέψει τα αποδεικτικά στοιχεία που μπορεί να έχουν μείνει πίσω για τους ερευνητές. Η παρακολούθηση του δικτύου μπορεί μόνο να προσφέρει στοιχεία σχετικά με τον τύπο των επιθέσεων που έχουν ανιχνευθεί. Ως εκ τούτου, κατά τη διάρκεια ενός περιστατικού ασφάλειας των υπολογιστών, μπορείτε να επιλέξετε να ακολουθήσετε τα γρήγορα και απλά βήματα που περιγράφονται σε αυτό το κεφάλαιο για να ξεκινήσει η συλλογή της κυκλοφορίας του δικτύου. Η διαχείριση των πληροφοριών που συλλέγονται αποτελούν την επόμενη πρόκληση.

ΕΡΩΤΗΣΕΙΣ

- Ποιες είναι μερικές από τις συσκευές του δικτύου που φιλοξενούν αποδεικτικά στοιχεία;
- Γιατί πρέπει να αποκλειστεί το πρωτόκολλο ARP στον έλεγχο ασφαλείας του δικτύου;
- Αναφέρατε 4 διαφορετικά σενάρια όπου θα πραγματοποιούσατε πλήρες έλεγχο του δικτύου (π.χ σαν εργαζόμενος,μαθητής,σπουδαστής)

ΚΕΦΑΛΑΙΟ 6

ΧΕΙΡΙΣΜΟΣ ΑΠΟΔΕΙΚΤΙΚΩΝ ΣΤΟΙΧΕΙΩΝ

Υπάρχουν λίγα γεγονότα στον τομέα της ασφάλειας ηλεκτρονικών υπολογιστών ως ικανοποιητικά ή σημαντικά για μια επιτυχημένη εμπειρία στο δικαστήριο. Εάν κάποιο συμβάν ασφαλείας που έχετε ερευνήσει οδηγηθεί σε δικαστική διαδικασία τα ψηφιακά στοιχεία που έχετε αποκτήσει είναι πιθανό να χρησιμοποιηθούν στη δίκη. Υπάρχουν ειδικοί κανόνες για να διασφαλιστεί ότι τα στοιχεία αυτά είναι αυθεντικά. Ως εκ τούτου κατά τη διάρκεια αστικών ή ποινικών διαδικασιών, η συλλογή, ο χειρισμός, η αποθήκευση των ψηφιακών δεδομένων ή κάθε άλλο υλικό αποδεικτικό στοιχείο που έχετε ερευνήσει μπορεί να αμφισβητηθούν από τον αντίπαλο.
Είναι σημαντικό να ακολουθήσετε και να εφαρμόσετε διαδικασίες χειρισμού αποδεικτικών στοιχείων που θα ανταποκριθούν στις απαιτήσεις του φορέα αξιολόγησης και θα αντέξουν τις προκλήσεις. Σε αυτό το κεφάλαιο θα διασφαλίσουμε ότι οι πληροφορίες που συλλέγετε θα έχουν σωστό χειρισμό.

ΤΙ ΘΕΩΡΕΙΤΕ ΑΠΟΔΕΙΚΤΙΚΟ ΣΤΟΙΧΕΙΟ

Κατά τη διάρκεια μιας έρευνας σχετικά με ένα συμβάν ασφάλειας υπολογιστών, μπορεί να μην είστε σίγουροι αν ένα στοιχείο (όπως ένα cd) πρέπει να επισημανθεί ως αποδεικτικό στοιχείο. Μπορούμε να ορίσουμε αποδεικτικά στοιχεία ως οποιαδήποτε πληροφορία αποδεικτικής αξίας, που σημαίνει ότι αποδεικνύει κάτι ή βοηθά να αποδείξει κάτι σχετικό με την υπόθεση. Είναι πιο ασφαλές να αντιμετωπίζετε κάθε πληροφορία που αποκτάτε κατά τη διάρκεια της έρευνας ως αποδεικτικό στοιχείο. Επομένως κάθε ηλεκτρονικό αρχείο, έγγραφο, εκτύπωση ή άλλα αντικείμενα αποκτηθούν από την έρευνα σας πρέπει να αντιμετωπίζονται ως αποδεικτικά στοιχεία και πρέπει να τα χειριστείτε σύμφωνα με τη διαδικασία που ακολουθούμε σε κάθε έρευνα.

Ο ΚΑΛΥΤΕΡΟΣ ΚΑΝΟΝΑΣ ΑΠΟΔΕΙΞΕΩΝ

Ο κανόνας των βέλτιστων αποδεικτικών στοιχείων απαιτεί ουσιαστικά ότι, το πρωτότυπο ενός γραπτού ή ηχογραφημένου στοιχείου πρέπει να γίνει αποδεκτό στο δικαστήριο για να αποδειχθεί το περιεχόμενό του (εκτός φυσικά κάποιων περιπτώσεων). Ένας κανονισμός προβλέπει ότι αν τα δεδομένα αποθηκεύονται σε έναν υπολογιστή ή παρόμοια συσκευή, σε οποιαδήποτε εκτύπωση ή άλλη έξοδο ευανάγνωστη από την όραση, που φαίνεται να αντικατοπτρίζει με ακρίβεια τα δεδομένα, είναι ένα πρωτότυπο. Σύμφωνα με αυτόν τον κανονισμό πολλαπλά αντίγραφα ηλεκτρονικών αρχείων μπορεί να αποτελούν το καθένα ένα "πρωτότυπο".

ΓΝΗΣΙΕΣ ΑΠΟΔΕΙΞΕΙΣ

Μερικές φορές, η πορεία που λαμβάνει μια υπόθεση είναι εκτός του ελέγχου του πελάτη / θύματος. Ωστόσο, για να διασφαλίσουμε την κατάλληλη επιμέλεια, πάντα υποθέτουμε ότι μια υπόθεση θα καταλήξει σε δικαστική διαμάχη και αντιμετωπίζουμε τις αποδείξεις αναλόγως. Εάν υπάρχει ποινική ή αστική διαδικασία, συχνά παροτρύνουμε τον πελάτη / θύμα να μας επιτρέψει να πάρουμε τον έλεγχο των πρωτότυπων αποδεικτικών στοιχείων, αφού έχουμε εφαρμόσει διαδικασίες χειρισμού αποδεικτικών στοιχείων. Για τους σκοπούς μας, ορίζουμε ως πρωτότυπα τα αποδεικτικά στοιχεία που παρέχονται από τον πελάτη / θύμα.

ΟΙ ΠΡΟΚΛΗΣΕΙΣ ΤΟΥ ΧΕΙΡΙΣΜΟΥ ΤΩΝ ΑΠΟΔΕΙΞΕΩΝ

Ένα από τα πιο συνηθισμένα λάθη που έγιναν από τους επαγγελματίες της ασφάλειας υπολογιστών είναι η αποτυχία επαρκούς τεκμηρίωσης κατά την απάντηση σε ένα περιστατικό ασφάλειας υπολογιστών. Σημαντικά στοιχεία ενδέχεται να μην συλλεχθούν ποτέ ή να χαθούν ή η προέλευση και η σημασία τους να μην γίνει ποτέ γνωστή. Στην τεχνική πολυπλοκότητα της συλλογής στοιχείων προστέθηκε επίσης το το γεγονός ότι τα συλλεγμένα αρχεία θα πρέπει να πάρουν γραπτή πιστοποίηση. Τέτοια τεκμηρίωση είναι φαινομενικά ενάντια στα φυσικά ένστικτα των τεχνικών που συχνά ερευνούν συμβάντα ασφάλειας υπολογιστών. Όλοι οι ερευνητές πρέπει να κατανοήσουν τις προκλήσεις του χειρισμού των αποδεικτικών στοιχείων και πώς να τις αντιμετωπίσουν. Αυτός είναι ο λόγος για τον οποίο κάθε οργανισμός που εκτελεί ασφάλεια υπολογιστών απαιτεί μια επίσημη διαδικασία χειρισμού. Η μεγαλύτερη πρόκληση όσον αφορά τη διεξαγωγή αποδείξεων είναι ότι τα στοιχεία που συλλέγονται πρέπει να επικυρώνονται μέσω δικαστικής διαδικασίας

ΓΝΗΣΙΟΤΗΤΑ ΣΤΟΙΧΕΙΩΝ

Οι νόμοι πολλών κρατών ορίζουν ως στοιχεία-δεδομένα ενός υπολογιστή ό,τι έχει καταγραφεί. Απλώς τα αρχεία που έχουν καταγραφεί πρέπει να έχουν επικυρωθεί για να θεωρηθούν αποδεικτικά στοιχεία. Η επικύρωση καθορίζεται με την κατάθεση κατά την εξέταση, αυτού που έχει συλλέξει τα στοιχεία έτσι ώστε να επιβεβαιώσει τα όσα ισχυρίζεται. Με άλλα λόγια η επικύρωση γίνεται με μάρτυρα ο οποίος έχει γνώσεις πάνω στην προέλευση των στοιχείων που έχουν συλλεχθεί. Εάν τα αποδεικτικά στοιχεία δεν είναι δυνατόν να επικυρωθούν, θεωρείται συνήθως απαράδεκτο και οι πληροφορίες αυτές δεν μπορούν να παρουσιαστούν στο σώμα δικαστών. Επίσης είναι σημαντικό να αναπτυχθεί ένα είδος εσωτερικού εγγράφου που να καταγράφει τον τρόπο με τον οποίο συλλέγονται τα αποδεικτικά στοιχεία.

ΕΠΙΣΚΟΠΗΣΗ ΤΩΝ ΔΙΑΔΙΚΑΣΙΩΝ ΔΙΑΧΕΙΡΙΣΗΣ ΑΠΟΔΕΙΞΕΩΝ ½

Όταν χειρίζεστε αποδεικτικά στοιχεία κατά τη διάρκεια μιας έρευνας, θα τηρείτε γενικά τις παρακάτω διαδικασίες:

- Εάν εξετάζετε τα περιεχόμενα ενός σκληρού δίσκου που βρίσκεται αυτήν τη στιγμή μέσα σε έναν υπολογιστή, καταγράψτε πληροφορίες σχετικά με σύστημα του υπολογιστή.
- Βγάλτε ψηφιακές φωτογραφίες του αρχικού συστήματος ή / και των μέσων που αντιγράφονται.
- Βάλτε ετικέτες στα αποδεικτικά στοιχεία και στα αντίγραφα που έχετε δημιουργήσει.
- Αποθηκεύστε το βέλτιστο αντίγραφο των αποδεικτικών στοιχείων κάπου ασφαλή.

ΕΠΙΣΚΟΠΗΣΗ ΤΩΝ ΔΙΑΔΙΚΑΣΙΩΝ ΔΙΑΧΕΙΡΙΣΗΣ ΑΠΟΔΕΙΞΕΩΝ 2/2

- Ο φύλακας των αποδεικτικών στοιχείων εισάγει ένα αρχείο με τα καλύτερα στοιχεία σε ένα φύλλο καταγραφής. Για κάθε κομμάτι των καλύτερων αποδεικτικών στοιχείων, θα υπάρχει αντίστοιχη καταχώρηση στο μητρώο αποδεικτικών στοιχείων.
- Όλες οι έρευνες εκτελούνται σε ένα εγκληματολογικό αντίγραφο των καλύτερων αποδεικτικών στοιχείων, που ονομάζεται αντίγραφο εργασίας.
- Ο φύλακας των αποδεικτικών στοιχείων διασφαλίζει πως υπάρχουν σωστές ημερομηνίες στα στοιχεία. Ημερομηνίες στα στοιχεία ορίζει ο κύριος ερευνητής.
- Ο φύλακας εκτελεί μηνιαίο έλεγχο για την ασφάλεια των στοιχείων,ελέγχει αν έχουν αποθηκευτεί σωστά και αν υπάρχουν ετικέτες.

ΠΕΡΙΓΡΑΦΗ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ ΑΠΟΔΕΙΞΕΩΝ 1/2

Πριν συγκεντρωθούν τυχόν ηλεκτρονικά στοιχεία, πρέπει να καταγράφονται ορισμένα δεδομένα σχετικά με την κατάσταση και την ταυτοποίηση του καταγόμενου ηλεκτρονικού συστήματος. Ο τύπος των πληροφοριών που καταγράφεται τυπικά περιλαμβάνει τα ακόλουθα:

- Τα άτομα που κατέχουν ή έχουν πρόσβαση τον χώρο στον οποίο βρέθηκαν τα στοιχεία
- Τους χρήστες που χρησιμοποιούν το σύστημα (χρησιμοποιείται από τον οποιοδήποτε ή έχουν πρόσβαση συγκεκριμένοι χρήστες).
- Ποια η θέση του υπολογιστή στο χώρο (που είναι τοποθετημένος)
- Ποια η κατάσταση του συστήματος είναι ενεργό ή απενεργοποιημένο; Ποια τα δεδομένα που εμφανίζονται στην οθόνη;
- Η ώρα και η ημερομηνία από τα BIOS

ΠΕΡΙΓΡΑΦΗ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ ΑΠΟΔΕΙΞΕΩΝ 2/2

- Τι συνδέσεις έχει πραγματοποιήσει το δίκτυο
- Ποια άτομα ήταν παρόντα κατά τη δημιουργία αντιγράφων των αποδεικτικών στοιχείων
- Καταγραφή σειριακών αριθμών, μοντέλα, μάρκες των σκληρών δίσκων και των εξαρτημάτων του συστήματος καθώς και τι περιφερειακά είναι συνδεδεμένα στο σύστημα.
- Το έντυπο λεπτομερών στοιχείων του συστήματος εξυπηρετεί την καλύτερη οργάνωση των πληροφοριών καθώς περιλαμβάνει και έχει συγκεντρωμένες όλες τις λεπτομέρειες του συστήματος.

ΨΗΦΙΑΚΕΣ ΕΙΚΟΝΕΣ 1/2

Αφού καταγράψετε τα στοιχεία του συστήματος (ή ακόμη και πριν από αυτό), μπορεί αν θέλετε να τραβήξετε αρκετές φωτογραφίες των αποδείξεων του συστήματος. Υπάρχουν διάφοροι λόγοι για αυτό:

- Προστασία των ερευνητών σας
- Για να διασφαλίσετε ότι θα επιστρέψετε το σύστημα στην ακριβή κατάστασή του πριν από την δικαστική έρευνα.
- Για να καταγράψετε την τρέχουσα διαμόρφωση, όπως συνδέσεις δικτύου, συνδέσεις modem και άλλα εξωτερικά περιφερειακά.

ΨΗΦΙΑΚΕΣ ΕΙΚΟΝΕΣ 2/2

Μπορεί να θέλετε να τραβήξετε φωτογραφίες από όλες τις συνδέσεις του δικτύου και μπορείτε ακόμη να τραβήξετε φωτογραφίες ειδικά για τον σειριακό αριθμό του συστήματος και την ετικέτα του σκληρού δίσκου. Κάποιες επιπλέον οδηγίες που ακολουθούμε όταν φωτογραφίζουμε ένα συμβάν είναι:

- Μην συμπεριλάβετε κανένα άτομο στις φωτογραφίες σας (αν είναι δυνατόν).
- Τοποθετήστε τις ετικέτες σε κάθε φωτογραφία για να περιγράψετε ακριβώς τι απεικονίζει η φωτογραφία (αριθμός δωματίου, όνομα ιδιοκτήτη υπολογιστή, αριθμός υπόθεσης, αριθμός ετικέτας αποδεικτικών στοιχείων κλπ.). Αυτό εξαλείφει τα σφάλματα που σχετίζονται με τη δημιουργία ενός αρχείου καταγραφής για κάθε φωτογραφία που τραβήξατε.
- Κρατήστε στη φωτογραφική μηχανή μόνο φωτογραφίες που αφορούν την έρευνά σας.

ΕΠΙΣΗΜΑΝΣΕΙΣ ΑΠΟΔΕΙΞΕΩΝ

Τα καλύτερα στοιχεία που συλλέγονται πρέπει να επισημαίνονται κατά τρόπο που να ικανοποιεί την ομοσπονδιακούς και την κρατικούς μηχανισμούς. Η πρακτική που πρέπει να ακολουθούμε απαιτεί να καταγράφονται σε ετικέτες τα ακόλουθα:

- Αν το στοιχείο απαιτεί συγκατάθεση για έρευνα ή αναζήτηση
- Ο τόπος ή τα πρόσωπα από τα οποία έγινε η παραλαβή του αντικειμένου
- Περιγραφή του (των) αντικειμένου (ων) που έχει ληφθεί.

- Εάν το στοιχείο είναι μια συσκευή αποθήκευσης, καταγράψτε τις πληροφορίες που περιέχονται μέσα.
- Ημερομηνία και ώρα λήψης του στοιχείου.
- Πλήρες όνομα και υπογραφή του ατόμου που αρχικά έλαβε τα αποδεικτικά στοιχεία.
- Αριθμός υπόθεσης.

ΕΤΙΚΕΤΟΠΟΙΗΣΗ ΑΠΟΔΕΙΞΕΩΝ

Αφού επισημανθούν οι αποδείξεις θα πρέπει να αποκτήσουν ετικέτες. Χρησιμοποιούμε ετικέτες που μας επιτρέπουν την αλλαγή ή διαγραφή τους όποτε χρειαστεί. Προτείνουμε την ετικετοποίηση με ημερομηνία στην αρχική μονάδα δίσκου. Οι περισσότεροι άνθρωποι επιλέγουν να χρησιμοποιούν μαρκαδόρους, αλλά θα μπορούσατε πραγματικά να χαράξετε τα αρχικά σας στα αρχικά μέσα μαρτυρίας σε μια ξεχωριστή τοποθεσία. Στόχος σας είναι απλώς να επισημάνετε τα στοιχεία έτσι ώστε να αναγνωρίζονται εύκολα ως αποδεικτικά στοιχεία και να είναι εμφανές το ποιος τα σύλλεξε έτσι ώστε να χρησιμοποιηθούν στο δικαστήριο. Στη συνέχεια τοποθετήστε τα στοιχεία σε έναν φάκελο συμπληρώνοντας εξωτερικά του φακέλου τις εξής πληροφορίες:

- Αριθμό αρχείου ,αριθμό ετικέτας, ημερομηνία και ώρα συλλογής στοιχείων και σύντομη περιγραφή των αντικειμένων που εμπεριέχονται στο φάκελο.

ΑΠΟΘΗΚΕΥΣΗ ΑΠΟΔΕΙΚΤΙΚΩΝ ΣΤΟΙΧΕΙΩΝ

Ο ερευνητής που συλλέγει τα αποδεικτικά στοιχεία (και όλοι οι άλλοι που έχουν την επιμέλεια των στοιχείων) πρέπει να διατηρούν θετικό έλεγχο των αποδεικτικών στοιχείων ανά πάσα στιγμή. Αυτό απαιτεί οι εργαζόμενοι σε μια τοποθεσία να έχουν ένα μέσο για την αποθήκευση και τη μεταφορά κάθε αποδεικτικού στοιχείου με τέτοιο τρόπο που να προστατεύει τα αποδεικτικά στοιχεία και να εμποδίζει την άνευ αδείας πρόσβαση. Τα αποδεικτικά στοιχεία πρέπει επίσης να προστατεύονται από αλλοίωση από το περιβάλλον. Αυτό σημαίνει ότι τα αποδεικτικά στοιχεία δεν πρέπει να εκτίθενται σε πιθανώς καταστρεπτικά ηλεκτρομαγνητικά πεδία ή να διατηρούνται σε περιοχές ακραίων θερμοκρασιών ή καταστάσεων.

ΜΕΤΑΦΟΡΑ ΑΠΟΔΕΙΚΤΙΚΩΝ ΣΤΟΙΧΕΙΩΝ

Όταν εκτελείτε την εγκληματολογική ανάλυση εκτός του χώρου, μπορεί να μην είστε σε θέση να παραδώσετε αυτοπροσώπως τα αποδεικτικά στοιχεία σε αυτόν που θα τα φυλάει. Επομένως θα πρέπει να αποστείλετε τα καλύτερα στοιχεία που έχετε συλλέξει. Όταν στέλνετε μέσα ενημέρωσης (ή οποιαδήποτε αποδεικτικά στοιχεία) σε αυτόν που θα τα φυλάει θα πρέπει να τα αποθηκεύσετε σωστά.
Θα πρέπει να συσκευαστούν κατάλληλα με προστατευτικό υλικό το οποίο θα είναι ανθεκτικό στον στατικό ηλεκτρισμό και να μεταφερθούν μέσω φορέα που παρέχει δυνατότητα παρακολούθησης της διαδρομής τους. Επομένως το εμπορευματοκιβώτιο θα πρέπει να πληρεί τις εξής προϋποθέσεις:

- Το κιβώτιο πρέπει να μπορεί να παρουσιάζει σημάδια παραβίασης.
- Πρέπει να εμποδίζει τη βλάβη στα μέσα που μεταφέρονται.
- Πρέπει να αποτρέπει τη μεταβολή των μέσων από το περιβάλλον (Ηλεκτρομαγνητικά πεδία ή ακραίες θερμοκρασίες)

ΑΣΦΑΛΕΙΑ ΕΓΓΡΑΦΩΝ

Κάθε οργάνωση που συλλέγει αποδεικτικά στοιχεία ως αποτέλεσμα κάποιας έρευνας προϋποθέτει ότι τα αποδεικτικά στοιχεία είναι ασφαλή. Η ασφάλεια παρέχετε διασφαλίζοντας την παραβίαση ή την άνευ αδείας πρόσβαση στα έγγραφα που είναι σημαντικά στην υπόθεση. Τα έγγραφα επομένως παραμένουν καλά κλειδωμένα και φυλαγμένα και πρόσβαση έχουν μόνο όσοι τα φυλάνε ή έχουν εξουσιοδοτημένη πρόσβαση σε αυτά. Τα κλειδιά του χώρου φύλαξης τα έχουν μόνο όσοι φυλάνε το χώρο και τα αποδεικτικά στοιχεία.

Αυτό βοηθά στη διατήρηση της αλυσίδας επιμέλειας και ασφάλειας των σημαντικότερων αποδεικτικών στοιχείων.

ΑΡΧΕΙΟ ΑΠΟΔΕΙΞΕΩΝ

Οι φύλακες των αποδεικτικών στοιχείων θα πρέπει να λαμβάνουν και να αποθηκεύουν τα καλύτερα αποδεικτικά στοιχεία για κάθε περίπτωση που χρήζει διερεύνησης. Επομένως όταν παραλάβουν τα στοιχεία καταγράφουν την παραλαβή αυτή στο μητρώο αποδεικτικών στοιχείων. Πλήρης κατάλογος των αποδεικτικών στοιχείων που περιέχονται στο "χρηματοκιβώτιο" θα πρέπει να φυλάσσονται στο αρχείο αποδεικτικών στοιχείων. Κάθε φορά που λαμβάνονται μέτρα για μια συγκεκριμένη περίπτωση, οι ακόλουθες πληροφορίες πρέπει να καταγραφούν:

- Αριθμός ετικέτας
- Ημερομηνία
- Δράσεις που έχουν γίνει
- Ποιος εκτελεί τη διαδικασία.
- Πληροφορίες για τα μέσα που επηρεάζονται.

ΑΝΤΙΓΡΑΦΑ ΕΡΓΑΣΙΑΣ

Οι έρευνες πραγματοποιούνται σε αντίγραφα εργασίας των καλύτερων αποδεικτικών στοιχείων. Τα αντίγραφα των εργασιών που έχουν γίνει δεν είναι απαραίτητο να φυλαχθούν κάπου εκτός εάν η υπόθεση αξίζει πρόσθετες διασφαλίσεις. Εάν έχετε πολλούς ερευνητές να δουλεύουν ταυτόχρονα και πρέπει να διαβιβάζουν τα όσα συλλέγουν στον φύλακα των αποδεικτικών στοιχείων η καλύτερη πολιτική είναι οι ίδιοι οι ερευνητές να είναι υπεύθυνοι για τη δημιουργία αντιγράφων της εργασίας που πραγματοποίησαν. Τα μόνα δεδομένα που πρέπει να διαβιβαστούν για αποθήκευση στα αποδεικτικά στοιχεία είναι τα καλύτερα και σημαντικότερα στοιχεία που έχουν συλλεχθεί. Αυτό ανακουφίζει τους φύλακες από το βάρος της δημιουργίας αντιγράφων εργασίας για ανάλυση και διανομή αυτών των αντιγράφων.

ΑΡΧΕΙΟ ΑΝΤΙΓΡΑΦΩΝ ΑΣΦΑΛΕΙΑΣ (BACKUPS)

Ένα από τα πλεονεκτήματα των ψηφιακών αποδεικτικών στοιχείων σε σχέση με άλλα είδη φυσικών αποδεικτικών στοιχείων είναι ότι μπορείτε να δημιουργήσετε αντίγραφα άπειρες φορές. Ένα από τα μειονεκτήματα των ψηφιακών στοιχείων είναι ότι οι σκληροί δίσκοι και ο ηλεκτρονικός εξοπλισμός μπορεί να αποτύχουν. Επομένως, προκειμένου να ελαχιστοποιηθούν τα κακά αποτελέσματα μιας ενδεχόμενης αποτυχίας του εξοπλισμού ή των φυσικών καταστροφών, είναι συνετό να δημιουργήσετε αντίγραφα ασφαλείας όλων των ηλεκτρονικών αποδείξεων. Οι φύλακες των αποδεικτικών στοιχείων θα πρέπει να διασφαλίζουν ότι υπάρχει μία εφεδρική ταινία για κάθε βέλτιστο αποδεικτικό στοιχείο. Τα αντίγραφα ασφαλείας ταινιών θα λάβουν τη δική τους ετικέτα αποδείξεων και θα αποθηκευτούν.

ΕΛΕΓΧΟΣ ΑΠΟΔΕΙΚΤΙΚΩΝ ΣΤΟΙΧΕΙΩΝ

Οι φύλακες αποδεικτικών στοιχείων θα πρέπει να διενεργούν μηνιαίο έλεγχο, ώστε να διασφαλίζεται ότι υπάρχουν όλα τα βέλτιστα αποδεικτικά στοιχεία σωστά αποθηκευμένα και επισημασμένα. Οι μηνιαίες επιθεωρήσεις απαιτούνται για να διασφαλιστεί η ετοιμότητα των αποδεικτικών στοιχείων σε περίπτωση που χρειαστούν. Ενώ κάνετε αυτόν τον έλεγχο, μπορείτε επίσης να επιλέξετε να εκτελέσετε απογραφή αδειών λογισμικού. Η παρακάτω λίστα εξασφαλίζει ότι οι φύλακες των αποδεικτικών στοιχείων εξετάζουν τα εξής:

- Εξασφάλιση της συμμόρφωσης με τις διαδικασίες ασφαλούς πρόσβασης σε αποδεικτικά στοιχεία.
- Έλεγχος των απαιτήσεων διάθεσης οποιουδήποτε αποδεικτικού στοιχείου για να καθοριστεί εάν υπάρχουν αποδεικτικά στοιχεία που μπορούν να καταστραφούν.
- Έλεγχος για να διαπιστώσετε αν οποιαδήποτε απόδειξη απαιτεί δημιουργία αντιγράφου ασφαλείας.

ΣΥΜΠΕΡΑΣΜΑΤΙΚΑ

Η σωστή διεκπεραίωση των αποδεικτικών στοιχείων είναι μια κρίσιμη πτυχή της ανταπόκρισης περιστατικών και της εγκληματολογικής έρευνας στους υπολογιστές. Πρέπει να αναπτύξετε διαδικασίες που βοηθούν τους ερευνητές σας να απαντήσουν σε τυχόν προκλήσεις για την ακεραιότητα των δεδομένων που παρουσιάζουν. Θα πρέπει να εκτελέσετε μια ξεκάθαρη διαδικασία για τον χειρισμό και να είστε ικανοί να επικοινωνήσετε με τους φύλακες και χειριστές των αποδεικτικών σας στοιχείων. Το σημαντικότερο είναι να διασφαλίσετε ότι τα αποδεικτικά στοιχεία που συλλέγονται είναι απαράβατα και αναλλοίωτα.

ΕΡΩΤΗΣΕΙΣ

- Ποια είναι τα καθήκοντα που πρέπει να εκτελεί ένας φύλακας αποδεικτικών στοιχείων;
- Γιατί ο κανόνας των καλύτερων αποδεικτικών στοιχείων είναι ιδιαίτερα σημαντικός για τους εξεταστές εγκληματολογίας υπολογιστών;
- Πότε πρέπει να διαγράψετε ή να καταστρέψετε τα δεδομένα / αποδεικτικά στοιχεία που αφορούν ένα περιστατικό;

ΚΕΦΑΛΑΙΟ 7

ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΑΠΟΘΗΚΕΥΣΗΣ

Προτού να μπορέσετε να εισχωρήσετε στις συναρπαστικές έρευνες που αφορούν εισβολές υπολογιστών από ξένες χώρες, διεθνή συστήματα νομιμοποίησης εσόδων από παράνομες δραστηριότητες κτλ, θα πρέπει να έχετε κατανόηση στις βασικές λειτουργίες του υλικού του υπολογιστή, του λογισμικού και του λειτουργικού συστήματος. Σε αυτό το κεφάλαιο, εστιάζουμε στους σκληρούς δίσκους αποθήκευσης συστημάτων και στα συστήματα αρχείων. Ξεκινά με μια επισκόπηση των διαφόρων προτύπων διασύνδεσης του σκληρού δίσκου και του τρόπου με τον οποίο επηρεάζουν τα εγκληματολογικά αντίγραφά σας (συμπεριλαμβανομένου του τρόπου αποφυγής της καταστροφής ακριβού SCSI hardware). Στη συνέχεια, καλύπτει τον τρόπο προετοιμασίας του σκληρού δίσκου για χρήση κατά τη διάρκεια της έρευνάς σας. Το τελευταίο τμήμα εισάγει τις αρχές και την οργάνωση αποθήκευσης δεδομένων.

ΣΚΛΗΡΟΙ ΔΙΣΚΟΙ ΚΑΙ ΔΙΕΠΑΦΕΣ

Υπάρχουν καταστάσεις πιο απογοητευτικές στην προετοιμασία εκτέλεσης μερικών γρήγορων αναζητήσεων στο αντίγραφό σας, όπως το να αντιμετωπίσετε τεχνικές δυσκολίες σε κάθε σας βήμα. Η κατανόηση του hardware και του συνόλου προτύπων στα οποία το σύστημα χτίστηκε περιορίζει σημαντικά τον αριθμό των τομέων στη μήτρα ανίχνευσης μηχανικών βλαβών σας. Σε αυτή την ενότητα, θα καλύψουμε γρήγορα τα βασικά στοιχεία των μορφών διεπαφής σκληρού δίσκου. Ο όρος διεπαφή είναι μια εσφαλμένη ονομασία εδώ. Συμπιέζουμε τις έννοιες της διεπαφής , τα πρότυπα και τα πρωτόκολλα σε ένα τμήμα σε μια προσπάθεια απλοποίησης της συζήτησης.

ΠΡΟΤΥΠΟ ΤΑΧΕΙΑΣ ΜΕΤΑΚΙΝΗΣΗΣ ATA

Το πρότυπο ATA ξεκίνησε αρκετά απλοϊκά. Το ATA-1 σχεδιάστηκε με ένα μόνο κανάλι δεδομένων που θα μπορούσε να υποστηρίξει δύο σκληρούς δίσκους, έναν κύριο και έναν δευτερεύον. Αυτό το πρότυπο υποστηρίζει προγραμματισμένες λειτουργίες I / O (PIO) 0 έως 2, αποδίδοντας μέγιστο ρυθμό μεταφοράς 8.3MB / sec. Η επόμενη μεγάλη βελτίωση ήρθε με την υιοθέτηση της άμεσης πρόσβασης μνήμης (DMA). Η χρήση της μεθόδου DMA επέτρεψε στον υπολογιστή να μεταφέρετε δεδομένα χωρίς να χρησιμοποιείτε πολύ CPU. Μετά από σύντομο χρονικό διάστημα υπήρξε αύξηση της ταχύτητας σε 16MB/sec αλλά ήταν ανεπαρκής. Το πρότυπο εξελίχθηκε σε έκδοση υψηλότερης ταχύτητας γνωστή ως Ultra-DMA. Η τρέχουσα επανάληψη είναι η λειτουργία Ultra-DMA 5, η οποία διαθέτει μέγιστη ταχύτητα μεταφοράς 100MB / sec. Τα προηγούμενα πρότυπα μεταβίβαζαν δεδομένα με ρυθμούς 66, 44 και 33 MB/sec, δίνοντάς μας την εξήγηση πίσω από τις ετικέτες που εκτυπώνονται σε πακέτα σκληρών δίσκων: ATA / 33, ATA / 44, ATA / 66 ή ATA / 100.

ΟΡΙΑ ΜΕΓΕΘΟΥΣ ΚΙΝΗΣΗΣ

Μαζί με το ρυθμό μεταφοράς δεδομένων, το αυξανόμενο μέγεθος των μέσων κίνησης αποτελεί επίσης ανησυχία για την επιτροπή T13 (η ομάδα που εκδίδει τα πρότυπα της ATA).Η Western Digital πωλεί σκληρούς δίσκους 200GB. Δυστυχώς, οι ελεγκτές ATA στην αγορά δεν είναι σε θέση να χειριστούν τίποτα πάνω από 137GB. Οι κατασκευαστές δίσκων φτιάχνουν ATA interfaces βασισμένα στο πρότυπο UDMA Mode 6. Οι τωρινές ATA διεπαφές χρησιμοποιούν 28bit διευθύνσεις και φτάνουν τα 137.4 GB. Επιπλέον τα βοηθητικά λειτουργικά συστήματα όπως το Scandisk της Microsoft και το Disk Defragmenter δεν

λειτουργούν κανονικά σε δίσκους άνω των 137GB, ακόμα και αν η κάρτα ATA κάνει update. Με τον χρόνο όμως θα ελαχιστοποιηθούν αυτά τα προβλήματα.

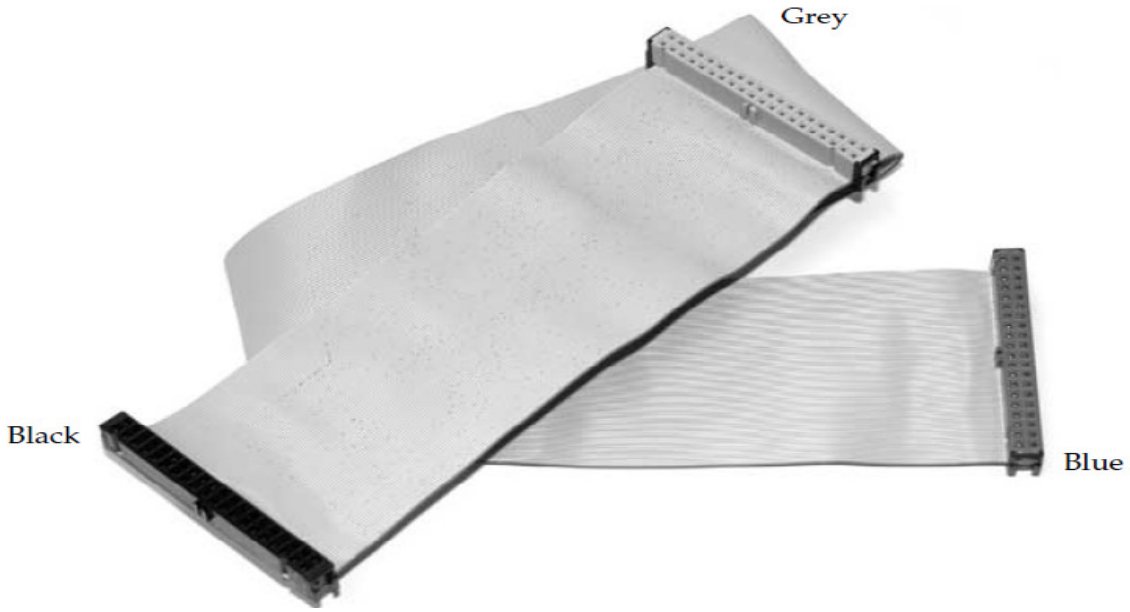
ΚΑΛΩΔΙΩΣΗ

Στόχος της αποδοτικής δημιουργίας αντιγράφου είναι η μέγιστη λήψη δεδομένων στο συντομότερο χρονικό διάστημα. Η σωστή καλωδίωση παίζει σημαντικό ρόλο στην επίτευξη αυτών των στόχων. Τα καλώδια έχουν συγκεκριμένα χρώματα όπως μπλε, γκρι και μαύρο και κάθε ένα από αυτά έχει έναν ρόλο.

* Ο μπλε σύνδεσμος συνδέεται με τον ελεγκτή κεντρικού υπολογιστή στη μητρική πλακέτα ή κάρτα PCI.
* Ο γκρίζος σύνδεσμος βρίσκεται στο μέσο του καλωδίου και συνδέεται με την δευτερεύουσα συσκευή αν υπάρχει.
* Ο μαύρος σύνδεσμος πρέπει να είναι συνδεδεμένος στη κύρια μονάδα δίσκου.

ΚΑΛΩΔΙΩΣΗ

Παράδειγμα καλωδίου 80-conductor/40-pin για ATA/44 και πάνω



ATA BRIDGES

Τα δύο κύρια πλεονεκτήματα της χρήσης γέφυρας υποδοχής ATA για τους ερευνητές είναι η διαθεσιμότητα βάση hardware, προστασία γραφής και η ικανότητα ανταλλαγής δεδομένων σε σκληρούς δίσκους. Στο παρελθόν, προστατεύσαμε τους σκληρούς δίσκους από αλλοίωση χρησιμοποιώντας software για την προστασία εγγραφής. Αρκετές εταιρείες πρόσφεραν προϊόντα που εμπόδιζαν τη μεταφορά δεδομένων στο δίσκο κατά τη διάρκεια λειτουργιών εγγραφής. Οι ATA bridges προσέφεραν ευκολότερη λύση για να εφαρμοστεί κάτι τέτοιο.

SCSI

Το SCSI αποτελεί καιρό interface που επιλέγουν για συστήματα υπολογιστών κατηγορίας server, RAID (Redundant Array of Independent Disks) και υπολογιστές της Apple. Τον περισσότερο καιρό βέβαια θα

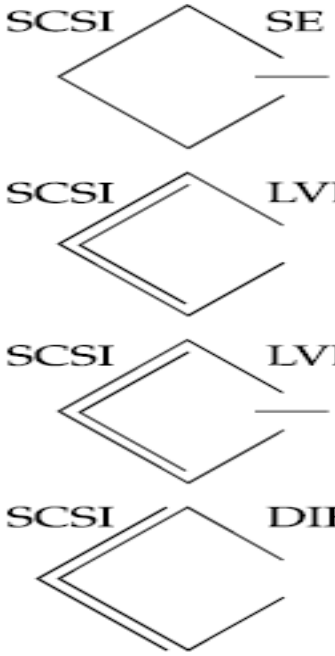
ασχοληθείτε με συσκευές ATA / IDE. Ωστόσο, είναι σημαντικό να κατανοήσουμε το SCSI και πώς διαφέρει από το πρότυπο ATA τόσο σε θεωρητικό όσο και σε πρακτικό επίπεδο. Η διαφορά στη ροή δεδομένων μεταξύ ATA και SCSI είναι πολύ μικρή. Ενώ ο εξωτερικός ρυθμός μεταφοράς για την έκδοση SCSI μπορεί να προσεγγίσει 320MB / sec (τρεις φορές μεγαλύτερη από την τρέχουσα τεχνολογία ATA), οι εσωτερικοί ρυθμοί μεταφοράς (από τις πλατφόρμες στη διεπαφή) είναι ίδιοι. Θα αρχίσετε να παρατηρείτε τα πλεονεκτήματα του SCSI όταν υπάρχουν πολλές συσκευές στο δίαυλο SCSI. Οι συσκευές ATA θα αναλάβουν ολόκληρο τον δίαυλο για τη διάρκεια μιας λειτουργίας ανάγνωσης ή εγγραφής. Μόνο μία συσκευή ATA μπορεί να είναι ενεργή κάθε φορά σε κάθε δίαυλο ATA ενώ το SCSI υποστηρίζει παράλληλα εντολές ταυτόχρονα σε πολλές συσκευές εάν το λειτουργικό σύστημα το υποστηρίζει. Αυτός είναι ένας λόγος που τα SCSI RAIDs θα ξεπέρασαν τις επιδόσεις του ATA RAID. Μιλώντας για πολλές συσκευές, οι αλυσίδες σήματος SCSI μπορεί να χωρέσουν έως και 7 ή 14 συσκευές.

ΤΥΠΟΙ ΣΗΜΑΤΟΔΟΣΙΑΣ SCSI

Υπάρχουν μερικοί τρόποι ακούσια εντελώς να καταστραφεί το hardware των υπολογιστών. Για SCSI συσκευές η ανάμειξη συσκευών που είναι για διαφορετικούς τύπους διαύλων είναι ένας σίγουρος τρόπος καταστροφής. Παράδειγμα SCSI standarts :

SCSI Standard	Common Name	External Transfer Speed	Cable Type
SCSI-1	Asynchronous	4 MB/s	A (50 pin)
SCSI-2	Wide	10 MB/s	P (68 pin)
SCSI-2	Fast	10 MB/s	A (50 pin)
SCSI-2	Wide / Fast	20 MB/s	P (68 pin)
SCSI-3	Ultra / Wide	20 / 40 MB/s	P (68 pin)
SCSI-3	Ultra2 / Wide	40 / 80 MB/s	A or P (50/68 pin)
SCSI-3	Ultra3 / Ultra160	160 MB/s	P (68 pin)
SCSI-3	Ultra4 / Ultra320	320 MB/s	P (68 pin)

Οι τέσσερις τύποι σηματοδότησης SCSI που πρέπει να αναγνωρίσετε παρατίθενται εδώ, μαζί με σύμβολα που βρίσκονται στη
συσκευή:



Single-ended

Low voltage differential

Low voltage differential / multimode

High voltage differential

ΠΡΟΕΤΟΙΜΑΣΙΑ ΣΚΛΗΡΟΥ ΔΙΣΚΟΥ

Όπως έχουμε δηλώσει επανειλημμένα στα προηγούμενα κεφάλαια, η προετοιμασία είναι βασική στη άμεση ανταπόκριση. Επομένως και η προετοιμασία του σκληρού δίσκου δεν αποτελεί εξαίρεση καθώς θα πρέπει να είναι έτοιμος σε περίπτωση που χρειαστεί να αποθηκεύσει κάτι. Πρώτα θα καλύψουμε το πως θα καθαρίσουμε όλα τα δεδομένα από μια μονάδα δίσκου και, στη συνέχεια, θα μιλήσουμε για κατανομή (partition) και μορφοποίηση.

ΚΑΘΑΡΙΣΜΟΣ ΔΕΔΟΜΕΝΩΝ ΔΙΣΚΟΥ

Παλιότερα ο καθαρισμός των δεδομένων ήταν ένα από τα βασικότερα βήματα προετοιμασίας. Ο καθαρισμός των μέσων αποθήκευσης είναι λιγότερο σημαντικός σήμερα, δεδομένων των πιο προηγμένων μεθόδων ανάλυσης που είναι διαθέσιμοι. Στα πραγματικά εγκληματολογικά αντίγραφα δεν απαιτείτε ανάκτηση εικόνων εκτός συγκεκριμένων περιπτώσεων. Όταν η ανάλυση πραγματοποιείται μέσω της τοποθέτησης εικονικού δίσκου, η φύση του διπλού αρχείου εικόνας θα διατηρήσει τα παλιά δεδομένα που εμπίπτουν στην έρευνα. Η πλέον προτιμώμενη μέθοδος για να καθαρίσετε τα μέσα αποθήκευσης είναι η εντολή Unix dd. Η εντολή dd θα αντιγράψει τα δεδομένα από το ένα αρχείο στο άλλο. Σε αυτή την περίπτωση, χρησιμοποιούμε τη συσκευή / dev / zero ως πηγή, γιατί αυτό θα μας δώσει συνεχή πηγή τιμών NULL (δεκαεξαδικό χαρακτήρα 0x00). Η ακόλουθη γραμμή εντολών θα καθαρίσει τα δεδομένα στο δεύτερο σκληρό δίσκο σε περιβάλλον linux:

```
# dd if=/dev/zero of=/dev/hdb
```

ΔΙΑΜΟΙΡΑΣΜΟΣ ΚΑΙ ΜΟΡΦΟΠΟΙΗΣΗ

Η εμπειρία μας έχει δείξει ότι το πιο ευέλικτο σύστημα διαμερισμού αποτελείται από μια σειρά από 20GB διαμερίσματα FAT32. Αυτό θα επιτρέψει στον ερευνητή να συλλέξει εγκληματολογικά αντίγραφα (για παράδειγμα, χρησιμοποιώντας το EnCase ή το Safeback) ή το Unix (χρησιμοποιώντας dd ή dcfldd). Είναι μερικοί τρόποι για γρήγορο διαχωρισμό και διαμόρφωση μιας μονάδας δίσκου. Για πιο αξιόπιστα αποτελέσματα κατά τη διαμόρφωση ενός διαμερισμού, χρησιμοποιήστε λειτουργικό σύστημα που να είναι συμβατό. Για παράδειγμα για τη δημιουργία partitions FAT32 χρησιμοποιείστε Windows. Κάποια εργαλεία λειτουργικών συστημάτων όπως το fdisk των Linux ενδέχεται να μην ανταποκρίνονται σωστά άμα οι συνθήκες δεν ταιριάζουν.

ΔΙΑΜΟΙΡΑΣΜΟΣ ΚΑΙ ΜΟΡΦΟΠΟΙΗΣΗ ΜΕ WINDOWS

Μόλις συνδεθεί ο σκληρός δίσκος (ονομάζεται μονάδα αποθήκευσης) στο σύστημα του υπολογιστή και έχει αναγνωριστεί από το BIOS, είστε έτοιμοι να προχωρήσετε στα Windows. Αφήστε το σύστημα να εκκινήσει και εισαγάγετε τη μικρο εφαρμογή διαχείρισης δίσκων, στη διαχείριση υπολογιστών στον πίνακα ελέγχου. Μια άλλη διαδρομή προς τη μικρο εφαρμογή είναι να κάνετε δεξί κλικ στο εικονίδιο ο "Υπολογιστής μου" ,επιλέξτε "Διαχείριση" και στη συνέχεια, επιλέξτε "Διαχείριση δίσκων". Βεβαιωθείτε ότι η μονάδα αποθήκευσης έχει αναγνωριστεί. Κάντε δεξί κλικ στη μονάδα δίσκου και επιλέξτε "Δημιουργία διαμερίσματος" (create partition). Αποφύγετε τα πολλαπλά partitions, καλύτερα να δημιουργήσετε ένα κύριο.

ΔΙΑΜΟΙΡΑΣΜΟΣ ΚΑΙ ΜΟΡΦΟΠΟΙΗΣΗ ΜΕ LINUX 1/2

Μπορείτε να επαληθεύσετε ότι ο σκληρός δίσκος (target drive) έχει αναγνωριστεί από το BIOS και το λειτουργικό σύστημα εκτελώντας την εντολή dmesg. Στο παρακάτω παράδειγμα, εμφανίζουμε όλους τους σκληρούς δίσκους ATA εκτελώντας την έξοδο της εντολής dmesg μέσω grep ψάχνοντας για hd. Παρατηρήστε ότι ο κατασκευαστής ονομάζεται CntxCorpHD στο παράδειγμα. Επίσης στο παράδειγμα θα δείτε πως έχουμε δύο ATA δίσκους που ονομάζονται hda και hdb. Επιπλέον δείχνει ότι τα Linux αναγνωρίζουν τους πίνακες διαμοιρασμού στο δίσκο στον πρώτο υπάρχουν 3 τμήματα (partitions) και στον δεύτερο 0. Ας δούμε λοιπόν το παράδειγμα:

ΔΙΑΜΟΙΡΑΣΜΟΣ ΚΑΙ ΜΟΡΦΟΠΟΙΗΣΗ ΜΕ LINUX 2/2

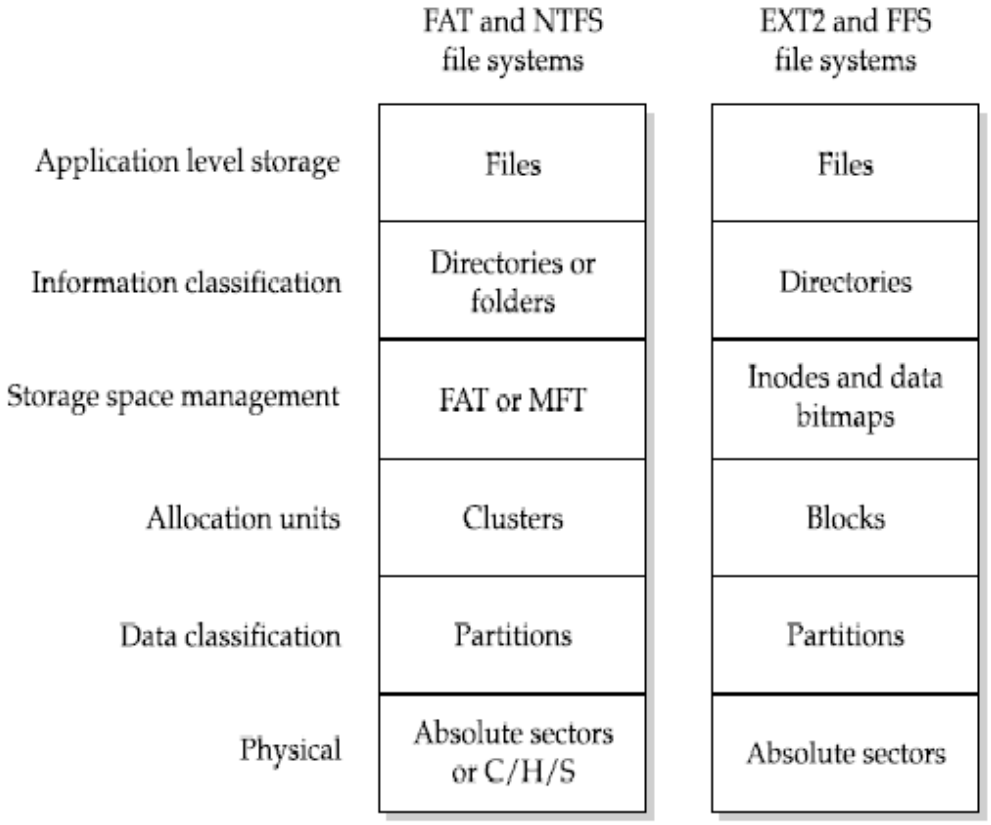
```
[root@localhost root]# dmesg | grep hd
Kernel command line: ro root=/dev/hda2
ide0: BM-DMA at 0x1000-0x1007, BIOS settings: hda:pio, hdb:pio
ide1: BM-DMA at 0x1008-0x100f, BIOS settings: hdc:pio, hdd:pio
hda: CntxCorpHD, ATA DISK drive
hdb: CntxCorpHD, ATA DISK drive
hdc: CntxCorpCD, ATAPI CD/DVD-ROM drive
hda: 4194288 sectors (2147 MB) w/64KiB Cache, CHS=520/128/63, DMA
hdb: 31456656 sectors (16106 MB) w/64KiB Cache, CHS=1958/255/63, DMA
hda: hda1 hda2 hda3
hdb:
hdc: ATAPI DVD-ROM drive, 128kB Cache
hdc: DMA disabled
```

ΣΥΣΤΗΜΑΤΑ ΑΡΧΕΙΩΝ ΚΑΙ ΕΠΙΠΕΔΑ ΑΠΟΘΗΚΕΥΣΗΣ 1/2

Η γνώση του τόπου όπου βρίσκονται τα στοιχεία στα μέσα αποθήκευσης δεδομένων είναι απαραίτητη για να γίνει σωστή έρευνα. Μπορείτε να δείτε το σύστημα αρχείων ως πολυεπίπεδο μοντέλο, παρόμοιο με το OSI και προσδιορίζεται σε 6 layers:

- Physical
- Data classification (Ταξινόμηση δεδομένων)
- Allocation units (Μονάδες κατανομής)
- Storage space management (Διαχείρηση χώρου αποθήκευσης)
- Information classification (Ταξινόμηση πληροφοριών)
- Application-level storage(Αποθήκευση σε επίπεδο εφαρμογής)

ΣΥΣΤΗΜΑΤΑ ΑΡΧΕΊΩΝ ΚΑΙ ΕΠΙΠΕΔΑ ΑΠΟΘΗΚΕΥΣΗΣ 2/2



PSYSICAL LAYER

Το χαμηλότερο επίπεδο αποθήκευσης αρχείων είναι το φυσικό επίπεδο, το οποίο είναι πάντα παρόν, ανεξαρτήτως των λειτουργικών συστημάτων ή των αρχείων του συστήματος που βρίσκονται στο σκληρό δίσκο. Το μηχάνημα θα διαβάσει και θα γράψει τον σκληρό δίσκο ανά τομέα. Τα περισσότερα λειτουργικά συστήματα που θα τρέξετε θα διαβάσουν και θα γράψουν κομμάτια ανά 512byte. Οι τομείς αριθμούνται διαδοχικά, ξεκινώντας από το μηδέν συνεχίζοντας μέχρι το τέλος του δίσκου. Εάν καταλήξετε να εργάζεστε σε μια περίπτωση όπου τα εμπλεκόμενα μέρη έχουν υψηλό βαθμό εξειδίκευσης, μπορείτε να αναγκάσετε το λογισμικό αλληλεπικάλυψης να αγνοήσει αυτό που εντοπίζει ως τον τελευταίο απόλυτο τομέα και να συνεχίσει μέχρι να λάβει κωδικούς σφάλματος από το σκληρό δίσκο.

DATA CLASSIFICATION LAYER

Ακριβώς πάνω από το φυσικό επίπεδο βρίσκεται το σχήμα κατανομής που έχει ρυθμιστεί από το λειτουργικό σύστημα. Αυτό το σύστημα επιτρέπει στον χρήστη να διαχωρίζει πληροφορίες προς συμφέρον της ασφάλειας, βελτιστοποίηση συστήματος αρχείων ή απλά οργάνωση. Σε εγκαταστάσεις Unix που έχουν δημιουργηθεί σε διακομιστές (διακομιστές ιστού ή διακομιστές ηλεκτρονικού ταχυδρομείου), οι διαφορετικοί τύποι δεδομένων διατηρούνται σε χωριστά partitions. Αυτό επιτρέπει στο λειτουργικό σύστημα να λειτουργεί αξιόπιστα, ανεξάρτητα με το πόσο γρήγορα γεμίζουν τα αρχεία αλληλογραφίας ή τα αρχεία καταγραφής λόγω της κυκλοφορίας του δικτύου. Κατά τη δημιουργία, το partition θα διαθέτει ένα αναγνωριστικό. Αυτός ο single-byte κώδικας θα δώσει στο λειτουργικό σύστημα την ικανότητα να γνωρίζει τι είδους αρχεία να αναμένει. Εάν τα Windows παρατηρούν ένα άγνωστο partition ID θα αγνοήσει εντελώς το συγκεκριμένο partition ακόμα και αν έχει διαμορφωθεί σωστά και έχει έγκυρα δεδομένα.

ALLOCATION UNITS LAYER

Το επόμενο επίπεδο αποθήκευσης του συστήματος αρχείων αναφέρεται στη μέθοδο αποκλεισμού ή στη μέθοδο κατανομής που χρησιμοποιείται από το λειτουργικό σύστημα. Το μέγεθος κάθε μονάδας κατανομής εξαρτάται από τρεις μεταβλητές: τον τύπο του συστήματος αρχείων, το μέγεθος του partition και τις γνώσεις του διαχειριστή του συστήματος. Κάθε σύστημα αρχείων ορίζει το δικό του σχήμα για τη διαμόρφωση δεδομένων στο μέσο αποθήκευσης. Οι περισσότεροι χρησιμοποιούν ένα μέγεθος block που βελτιστοποιείται για το μέγεθος του partition. Ο διαχειριστής του συστήματος έχει την επιλογή να παρακάμπτει τα προεπιλεγμένα μεγέθη των block σε ορισμένες περιπτώσεις. Για παράδειγμα, αν ένας διακομιστής Unix αναμένεται να χρησιμοποιήσει το χώρο μονάδας δίσκου σε μεγάλα block (Όπως συμβαίνει με τους διακομιστές βάσης δεδομένων) και μερικά αρχεία μικρού μεγέθους, ο διαχειριστής μπορεί να δει αύξηση της ταχύτητας εάν δημιουργήσει το σύστημα αρχείων με μέγεθος block 8KB. Αυτές οι πληροφορίες αποθηκεύονται σε ειδικούς πίνακες σε όλο το σύστημα αρχείων και μπορούν να ανακτηθούν εάν είναι απαραίτητες για διαδικασίες ανάκτησης δεδομένων.

STORAGE SPACE MANAGMENT LAYER

Αυτό το επίπεδο διαχειρίζεται χιλιάδες μονάδες κατανομής παρούσες σε ένα σύστημα αρχείων, όπου η μονάδα κατανομής είναι το μικρότερο προσπελάσιμο κομμάτι των στοιχείων που το λειτουργικό σύστημα μπορεί να χειριστεί. Κοινά μεγέθη μονάδων κατανομής συστήματος αρχείων:

Hard Disk Size	FAT12	FAT16	FAT32	NTFS	Ext2
0 to 16MB	4,096 bytes	2,048 bytes	512 bytes	512 bytes	4,096 bytes
16 to 128MB	n/a	2,048 bytes	512 bytes	512 bytes	4,096 bytes
128 to 256MB	n/a	4,096 bytes	512 bytes	512 bytes	4,096 bytes
256 to 512MB	n/a	8,192 bytes	4,096 bytes	512 bytes	4,096 bytes
512 to 1,024MB	n/a	16,384 bytes	4,096 bytes	1,024 bytes	4,096 bytes
1,024 to 2,048MB	n/a	32,768 bytes	4,096 bytes	4,096 bytes	4,096 bytes
2,048 to 6,128MB	n/a	n/a	4,096 bytes	4,096 bytes	4,096 bytes

INFORMATION CLASSIFICATION KAI APPLICATION-LEVEL LAYERS

Αυτά είναι τα δύο πρώτα επίπεδα του μοντέλου αποθήκευσης συστημάτων αρχείων και αποτελούνται από καταλόγους και αρχεία. Αυτά τα layers είναι τα πιο γνωστά για τους χρήστες. Αρκετοί τύποι αρχείων είναι σημαντικοί για μια εγκληματολογική έρευνα για παράδειγμα οι εξής τύποι:

- Λειτουργικό σύστημα και αρχεία χρησιμότητας
- Αρχεία ρυθμίσεων λειτουργικού συστήματος
- Αρχεία εφαρμογών και υποστήριξης
- Αρχεία ρυθμίσεων εφαρμογής
- Αρχεία δεδομένων χρήστη

ΣΥΜΠΕΡΑΣΜΑΤΙΚΑ

Οι πληροφορίες αποθήκευσης του σκληρού δίσκου και του συστήματος αρχείων που παρουσιάζονται σε αυτό το κεφάλαιο απλά επιτρέπουν στον ερευνητή να φτάσει στο σημείο της ανάλυσης γρήγορα. Προβλήματα στο hardware θα παρουσιάζονται πάντα. Τα μέσα αποδείξεων θα αρνηθούν να αναγνωριστούν από το BIOS. Οι συσκευές SCSI δεν θα λειτουργήσουν πλήρως και τα λειτουργικά συστήματα δεν θα αναγνωρίσουν τα partitions που γνωρίζετε ότι υπάρχουν. Είναι πιο σημαντικό να γνωρίζεις τον τρόπο που οι σκληροί δίσκοι και τα αρχεία καταγραφής και αποθήκευσης δουλεύουν παρά πως δουλεύει ένα εμπορικό software έρευνας. Η αρχή είναι απλή: Όσο πιο εξοικειωμένοι είστε με το πώς λειτουργεί το σύστημα και τι μπορεί να πάει στραβά, τόσο πιο προετοιμασμένοι θα είστε να αντιμετωπίζετε απροσδόκητα ζητήματα και αποτυχίες.

ΕΡΩΤΗΣΕΙΣ

- Σε ένα σκληρό δίσκο ATA ένα partition δεν αναγνωρίζεται στον σταθμό εργασίας εγκληματολογικών στοιχείων και "τρέχει" linux. Ποια βήματα αντιμετώπισης προβλημάτων πρέπει να ληφθούν;
- Έχετε ξεκινήσει έναν εγκληματολογικό έλεγχο και ένας συνδεδεμένος σκληρός δίσκος SCSI δεν ανιχνεύετε. Πως θα επιλύσετε αυτό το πρόβλημα;
- Από την περιγραφή των επιπέδων του συστήματος αρχείων, ποια θα ήταν η διαδικασία για να προσδιορίσετε τον μη διατεθέντα χώρο σε έναν σκληρό δίσκο;

ΚΕΦΑΛΑΙΟ 8

ΤΕΧΝΙΚΕΣ ΑΝΑΛΥΣΗΣ ΔΕΔΟΜΕΝΩΝ

Εάν εστιάσετε στην εξαγωγή των δεδομένων πριν την ερμηνεία τους θα λάβετε πιθανόν μια πολύ πιο εμπεριστατωμένη και πλήρη εγκληματολογική ανάλυση. Μπορεί επίσης να εξοικονομήσετε χρόνο. Σε αυτό το κεφάλαιο, συζητούμε πώς να εντοπίσετε και να οργανώσετε όλα τα κομμάτια των μέσων πληροφορικής και να τα συναρμολογήσετε προτού ξεκινήσετε οποιαδήποτε ερμηνεία των περιεχομένων. Καλύπτουμε τα ακόλουθα θέματα:

- Ανάκτηση διπλής ή πανομοιότυπης ανάλυσης
- Ανάκτηση μιας εικόνας που έχει εγκριθεί για ανάλυση
- Ανάκτηση διαγραμμένων αρχείων
- Ανάκτηση χώρου που δεν έχει διατεθεί
- Δημιουργία,παράγωγη λίστας αρχείων
- Εκτέλεση αναζήτησης συμβολοσειρών (strings search)

ΠΡΟΕΤΟΙΜΑΣΙΑ ΓΙΑ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΗ ΑΝΑΛΥΣΗ

Παλαιότερα συζητήσαμε πως δημιουργείς αντίγραφα εγκληματολογικά και εγκεκριμένα αντίγραφα σκληρών δίσκων Και οι δυο τύποι αντιγράφων μπορεί να απαιτήσουν περαιτέρω προετοιμασία ώστε οι πληροφορίες που περιλαμβάνουν να είναι σε θέση να χρησιμοποιηθούν. Είτε αποθηκεύσεις το αντίγραφο είτε το αναλύσεις στη μητρική του μορφή εξαρτάται από πολλές παραμέτρους :

- Τη μεθοδολογία ανάλυσης
- Τη μορφή των αρχικών δεδομένων (υπάρχον σύστημα αρχείων ' τύπων αρχείων λιγο λιγότερο γνωστών)
- Την κατάσταση των αρχικών δεδομένων
- Εαν χρειάζεται να αξιολογήσεις το λειτουργικό περιβάλλον του χρήστη και την αρχική του κατάσταση

ΑΠΟΚΑΤΑΣΤΑΣΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΟΥ ΑΝΤΙΓΡΑΦΟΥ

Η αποκατάσταση μπορεί να αποτελέσει πρόκληση. Σιγουρευτείτε ότι έχετε ένα σκληρό δίσκο μεγαλύτερο από τον αρχικό. Είναι πιθανό να χρησιμοποιήσετε ίδιου μεγέθους άλλα τότε σιγουρευτείτε ότι ο δίσκος προέρχεται από τον ίδιο κατασκευαστή. Σε πολλές περιπτώσεις έχουμε αρχίσει αποκατάσταση μιας εικόνας σε έναν σκληρό δίσκο άλλου κατασκευαστή και καταλήξαμε με κάποιους τομείς λιγότερους,Αυτό συνήθως γίνεται λόγω διάφορων λεπτομερειών ή υλικών βλαβών. Όταν αποκαθίσταται ένας σκληρός είναι ζωτικής σημασίας ο δίσκος προορισμού να είναι εντελώς καθαρός, άδειος. Συζητήσαμε πως θα γίνει αυτό με Linux σε προηγούμενο κεφάλαιο. Μια δωρεάν dos εφαρμογή εκκαθάρισης σκληρών δίσκων μπορεί να βρεθεί στην ιστοσελίδα του Eraser.

ΑΠΟΚΑΤΑΣΤΑΣΗ ΑΝΤΙΓΡΑΦΟΥ ΣΕ ΣΚΛΗΡΟ ΔΙΣΚΟ 1/5

Σε προηγούμενο κεφάλαιο χρησιμοποιήσαμε την εφαρμογή dd για να φτιάξουμε αντίγραφο σκληρού δίσκου Το script που παρουσιάσαμε σχεδιάστηκε για να δημιουργήσει αντίγραφο εικόνας σκληρού δίσκου ο οποίος

έχει σπάσει σε πολλαπλά αρχεία Στο παρακάτω παράδειγμα τρέξαμε το script αντιγράφων στον ύποπτο σκληρό δίσκο. Στον ύποπτο σκληρό δόθηκε το όνομα */dev/Mode* by Linux.

```
[root@localhost evid]# sh /root/disk_dupe.sh
1000000+0 records in
1000000+0 records out
#1000000+0 records in
1000000+0 records out
#1000000+0 records in
1000000+0 records out
#1000000+0 records in
1000000+0 records out
#1000000+0 records in
1000000+0 records out
#1000000+0 records in
1000000+0 records out
#342840+0 records in
342840+0 records out
Done. Verify the image with md5sum.
```

ΑΠΟΚΑΤΑΣΤΑΣΗ ΑΝΤΙΓΡΑΦΟΥ ΣΕ ΣΚΛΗΡΟ ΔΙΣΚΟ 2/5

Με μια γρήγορη αξιολόγηση των καταγραφών in and out αποδεικνύει ότι δεν χάθηκαν τμήματα ούτε καταστράφηκαν Αυτό το script όταν χρησιμοποιήθηκε για ανάκτηση 6gb ύποπτου σκληροί δίσκου θα δημιουργούσε 6 αρχεία του 1gb και ένα 35mb.(ένας σκληρός 6gb είναι ακριβώς 6,495gb).

```
[root@localhost evid]# ls -al
total 6342848
drwxr-xr-x    2 root     root         4096 Apr  9 21:38 .
drwxr-xr-x    9 root     root         4096 Apr  9 18:18 ..
-rwxr-xr-x    1 root     root     1024000000 Apr  9 21:24 dd_Image.1
-rwxr-xr-x    1 root     root     1024000000 Apr  9 21:26 dd_Image.2
-rwxr-xr-x    1 root     root     1024000000 Apr  9 21:29 dd_Image.3
-rwxr-xr-x    1 root     root     1024000000 Apr  9 21:31 dd_Image.4
-rwxr-xr-x    1 root     root     1024000000 Apr  9 21:35 dd_Image.5
-rwxr-xr-x    1 root     root     1024000000 Apr  9 21:37 dd_Image.6
-rwxr-xr-x    1 root     root      351068160 Apr  9 21:39 dd_Image.7
```

Όταν ένα εγκληματολογικό αντίγραφο έχει δημιουργηθεί θα θέλεις να επιβεβαιώσεις ότι η αντιγραφή ήταν σωστή και ακριβής. Μπορείς να το κάνεις αυτό χρησιμοποιώντας την εντολή md5sum:
[root@localhost]# md5sum -b /dev/hde
b57be804f2fb945fba15d652c3770fd5 */dev/hde

ΑΠΟΚΑΤΑΣΤΑΣΗ ΑΝΤΙΓΡΑΦΟΥ ΣΕ ΣΚΛΗΡΟ ΔΙΣΚΟ 3/5

Στο προηγούμενο παράδειγμα χρησιμοποιήσαμε την εντολή cat για να επαναδημιουργήσουμε την εικόνα και να δώσουμε στο Md5sum δεδομένα. Η εντολή cat επίσης χρησιμοποιείται για να αποθηκεύσεις εγκληματολογικά αντίγραφα. Μπορείς να ενώσεις και πάλι τα τμήματα του αντιγράφου σε ένα αρχείο ή να το επαναφερεις σε ένα σκληρό δίσκο. Η παρακάτω εντολή θα ενώσει τα 7 τμήματα και θα δώσει ένα ενιαίο αρχείο που θα περιερχει το αντίγραφο.

```
[root@localhost evid]# cat dd_Image.1 dd_Image.2 dd_Image.3 dd_Image.4
dd_Image.5 dd_Image.6 dd_Image.7 > /mnt/ext2/dd_Image.full.bin
[root@localhost evid]# ls -al /mnt/ext2/dd_Image.full.bin
-rw-r--r-- 1 root root 6495068160 Apr 9 21:54
/mnt/ext2/dd_Image.full.bin
```

ΑΠΟΚΑΤΑΣΤΑΣΗ ΑΝΤΙΓΡΑΦΟΥ ΣΕ ΣΚΛΗΡΟ ΔΙΣΚΟ 4/5

Το αρχείο εγκληματολογικής εικόνας dd_Image.full.bin φαίνεται να είναι ένα αρχείο 6.495GB. Δημιουργία ενός MD5hash αυτού του αρχείου εξασφαλίζει ότι αυτό το αρχείο είναι ένα ακριβές αντίγραφο του αρχικού σκληρού δίσκου

```
[root@localhost evid]# md5sum -b /mnt/ext2/dd_Image.full.bin
b57be804f2fb945fba15d652c3770fd5 */mnt/ext2/dd_Image.full.bin
```

Η επαναφορά της εικόνας σε έναν νέο σκληρό δίσκο είναι παρόμοια. Σε αυτό το παράδειγμα, έχουμε συνδέσει έναν νέο, καθαρό σκληρό δίσκο 6GB στον εγκληματολογικό σταθμό εργασίας. Όταν εκκινήσαμε το Linux, του αποδόθηκε το όνομα της συσκευής / dev / hdg (μέχρι τώρα, θα έπρεπε να έχετε κλειδώσει τα αρχικά στοιχεία). Ως προφύλαξη, χρησιμοποιήστε την εντολή dmesg για να προσδιορίσετε τους σκληρούς δίσκους που είναι συνδεδεμένοι στο σταθμό εργασίας. Οι παρακάτω γραμμές είναι ένα απόσπασμα της εξόδου της εντολής dmesg:

```
 hda: 30015216 sectors (15368 MB) w/2048KiB Cache, CHS=1868/255/63, UDMA(100)
hdb: 78165360 sectors (40021 MB) w/2048KiB Cache, CHS=4865/255/63, UDMA(100)
hdg: 12685680 sectors (6495 MB) w/420KiB Cache, CHS=13424/15/63, UDMA(33)
```

ΑΠΟΚΑΤΑΣΤΑΣΗ ΑΝΤΙΓΡΑΦΟΥ ΣΕ ΣΚΛΗΡΟ ΔΙΣΚΟ 5/5

Μπορείτε να δείτε από αυτήν την έξοδο ότι το λειτουργικό σύστημα ανίχνευσε τρεις χωριστούς σκληρούς δίσκους IDE:

- / Dev / hda Αυτή η μονάδα φιλοξενεί το εγγενές λειτουργικό σύστημα για την εγκληματολογική έρευνα.
- / Dev / hdb Αυτή η μονάδα είναι μια μονάδα αποθήκευσης 40 GB για την αποθήκευση εγκληματολογικών εικόνων.
- / Dev / hdg Αυτή η μονάδα είναι η νέα μονάδα δίσκου, προετοιμασμένη για την αποκατάσταση.
- Είμαστε πλέον έτοιμοι να επαναφέρουμε την εγκληματολογική εικόνα στο νέο σκληρό δίσκο για ανάλυση. Χρησιμοποιήστε την εντολή cat για να συγκολλήσετε τα πολλαπλά τμήματα του ιατροδικαστικού διπλότυπου με το νέο σκληρό δίσκο.
- / dev / hdg. [root@localhost]# cat dd_Image.1 dd_Image.2 dd_Image.3 dd_Image.4
- dd_Image.5 dd_Image.6 dd_Image.7 > /dev/hdg

```
[root@localhost ]# md5sum -b /dev/hdg
b57be804f2fb945fba15d652c3770fd5 */dev/hdg
```

ΑΠΟΚΑΤΑΣΤΑΣΗ ΕΝΟΣ ΕΓΚΕΚΡΙΜΕΝΟΥ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΟΥ ΑΝΤΙΓΡΑΦΟΥ ΣΚΛΗΡΟΥ ΔΙΣΚΟΥ

Περιστασιακά θα χρειαστεί να αποκαταστήσετε ένα εγκεκριμένο αντίγραφο με σκοπό να κάνετε μια πιο πλήρη ανάλυση. Όταν ο σκληρός προέλευσης είναι κατεστραμμένος η έχει κάποιο περίεργο τύπο αρχείων η ακολουθία της εκλαΐκευσης δεν θα μπορέσει να ερμηνεύσει σωστά τα δεδομένα Σε κάποιες περιπτώσεις

ίσως χρειαστεί να εξασκήσετε τις κανονικότητες σας στην αποκατάσταση ώστε να μπορέσετε να ενώσετε ένα δύσμορφο διαχωρισμένο αρχείο εκκίνησης Το να γνωρίζεις τον τρόπο να μετατρέψεις τον ύποπτο σκληρό που είναι κλειδωμένος σε ένα σκληρό με το δικό του τύπο αρχείων σε μια μορφή με την οποία μπορείς να δουλέψεις είναι μια σημαντική ικανότητα. Πως συζητήσαμε στο προηγούμενο μέρος θα χρειαστείς ένα σκληρό καθαρό ίδιας ή μεγαλύτερης χωρητικότητας Και πάλι ο σκληρός προορισμού πρέπει να είναι απολυτά καθαρός από δεδομένα πριν αποθηκεύσετε οποιοδήποτε τύπο εγκληματολογικού αντιγράφου.

ΑΠΟΚΑΘΙΣΤΩΝΤΑΣ ΕΝΑ EnCase ΑΡΧΕΙΟ

Η αποκατάσταση ενός αρχείου αποδείξεων EnCase σε ένα καθαρό σκληρό δίσκο είναι αρκετά απλή. Δυστυχώς το EnCase δεν παρέχει τα μέσα για να μετατρέψεις την αρχική εικόνα σε ένα πραγματικό εγκληματολογικό αρχείο όπως θα δούμε σε κάποιες περιπτώσεις. Για να αρχίσει η διαδικασία αποκατάστασης θα χρειαστεί να δημιουργήσετε μια νέα υπόθεση .Διαλέξτε από το μενού Φάκελος/Νέο/Νέα υπόθεση. Μόλις η νέα υπόθεση έχει δημιουργηθεί μπορείς να προσθέσεις αποδεικτικά στοιχεία Επιλέγεις το πρώτο EnCase αποδεικτικό αρχείο του συνόλου αν έχετε ένα τμηματικό αρχείο εικόνας .Το Encase θα φορτώσει τα αποδεικτικά και θα αρχίσει να επικυρώνει τις αξίες hash ώστε να επιβεβαιώσει ότι οι πληροφορίες δεν έχουν αλλάξει από τότε που αποκτήθηκαν τα αποδεικτικά Στην αριστερή πλευρά της πλατφόρμας EnCase θα δείτε μια λίστα σκληρών δίσκων οι οποίοι έχουν προστεθεί στα αρχεία της υποθέσεως. Για αποκατάσταση ενός δίσκου πατήστε δεξί κλικ στο εικονίδιο. Αυτό θα προβάλλει μια λίστα των σκληρών που το Encase αναγνωρίζει σαν έγκυρους προορισμούς αποθήκευσης.

ΑΠΟΚΑΘΙΣΤΩΝΤΑΣ ΕΝΑΝ ΦΑΚΕΛΟ ΑΡΧΕΙΩΝ SAFEBACK

Αντίθετα από το EnCase,το SafeBack λειτουργεί εξ ολοκλήρου σε περιβάλλον DOS. Αυτή μάλιστα είναι μια καλύτερη περίπτωση από το να δουλεύεις σε windows. Αν αποθηκεύσεις ένα αντίγραφο σκληροί αποδείξεων με EnCase διατρεχεις τον κίνδυνο να αναγνωρίσει το λειτουργικό σύστημα την αποκατεστημένη εικόνα. Μόλις τα Windows αναγνωρίσουν ένα σωστό σύστημα αρχείων θα μετατρέψει τα αρχεία και τη δομή τους. Όταν αρχίσει η αποκατάσταση η εφαρμογή κάνει καλή δουλειά στο να κρατάει το χρήστη ενημερωμένο για την εξέλιξη. Αν προκύψουν σφάλματα το SafeBack θα κρατήσει καταγραφή στο φάκελο ελέγχου ο οποίος τυπικά δημιουργείται στο κατάλογο όπου το .exe βρίσκεται.

ΠΡΟΕΤΟΙΜΑΖΟΝΤΑΣ ΕΝΑ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΟ ΑΝΤΙΓΡΑΦΟ ΓΙΑ ΑΝΑΛΥΣΗ ΜΕ LINUX 1/3

Τα Linux είναι ένα ιδανικό περιβάλλον για εγκληματολογική ανάλυση. Έχουν την δυνατότητα να να ερμηνεύουν ένα τεράστιο αριθμό συστημάτων και τύπων διαχωρισμού σκληρών. Με σκοπό να εκμεταλλευτείτε όλες τς δυνατότητες που σας προσφέρουν θα πρέπει να ενεργοποιήσετε κάποιες επιλογές και να ανασυντάξετε τον πυρήνα. Ανακαλύψαμε ότι ο κορμός των πυρήνων RedHat αποτελεί μια καλή βάση πάνω στην οποία μπορεί να πραγματοποιηθεί ανάλυση. Επιπρόσθετα σε μια πλήρη εγκατάσταση RedHat των εκδόσεων 8 και 9 θα χρειαστείς μια σειρά εργαλείων τα οποία προέρχονται από την εγκληματολογική βάση της Nasa (Computer Crime Division). Έχουν τροποποιήσει τον πυρήνα και τον κωδικό εγκατάστασης του loopback για να επιτρέψουν στο σύστημα να αναγνωρίσει πολλαπλά χωρίσματα μέσα σε μια διπλή εικόνα-αντίγραφο. Αυτό θα σας επιτρέψει να αναλύσετε το διπλό αρχείο χωρίς να το επαναφέρετε σε άλλο σκληρό δίσκο.

ΠΡΟΕΤΟΙΜΑΖΟΝΤΑΣ ΕΝΑ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΟ ΑΝΤΙΓΡΑΦΟ ΓΙΑ ΑΝΑΛΥΣΗ ΜΕ LINUX 2/3

Η προσθήκη του κώδικα NASA στο σύστημά σας είναι μια διαδικασία τεσσάρων σταδίων. Για το τρίτο βήμα, έχετε μια επιλογή, ανάλογα με το επίπεδο άνεσης σας στη χειροκίνητη ανασύνταξη του kernel. Το λογισμικό μπορεί να κατεβαστεί από ftp://ftp.hq.nasa.gov/pub/ig/ccd/enhanced_loopback.

1. Δημιουργήστε ονόματα συσκευών για τις νέες συσκευές loopback(βρόγχος επιστροφής).
2. Προσθέστε το πακέτο loop-utils.
3. Επισκευάστε έναν υπάρχοντα πυρήνα ή χρησιμοποιήστε μια εκ των προτέρων συμπυκνωμένη έκδοση που παρέχεται από τη NASA.
4. Τροποποιήστε το boot εκκίνησης για να ενεργοποιήσετε τον νέο πυρήνα.

ΠΡΟΕΤΟΙΜΑΖΟΝΤΑΣ ΕΝΑ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΟ ΑΝΤΙΓΡΑΦΟ ΓΙΑ ΑΝΑΛΥΣΗ ΜΕ LINUX 3/3

Καταρχήν, δημιουργήστε τα ονόματα συσκευών για τις νέες συσκευές loopback εκτελώντας το script δημιουργίας που έχετε κατεβάσει.
[root@localhost]# sh ./ccreatedev start
Στη συνέχεια, εγκαταστήστε το RPM package loopback-utils. Αυτό το πακέτο περιέχει αντικαταστάσεις για το βοηθητικό πρόγραμμα losetup συστήματος και τρία νέα βοηθητικά προγράμματα, loimginfo, losetgeo και partinfo. Μπορείτε να επιβεβαιώσετε ότι το RPM του loop-utils έχει εγκατασταθεί σωστά εκτελώντας την εντολή losetup και αναζητώντας την επιλογή "-r read only". Στη συνέχεια, θα πρέπει να εγκαταστήσετε ένα νέο πυρήνα.

ΕΠΑΝΕΞΕΤΑΣΗ ΑΡΧΕΙΩΝ ΕΙΚΟΝΑΣ

Όταν εργάζεστε με το EnCase ή κάποιο εγκληματολογικό εργαλείο όπως το Forensic Tool, η διαδικασία δημιουργίας μιας νέας περίπτωσης και η συμπλήρωσή της με εγκληματολογικά διπλότυπα είναι αρκετά απλή. Μπορεί να συναντήσετε μερικές μικρές δυσκολίες όταν εισάγετε μια διαχωρισμένη εγκληματολογική διπλότυπη εικόνα. Σε αυτήν την ενότητα θα δείξουμε πώς να ξεκινήσουμε μια υπόθεση σε αυτά τα δύο περιβάλλοντα και να εισαγάγουμε το κατατετμημένο αντίγραφο για να προετοιμαστούμε για ανάλυση.

ΕΜΦΑΝΙΣΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΩΝ ΑΝΤΙΓΡΑΦΩΝ ΜΕ EnCase

Το EnCase, με την ισχυρή του σειρά από εργαλεία και την εύχρηστη διασύνδεση, είναι μια εύκολη μέθοδος για την αποκατάσταση και ανάλυση των αρχείων dd, των αρχείων SafeBack και φυσικά των αρχείων στοιχείων EnCase. Όταν αποκτήσετε για πρώτη φορά αρχεία αποδεικτικών στοιχείων στο EnCase, πρέπει να δημιουργήσετε μια νέα υπόθεση. Απλώς επιλέξτε Αρχείο | Νέα | Νέα υπόθεση. Το EnCase εμφανίζει το παράθυρο διαλόγου δημιουργία νέας υπόθεσης. Μόλις δημιουργήσετε μια νέα περίπτωση, μπορείτε να προσθέσετε αρχεία αποδεικτικών στοιχείων στην υπόθεση.

ΕΜΦΑΝΙΣΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΩΝ ΑΝΤΙΓΡΑΦΩΝ ΜΕ Forensic Tool

Το εργαλείο Forensic Toolkit από την AccessData είναι μια άλλη ισχυρή εφαρμογή που έχετε σαν εργαλείο. Οι διεργασίες εισαγωγής διεπαφών και αποδεικτικών στοιχείων είναι λίγο πιο περίπλοκες από το EnCase, ωστόσο, μπορεί να ξεπεράσει την απόδοση του EnCase όταν ασχολείται με αρχεία ηλεκτρονικού ταχυδρομείου και σύνθετες αναζητήσεις συμβολοσειρών. Για να ξεκινήσετε ένα session λειτουργίας, επιλέξτε την επιλογή "Έναρξη νέας υπόθεσης" από το παράθυρο διαλόγου που εμφανίζεται όταν ξεκινάτε την εφαρμογή.

ΕΜΦΑΝΙΣΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΩΝ ΑΝΤΙΓΡΑΦΩΝ ΜΕ Forensic Tool

Το εργαλείο Forensic Toolkit από την AccessData είναι μια άλλη ισχυρή εφαρμογή που έχετε σαν εργαλείο. Οι διεργασίες εισαγωγής διεπαφών και αποδεικτικών στοιχείων είναι λίγο πιο περίπλοκες από το EnCase, ωστόσο, μπορεί να ξεπεράσει την απόδοση του EnCase όταν ασχολείται με αρχεία ηλεκτρονικού ταχυδρομείου και σύνθετες αναζητήσεις συμβολοσειρών. Για να ξεκινήσετε ένα session λειτουργίας,

επιλέξτε την επιλογή "Έναρξη νέας υπόθεσης" από το παράθυρο διαλόγου που εμφανίζεται όταν ξεκινάτε την εφαρμογή.

ΜΕΤΑΤΡΟΠΗ ΕΝΟΣ ΕΞΕΙΔΙΚΕΥΜΕΝΟΥ ΑΝΤΙΓΡΑΦΟΥ ΣΕ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΟ ΑΝΤΙΓΡΑΦΟ

Τι συμβαίνει όταν έχετε συγκεντρώσει ένα εξειδικευμένο ιατροδικαστικό αντίγραφο και κάτι πάει στραβά; Το εγκληματολογικό Toolkit (FTK) θα μετατρέψει το εξειδικευμένο ιατροδικαστικό αντίγραφο που δημιουργήθηκε από το EnCase ή το SafeBack σε ένα πραγματικό αντίγραφο bit-to-bit του πρωτοτύπου. Το πακέτο λογισμικού FTK συνοδεύεται από ένα πρόγραμμα εξερευνητών που επιτρέπει σε έναν ερευνητή να φορτώνει γρήγορα και να εξετάζει διπλές εικόνες

ΑΝΑΚΤΗΣΗ ΔΙΕΓΡΑΜΜΕΝΩΝ ΑΡΧΕΙΩΝ ΣΕ WINDOWS

Υπάρχουν πολλές περιπτώσεις που θέλετε να ψάξετε τον μη διατεθέντα χώρο σε μια αποκατεστημένη εγκληματολογική εικόνα, προκειμένου να ξεδιαλύνετε ή να ανακτήσετε όσο το δυνατόν περισσότερα αρχεία. Σίγουρα θα θέλατε να ανακτήσετε οποιαδήποτε απόδειξη που είχε διαγραφεί από κακόβουλους χρήστες. Σε αυτή την ενότητα, εξετάζουμε τους διαφορετικούς τρόπους απόκτησης αρχείων τα οποία οι ύποπτοι πιστεύουν ότι δεν υπάρχουν πλέον. Αυτά τα διαγραμμένα αρχεία είναι συχνά αυτά που διαλύουν την έρευνά σας, έτσι οι τεχνικές σας για ανάκτηση δεδομένων πρέπει να είναι εξαιρετικές. Όπως ίσως γνωρίζετε, τα διαγραμμένα αρχεία δεν διαγράφονται πραγματικά, απλώς επισημαίνονται για διαγραφή. Για παράδειγμα, όταν ένα αρχείο ή ένας κατάλογος διαγράφεται από ένα σύστημα αρχείων FAT, το πρώτο γράμμα του αρχείου του έχει οριστεί στον χαρακτήρα sigma (Ó) ή, σε hex, 0xE5. Αυτό σημαίνει ότι αυτά τα αρχεία θα παραμείνουν άθικτα έως ότου τα νέα δεδομένα έχουν αντικαταστήσει τη φυσική περιοχή όπου βρίσκονται αυτά τα διαγραμμένα αρχεία που βρίσκονται στο σκληρό δίσκο. Τα ειδικά εργαλεία μπορούν να βρουν αυτά τα "άθικτα" διαγραμμένα αρχεία και να τα ανακτήσουν για έλεγχο.

WINDOWS-Based Tools ΓΙΑ ΑΝΑΚΤΗΣΗ ΑΡΧΕΙΩΝ ΣΕ ΣΥΣΤΗΜΑΤΑ ΑΡΧΕΙΩΝ FAT

Συνιστούμε τα εργαλεία EnCase και FTK για την ανάκτηση αρχείων σε συστήματα αρχείων FAT. Τόσο το EnCase όσο και το FTK έχουν ενσωματωμένη αυτή τη δυνατότητα και ανακτούν αυτόματα όλα τα αρχεία. Χρησιμοποιήσαμε τα παλιά βοηθήματα Norton Utilities και MS-Dos, αλλά η χρήση τους σπάνια είναι απαραίτητη, καθώς τα τρέχοντα εργαλεία είναι πολύ αποτελεσματικά. Ωστόσο, αν ενδιαφέρεστε, απλώς να βρείτε τον χαρακτήρα 0xe5 χρησιμοποιήστε ένα hex editor και ξαναχτίστε με το χέρι την αλυσίδα συμπλέγματος (Dir / FAT / raw clusters).

LINUX-Based Tools ΓΙΑ ΑΝΑΚΤΗΣΗ ΑΡΧΕΙΩΝ ΣΕ ΣΥΣΤΗΜΑΤΑ ΑΡΧΕΙΩΝ FAT

Για να είναι ένα λειτουργικό σύστημα χρήσιμο για έναν ερευνητή, πρέπει να παρέχει τουλάχιστον τις ακόλουθες δυνατότητες:

- Υποστηρίζει μια μεγάλη ποικιλία συστημάτων αρχείων, συμπεριλαμβανομένων των FAT12, FAT16, FAT32,NTFS, HPFS, Macintosh, OS / 2, EXT2, EXT3 και UFS (Solaris).
- Ανακτά το αρχείο και το μη εκχωρημένο χώρο. Ο ενισχυμένος πυρήνας loopback καθιστά εύκολο τον εντοπισμό του χαλαρού και μη κατανεμημένου χώρου κίνησης.
- Παρέχει δυνατότητες αναζήτησης λέξεων-κλειδιών.
- Εκτελεί όλες τις λειτουργίες σε κατάσταση μόνο ανάγνωσης στο επεξεργασμένο σύστημα αρχείων.
- Ο πυρήνας της NASA παρέχει επίσης την επιλογή μόνο για ανάγνωση στο losetup.
- Χειρίζεται συμπιεσμένες μονάδες δίσκου (Drvspace, Dblspace και Drvspace 3).
- Παρέχει εκτενή έλεγχο και καταγραφή όλων των εγκληματολογικών δραστηριοτήτων.
- Παρέχει επικύρωση δεδομένων και ακεραιότητα

ΠΙΘΑΝΟΤΗΤΕΣ ΑΝΑΚΤΗΣΗΣ ΑΡΧΕΙΩΝ 1/2

Κατά την έρευνα, οι δικηγόροι συχνά μας ρωτούν εάν θα μπορέσουμε να ανακτήσουμε συγκεκριμένα δεδομένα από έναν σκληρό δίσκο. Πάντα απαντάμε ότι "εξαρτάται", και ότι τα ακόλουθα είναι δυνητικοί παράγοντες που θα μπορούσαν να αντικαταστήσουν τα δεδομένα που επιθυμούμε να ανακτήσουμε:

- Δημιουργούνται νέα αρχεία στο partition.
- Τα υπάρχοντα αρχεία μεγαλώνουν.
- Στο partition έχει εγκατασταθεί νέο λογισμικό.
- Εάν το partition περιέχει κοινόχρηστο στοιχείο δικτύου, οι χρήστες δικτύου ενδέχεται να τροποποιήσουν εν αγνοία τους τον τόμο κατά την πρόσβαση σε κοινόχρηστα αρχεία
- Οι εφαρμογές που εκτελούνται στον υπολογιστή ενδέχεται να ενημερώσουν το partition.

ΠΙΘΑΝΟΤΗΤΕΣ ΑΝΑΚΤΗΣΗΣ ΑΡΧΕΙΩΝ 2/2

- Οι εφαρμογές που εκτελούνται στον υπολογιστή ενδέχεται να ενημερώσουν το partition.
- Εάν το partition αποθηκεύει τον κατάλογο% systemroot%, τα Windows ενδέχεται να τροποποιηθούν.
- Το partition για εσωτερικές εργασίες καθαρισμού.
- Εάν το διαμέρισμα περιέχει την προσωρινή μνήμη του προγράμματος περιήγησης στο Web, ενδέχεται να τροποποιηθεί όταν ξεκινήσει ένα πρόγραμμα περιήγησης.
- Η εκκίνηση / κλείσιμο του συστήματος, που περιλαμβάνει πολλά από τα παραπάνω στοιχεία, μπορεί επίσης να μειώσει την πιθανότητα ανάκτησης δεδομένων.

ΧΡΗΣΗ ΤΟΥ FATBACK ΓΙΑ ΑΝΑΚΤΗΣΗ ΑΡΧΕΙΩΝ

Η χρήση του FatBack για την ανάκτηση των διαγραμμένων αρχείων προσφέρει έναν εξαιρετικό τρόπο αποκατάστασης αρχείων σε συστήματα αρχείων FAT12, FAT16 και FAT32 από πλατφόρμα εγκληματολογίας Linux. Ορισμένα από τα χαρακτηριστικά του περιλαμβάνουν τα ακόλουθα:

- Υποστήριξη μεγάλου ονόματος αρχείου
- Επαναληπτική αναίρεση των καταλόγων
- Ανάκτηση αλυσίδας συμπλέγματος (cluster chain)
- Δυνατότητα εργασίας μέσα σε μεμονωμένα partition ή ολόκληρους δίσκους

ΧΡΗΣΗ ΤΟΥ TASK ΓΙΑ ΑΝΑΚΤΗΣΗ ΑΡΧΕΙΩΝ

Το task είναι ένα open source εργαλείο εγκληματολογικής ανάλυσης αρχείων που χρησιμοποιείται για την ανάλυση συστημάτων αρχείων Microsoft και Unix. Υποστηρίζει την προσπάθεια αποκατάστασης αρχείων από μια ποικιλία συστημάτων αρχείων, συμπεριλαμβανομένων των FAT, FAT12, FAT16, FAT32, FreeBSD, EXT2, EXT3, OpenBSD και UFS. Το Task λειτουργεί επίσης σε αρχεία δυαδικών εικόνων, εφόσον δεν υπάρχουν ενσωματωμένες τιμές ελέγχου αθροίσματος. Αυτό σημαίνει ότι το TASK δεν θα λειτουργεί επί του παρόντος σε αρχεία αποδεικτικών στοιχείων EnCase και σε αρχεία SafeBack. Το Task λειτουργεί με ένα μόνο partition. Επομένως, πρέπει να απεικονίσετε κάθε partition σε μια μονάδα δίσκου ξεχωριστά για να χρησιμοποιήσετε αυτό το εργαλείο. Χρησιμοποιώντας το TASK, ίσως μπορέσετε να ανακτήσετε τα αρχεία που διαγράφηκαν προηγουμένως στο δυαδικό αρχείο εικόνας που δημιούργησε η dd.

ΕΚΤΕΛΕΣΗ ΑΥΤΟΨΙΑΣ ΩΣ GUI ΓΙΑ ΑΝΑΚΤΗΣΗ ΑΡΧΕΙΩΝ

Ο Autopsy Forensic Browser είναι μια γραφική διεπαφή για τα βοηθητικά προγράμματα που βρέθηκαν στο TASK. Σας επιτρέπει να αναλύετε τα αρχεία που έχουν διατεθεί, τα αρχεία που έχουν διαγραφεί στο παρελθόν, τους καταλόγους, τις μονάδες δεδομένων και τα μεταδεδομένα ιατροδικαστικών εικόνων σε περιβάλλον μόνο για ανάγνωση. Η αυτοψία παρέχει ένα front-end GUI για τους ακόλουθους τύπους λειτουργιών:

- Ξεκινώντας αναζητήσεις συμβολοσειρών και κανονικών εκφράσεων.
- Ανάκτηση διαγραμμένου υλικού.
- Δημιουργία χρονικού πλαισίου συμβάντων, εξετάζοντας τις τροποποιημένες, προσβάσιμες και τροποποιημένες ώρες αρχείων.
- Εισαγάγετε βάσεις δεδομένων κατακερματισμού των αρχείων "γνωστών-καλών", ώστε να μπορείτε να πραγματοποιείτε αντισταθμίσεις κατακερματισμού με τα αρχεία αποδεικτικών στοιχείων.

ΧΡΗΣΗ FOREMOST ΓΙΑ ΑΝΑΚΤΗΣΗ ΧΑΜΕΝΩΝ ΑΡΧΕΙΩΝ

Το Foremost είναι ένα πρόγραμμα Linux που χρησιμοποιείται για την ανάκτηση ή την "εξόρυξη" αρχείων με βάση τις κεφαλίδες αρχείων και τα υποσέλιδα. (Στην πραγματικότητα, βρίσκει όλα τα αρχεία που έχουν τις κεφαλίδες και τα υποσέλιδα που καθορίζετε, ανεξάρτητα από το αν έχουν διαγραφεί ή όχι.). Είναι ένα πραγματικά εξαιρετικό, φορητό εργαλείο για ανάκτηση δεδομένων. Πρώτα διαβουλεύεται ένα αρχείο ρυθμίσεων κατά το χρόνο εκτέλεσης. Αυτό το αρχείο ρυθμίσεων καθορίζει τις κεφαλίδες και τα υποσέλιδα που ψάχνει το Foremost, ώστε να μπορείτε να επιλέξετε ποια θέλετε να αναζητήσετε απλά επεξεργάζοντας το αρχείο foremost.conf

ΑΝΑΚΤΗΣΗ ΔΙΕΓΡΑΜΜΕΝΩΝ ΑΡΧΕΙΩΝ ΑΠΟ ΣΥΣΤΗΜΑΤΑ UNIX

Η ανάκτηση αρχείων που έχουν διαγραφεί στο παρελθόν σε συστήματα Unix μπορεί να είναι μια μεγάλη πρόκληση. Δεδομένου ότι τα περισσότερα από τα αρχεία που προσπαθείτε να ανακτήσετε σε συστήματα Unix είναι αρχεία κειμένου, συνήθως μια αναζήτηση grepword παρέχει αρκετά αποτελέσματα για να αναθεωρήσετε τον διατεθέντα χώρο για να εντοπίσετε πιθανά αρχεία που μπορείτε να ανακτήσετε. Ωστόσο, μια τέτοια μεθοδολογία "κυνηγίου και συσσώρευσης" σε έναν σκληρό δίσκο για κομμάτια δεδομένων που περιβάλλουν τις λέξεις-κλειδιά σας είναι περισσότερο τέχνη παρά επιστήμη. Στις περισσότερες περιπτώσεις, τα αρχεία που βρίσκετε μέσω της αναζήτησης συμβολοσειρών αποθηκεύτηκαν σε ένα συνεχόμενο μπλοκ και η αποκατάσταση μπορεί να είναι απλή. Αλλά είναι πιθανό να υπάρχουν διαφορετικά κομμάτια του αρχείου διάσπαρτα χωρίς συνοχή σε ολόκληρο το partition. Ωστόσο, όταν δεν γνωρίζετε το περιεχόμενο του αρχείου που θέλετε να ανακτήσετε, η πολυπλοκότητα της ανάκτησης σας πιθανότατα θα αυξηθεί.

ΕΡΓΑΛΕΙΟ DEBUGFS ΓΙΑ ΑΝΑΚΤΗΣΗ ΕΝΟΣ ΑΡΧΕΙΟΥ

Το Debugfs είναι ένα πολύ ισχυρό εργαλείο στα χέρια του εξεταστή εγκληματολογίας υπολογιστών. Είναι ένα διαδραστικό εργαλείο εντοπισμού σφαλμάτων που χρησιμοποιείται για την εξέταση και την αλλαγή της κατάστασης των συστημάτων αρχείων ext2. Χρησιμοποιώντας το Debugfs εκτενώς, διαπιστώσαμε ότι αυτή τη στιγμή παρέχει το καλύτερο μέσο για την ανάκτηση αρχείων σε μέσα που χρησιμοποιούν το σύστημα αρχείων ext2.

UNALLOCATED SPACE, FREE SPACE, ΚΑΙ SLACK SPACE

Αφού πραγματοποιήσετε μια εγκληματολογική έρευνα μέσων και έχετε ανακτήσει τόσα πολλά αρχεία εξακολουθούν να υπάρχουν δεδομένα σχετικά με τα μέσα ενημέρωσης που θα θέλετε να επανεξετάσετε. Τα υπόλοιπα δεδομένα αποθηκεύονται σε slack space (χαλαρό χώρο), μη unallocated space (διατεθέντα χώρο) και free space (ελεύθερο χώρο). Για να καταλάβουμε τι είναι το slack space και το unallocated space, πρέπει

πρώτα να εξετάσουμε τι είναι μια μονάδα κατανομής(allocation unit) ή ένα (cluster) σύμπλεγμα. Τα λειτουργικά συστήματα οργανώνουν όλα τα δεδομένα που είναι αποθηκευμένα σε σκληρό δίσκο σε τμήματα που ονομάζονται allocation units (που ονομάζονται επίσης clusters). Για παράδειγμα, ένα λειτουργικό σύστημα που χρησιμοποιεί συστοιχίες 32K διαβάζει και γράφει δεδομένα από ένα σκληρό δίσκο 32K κάθε φορά. Δεν μπορεί να διαβάσει λιγότερο από 32K δεδομένα από έναν σκληρό δίσκο και δεν μπορεί να γράψει λιγότερο από 32K κάθε φορά στον σκληρό δίσκο. Ωστόσο πολύ λίγα αρχεία έχουν την ακριβή ποσότητα δεδομένων για να καταλάβουν ένα ολόκληρο σύμπλεγμα ή σύνολο συμπλεγμάτων.

ΝΟΜΙΚΗ ΧΡΗΣΗ SLACK SPACE ΚΑΙ UNALLOCATED SPACE

Μην εκπλαγείτε αν η επιβολή του νόμου σας παρέχει μέσα ενημέρωσης που περιέχουν ένα φάκελο για κάθε έναν από τους ακόλουθους τύπους δεδομένων:

- Όλα τα λογικά αρχεία
- Όλα τα ανακτημένα αρχεία
- Ένα μόνο αρχείο που περιέχει όλα τα δεδομένα που ανακτώνται από το slack space
- Ένα μόνο αρχείο που περιέχει όλα τα δεδομένα που ανακτώνται από τον unallocated space και το slack space
- Πολλοί οργανισμοί επιβολής του νόμου εξακολουθούν να χρησιμοποιούν εργαλεία γραμμής εντολών τα οποία διαμορφώνουν το slack και unallocated space.

ΔΗΜΙΟΥΡΓΙΑ ΚΑΤΑΛΟΓΩΝ ΑΡΧΕΙΩΝ

Ένα από τα πιο κρίσιμα βήματα, αν και συχνά παραβλέπετε κατά την ανάλυση του περιεχομένου ενός σκληρού δίσκου είναι η δημιουργία ενημερωτικών λιστών αρχείων. Αυτές οι λίστες αρχείων πρέπει να περιλαμβάνουν τις ακόλουθες πληροφορίες:

- Πλήρης διαδρομή κάθε αρχείου που βρέθηκε στα μέσα μαζικής ενημέρωσης.
- Τελευταία γραπτά και τροποποιημένα σήματα ώρας / ημερομηνίας για κάθε αρχείο.
- Δημιουργία χρόνου / ημερομηνίας σφραγίδων, αν υπάρχουν (τα Linux δεν διατηρούν Ώρα / ημερομηνία).
- Τελευταία σφραγίδα χρόνου / ημερομηνίας πρόσβασης.
- Λογικό μέγεθος κάθε αρχείου.
- Ένα hash MD5 από κάθε αρχείο

ΕΝΤΟΠΙΣΜΟΣ ΓΝΩΣΤΩΝ ΑΡΧΕΙΩΝ ΣΥΣΤΗΜΑΤΟΣ

Όπως αναφέρθηκε προηγουμένως, ένα μεγάλο μέρος των δεδομένων σε οποιονδήποτε σκληρό δίσκο αποτελείται από γνωστά αρχεία, όπως το λειτουργικό σύστημα και τα αρχεία εφαρμογών, τα οποία συνήθως δεν έχουν αποδεικτική αξία σε καμία περίπτωση. Ως εκ τούτου, σε μια συνετή προσπάθεια να μειωθεί ο αριθμός των αρχείων για επανεξέταση, είναι πολύ χρήσιμο για τον εντοπισμό και τον αποκλεισμό από την αναθεώρηση των γνωστών αρχείων λειτουργικού συστήματος. Μπορείτε να το κάνετε αυτό παίρνοντας τις τιμές κατακερματισμού τους(hash values). Οι δικαστικοί εξεταστές συγκρίνουν τις γνωστές τιμές hash με τις τιμές κατακερματισμού άγνωστων αρχείων στο κατασχεμένο σύστημα υπολογιστή. Όταν οι τιμές αυτές ταιριάζουν, ο εξεταστής μπορεί να πει, με βεβαιότητα, ότι τα άγνωστα αρχεία του κατασχεθέντος συστήματος έχουν πιστοποιηθεί και κατά συνέπεια δεν χρειάζεται να εξεταστούν. Μια άλλη ιδέα είναι να δημιουργήσετε δικά σας σύνολα κατακερματισμού χρησιμοποιώντας τη εντολή md5sum.

ΠΡΟΕΤΟΙΜΑΣΙΑ ΣΚΛΗΡΟΥ ΔΙΣΚΟΥ ΓΙΑ ΑΝΑΖΗΤΗΣΕΙΣ STRING 1/2

Υπάρχουν πολλές διαφορετικές προκλήσεις όταν εκτελείτε εγκληματολογική έρευνα σε σκληρό δίσκο. Ίσως η πιο κοινή πρόκληση είναι ότι υπάρχουν απλά πάρα πολλά δεδομένα για να επανεξετάσουμε σε κάθε σκληρό δίσκο, καθώς η χωρητικότητα αποθήκευσης των μονάδων δίσκου είναι συνήθως πάνω από 100GB. Επομένως, η μείωση της ποσότητας των δεδομένων που πρέπει να ελέγξετε κατά την ανάλυσή σας είναι κρίσιμη. Μια άλλη πρόκληση είναι πώς να ανακτήσετε τεράστια ποσά από unallocated και slack space. Για να ελαχιστοποιήσετε τα δεδομένα που χρειάζεται να ερευνήσετε πραγματοποιήστε αναζητήσεις string.

- Ωστόσο, για την κατάλληλη αναζήτηση συμβολοσειρών, πρέπει να ξεπεράσετε τις ακόλουθες προκλήσεις:

ΠΡΟΕΤΟΙΜΑΣΙΑ ΣΚΛΗΡΟΥ ΔΙΣΚΟΥ ΓΙΑ ΑΝΑΖΗΤΗΣΕΙΣ STRING 2/2

- Πολλές μορφές αρχείων αποτελούν εμπόδιο όταν προσπαθούμε να πραγματοποιήσουμε αναζητήσεις string στα περιεχόμενα ενός σκληρού δίσκου. Αρχεία όπως του Outlook, Windows αρχεία μητρώου, αρχεία καταγραφής συμβάντων, αρχεία ιστορικού προγράμματος περιήγησης και πολλά άλλα απαιτούν ειδικά εργαλεία για την ορθή εγκληματολογική ανάλυση.
- Πολλές μορφές συμπιεσμένων αρχείων καθιστούν την παραδοσιακή αναζήτηση συμβολοσειρών ατελέσφορη.
- Τα κρυπτογραφημένα αρχεία ή τα αρχεία που προστατεύονται με κωδικό πρόσβασης δεν μπορούν να ελεγχθούν μέχρι να αποκρυπτογραφηθούν.
- Επομένως, προτού να μπορέσετε να εκτελέσετε αποτελεσματικές, πλήρεις αναζητήσεις συμβολοσειρών, πρέπει να προσδιορίσετε όλα τα συμπιεσμένα,κρυπτογραφημένα αρχεία και να τα αποσυμπιέσετε.

ΣΥΜΠΕΡΑΣΜΑΤΙΚΑ

Η σωστή αποκατάσταση των εγκληματολογικών ερευνών και η επανεξέταση των εξειδικευμένων εγκληματολογικών αντιγράφων είναι τα βασικά βήματα που έχουν ληφθεί πριν από την αναθεώρηση του περιεχομένου ενός υπολογιστή. Κάθε φορά που εξετάζετε το περιεχόμενο ενός σκληρού δίσκου, θέλετε να είστε εμπεριστατωμένοι και να μην χάσετε κανένα σχετικό στοιχείο που μπορεί να είναι χρήσιμο ή να διακόψει την έρευνα σας. Ως εκ τούτου, συζητήσαμε πώς να συγκεντρώσουμε όλα τα δεδομένα που βρίσκονται στον σκληρό δίσκο πριν από την ανάλυση. Μπορείτε να ανατρέξετε σε λογικά αρχεία, να ανακτήσετε αρχεία που είχαν διαγραφεί στο παρελθόν αλλά εξακολουθούν να είναι άθικτα και να ελέγξετε το unallocated και slack space με τις ισχυρές αναζητήσεις λέξεων-κλειδιών. Όλα αυτά τα σύνολα δεξιοτήτων είναι πυλώνες στον τομέα της εγκληματολογίας υπολογιστών.

ΕΡΩΤΗΣΕΙΣ

- Ποιες είναι μερικές από τις εργασίες που πρέπει να εκτελέσετε σε ένα εγκληματολογικό αντίγραφο πριν από την αναζήτηση string σε ολόκληρο το περιεχόμενο του συνόλου δεδομένων;
- Ποιο είναι το πλεονέκτημα της χρήσης της δυνατότητας loopback του Linux και του ενισχυμένου kernel της NASA;
- Κατά την άποψή σας, είναι ευκολότερο να εκτελέσετε ιατροδικαστική ανάλυση ενός συστήματος των Windows ή ενός συστήματος Unix;

ΚΕΦΑΛΑΙΟ 9

ΕΞΕΡΕΥΝΩΝΤΑΣ ΤΑ ΣΥΣΤΗΜΑΤΑ WINDOWS

Όταν η αρχική ανταπόκρισή σας υποδεικνύει ότι απαιτείται περαιτέρω διερεύνηση, έχετε δύο επιλογές: Θα μπορούσατε να εκτελέσετε έρευνα στα ίδια τα μέσα ή θα μπορούσατε να δημιουργήσετε αντίγραφο των αποδεικτικών στοιχείων και να εκτελέσετε στη συνέχεια έρευνα στην εικόνα που δημιουργήσατε. Εάν επιλέξετε να ερευνήσετε τα ίδια τα δεδομένα χωρίς να δημιουργήσετε αντίγραφο, θα αλλάξετε τα πραγματικά στοιχεία και δεν θα έχετε μια βασική γραμμή για σύγκριση μετά από την παρέμβασή σας, καθώς τα βήματα που ακολουθήσατε για την έρευνά σας θα έχουν αλλάξει το σύστημα.

Για παράδειγμα, η απλή προβολή ενός αρχείου ή καταχώρησης καταλόγου στο σύστημα αποδείξεων προκαλεί την αλλαγή των πληροφοριών σχετικά με το σύστημα. Αλλά αυτές οι πληροφορίες θα μπορούσαν να αποτελέσουν το βασικό στοιχείο για τις κινήσεις που πραγματοποίησε ο ύποπτος σας. Επομένως προτείνουμε τη δημιουργία αντιγράφου ασφαλείας και έρευνα πάνω σε αυτό.

ΠΟΥ ΥΠΑΡΧΟΥΝ ΑΠΟΔΕΙΞΕΙΣ ΣΕ ΕΝΑ ΣΥΣΤΗΜΑ WINDOWS 1/2

Πριν ξεκινήσετε την έρευνα είναι σημαντικό να γνωρίζετε πού σκοπεύετε να αναζητήσετε τα αποδεικτικά στοιχεία. Η τοποθεσία εξαρτάται από τη συγκεκριμένη περίπτωση, αλλά σε γενικές γραμμές τα στοιχεία μπορούν να βρεθούν στους ακόλουθους τομείς :

- Ευμετάβλητα δεδομένα στον πυρήνα του συστήματος
- Κενούς χώρους που μπορείτε να λάβετε παλιότερα διαγραμμένα αρχεία που δεν μπορούν να ανακτηθούν.
- Ελεύθερους ή μη κατανεμημένους χώρους, όπου μπορείτε να αποκτήσετε αρχεία που διαγράφηκαν προηγουμένως, συμπεριλαμβανομένων των κατεστραμμένων ή απρόσιτων clusters.
- Στο λογικό σύστημα αρχείων.
- Στα αρχεία καταγραφής συμβάντων.

ΠΟΥ ΥΠΑΡΧΟΥΝ ΑΠΟΔΕΙΞΕΙΣ ΣΕ ΕΝΑ ΣΥΣΤΗΜΑ WINDOWS 2/2

- Στο μητρώο, το οποίο θα πρέπει να σκεφτείτε ως ένα τεράστιο αρχείο καταγραφής.
- Στα μητρώα εφαρμογών που δεν διαχειρίζεται η υπηρεσία καταγραφής συμβάντων των Windows.
- Τα αρχεία ανταλλαγής, τα οποία περιέχουν πληροφορίες που βρέθηκαν πρόσφατα στη RAM.
- Ειδικά αρχεία σε επίπεδο εφαρμογής, όπως αρχεία ιστορικού του Internet Explorer και την προσωρινή μνήμη των προγραμμάτων περιήγησης.
- Προσωρινά αρχεία που έχουν δημιουργηθεί από εφαρμογές.
- Στον κάδο ανακύκλωσης.
- Στην ουρά εκτύπωσης του εκτυπωτή.
- Απεσταλμένα ή ληφθέντα e-mail.

ΔΙΕΞΑΓΩΓΗ ΕΡΕΥΝΑΣ ΓΙΑ ΤΑ WINDOWS

Αφού εγκαταστήσετε το σταθμό εγκληματολογικής έρευνας με τα σωστά εργαλεία είστε έτοιμοι να διεξάγετε την έρευνα σας. Τα ακόλουθα βασικά ερευνητικά βήματα απαιτούνται για την επίσημη εξέταση ενός συστήματος- στόχου:

- Ελέγξτε όλα τα σχετικά αρχεία καταγραφής.
- Εκτελέστε αναζητήσεις λέξεων-κλειδιών.
- Ελέγξτε τα σχετικά αρχεία.
- Προσδιορίστε μη εξουσιοδοτημένους λογαριασμούς ή ομάδες χρηστών.
- Αναζητήστε ασυνήθιστα ή κρυμμένα αρχεία / καταλόγους.
- Ελέγξτε για μη εξουσιοδοτημένα σημεία πρόσβασης.
- Αναλύστε σχέσεις εμπιστοσύνης.
- Ελέγξτε τα αναγνωριστικά ασφαλείας.

ΑΝΑΣΚΟΠΗΣΗ ΟΛΩΝ ΤΩΝ ΣΧΕΤΙΚΩΝ ΑΡΧΕΙΩΝ ΚΑΤΑΓΡΑΦΗΣ

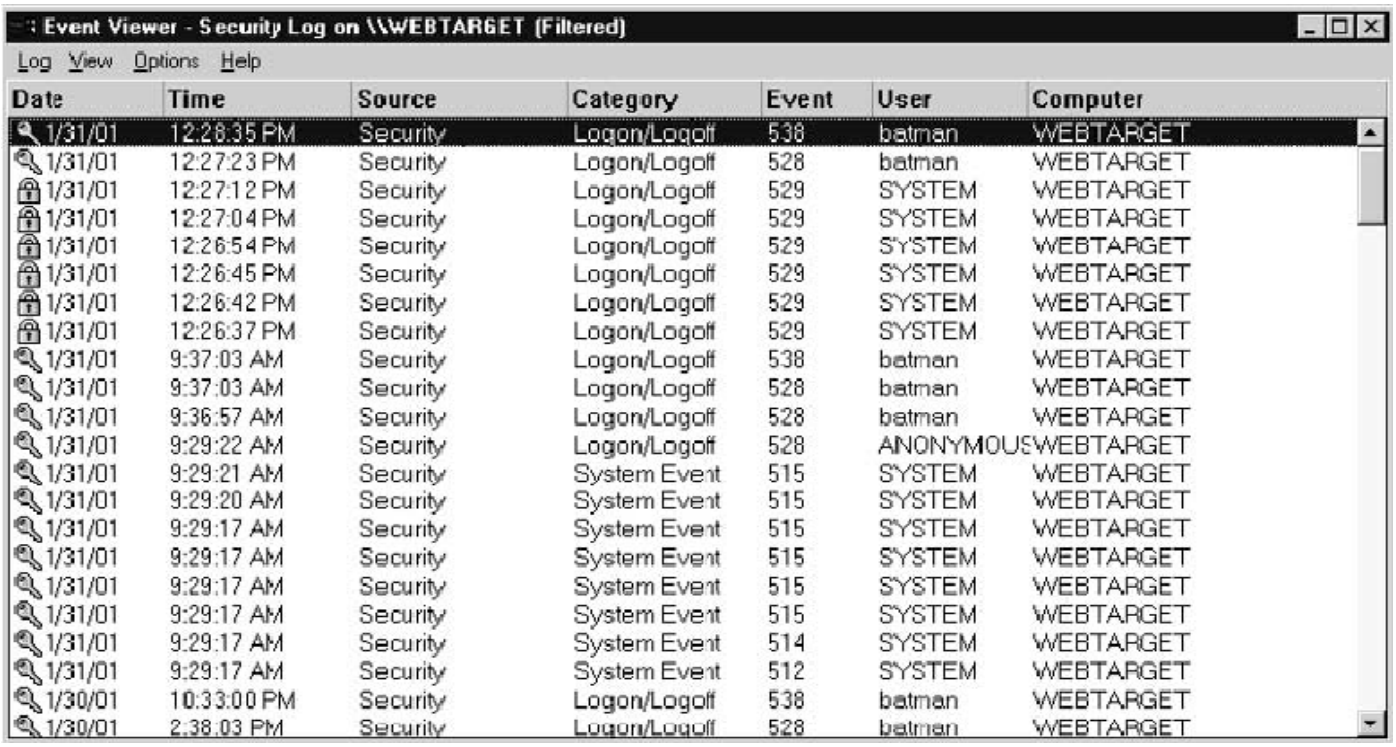
Τα λειτουργικά συστήματα Windows διατηρούν τρία χωριστά αρχεία καταγραφής: το Μητρώο συστήματος, Μητρώο εφαρμογών και Μητρώο ασφαλείας. Με τον έλεγχο αυτών των αρχείων καταγραφής, μπορεί να είστε σε θέση να λάβετε τις ακόλουθες πληροφορίες:

- Τους χρήστες που έχουν πρόσβαση σε συγκεκριμένα αρχεία
- Ποιος έχει συνδεθεί επιτυχώς σε ένα σύστημα
- Ποιος προσπαθούσε ανεπιτυχώς να συνδεθεί σε ένα σύστημα
- Τη χρήση συγκεκριμένων εφαρμογών
- Αλλαγές στην πολιτική ελέγχου
- Αλλαγές στα δικαιώματα χρήστη (όπως αυξημένη πρόσβαση)

LIVE ΚΑΤΑΓΡΑΦΕΣ ΣΕ ΕΝΑ ΣΥΣΤΗΜΑ

Τα Windows παρέχουν ένα βοηθητικό πρόγραμμα που ονομάζεται πρόγραμμα προβολής συμβάντων(event viewer) για πρόσβαση στα αρχεία καταγραφής ελέγχου σε έναν τοπικό κεντρικό υπολογιστή. Επιλέξτε Έναρξη | Προγράμματα | Εργαλεία διαχείρισης Πρόγραμμα προβολής συμβάντων για να ανοίξετε το Πρόγραμμα προβολής συμβάντων. Στο πρόγραμμα προβολής συμβάντων, επιλέξτε το αρχείο καταγραφής που θέλετε να προβάλετε από το μενού Καταγραφή. Οι ερευνητές ενδιαφέρονται περισσότερο για τα αναγνωριστικά ID στη στήλη συμβάντος καθώς κάθε ID αντιπροσωπεύει ένα συγκεκριμένο συμβάν. Οι διαχειριστές του συστήματος είναι έμπειροι και εξοικειωμένοι με τα συμβάντα των αναγνωριστικών ID.

ΠΑΡΑΔΕΙΓΜΑ ΤΟΥ EVENT VIEWER



ΠΑΡΑΔΕΙΓΜΑ ΣΥΜΒΑΝΤΩΝ ΑΝΑΓΝΩΡΙΣΤΙΚΩΝ ID

ID	Description
516	Some audit event records discarded
517	Audit log cleared
528	Successful logon
529	Failed logon
531	Failed logon, locked
538	Successful logoff
576	Assignment and use of rights

OFFLINE ΔΙΕΡΕΥΝΗΣΗ ΑΡΧΕΙΩΝ ΚΑΤΑΓΡΑΦΗΣ 1/2

Για να προβάλετε τα αρχεία καταγραφής συμβάντων από ένα σύστημα χωρίς σύνδεση, πρέπει να λάβετε αντίγραφα του αρχείου secevent.evt, Appevent.evt και sysevent.evt. Αυτά τα αρχεία καταγραφής είναι συνήθως αποθηκεύονται στην προεπιλεγμένη θέση του \% systemroot% \ System32 \ Config. Μπορείτε να αποκτήσετε αυτά τα αρχεία μέσω DOS ή Linux boot disk. Αφού ανακτήσετε τα τρία αρχεία .evt, μπορείτε να τα δείτε. Στο πρόγραμμα προβολής συμβάντων, επιλέξτε Σύνδεση | Ανοίξτε και καθορίστε τη διαδρομή

προς τα αντιγραμμένα αρχεία .evt. Επιλέγετε τον τύπο αρχείου καταγραφής (Ασφάλεια, εφαρμογή ή Σύστημα) κατά την επιλογή του αρχείου .evt και στη συνέχεια ελέγχετε. Είναι πιθανόν βέβαια ο σταθμός εγκληματολογικής έρευνας που έχετε να μην μπορεί να διαβάσει τα αρχεία αυτά αλλά αυτό συμβαίνει σπάνια. Σε αυτήν την περίπτωση, εκτελέστε τα παρακάτω βήματα για να αποκτήσετε πρόσβαση στα αρχεία καταγραφής:

OFFLINE ΔΙΕΡΕΥΝΗΣΗ ΑΡΧΕΙΩΝ ΚΑΤΑΓΡΑΦΗΣ 2/2

- Απενεργοποιήστε την υπηρεσία EventLog στον εγκληματολογικό σταθμό ανοίγοντας τον πίνακα ελέγχου | Υπηρεσίες και επιλέξτε Απενεργοποίηση για την επιλογή EventLog (Αυτή η αλλαγή δεν θα είναι αποτελεσματική έως ότου επανεκκινήσετε τον σταθμό εργασίας).
- Χρησιμοποιήστε τη Διαχείριση χρηστών για να αλλάξετε την πολιτική ελέγχου του εγκληματολογικού σταθμού για να μην καταγράψετε τίποτα.
- Επανεκκινήστε τον εγκληματολογικό σταθμό εργασίας και στη συνέχεια βεβαιωθείτε ότι η υπηρεσία EventLog δεν είναι ενεργοποιημένη.
- Εφόσον το πρόγραμμα προβολής συμβάντων προεπιλεγεί αυτόματα για τη συγκέντρωση των τριών αρχείων .evt στο \% systemroot% \ System32 \ Config, θα πρέπει είτε να τα μετονομάσετε είτε να τα αντιγράψετε στο σύστημα που χρησιμοποιείτε.
- Εκκινήστε από τον Πίνακα ελέγχου χειροκίνητα την υπηρεσία EventLog.
- Τέλος εκκινήστε το Πρόγραμμα προβολής συμβάντων.

ΑΔΥΝΑΜΙΑ ΚΑΤΑΓΡΑΦΗΣ ΣΥΜΒΑΝΤΩΝ 1/2

Οι προεπιλεγμένες ρυθμίσεις καταγραφής συμβάντων ασφαλείας για τα Windows δεν καταγράφουν τίποτα. Αυτό σημαίνει ότι, από προεπιλογή, τα συστήματα των Windows δεν καταγράφουν επιτυχείς συνδέσεις, πρόσβαση σε αρχεία, τερματισμούς λειτουργίας και πολλά άλλα σημαντικά γεγονότα. Αυτό μπορεί να αποτελέσει πρόκληση για τη διερεύνηση των συστημάτων των Windows. Μία από τις δυσκολίες στην καταγραφή των Windows είναι ότι το Πρόγραμμα προβολής συμβάντων σάς επιτρέπει να βλέπετε μόνο μία εγγραφή κάθε φορά. Αυτό συχνά κάνει τον έλεγχο των αρχείων καταγραφής των Windows χρονοβόρο και δύσκολο. Ένα άλλο πιο περίπλοκο και σοβαρό μειονέκτημα είναι ότι αυτά τα αρχεία καταγραφής καταγράφουν μόνο το όνομα του πηγαίου NetBIOS και όχι τη διεύθυνση IP του απομακρυσμένου συστήματος. Αυτό καθιστά δύσκολο τον εντοπισμό των απομακρυσμένων συνδέσεων σε συστήματα Windows και αδύνατο μόνο με χρήση αρχείων καταγραφής συμβάντων.

ΑΔΥΝΑΜΙΑ ΚΑΤΑΓΡΑΦΗΣ ΣΥΜΒΑΝΤΩΝ 2/2

Οι προεπιλεγμένες ρυθμίσεις για τα αρχεία καταγραφής συμβάντων των Windows περιορίζουν κάθε αρχείο καταγραφής σε μέγιστο μέγεθος 512KB και ένα χρονικό διάστημα επτά ημερών. Όταν φτάσει αυτό το σταθερό μέγεθος, το αρχείο καταγραφής κλείνει και πρέπει να διαγραφεί πριν μπορέσετε να συνδεθείτε ξανά στο συγκεκριμένο αρχείο καταγραφής. Μπορείτε να αλλάξετε αυτές τις επιλογές στο μενού ρυθμίσεις καταγραφής, αλλά να θυμάστε ότι το μέγεθος και το χρονικό μήκος κάθε καταγραφής (Ασφάλεια, Εφαρμογή και Σύστημα) πρέπει να ρυθμιστεί ξεχωριστά.

ΚΑΤΑΓΡΑΦΗ Internet Information Services (IIS)

Εάν διερευνάτε ένα διακομιστή των Windows που εκτελεί τις υπηρεσίες Internet Information Services (IIS), θα χρειαστεί να ελέγξετε τα αρχεία καταγραφής για κάθε υπηρεσία IIS, ειδικά τον web server. Αυτά τα Τα αρχεία καταγραφής βρίσκονται συνήθως στον κατάλογο \% systemroot% \ System32 \ LogFiles, στους αντίστοιχους υποκαταλόγους κάθε υπηρεσίας. Για το IIS το προεπιλεγμένο όνομα αρχείου καταγραφής βασίζεται στην τρέχουσα ημερομηνία, στη μορφή exyymmdd.log. Ένα νέο αρχείο καταγραφής δημιουργείται κάθε μέρα. Η προεπιλεγμένη μορφή για τα αρχεία καταγραφής IIS είναι η εκτεταμένη μορφή

αρχείου καταγραφής W3C (World Wide Web Consortium), μια τυποποιημένη μορφή που ερμηνεύουν και αναλύουν πολλά βοηθητικά προγράμματα άλλων κατασκευαστών. Άλλες διαθέσιμες μορφές περιλαμβάνουν καταγραφή IIS, η οποία παρέχει σταθερή μορφή ASCII και το ODBC (Open Database Connectivity) καταγράφει τα Windows συστήματα, τα οποία στέλνουν μια σταθερή μορφή σε μια καθορισμένη βάση δεδομένων.

ΑΝΑΖΗΤΗΣΗ ΜΕ ΛΕΞΕΙΣ-ΚΛΕΙΔΙΑ

Κατά τη διάρκεια ερευνών σχετικά με την κατοχή πνευματικής ιδιοκτησίας ή πληροφοριών ιδιοκτησίας, σεξουαλικά αδικήματα και πρακτικά σε οποιαδήποτε περίπτωση που αφορά την επικοινωνία μέσω κειμένου, είναι σημαντικό να πραγματοποιήσετε αναζητήσεις συμβολοσειρών (string search) στο σκληρό δίσκο του ατόμου. Πολλές διαφορετικές λέξεις-κλειδιά μπορούν να είναι σημαντικές για μια έρευνα, συμπεριλαμβανομένων των ID των χρηστών, των κωδικών πρόσβασης, των ευαίσθητων δεδομένων, των γνωστών ονομάτων αρχείων και των ειδικών όρων (για παράδειγμα η λέξη μαριχουάνα ή ναρκωτικά). Οι αναζητήσεις συμβολοσειρών μπορούν να πραγματοποιηθούν στη λογική δομή του αρχείου ή σε φυσικό επίπεδο για να εξεταστούν τα περιεχόμενα μιας ολόκληρης μονάδας δίσκου. Τα περισσότερα εργαλεία αναζήτησης δίσκου που κυκλοφορούν στο εμπόριο ως λογισμικό εγκληματολογίας εκτελούν απλές αναζητήσεις, διεξάγοντας αναζήτηση των φυσικών επιπέδων της μονάδας δίσκου. Αυτοί οι τύποι εργαλείων απαιτούν την εκκίνηση του συστήματος-στόχου από μια ελεγχόμενη δισκέτα εκκίνησης ή άλλο μέσο (καθώς δεν μπορούν να εκτελεστούν από ενεργούς σκληρούς δίσκους) η χρήση αυτού τέτοιου εργαλείου γίνεται επειδή δεν μπορείτε να διαβάσετε φυσικά μια μονάδα που εκτελεί λειτουργικό σύστημα Windows.

ΑΝΑΣΚΟΠΗΣΗ ΣΧΕΤΙΚΩΝ ΑΡΧΕΙΩΝ

Ο καθορισμός των αρχείων που περιέχουν αποδείξεις επίθεσης ή κατάχρησης στα συστήματα των Windows μπορεί να είναι ένα δύσκολο, συναρπαστικό και αποθαρρυντικό έργο. Υπάρχει συνήθως κάποιο ίχνος ανίχνευσης κάπου στο σύστημα που βοηθά να επιβεβαιώσετε ή να διαλύσετε τις υποψίες σας. Τα συστήματα Windows γράφουν input και output σε τόσα πολλά αρχεία τη φορά που σχεδόν όλες οι ενέργειες που έγιναν στο σύστημα αφήνουν κάποιο ίχνος της εμφάνισής τους. Τα Windows διαθέτουν προσωρινά αρχεία προσωρινής αποθήκευσης, αρχεία προσωρινής μνήμης, μητρώο που παρακολουθεί τα πρόσφατα χρησιμοποιημένα αρχεία, έναν Κάδο Ανακύκλωσης που διατηρεί τα διαγραμμένα αρχεία και αμέτρητες άλλες τοποθεσίες όπου αποθηκεύονται δεδομένα χρόνου εκτέλεσης. Είναι σημαντικό να αναγνωρίζετε τα αρχεία από τις επεκτάσεις τους καθώς και από τις αληθινές επικεφαλίδες αρχείων τους (αν είναι δυνατόν). Τουλάχιστον, πρέπει να ξέρετε τι αρχεία είναι τα .doc, .tmp, .log, .txt, .wpd, .gif, .exe και .jpg.

ΧΡΟΝΟΣ ΚΑΙ ΩΡΑ ΣΥΜΒΑΝΤΟΣ/ΣΦΡΑΓΙΔΕΣ ΗΜΕΡΟΜΗΝΙΑΣ

Ο στόχος για έναν ερευνητή είναι να γνωρίζει ποια αρχεία μπορεί να είναι σχετικά με το τρέχον περιστατικό. Ο πιο συνηθισμένος τρόπος με τον οποίο επιτυγχάνεται αυτό είναι ο καθορισμός του χρονικού πλαισίου στο οποίο συνέβη το περιστατικό και στη συνέχεια ο έλεγχος αυτών των αρχείων που δημιουργήθηκαν, τροποποιήθηκαν ή προσεγγίστηκαν κατά τη διάρκεια αυτού του χρονικού πλαισίου. Τα αρχεία που "πειράχτηκαν" κατά τη διάρκεια του σχετικού χρονικού πλαισίου παρέχουν τις πληροφορίες που απαιτούνται για να καθορίσετε ποια αρχεία έχουν κλαπεί, εκτελεστεί, αφαιρεθεί (εάν τοποθετήθηκαν στον Κάδο Ανακύκλωσης) ή φορτώθηκαν σε ένα σύστημα. Θα χρειαστεί να καθαρίσετε τα αρχεία καταγραφής που βασίζονται στο δίκτυο ή να χρησιμοποιήσετε προφορική μαρτυρία για να προσδιορίσετε μια χρονική περίοδο που έχει συμβεί κάποιο περιστατικό. Τα αρχεία που τροποποιήθηκαν, δημιουργήθηκαν ή άλλαξαν κατά τη διάρκεια της ύπαρξης του ύποπτου συμβάντος μπορούν να θεωρηθούν σχετικά αρχεία. Όπως έχουμε ξανά αναφέρει μπορείτε να το χρησιμοποιήσετε την εντολή dir για να πάρετε μια λίστα καταλόγου που περιλαμβάνει την ημερομηνία πρόσβασης σε αρχεία, την τροποποίηση και τη δημιουργία τους

ΙΔΙΩΤΙΚΑ ΑΡΧΕΙΑ E-MAIL

Τα e-mail είναι συχνά τρόπος επικοινωνίας των υπόπτων που ερευνούμε. Οι πιο συνηθισμένοι clients ηλεκτρονικού ταχυδρομείου όπως είναι το Outlook έχουν το δικιά τους μορφή. Κατά την εξέταση του ηλεκτρονικού ταχυδρομείου που αποστέλλεται ή λαμβάνεται από έναν ύποπτο, πρέπει να χρησιμοποιήσετε το κατάλληλο software client για να δείτε το μήνυμα ηλεκτρονικού ταχυδρομείου του ύποπτου. Με άλλα λόγια θα πρέπει να αντιγράψετε τα ιδιωτικά αρχεία που έχουν ανακτηθεί και να τα ανοίξετε με το κατάλληλο λογισμικό. Διαφορετικά, θα εξετάσετε το μήνυμα ηλεκτρονικού ταχυδρομείου με ένα πρόγραμμα επεξεργασίας κειμένου, το οποίο δεν πρόκειται να δώσει ολοκληρωμένο και ακριβές συμπέρασμα.

ΔΙΑΓΡΑΜΜΕΝΑ ΑΡΧΕΙΑ ΚΑΙ ΔΕΔΟΜΕΝΑ

Υπάρχουν πολλές περιπτώσεις που η απόκριση περιστατικών απαιτεί την ανάκτηση χαμένων αρχείων που θα μπορούσαν να έχουν διαγραφεί από κακόβουλους χρήστες για να προκαλέσουν ζημιά. Σε αυτή την ενότητα, εξετάζουμε τους διαφορετικούς τρόπους απόκτησης αρχείων τα οποία οι ύποπτοι πιστεύουν ότι δεν υπάρχουν πλέον. Σε γενικές γραμμές, υπάρχουν τέσσερις τρόποι ανάκτησης των διαγραμμένων δεδομένων:

- Χρησιμοποιώντας εργαλεία αναίρεσης
- Επαναφορά αρχείων που βρίσκονται στον Κάδο Ανακύκλωσης
- Ανάκτηση αρχείων .tmp.
- Χρησιμοποιώντας εργαλεία low-level για την επιδιόρθωση του συστήματος αρχείων.

ΜΗΤΡΩΟ WINDOWS (REGISTRY)

Το μητρώο των Windows είναι μια συλλογή αρχείων που αποθηκεύει δεδομένα ζωτικής σημασίας για τη διαμόρφωση του συστήματος. Το λειτουργικό σύστημα χρησιμοποιεί το μητρώο για να αποθηκεύει πληροφορίες σχετικά με το hardware, το software και τα στοιχεία ενός συστήματος. Μπορείτε να σκεφτείτε το μητρώο ως αρχείο καταγραφής που φιλοξενεί πολλά δεδομένα που είναι χρήσιμα στους ερευνητές. Το μητρώο μπορεί να αποκαλύψει το λογισμικό που εγκαταστάθηκε στο παρελθόν, τις ρυθμίσεις παραμέτρων ασφαλείας του μηχανήματος, τα trojans της DLL, τα προγράμματα εκκίνησης και τα πιο πρόσφατα χρησιμοποιούμενα (MRU) αρχεία για πολλές διαφορετικές εφαρμογές. Το μητρώο αποτελείται από πέντε root keys (που αποκαλούνται κυψέλες):

ΜΗΤΡΩΟ WINDOWS (REGISTRY)-ROOT KEYS

HKEY_CLASSES_ROOT

- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE (συντομογραφία HKLM)
- HKEY_USERS
- HKEY_CURRENT_CONFIG
- Οι πέντε κυψέλες κατασκευάζονται από τέσσερα μεγάλα αρχεία του συστήματος: SAM, SECURITY, SOFTWARE και SYSTEM. Η προεπιλεγμένη θέση για αυτά τα αρχεία είναι το αρχείο \ WINNT \ System32 \Config directory. Αναζητήστε τα αρχεία ασφαλείας του μητρώου του συστήματος σας, καθώς τα αντίγραφα ασφαλείας του μητρώου μπορούν να χρησιμοποιηθούν για την ανίχνευση της εγκατάστασης και της απεγκατάστασης διάφορων εφαρμογών

ΑΡΧΕΙΟ ΑΝΤΑΛΛΑΓΗΣ (swap file)

Το αρχείο ανταλλαγής είναι ένα κρυφό αρχείο συστήματος που χρησιμοποιείται για εικονική μνήμη. Όταν το σύστημα είναι πολύ απασχολημένο το swap file χρησιμοποιείται για να λειτουργήσει προσωρινά ως

μνήμη RAM. Το λειτουργικό σύστημα θα ανταλλάξει τα λιγότερο χρησιμοποιούμενα τμήματα της RAM για να ελευθερώσει χώρο για ενεργές εφαρμογές. Το αρχείο ανταλλαγής είναι συνήθως περίπου διπλάσιο από τη ποσότητα της RAM σε ένα σύστημα. Τα κομμάτια μνήμης που ανταλλάσσονται στο swap file του σκληρού δίσκου ονομάζονται σελίδες. Το swap file μπορεί να περιέχει αποσπάσματα κειμένου από έγγραφα, κωδικούς πρόσβασης και άλλα στοιχεία πληροφοριών που ο χρήστης έχει δει πρόσφατα ή έχει δακτυλογραφήσει στο σύστημά του. Το κλειδί είναι ότι ο χρήστης μπορεί να μην συνειδητοποιήσει ότι τα δεδομένα υπάρχουν. Τα αρχεία ανταλλαγής στα συστήματα των Windows ονομάζονται pagefile.sys. Δεδομένου ότι το swap file είναι ένα κρυφό αρχείο συστήματος, πρέπει πρώτα να επιτρέψετε την εμφάνιση κρυφών αρχείων στο σύστημά σας. Μπορείτε να χρησιμοποιήσετε το dir / ah στη γραμμή εντολών ή μπορείτε να ρυθμίσετε την Εξερεύνηση των Windows για να προβάλετε κρυφά αρχεία επιλέγοντας Εργαλεία | Επιλογές φακέλων και επιλέξτε την επιλογή Εμφάνιση κρυφών αρχείων και φακέλων. Αυτό θα σας επιτρέψει να δείτε ανενεργά αρχεία ανταλλαγής.

BROKEN LINKS

Ένα άλλο σημαντικό βήμα είναι να ελέγξετε αν υπάρχουν συνδέσεις (links) που προδίδουν κάτι στο σύστημα. Συζητήσαμε ήδη τη χρήση του μητρώου για να προσδιορίσουμε το λογισμικό που είναι εγκατεστημένο σε ένα σύστημα και ίσως έτσι βρήκαμε στοιχεία εφαρμογών που καταργήθηκαν εσφαλμένα. Ο έλεγχος συνδέσμων μπορεί επίσης να σας βοηθήσει να προσδιορίσετε ποιο λογισμικό είχε υπάρξει σε ένα σύστημα. Οι συνδέσεις χρησιμοποιούνται για τη συσχέτιση μιας συντόμευσης επιφάνειας εργασίας ή ενός στοιχείου του μενού Έναρξη με μια εφαρμογή ή ένα έγγραφο. Η χειροκίνητη κατάργηση των εφαρμογών ή εγγράφων δεν αφαιρεί τις συνδέσεις (links) που δημιουργήθηκαν. Οι χρήστες μπορούν να διαγράψουν αρχεία αλλά να ξεχάσουν να διαγράψουν το εικονίδιο της επιφάνειας εργασίας στο σύστημα. Το εργαλείο NTRK chklnks.exe είναι εξαιρετικό για την ανίχνευση αρχείων που ήταν εγκατεστημένα αλλά τώρα δεν βρίσκονται πουθενά. Τα links είναι επίσης σημαντικά όταν εξετάζετε συνδέσεις που πραγματοποιήθηκαν στο δίκτυο και τι συντομεύσεις δημιούργησαν.

ΑΡΧΕΙΑ ΠΕΡΙΗΓΗΣΗΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Όσοι εργάζονται σε εταιρίες χρειάζονται εγκεκριμένη πρόσβαση για χρήση του διαδικτύου αλλά οι εργοδότες δεν επιθυμούν οι εργαζόμενοί τους να ξοδεύουν τις ώρες εργασίας του στο Internet. Το μεγαλύτερο ποσοστό εργαζομένων χρησιμοποιεί το διαδίκτυο για ψώνια,surfing, συνομιλία ή ακόμα και για λήψη πορνογραφικού υλικού. Αυτές οι δραστηριότητες απαιτούν τη χρήση περιηγητών ιστού. Τα προγράμματα περιήγησης στο Web, όπως το Netscape και ο Internet Explorer, διατηρούν αρχείο καταγραφής αρχείων το οποίο καταγράφει τους ιστότοπους που επισκέφτηκαν πρόσφατα. Διατηρούν επίσης μια προσωρινή μνήμη που περιέχει ένα ορισμένο ποσό των πραγματικών αρχείων και ιστοσελίδων που προβλήθηκαν πρόσφατα.

ΕΝΤΟΠΙΣΜΟΣ ΜΗ ΕΞΟΥΣΙΟΔΟΤΗΜΕΝΩΝ ΧΡΗΣΤΩΝ

Ένα κοινό τέχνασμα των επιτιθέμενων είναι η δημιουργία ψεύτικων λογαριασμών χρήστη σε ένα σύστημα ή η αύξηση προνομίων τους για να έχουν πρόσβαση σε δεδομένα που δεν θα έπρεπε. Υπάρχουν διάφοροι τρόποι ελέγχου των λογαριασμών χρηστών και των ομάδων χρηστών σε ένα ζωντανό σύστημα:

- Ανατρέξτε στο User Manager για μη εξουσιοδοτημένους λογαριασμούς χρηστών (κατά τη διάρκεια μιας ζωντανής απόκρισης συστήματος).
- Χρησιμοποιήστε το usrstat από το NTRK για να δείτε όλους τους λογαριασμούς , αναζητώντας ύποπτες καταχωρήσεις.
- Εξετάστε το αρχείο καταγραφής ασφαλείας.

- Ελέγξτε τους καταλόγους \% systemroot% \ Profiles στο σύστημα. Εάν για παράδειγμα ο ο λογαριασμός χρήστη υπάρχει, αλλά δεν υπάρχει αντίστοιχος φάκελος \% systemroot% \ Profiles \<Useraccount>, αυτός ο λογαριασμός χρήστη δεν έχει χρησιμοποιηθεί για τη σύνδεση στο σύστημα.
- Ελέγξτε τα SIDs στο Registry.

ΚΡΥΦΑ Ή ΑΣΥΝΗΘΙΣΤΑ ΑΡΧΕΙΑ

Όλοι οι κακοί θέλουν να κρύψουν κάτι, και οι εγκληματίες υπολογιστών δεν είναι διαφορετικοί. Μόλις ένας εισβολέας αποκτήσει παράνομη πρόσβαση σε ένα σύστημα των Windows, πρέπει να κρύψει τα αρχεία για μεταγενέστερη χρήση. Μόλις κάποιος πληροφοριοδότης πραγματοποιήσει μη εξουσιοδοτημένη χρήση στο σύστημα μπορεί να κάνει κάποια αρχεία "αόρατα". Και οι δύο αυτοί επιτιθέμενοι μπορούν να επωφεληθούν από τις ροές αρχείων NTFS για να αποκρύψουν δεδομένα πίσω από τα νόμιμα αρχεία. Το NTFS διαθέτει ένα χαρακτηριστικό, το οποίο αναπτύχθηκε αρχικά στο σύστημα ιεραρχικών αρχείων Macintosh Hierarchical File System (HFS), για την αποθήκευση πολλαπλών παρουσιών δεδομένων αρχείου κάτω από μία καταχώρηση αρχείου. Αυτές οι πολλαπλές ροές δεδομένων μπορούν να χρησιμοποιηθούν για την απόκρυψη δεδομένων, επειδή η Εξερεύνηση των Windows δεν υποδεικνύει την παρουσία των πρόσθετων ροών.

ΜΗ ΕΞΟΥΣΙΟΔΟΤΗΜΕΝΑ ΣΗΜΕΙΑ ΠΡΟΣΒΑΣΗΣ

Μία από τις μεγαλύτερες διαφορές μεταξύ των συστημάτων Windows NT και Unix είναι ότι τα NT δεν επιτρέπουν την πρόσβαση με τηλεχειρισμό χωρίς τη χρήση εξωτερικών βοηθητικών προγραμμάτων. Με την πάροδο του χρόνου και την εξέλιξη των Windows αυτό άλλαξε καθώς συνοδεύονται από έναν Telnet server για διαχείριση απομακρυσμένων εντολών. Κάθε υπηρεσία που επιτρέπει κάποιον βαθμό απομακρυσμένης πρόσβασης μπορεί να αποτελέσει σημείο εισόδου σε ανεπιθύμητους εισβολείς. Εκτός από τις ενσωματωμένες εφαρμογές και εφαρμογές τρίτων μπορούν και οι δούρειοι ίπποι (trojans) να παρέχουν τέτοιες υπηρεσίες. Αυτές οι υπηρεσίες περιλαμβάνουν μεταξύ άλλων τα εξής:

* Terminal server
* Υπηρεσίες απομακρυσμένης πρόσβασης (PPP και PPTP)
* SQL/Oracle
* Web servers (όπως Apache και IIS)
*

ΥΠΗΡΕΣΙΕΣ ΑΠΟΜΑΚΡΥΣΜΕΝΟΥ ΕΛΕΓΧΟΥ ΚΑΙ ΠΡΟΣΒΑΣΗΣ

Για απομακρυσμένη πρόσβαση σε ένα σύστημα Windows απαιτείται η χρήση βοηθητικών προγραμμάτων όπως είναι το Remote Access Service (RAS). Διαχωρίζουμε την απομακρυσμένη πρόσβαση των συστημάτων των Windows σε δύο κατηγορίες: αυτά που επιτρέπουν τον τηλεχειρισμό (remote control) και εκείνα που επιτρέπουν απομακρυσμένη πρόσβαση (remote access). Η διαφορά μεταξύ των δύο είναι κυρίως το traffic δικτύου και η ταχύτητα απόδοσης.

ΕΠΙΠΕΔΑ ΕΠΙΔΙΟΡΘΩΣΗΣ

Κανένα λειτουργικό σύστημα δεν κυκλοφορεί χωρίς κάποια ελαττώματα. Η Microsoft αντιμετωπίζει συχνά προβλήματα ασφαλείας των Windows με το λογισμικό που ονομάζεται Service Packs. Τα Service Pack είναι συλλογές επιδιορθώσεων, νέων εφαρμογών, βελτιώσεων και ρυθμίσεων που έχουν σχεδιαστεί για βελτιώσεις. Κάθε πακέτο έχει σχεδιαστεί για διαφορετικές ευπάθειες και κενά στην ασφάλεια του

συστήματος. Τα Service Pack διορθώνουν μια σειρά ζητημάτων ταυτόχρονα. Γνωρίζοντας τα επίπεδα επιδιόρθωσης σε ένα σύστημα μπορείτε να εξαλείψετε την πιθανότητα τυχόν επιθέσεων.

ADMINISTRATIVE SHARES

Τα Windows χρησιμοποιούν τον όρο κοινόχρηστο στοιχείο για να αναφερθούν σε οποιοδήποτε αρχείο ή φάκελο που είναι προσβάσιμος από ένα δίκτυο μέσω της δικτύωσης των Windows. Ο χρήστης μπορεί να μοιραστεί ένα αρχείο με οποιονδήποτε άλλο χρήστη που έχει συνδεθεί στο σύστημα του συγκεκριμένου χρήστη. Η επιλογή να μοιραστείς ένα αρχείο με απομακρυσμένα συστήματα είναι απλή:απλά επιλέξτε έναν φάκελο-αρχείο που θέλετε να μοιραστείτε, κάντε δεξί κλικ και επιλέξτε Κοινή χρήση από το αναδυόμενο μενού. Εάν δείτε ένα εικονίδιο ενός χεριού κάτω από ένα φάκελο, αυτό σημαίνει ότι το αρχείο μοιράζεται με απομακρυσμένους χρήστες που έχουν τα κατάλληλα διαπιστευτήρια για να συνδεθούν στο συγκεκριμένο κοινόχρηστο στοιχείο.

ΕΛΕΓΧΟΣ ΑΝΑΓΝΩΡΙΣΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ (SIDs)

Για να καθορίσετε τις ενέργειες ενός συγκεκριμένου ID χρήστη ίσως χρειαστεί να συγκρίνετε τα SID (**Security Identifiers**) που βρέθηκαν στη μηχανή θύματος με αυτά της κεντρικής αρχής ελέγχου ταυτότητας. Αναφέραμε τα SIDs προηγουμένως σε αυτό το κεφάλαιο. Εδώ, εξηγούμε πώς τα SIDs μπορούν να συμβάλουν στην ανταπόκριση των περιστατικών. Κάθε σύστημα έχει το δικό του αναγνωριστικό, και κάθε χρήστης έχει το δικό του αναγνωριστικό στοιχείο στο σύστημα. Το αναγνωριστικό υπολογιστή και το αναγνωριστικό χρήστη συνδυάζονται για να κάνουν το SID. Έτσι, τα SID μπορούν να αναγνωρίσουν μοναδικά τους λογαριασμούς χρηστών. Για παράδειγμα, το ακόλουθο είναι ένα SID που ανήκει στο λογαριασμό διαχειριστή: S-1-5-21-917267712-1342860078-1792151419-500
Το S υποδηλώνει τη σειρά ψηφίων ως SID. Το 1 είναι το επίπεδο αναθεώρησης, το 5 είναι η τιμή αναγνωριστικού-αρχής και το 21-917267712-1342860078-1792151419 περιλαμβάνει διάφορες τιμές και το 500 είναι το σχετικό αναγνωριστικό.

ΑΝΑΣΚΟΠΗΣΗ ΑΝΑΖΗΤΗΣΕΩΝ ΚΑΙ ΑΡΧΕΙΩΝ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΟΥΝΤΑΙ

Ένα από τα πρώτα βήματα που πρέπει να ακολουθήσετε όταν ένας εργαζόμενος εγκαταλείψει την εταιρία σας είναι να ελέγξετε τι έχει αναζητήσει ή αν έχει διαγράψει πληροφορίες που αφορούν την εταιρία, επομένως πρέπει να κάνετε ανάκτηση των αρχείων του κάδου ανακύκλωσης. Επίσης ελέγξτε αν είχε πρόσβαση σε αρχεία που δεν έπρεπε. Τέλος, εκτελέστε μια γρήγορη ανασκόπηση των πιο πρόσφατα χρησιμοποιημένων αρχείων χρησιμοποιώντας τη διεπαφή GUI ή την προβολή του Registry.

ΑΝΑΖΗΤΗΣΕΙΣ String ΣΕ ΣΚΛΗΡΟΥΣ ΔΙΣΚΟΥΣ

Μια άλλη επιλογή για τον έλεγχο του τι έψαχνε ένας πρώην χρήστης του δικτύου σας είναι η δημιουργία αναζήτησης συμβολοσειρών (strings) με τη βοήθεια boot disk. Οι λίστες λέξεων πρέπει να είναι προσεγμένες λαμβάνοντας υπόψιν τις πληροφορίες στις οποίες είχε πρόσβαση ο συγκεκριμένος χρήστης καθώς επίσης και σε τι δεδομένα είχε πρόσβαση παρόλο που δεν έπρεπε. Μπορείτε να έχετε επομένως ένα ελεγχόμενο cd εκκίνησης για να κάνετε αναζητήσεις String σε κάθε σκληρό δίσκο για να δείτε αν οι χρήστες του δικτύου σας συμμορφώνονται με την πολιτική της εταιρίας σας.

ΣΥΜΠΕΡΑΣΜΑΤΙΚΑ

Πολλοί επαγγελματίες της ασφάλειας πιστεύουν ότι οι προσπάθειες ανάκαμψης πρέπει να είναι το επίκεντρο μιας αντίδρασης σε περιστατικά. Ωστόσο, μερικά περιστατικά μπορεί να απαιτούν να διερευνηθούν πλήρως για να προσδιοριστεί το ποιος ,πότε,γιατί ή πως έλαβε μέρος στο συμβάν ασφαλείας κάποιος. Είμαστε

ευχάριστα έκπληκτοι από τον αυξανόμενο αριθμό των εμπορικών επιχειρήσεων που γνωρίζουν τις νομικές και δικαστικές πτυχές της έρευνας υπολογιστών,που αφορούν συμβάντα ασφαλείας. Η ανάπτυξη μιας μεθόδου εγκληματολογικής έρευνας σε συστήματα Windows είναι σημαντικός παράγοντας για κάθε επαγγελματία ασφαλείας υπολογιστών. Το κεφάλαιο αυτό περιγράφει μια ορθή προσέγγιση για την διεξαγωγή έρευνας σχετικά με τα συστήματα των Windows σε μια προσπάθεια να εξαλειφθούν οι απρόβλεπτες και τυχαίες προσεγγίσεις στις τεχνικές έρευνες. Ποτέ δεν γνωρίζετε πότε η ανώτατη διοίκηση της εταιρίας πρόκειται να απαιτήσει από τους διαχειριστές συστημάτων της να ελέγξουν για αποδεικτικά στοιχεία που αφορούν παράνομη ή μη εξουσιοδοτημένη πρόσβαση.

ΕΡΩΤΗΣΕΙΣ

- Τι συμβαίνει με τη διεύθυνση προέλευσης στα αρχεία καταγραφής συμβάντων των Windows;
- Γιατί είναι απαραίτητη η χρονική συσχέτιση κατά τη διερεύνηση συμβάντων που σχετίζονται με την IIS;
- Πόσοι Κάδοι Ανακύκλωσης υπάρχουν σε ένα σύστημα Windows;
- Πώς μπορούν οι SIDs να είναι σημαντικοί για μια έρευνα εγκληματολογίας;

ΚΕΦΑΛΑΙΟ 10

ΕΞΕΡΕΥΝΩΝΤΑΣ ΣΥΣΤΗΜΑΤΑ UNIX

Το λειτουργικό σύστημα Unix είναι ισχυρό, ευέλικτο και εξαιρετικά λειτουργικό. Η λειτουργικότητα του είναι εξαιρετικά χρήσιμη αλλά αποτελεί μια πρόκληση ως προς την προστασία και τη διερεύνηση. Αυτό το κεφάλαιο περιγράφει τα χαρακτηριστικά του λειτουργικού συστήματος Unix τα οποία είναι πιθανότερο να βοηθήσουν τον ερευνητή να προσδιορίσει τα ποιος, τι, πότε, πού και πώς σε ένα συμβάν. Παρουσιάζουμε τις ερευνητικές τεχνικές όσο πιο έγκυρα είναι δυνατό. Σε αυτό το σημείο υποθέτουμε πως έχετε ήδη ανταποκριθεί στο συμβάν με τον τρόπο που έχουμε περιγράψει παλιότερα και θα χρησιμοποιήσετε τα δεδομένα που έχετε συλλέξει κατά την αρχική σας ανταπόκριση με τα βήματα που θα περιγράψουμε παρακάτω. Επιπλέον λάβετε υπόψιν ότι η παρούσα ανάλυση βημάτων δεν μπορεί να καλύψει κάθε πιθανό περιστατικό στα συστήματα Unix. Βέβαια οι θεμελιώδεις γνώσεις κατανόησης και λειτουργίας των συστημάτων Unix είναι απαραίτητες.

ΣΤΑΔΙΑ ΕΡΕΥΝΑΣ ΣΕ ΣΥΣΤΗΜΑΤΑ UNIX

Για να μπορέσετε να διερευνήσετε ένα σύστημα Unix, θα χρειαστεί να ρυθμίσετε τον υπολογιστή σας και να έχετε κατανοήσει ακριβώς τι ψάχνετε - το αρχείο διαμόρφωσης συστήματος, πίνακα κατατμήσεων κτλ – όπως έχουμε λεπτομερώς περιγράψει νωρίτερα. Μόλις είστε έτοιμοι να ξεκινήσετε την έρευνα του συστήματος Unix, οι παρακάτω ενέργειες παρέχουν τον πιο πιθανό τρόπο για τον εντοπισμό σχετικών στοιχείων:

- Ελέγξτε όλα τα σχετικά αρχεία καταγραφής
- Εκτελέστε αναζητήσεις λέξεων-κλειδιών
- Ελέγξτε τα αρχεία που συσχετίζονται
- Προσδιορίστε μη εξουσιοδοτημένους λογαριασμούς ή ομάδες χρηστών
- Προσδιορίστε περίεργες και ψεύτικες διαδικασίες

- Ελέγξτε για μη εξουσιοδοτημένα σημεία πρόσβασης
- Αναλύστε σχέσεις εμπιστοσύνης
- Ελέγξτε για τα rootkits στον πυρήνα.

ΕΛΕΓΧΟΣ ΣΧΕΤΙΚΩΝ ΦΥΛΛΩΝ ΚΑΤΑΓΡΑΦΗΣ

Τα λειτουργικά συστήματα Unix διαθέτουν μια ποικιλία αρχείων καταγραφής που μπορούν να δώσουν σημαντικές ενδείξεις κατά τη διάρκεια της απόκρισης των περιστατικών. Δεν είναι μόνο δραστηριότητες του συστήματος, όπως συνδέσεις, ξεκινήματα και τερματισμοί λειτουργίας αλλά και συμβάντα που σχετίζονται με υπηρεσίες δικτύου Unix. Τα περισσότερα αρχεία καταγραφής βρίσκονται σε έναν κοινό κατάλογο, συνήθως / var / log. Ωστόσο, μερικές εκδόσεις του Unix χρησιμοποιούν έναν εναλλακτικό κατάλογο, όπως / usr / adm ή / var / adm. Ορισμένα αρχεία καταγραφής τοποθετούνται σε μη συγκεκριμένες τοποθεσίες, όπως / etc. Για να είστε σίγουροι συμβουλευτείτε το ειδικό εγχειρίδιο του συστήματος. Επιπλέον δεν είναι πάντα όλα τα αρχεία καταγραφής αποθηκευμένα στο σύστημα. Μπορείτε να βρείτε σχετικά αρχεία καταγραφής στον server δικτύου ή σε συσκευή ασφαλείας, όπως ένα τείχος προστασίας ή ένα IDS.

ΦΥΛΛΟ ΚΑΤΑΓΡΑΦΗΣ ΔΙΚΤΥΟΥ 1/2

Πιθανώς η πιο χρήσιμη δυνατότητα καταγραφής στο Unix είναι το αρχείο syslog (System log). Αυτό το ημερολόγιο καταγράφει συμβάντα από προγράμματα και υποσυστήματα εντός του Unix. Οι δραστηριότητες του syslog ελέγχονται συνήθως μέσω του αρχείου διαμόρφωσης syslog /etc/syslog.conf. Ένας syslog daemon (syslogd) τρέχει στο σύστημα για να καταγράψει μηνύματα. Το Syslog προσφέρει επίσης τη δυνατότητα καταγραφής μηνυμάτων από απόσταση, σε ένα δίκτυο. Συνολικά, η δυνατότητα καταγραφής που παρέχεται από το syslog είναι εξαιρετικά ισχυρή και ευέλικτη. Στις περισσότερες εκδόσεις Unix, το syslog καταγράφει κάποιο συνδυασμό αρχείων στον προεπιλεγμένο κατάλογο αρχείων καταγραφής, αλλά τα πιο χρήσιμα αρχεία καταγραφής είναι συνήθως τα μηνύματα, η ασφάλεια και τα αρχεία syslog. Το αρχείο διαμόρφωσης syslog ελέγχει τους τύπους μηνυμάτων που αποστέλλονται σε ποια αρχεία καταγραφής πάνε.

ΦΥΛΛΟ ΚΑΤΑΓΡΑΦΗΣ ΔΙΚΤΥΟΥ 2/2

Κάθε γραμμή στο αρχείο ρυθμίσεων περιέχει τρία πεδία:

- Το πεδίο εγκατάστασης υποδηλώνει το υποσύστημα που παρήγαγε το αρχείο καταγραφής. Για παράδειγμα, το sendmail καταγράφει την εγκατάσταση αλληλογραφίας. Οι τύποι εγκαταστάσεων είναι auth (security), authpriv, cron, daemon, kern, lpr, mail, mark, news, syslog, user, uucp και local0-7.
- Το πεδίο προτεραιότητας υποδεικνύει τη σοβαρότητα του αρχείου καταγραφής. Υπάρχουν οκτώ επίπεδα προτεραιότητας: debug, info, notice, warning, err, crit, alert, emerg.
- Το πεδίο δράσης καθορίζει τον τρόπο εγγραφής του αρχείου καταγραφής. Η ενέργεια θα μπορούσε να είναι το όνομα ενός αρχείου καταγραφής ή ακόμα και της διεύθυνσης IP ενός απομακρυσμένου ξενιστή

ΑΠΟΜΑΚΡΥΣΜΕΝΑ Syslog Server ΦΥΛΛΑ ΚΑΤΑΓΡΑΦΗΣ

Τα αρχεία καταγραφής που δημιουργούνται τοπικά από τον syslogd είναι αρχεία κειμένου τα οποία είναι συνήθως αναγνώσιμα από τον κόσμο αλλά μπορούν να εγγραφούν μόνο από τον root. Αυτό σημαίνει ότι οποιοσδήποτε εισβολέας έχει αποκτήσει πρόσβαση σε επίπεδο διαχειριστή μπορεί εύκολα να τροποποιήσει τα αρχεία καταγραφής syslog, αφαιρώντας επιλεγμένες καταχωρίσεις, τροποποιώντας τις επιλεγμένες καταχωρίσεις ή προσθέτοντας παραπλανητικές καταχωρήσεις. Αυτές οι τροποποιήσεις είναι σχεδόν αδύνατο να εντοπιστούν. Εάν υποψιάζεστε ότι ένας εισβολέας έχει αποκτήσει πρόσβαση σε επίπεδο root στο σύστημα όπου αποθηκεύονται τα αρχεία καταγραφής, μην εμπιστεύεστε τα αρχεία καταγραφής. Ο

μόνος τρόπος για να βεβαιωθείτε ότι κάποιος εισβολέας τροποποίησε τα αρχεία καταγραφής είναι να εκτελέσει εφεδρική καταγραφή σε έναν ασφαλή απομακρυσμένο διακομιστή syslog. Σε περίπτωση λοιπόν που ένα σύστημα έχει παραβιαστεί και τα αρχεία καταγραφής του χειραγωγούνται θα πρέπει να υπάρχει ένα ανέγγιχτο αντίγραφο σε έναν απομακρυσμένο syslog server.

TCP WRAPPER

Εκτός από όλες τις εφαρμογές που εκμεταλλεύονται τη δυνατότητα καταγραφής του συστήματος, ένα άλλο εξαιρετικά πολύτιμο πρόγραμμα που χρησιμοποιεί το syslog είναι το TCP Wrappers. Το TCP Wrappers είναι έλεγχος πρόσβασης βασισμένος στον κεντρικό υπολογιστή για υπηρεσίες TCP και UDP.

ΑΛΛΑ ΦΥΛΛΑ ΚΑΤΑΓΡΑΦΗΣ ΔΙΚΤΥΟΥ 1/2

Εκτός από το syslog, τα συστήματα Unix μπορούν να διατηρούν και άλλα αρχεία καταγραφής δραστηριότητας δικτύου. Αυτά τα αρχεία καταγραφής είναι κατά κύριο λόγο υπηρεσίες, όπως τα αρχεία καταγραφής για web servers. Ένα παράδειγμα μεταφοράς αρχείου είναι το εξής:

* **Thu May 10 18:17:05 2003 1 10.1.1.1 85303 /tftpboot/rinetd.zip b _ o r chris ftp 0 * c**

Αυτές οι καταχωρήσεις παρέχουν τις εξής πληροφορίες:

- Η ώρα και η ημερομηνία που συνέβη η μεταφορά
- Ο αριθμός των δευτερολέπτων που έλαβε η μεταφορά (1)
- Ο απομακρυσμένος κεντρικός υπολογιστής (10.1.1.1)
- Ο αριθμός των bytes που μεταφέρθηκαν

ΑΛΛΑ ΦΥΛΛΑ ΚΑΤΑΓΡΑΦΗΣ ΔΙΚΤΥΟΥ 2/2

- Το όνομα του μεταφερόμενου αρχείου
- Ο τύπος μεταφοράς αρχείων (b-binary)
- Μια σημαία ειδικής ενέργειας (δεν δείχνει καμία ειδική ενέργεια)
- Η κατεύθυνση της μεταφοράς (0 για εξερχόμενη ή i για εισερχόμενη)
- Ο τρόπος πρόσβασης (r-real)
- Το όνομα χρήστη (chris)
- Το όνομα υπηρεσίας (ftp)
- Η μέθοδος ελέγχου ταυτότητας (0 για κανένα)
- Το user ID (* δηλώνει ότι δεν υπάρχει διαθέσιμο)
- Η κατάσταση της μεταφοράς (c-complete)

ΚΑΤΑΓΡΑΦΗ ΤΩΝ HOST

Το Unix παρέχει μια ποικιλία αρχείων καταγραφής που παρακολουθούν τις λειτουργίες του κεντρικού υπολογιστή. Ορισμένα από τα πιο χρήσιμα αρχεία καταγραφής καταγράφουν την εκτέλεση της εντολής su, τους συνδεδεμένους χρήστες, τις προσπάθειες σύνδεσης και την εκτέλεση της εργασίας που πραγματοποίησαν. Η εντολή su επιτρέπει σε ένα χρήστη να αλλάξει ID χρήστη κατά τη διάρκεια μιας περιόδου σύνδεσης. Οι επιτιθέμενοι χρησιμοποιούν μερικές φορές αυτήν την εντολή για να προσπαθήσουν να αποκτήσουν πρόσβαση root σε ένα σύστημα. Το Unix καταγράφει κάθε προσπάθεια εκτέλεσης της εντολής su στο σύστημα. Το ημερολόγιο δείχνει την ώρα και την ημερομηνία της προσπάθειας su και αν η προσπάθεια ήταν επιτυχής, επίσης δείχνει την τερματική συσκευή από την οποία επιχείρησε ο χρήστης για την εκτέλεση της εντολής καθώς και την ID πριν και μετά την απόπειρα. Σε κάποια συστήματα Unix

υπάρχει ξεχωριστό αρχείο καταγραφής su ενώ σε κάποια άλλα οι προσπάθειες su καταγράφονται στο αρχείο syslog.

ΚΑΤΑΓΕΓΡΑΜΜΕΝΑ ΑΡΧΕΙΑ ΚΑΤΑΓΡΑΦΗΣ ΧΡΗΣΤΩΝ

Το αρχείο utmpor wtmpfile χρησιμοποιείται για την αποθήκευση πληροφοριών σχετικά με τους χρήστες που είναι συνδεδεμένοι στο σύστημα. Το αρχείο καταγραφής ονομάζεται διαφορετικά και αποθηκεύει ελαφρώς διαφορετικές πληροφορίες, ανάλογα την έκδοση του συστήματος Unix. Οι βασικές πληροφορίες που αποθηκεύονται είναι το όνομα του χρήστη, το τερματικό που χρησιμοποιείται για την σύνδεση και ο χρόνος της σύνδεσης. Το αρχείο αποθηκεύεται σε μορφή δυαδικών δεδομένων και όχι ως αρχείο κειμένου. Παρά το γεγονός ότι τα wtmpor utmplogs αποθηκεύονται σε δυαδική μορφή και δεν μπορούν εύκολα να τροποποιηθούν με vi ή παρόμοιους επεξεργαστές, δεν μπορείτε να υποθέσετε την ακεραιότητα αυτών των αρχείων. Πολλά κοινά προγράμματα χάκερ, όπως το zap, μπορούν να καταργήσουν επιλεκτικά καταχωρήσεις από αυτά τα αρχεία. Λάβετε υπόψη ότι τα δυαδικά αρχεία καταγραφής περιέχουν συχνά περισσότερες πληροφορίες από ό, τι παρουσιάζουν οι προεπιλεγμένες εντολές.

ΚΑΤΑΓΡΑΦΗ ΠΡΟΣΠΑΘΕΙΑΣ ΣΥΝΔΕΣΗΣ

Οι προσπάθειες σύνδεσης, τόσο οι αποτυχημένες όσο και οι επιτυχείς, καταγράφονται από προεπιλογή στα περισσότερα συστήματα Unix. Παράλληλα με τις προσπάθειες σύνδεσης για υπηρεσίες δικτύου όπως FTP ή ssh, οι συνδέσεις κονσόλας αποθηκεύονται επίσης σε ένα από τα αρχεία καταγραφής, όπως το αρχείο μηνυμάτων στο Linux Systems. Εδώ είναι ένα παράδειγμα αποτυχημένων προσπαθειών σύνδεσης που έχουν καταγραφεί στο αρχείο μηνυμάτων:
Dec 10 18:58:03 victim login[744]:FAILED LOGIN 1 FROM (null) FOR root,
Authentication failure
Dec 11 20:47:10 victim login[688]:FAILED LOGIN 1 FROM (null) FOR chris,
User not known to the underlying authentication module
Η πρώτη καταχώρηση δείχνει μια αποτυχημένη προσπάθεια σύνδεσης για το root χρήστη και στη δεύτερη καταχώρηση εμφανίζεται κάποιος που προσπαθεί να συνδεθεί με ανύπαρκτο όνομα χρήστη.

ΚΑΤΑΓΡΑΦΕΣ CRON

Το Cron είναι ένα χαρακτηριστικό στο Unix που επιτρέπει στους χρήστες να προγραμματίζουν προγράμματα για μελλοντική εκτέλεση και χρησιμοποιείται συχνά για επιθέσεις. Όλες οι εκτελέσιμες εργασίες cron καταγράφονται, συνήθως στο / var / cron / log ή στον προεπιλεγμένο κατάλογο καταγραφής, σε ένα αρχείο που ονομάζεται cron. Θα συζητήσουμε το cron με περισσότερες λεπτομέρειες όταν δούμε τα αρχεία εκκίνησης στην ενότητα "Ειδικά Αρχεία" αργότερα.

ΚΑΤΑΓΡΑΦΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑΣ ΧΡΗΣΤΗ

Μαζί με τις συνδέσεις, άλλοι τύποι δραστηριοτήτων χρήστη καταγράφονται σε αρχεία καταγραφής Unix. Τα αρχεία καταγραφής λογιστικών διαδικασιών και τα αρχεία ιστορικού περιεχομένου καταγράφουν τις εντολές που εκτελούνται από τους χρήστες. Όπως έχει προαναφερθεί η διαδικασία καταγραφής είναι χαρακτηριστικό των Unix καθώς καταγράφεται κάθε εντολή που εκτελείται από κάθε χρήστη. Αυτός ο τύπος καταγραφής δεν είναι ενεργοποιημένος από προεπιλογή. Εάν το αρχείο καταγραφής acct ή pacct δεν υπάρχει στο σύστημα, δεν θα μπορείτε να χρησιμοποιήσετε αυτήν τη δυνατότητα. Εάν υπάρχει κάποιο από αυτά τα αρχεία, μπορείτε να χρησιμοποιήσετε την εντολή lastcomm ή acctcom για να ελέγξετε τα περιεχόμενα του αρχείου. Το αρχείο καταγραφής είναι ένα δυαδικό αρχείο και γνωρίζουμε ότι δεν υπάρχουν δημόσια εργαλεία επίθεσης για την επεξεργασία αυτού του αρχείου. Για να καταργήσει αυτά τα στοιχεία, ο επιτιθέμενος θα πρέπει να διαγράψει το αρχείο καταγραφής.

ΙΣΤΟΡΙΚΟ SHELL

Οι χρήστες με ενεργή πρόσβαση στα συστήματα Unix έχουν ένα σχετικό κέλυφος εντολών(shell command), όπως το shell Bourne (sh), Korn (ksh) ή το shell Bourne-Again (bash). Τα shell αυτά παρέχουν τη δυνατότητα να καταγράψετε όλες τις εντολές μαζί με τις επιλογές της γραμμής εντολών. Συνήθως, το αρχείο ιστορικού αποθηκεύεται ως κρυφό αρχείο στον κατάλογο του χρήστη. Το παρακάτω είναι ένα απόσπασμα από ένα αρχείο ιστορικού για το shell bash:
[root@lucky]# more .bash_history
su
ssh root@test.victim.cz
ping test.victim.cz
nc -v -z -n 10.1.1.134 22

ΠΟΥ ΝΑ ΨΑΞΕΤΕ ΓΙΑ ΣΤΟΙΧΕΙΑ

Κάθε φορά που διερευνάτε ένα σύστημα Unix που είναι ύποπτο ότι είναι παραβιασμένο, ελέγξτε για αρχεία ιστορικού κελύφους(shell history files). Εάν η λειτουργία ιστορικού είναι ενεργοποιημένη και το αρχείο ιστορικού δεν υπάρχει, υπάρχει μια πιθανότητα ο χάκερ να έχει διαγράψει το αρχείο ιστορικού. Εάν το αρχείο ιστορικού υπάρχει ως σύνδεσμος / Dev / null, όπως φαίνεται παρακάτω, τότε υπάρχει σοβαρή πιθανότητα το σύστημα να έχει παραβιαστεί.
[root@lucky /root]# ls –al
total 52
drwxr-x--- 5 root root 4096 Dec 12 04:47 .
drwxr-xr-x 18 root root 4096 Dec 8 01:54 ..
-rw------- 1 root root 108 Dec 12 04:47 .Xauthority
-rw-r--r-- 1 root root 1126 Aug 23 1995 .Xdefaults
lrwxrwxrwx 1 root tty 9 Dec 8 14:50 **.bash_history ->**
/dev/null

ΑΝΑΖΗΤΗΣΗ ΛΕΞΕΩΝ-ΚΛΕΙΔΙΩΝ

Οι αναζητήσεις λέξεων-κλειδιών αποτελούν κρίσιμο μέρος σχεδόν σε κάθε έρευνα και αντιμετώπιση περιστατικών, που κυμαίνεται από την παρενόχληση μέσω ηλεκτρονικού ταχυδρομείου έως τις περιπτώσεις παραβίασης από απομακρυσμένο δίκτυο. Λέξεις-κλειδιά μπορεί να είναι ένα ευρύ φάσμα των συμβολοσειρών ASCII, συμπεριλαμβανομένου του κωδικού πρόσβασης του εισβολέα, ενός ονόματος χρήστη μιας διεύθυνσης MAC ή μιας διεύθυνσης IP. Μπορείτε να πραγματοποιήσετε αναζητήσεις λέξεων-κλειδιών στη λογική δομή αρχείων ή σε φυσικό επίπεδο, εξετάζοντας τα περιεχόμενα μιας ολόκληρης μονάδας δίσκου.

ΑΝΑΖΗΤΗΣΗ ΑΚΟΛΟΥΘΙΩΝ ΜΕ GREP

Η ισχυρή, ευέλικτη εντολή grep είναι ένα βασικό εργαλείο για τις αναζητήσεις string. Χρησιμοποιήστε την εντολή ως εξής:

* **[root@lucky]# grep root /etc/passwd**
  root:x:0:0:root:/root:/bin/bash

Παρατηρήστε ότι η γραμμή στο αρχείο passwd εμφανίζεται ως έξοδος. Το αρχείο passwd είναι ένα αρχείο κειμένου.
Ας το δοκιμάσουμε σε ένα binary αρχείο:
[root@lucky]# grep PROMISC /sbin/ifconfig

Binary file /sbin/ifconfig matches
Αυτή τη φορά, το String δεν εμφανίζεται. Αντίθετα, βλέπετε μια ειδοποίηση ότι ένα αρχείο τύπου binary έχει μια αντίστοιχη καταχώρηση.

ΑΝΑΖΗΤΗΣΗ ΑΡΧΕΙΩΝ ΜΕ FIND

Μια άλλη χρήσιμη εντολή για αναζητήσεις String είναι η εντολή find. Μπορείτε να χρησιμοποιήσετε την εντολή find για να βρείτε οποιοδήποτε όνομα αρχείου που ταιριάζει με μια απλή έκφραση. Ακολουθεί ένα παράδειγμα αναζήτησης ολόκληρου του συστήματος αρχείων για ένα όνομα αρχείου ή καταλόγου που ονομάζεται "..." :

```
[root@aplinux /]# find / -name "\.\.\." –print
    /home/mugge/MDAc/temp/.../root/...
```

Η πρώτη εμπρόσθια κάθετος (/) υποδεικνύει ότι η λειτουργία εύρεσης θα αναζητήσει ολόκληρο το σύστημα αρχείων. Η επιλογή -name ορίζει ότι το χαρακτηριστικό που θα αναζητηθεί είναι το όνομα του αρχείου. Η πίσω κάθετος (backslash) (\) που προηγείται κάθε τελείας (.) είναι απαραίτητη για να ξεφύγει από την ειδική έννοια της κουκκίδας, επειδή, από προεπιλογή, αυτός ο χαρακτήρας είναι μπαλαντέρ. Παρατηρήστε ότι βρέθηκαν δύο αντιστοιχίες. Εάν η εντολή εκτελεστεί χωρίς τα τρία backslash, τα αποτελέσματα θα ήταν οποιοδήποτε αρχείο ή κατάλογος που είχε τρεις χαρακτήρες στο όνομά της.

ΕΛΕΓΧΟΣ ΣΥΣΧΕΤΙΖΟΜΕΝΩΝ ΑΡΧΕΙΩΝ

Είναι σχεδόν βέβαιο ότι πολλά αρχεία θα φιλοξενούν στοιχεία που σχετίζονται με οποιοδήποτε δεδομένο περιστατικό. Ωστόσο, η επιτυχία σας στην αναγνώριση όλων των σχετικών αρχείων είναι λιγότερο σημαντική. Χρησιμοποιούμε μερικές βοηθητικές τεχνικές για να προσδιορίσουμε ποια αρχεία είναι πιθανόν να είναι σχετικά με οποιοδήποτε δεδομένο περιστατικό. Αυτές οι τεχνικές περιλαμβάνουν τον εντοπισμό σχετικών αρχείων με τις σφραγίδες χρόνου / ημερομηνίας τους και με τις πληροφορίες που αποκτήθηκαν κατά την αρχική απόκριση στο σύστημα Unix. Επίσης, αναζητούμε αρχεία διαμόρφωσης και συστήματος τα οποία συνήθως καταχράζονται από εισβολείς.

ΣΦΡΑΓΙΔΕΣ ΗΜΕΡΟΜΗΝΙΑΣ 1/2

Για να αναζητήσετε αρχεία και καταλόγους που έχουν παραβιαστεί ή τροποποιηθεί σε ένα συγκεκριμένο χρονικό πλαίσιο θα πρέπει να γνωρίζεται και το χρονικό του υποτιθέμενου περιστατικού. Το χρονοδιάγραμμα μπορεί να είναι πολύ συγκεκριμένο, όπως όταν ένα IDS δικτύου ανακάλυψε και κατέγραψε την επίθεση όπως συνέβη. Από την άλλη πλευρά, το χρονοδιάγραμμα μπορεί να είναι γενικό, όπως στην περίπτωση όπου ένας διαχειριστής συστήματος συνδέει το σύστημα με το διαδίκτυο πριν από δύο εβδομάδες και αποδεικτικά στοιχεία παραβίασης βρέθηκαν σήμερα. Εάν έχετε καλή εγγραφή από μια εξωτερική πηγή (όπως το network IDS) από τη στιγμή της επίθεσης, το πρώτο βήμα είναι να βεβαιωθείτε ότι ο χρόνος του συστήματος στο IDS ταιριάζει με εκείνον του παραβιασμένου συστήματος.

ΣΦΡΑΓΙΔΕΣ ΗΜΕΡΟΜΗΝΙΑΣ 2/2

Το σύστημα αρχείων Unix αποθηκεύει τρία διαφορετικά χρονικά σήματα για κάθε αρχείο ή κατάλογο:

- Η ώρα atime (access time) είναι η τελευταία φορά που είχατε πρόσβαση σε ένα αρχείο ή κατάλογο. Αυτό περιλαμβάνει ακόμα και την πρόσβαση απλής ανάγνωσης.
- Η ώρα mtime (modification time) καταγράφει την τελευταία φορά που τροποποιήθηκε ένα αρχείο.
- Το ctime, είναι παρόμοιο με το mtime, αλλά καταγράφει την τελευταία φορά που άλλαξε η τιμή inode. Αυτή η τιμή μπορεί να αλλάξει με συμβάντα όπως είναι η αλλαγή αδειών ή ιδιοκτησίας.

ΕΙΔΙΚΑ ΑΡΧΕΙΑ

Ορισμένα είδη αρχείων και καταλόγων φαίνεται να εμφανίζονται τακτικά σε συμβάντα. Αυτά τα αρχεία και οι κατάλογοι περιλαμβάνουν αρχεία SUID και SGID, ασυνήθιστα και κρυφά αρχεία και καταλόγους, αρχεία ρυθμίσεων και το /tmpdirectory. Ας δούμε πώς αυτά τα αρχεία μπορούν να σχετιστούν με τις έρευνες σε Unix. Το Unix περιέχει χαρακτηριστικά γνωστά ως set userid (SUID) και set groupid (SGID), τα οποία έχουν σχεδιαστεί για να επιτρέπουν στα προγράμματα να λειτουργούν με υψηλότερα προνόμια από αυτά του χρήστη που τρέχει το πρόγραμμα. Για παράδειγμα, εάν ο χρήστης "X" εκτελεί ένα πρόγραμμα, το πρόγραμμα εκτελείται με τα προνόμια του χρήστη "X". Ωστόσο, εάν το πρόγραμμα είναι SUID και το εκτελεί ο "X", το πρόγραμμα εκτελείται με τα δικαιώματα οποιουδήποτε χρήστη κατέχει την εκτέλεση. Το SGID λειτουργεί με τον ίδιο τρόπο, εκτός από το ότι το πρόγραμμα εκτελείται με τα προνόμια της συνδεδεμένης ομάδας. Τα SUID και SGID root προγράμματα αποτελούν την πηγή των περισσότερων επιθέσεων προτίμησης-κλιμάκωσης σε Unix, και είναι επίσης ένα αγαπημένο backdoor για εισβολείς.

ΑΣΥΝΗΘΙΣΤΑ ΚΑΙ ΚΡΥΜΜΕΝΑ ΑΡΧΕΙΑ

Οι επιτιθέμενοι συχνά αποκρύπτουν αρχεία και καταλόγους από τον απλό παρατηρητή. Μέσα στο Unix, οποιοδήποτε αρχείο ή κατάλογος αρχίζει με μια τελεία (.) είναι κρυμμένος από την απλή προβολή. Δεν θα εμφανιστεί σε ένα ls εάν δεν χρησιμοποιείται η επιλογή -a. Επιπλέον, οι εισβολείς συχνά ονομάζουν αρχεία και καταλόγους με φαινομενικά αβλαβή ονόματα. Ιδιαίτερα κοινό για τους καταλόγους είναι το όνομα μόνο τριών κουκίδων (...). Επομένως είναι λογικό ένας διαχειριστής συστήματος να μην υποπτευθεί αμέσως κάτι περίεργο. Συμπερασματικά το πρώτο βήμα είναι να είστε πιο προσεκτικοί και παρατηρητικοί σε περιπτώσεις καταλόγων με πολλαπλές κουκκίδες.

ΑΡΧΕΙΑ ΔΙΑΜΟΡΦΩΣΗΣ

Τα αρχεία διαμόρφωσης είναι μια σημαντική θέση των αποδεικτικών στοιχείων κατά τη διάρκεια πολλών περιστατικών. Με όλες τις ενσωματωμένες λειτουργίες του λειτουργικού συστήματος Unix, ένας έμπειρος επιτιθέμενος μπορεί εύκολα να τροποποιήσει τις εφαρμογές για την εκτέλεση κακών εργασιών. Οι συνήθεις στόχοι περιλαμβάνουν αρχεία που ελέγχουν την πρόσβαση στο σύστημα-θύμα, όπως τα αρχεία διαμόρφωσης του TCP Wrapper /etc/hosts.allow και /etc/hosts.deny. Οι επιτιθέμενοι μπορούν να τροποποιήσουν ή να διαγράψουν αυτά τα αρχεία για να επιτρέψουν σε ορισμένους υπολογιστές να συνδεθούν με το σύστημα-θύμα κατά βούληση. Το αρχείο διαμόρφωσης daemon inetd.conf (που βρίσκεται στον κατάλογο / etc) ελέγχει πολλές από τις υπηρεσίες δικτύου του Unix. Υπηρεσίες όπως Telnet, FTP και TFTP (Και πολλές άλλες υπηρεσίες) ξεκινούν μέσω αυτού του αρχείου. Ένας εισβολέας μπορεί να προσθέσει καταχωρήσεις σε αυτό το αρχείο, έτσι ώστε το σύστημα-θύμα να ακούει σε πολλές θύρες ή μπορεί να ενεργοποιήσει μια υπηρεσία που απενεργοποιήθηκε προηγουμένως, όπως το TFTP.

ΑΡΧΕΙΑ ΕΚΚΙΝΗΣΗΣ

Το λειτουργικό σύστημα Unix έχει αρκετές τοποθεσίες που χρησιμοποιούνται για την εκκίνηση υπηρεσιών και εφαρμογών. Αναφέραμε μόνο το αρχείο inetd.conf, ένα από τα πρωταρχικά αρχεία αυτού του τύπου. Άλλα παραδείγματα περιλαμβάνουν αρχεία εκκίνησης cron, rc και αρχεία εκκίνησης χρηστών. Όπως προαναφέρθηκε, η δυνατότητα cron χρησιμοποιείται για τον προγραμματισμό της μελλοντικής εκτέλεσης προγραμμάτων. Ο κατάλογος / var / spool / cron ή / usr / spool / cron αποθηκεύει εργασίες cron για διάφορους χρήστες. Τα αρχεία σε αυτόν τον κατάλογο ονομάζονται με βάση τους λογαριασμούς χρήστη και όλες οι εργασίες που είναι αποθηκευμένες σε αυτά τα αρχεία εκτελούνται με τα δικαιώματα αυτού του χρήστη. Μια άλλη θέση των αρχείων εκκίνησης είναι ο κατάλογος rc. Συνήθως ονομάζεται /etc/rc.d ή κάτι παρόμοιο, αυτός ο κατάλογος περιέχει μια λίστα προγραμμάτων που ξεκινούν όταν ένα σύστημα Unix τίθεται σε λειτουργία (boot). Ωστόσο, οι επιτιθέμενοι μπορούν εύκολα να προσθέσουν μια καταχώρηση σε

οποιαδήποτε από τις εκκινήσεις επομένως βεβαιωθείτε ότι τα προγράμματα που εκτελούνται από τον κατάλογο rc είναι νόμιμα και δεν έχουν τροποποιηθεί από κάποιον εισβολέα.

ΚΑΤΑΛΟΓΟΣ TMP

Από προεπιλογή, το / tmpdirectory είναι το μοναδικό σύστημα αρχείων που μπορεί να εγγραφεί σε ένα σύστημα Unix. Αυτό το κάνει ένα δημοφιλές hangout για επιτιθέμενους και έναν αγαπημένο χώρο αποθήκευσης για κακόβουλα εργαλεία. Επίσης πολλοί χρησιμοποιούν τον κατάλογο / tmp για την αποθήκευση προσωρινών αρχείων κατά τη διάρκεια επιθέσεων κλιμάκωσης προνομίων και μερικές φορές αφήνουν στοιχεία ανίχνευσης. Ελέγξτε προσεκτικά το / tmpdirectory σε περίπτωση συμβάντος για να διαπιστώσετε εάν υπάρχουν κρυφοί κατάλογοι ή ύποπτα αρχεία.

ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΜΗ ΕΞΟΥΣΙΟΔΟΤΗΜΕΝΩΝ ΧΡΗΣΤΩΝ ΚΑΙ ΟΜΑΔΩΝ

Οι επιτιθέμενοι συχνά θα τροποποιούν τις πληροφορίες λογαριασμού στα επιτιθέμενα συστήματα. Η τροποποίηση αυτή μπορεί να έχει τη μορφή πρόσθετων λογαριασμών ή κλιμάκωσης προνομίων τρεχόντων λογαριασμών. Ο στόχος είναι συνήθως να δημιουργηθεί ένα backdoor για μελλοντική πρόσβαση. Θα πρέπει να ελέγχετε τους χρήστες και τους λογαριασμούς ομάδας σε υποψήφια συστήματα-θύματα για να επιβεβαιώσετε ότι κανένας εισβολέας δεν παραποίησε αυτές τις πληροφορίες. Ο έλεγχος των πληροφοριών του λογαριασμού συστήματος Unix είναι μια απλή διαδικασία.

ΕΡΕΥΝΑ ΛΟΓΑΡΙΑΣΜΩΝ ΧΡΗΣΤΩΝ

Οι πληροφορίες χρηστών αποθηκεύονται στο αρχείο / etc / passwd. Αυτό είναι ένα αρχείο κειμένου που μπορείτε εύκολα να το δείτε μέσω διάφορων μηχανισμών. Κάθε χρήστης σε ένα σύστημα Unix έχει μια καταχώρηση στο αρχείο / etc / passwd. Μια τυπική καταχώρηση μοιάζει με αυτή:
lester:x:512:516:Lester Pace:/home/lester:/bin/bash
Η καταχώρηση αποτελείται από πεδία: το όνομα χρήστη (lester), τον κωδικό πρόσβασης (x), το user ID (512), το group ID (516) τον αρχικό κατάλογο (home directory) και το προεπιλεγμένο shell σύνδεσης. Οποιοσδήποτε επιπλέον λογαριασμός χρήστη δεν δημιουργήθηκε από το διαχειριστή του συστήματος είναι αιτία συναγερμού. Εξετάστε τους λογαριασμούς που θα πρέπει να απενεργοποιηθούν ή να μην είναι διαθέσιμοι για απομακρυσμένη σύνδεση για να διασφαλιστεί ότι δεν έχουν υποστεί επεξεργασία
ΕΡΕΥΝΑ ΛΟΓΑΡΙΑΣΜΩΝ ΟΜΑΔΩΝ

Οι λογαριασμοί ομάδας χρησιμοποιούν το αναγνωριστικό ομάδας που εμφανίζεται στο αρχείο / etc / passwd καθώς και το αρχείο / etc / groups. Ένα τυπικό αρχείο / etc / group μοιάζει με αυτό:

$ cat /etc/group
root::0:root,ashunn
bin::2:root,bin,daemon
sys::3:root,bin,sys,adm
adm::4:root,adm,daemon
uucp::5:root,uucp

Το αρχείο παραθέτει τις ομάδες, μαζί με τους χρήστες που σχετίζονται με αυτήν την ομάδα. Είναι σημαντικό να σημειώσετε ότι δεν χρειάζεται να υπάρχει μια καταχώρηση στο αρχείο ομάδας για να υπάρχει μια ομάδα.

ΕΛΕΓΧΟΣ ΜΗ ΕΞΟΥΣΙΟΔΟΤΗΜΕΝΩΝ ΣΗΜΕΙΩΝ ΠΡΟΣΒΑΣΗΣ

Το Unix είναι ένα πλήρως λειτουργικό, ισχυρό λειτουργικό σύστημα. Με την πάροδο του χρόνου το Unix συνεχώς προσθέτει λειτουργίες, και υπηρεσίες δικτύου όπως το NFS (Network File System), το Telnet κτλ. Τα συστήματα Unix μπορούν δυνητικά να επιτρέψουν κάποιο βαθμό απομακρυσμένης πρόσβασης σε ανεπιθύμητους εισβολείς. Μερικά από τα πιο κοινά σημεία πρόσβασης που έχουμε δει εισβολείς να επωφελούνται περιλαμβάνουν X Servers, FTP, Telnet, TFTP, DNS, sendmail, SNMP, IMAP, POP, HTTP, και HTTPS. Δυστυχώς, πρόκειται για μια μη ολοκληρωμένη λίστα. Καθώς διεξάγετε την έρευνά σας θα πρέπει να εξετάσετε όλες τις υπηρεσίες δικτύου ως πιθανά σημεία πρόσβασης. Οι υπηρεσίες δικτύου θα μπορούσαν να είναι ευάλωτες, επιτρέποντας στους εισβολείς να έχουν πρόσβαση στο σύστημά σας, ή οι υπηρεσίες δικτύου θα μπορούσαν ήδη να είναι ιοί από μια επιτυχημένη εισβολή.

ΑΝΑΛΥΣΗ ΣΧΕΣΕΩΝ ΕΜΠΙΣΤΟΣΥΝΗΣ

Οι σχέσεις εμπιστοσύνης μεταξύ των συστημάτων Unix αποτελούσαν κάποτε πρωταρχικό μηχανισμό επίθεσης. Η εμπιστοσύνη μπορεί να δημιουργηθεί μεταξύ των συστημάτων Unix με μια ποικιλία υπηρεσιών, οι πιο δημοφιλείς περιλαμβάνουν το rlogin, το rsh, την υπηρεσία πληροφοριών δικτύου (NIS και NIS +), το NFS και το ssh. Οι σχέσεις εμπιστοσύνης μπορούν να είναι βολικές εξοικονομήσεις χρόνου για τους διαχειριστές συστημάτων και τους χρήστες. Εάν το μηχάνημα A εμπιστεύεται το μηχάνημα B, τότε ο χρήστης στο μηχάνημα B μπορεί να αποκτήσει πρόσβαση στο μηχάνημα A χωρίς πρόσθετα διαπιστευτήρια. Εάν είστε διαχειριστής συστήματος σε δεκάδες συστήματα η χρήση αυτού του χαρακτηριστικού μπορεί να είναι πολύ δελεαστική. Οι σχέσεις εμπιστοσύνης συνήθως διαμορφώνονται μέσω αρχείων όπως /etc/hosts.equiv ή any.rhosts και μπορούν να δημιουργηθούν με το ssh μέσω κοινόχρηστων κλειδιών. Επιπλέον, τα firewall και οι έλεγχοι πρόσβασης που βασίζονται σε κεντρικούς υπολογιστές, όπως τα TCP Wrappers, διαμορφώνονται συχνά ώστε να επιτρέπουν σε ορισμένες διευθύνσεις IP προέλευσης να επικοινωνούν με προστατευμένους κεντρικούς υπολογιστές αυτή είναι μια άλλη μορφή εμπιστοσύνης.

ΣΥΜΠΕΡΑΣΜΑΤΙΚΑ

Η ανάπτυξη μιας μεθόδου για εγκληματολογικές έρευνες των συστημάτων Unix είναι ζωτικής σημασίας για κάθε περιστατικό επαγγελματικής ανταπόκρισης. Η κατανόηση των χαρακτηριστικών του λειτουργικού συστήματος είναι κρίσιμη συνιστώσα οποιασδήποτε απάντησης, και σε αυτό το κεφάλαιο περιγράφονται μερικά από τα πιο χρήσιμα στοιχεία των συστημάτων Unix που βοηθούν τις έρευνες απόκρισης. Αυτό το κεφάλαιο ανέφερε επίσης μερικές από τις δεξιότητες κριτικής σκέψης που είναι απαραίτητες για την κατανόηση περιστατικών και την αποτελεσματική ανταπόκριση.

ΕΡΩΤΗΣΕΙΣ

- Γιατί τα εξωτερικά αρχεία καταγραφής είναι σημαντικά κατά τη διάρκεια της έρευνας;
- Γιατί οι λειτουργίες του συστήματος που ξεκινούν αυτόματα προγράμματα είναι σημαντικές για τους εισβολείς;
- Ποια η διαφορά μεταξύ mtime και ctime;

ΚΕΦΑΛΑΙΟ 11

ΑΝΑΛΥΣΗ ΤΗΣ ΚΙΝΗΣΗΣ ΤΟΥ ΔΙΚΤΥΟΥ

Σε παλαιότερο κεφάλαιο περιγράψαμε πως εκτελείται ένας πλήρως ικανοποιητικός έλεγχος σε ένα δίκτυο καθώς και το πως συλλέγουμε τα στοιχεία. Εντούτοις, μόλις συλλεχθούν τα στοιχεία πρέπει να είμαστε σε θέση να αναλύσουμε τα όσα συλλέχθηκαν έτσι ώστε να προσδιορίσουμε την απειλή. Αυτό το κεφάλαιο περιγράφει μια πλήρη εξεταστική προσέγγιση της δραστηριότητας του δικτύου (network traffic).

ΕΥΡΕΣΗ ΤΩΝ ΣΤΟΙΧΕΙΩΝ ΠΟΥ ΒΑΣΙΖΟΝΤΑΙ ΣΤΟ ΔΙΚΤΥΟ

Αφού συλλεχθεί το network traffic θα πρέπει να προσδιοριστεί εάν τελικά τα στοιχεία περιλαμβάνουν κάποιο γεγονός που αφορά στην ασφάλεια του δικτύου. Τα στοιχεία που έχουν συλλεχθεί είναι αποθηκευμένα σε δυαδικά αρχεία των οποίων ο όγκος είναι πολύ μεγάλος. Επομένως θα χρειαστεί κάποια μεθοδολογία η οποία να επιτρέπει τον γρήγορο έλεγχό τους. Τα βασικά βήματα εξέτασης είναι τα εξής :

- Προσδιορίστε τα ύποπτα στοιχεία
- Επαναλάβετε ή αναδημιουργήστε τα ύποπτα sessions (εαν είναι TCP,UDP,ICMP ή οποιοδήποτε άλλο πρωτόκολλο)
- Ερμηνεύστε τι εμφανίστηκε

ΕΡΓΑΛΕΙΑ ΑΝΑΛΥΣΗΣ

- **tcptrace** Ένα εργαλείο της Unix. Προσδιορίζει οποιοδήποτε session tcp/udp το οποίο περιλαμβάνετε σε ένα binary αρχείο.
- **snort** Δημοφιλές ανοικτό σύστημα ανίχνευσης παρείσφρυσης δικτύων.

- **tcpflow** Αναδημιουργεί τα tcp sessions
- **ethereal** Είναι ένα δημοφιλές εργαλείο (network sniffer) που έχει καταπληκτικές δυνατότητες και μας επιτρέπει να δούμε τα ανακατασκευασμένα tcp sessions.

ΕΠΑΝΕΞΕΤΑΣΗ ΔΙΚΤΥΟΥ ΜΕ TCPDUMP

Ας υποθέσουμε πως ο web server μας με ip 172.16.1.7 έχει παραβιαστεί και βάση του κεντρικού υπολογιστή δεν έχουμε λάβει κάποιο σημαντικό στοιχείο. Συλλέγουμε λοιπόν την κίνηση του δικτύου για ένα χρονικό διάστημα χρησιμοποιώντας το tcpdump:

tcpdump -x -v -s 1500 -w capturelog host 172.16.1.7

Συλλέξαμε την κυκλοφορία για αρκετές ημέρες και τώρα έχουμε αρκετά binary αρχεία καταγραφής. Στόχος μας είναι να απομονώσουμε γρήγορα τα σημαντικά στοιχεία από τον μεγάλο όγκο δυαδικών αρχείων που έχουμε. Χρησιμοποιούμε συνήθως -X για να εμφανιστούν οι τιμές ASCII και -tttt για να εμφανιστεί ώρα/ημερομηνία. Σε αυτό το σενάριο το αρχείο καταγραφής ονομάζεται sample1.lpc

tcpdump –n –X –tttt –r sample1.lpc | more

Αυτή η εντολή δημιουργεί το ακόλουθο αποτέλεσμα στο παράδειγμά μας :

```
02/10/2003 19:18:18.374744 172.16.1.7.49921 > 66.45.25.71.53:  23864+ PTR?
128.1.16.172.in-addr.arpa. (43)
0x0000   4500 0047 a470 0000 4011 cdaa ac10 0107        E..G.p..@.......
0x0010   422d 1947 c301 0035 0033 b773 5d38 0100        B-.G...5.3.s]8..
0x0020   0001 0000 0000 0000 0331 3238 0131 0231        .........128.1.1
0x0030   3603 3137 3207 696e 2d61 6464 7204 6172        6.172.in-addr.ar
0x0040   7061 0000 0c00 01                              pa.....
02/10/2003 19:18:18.391519 arp who-has 172.16.1.7 tell 172.16.1.254
0x0000   0001 0800 0604 0001 00a0 c5e3 469c ac10        ............F...
0x0010   01fe 0000 0000 0000 ac10 0107 0000 0000        ................
0x0020   0000 0000 0000 0000 0000 0000 0000            ..............
02/10/2003 19:18:18.391566 arp reply 172.16.1.7 is-at 0:3:47:75:18:20
0x0000   0001 0800 0604 0002 0003 4775 1820 ac10        ..........Gu....
0x0010   0107 00a0 c5e3 469c ac10 01fe 0000 0000        ......F.........
0x0020   0000 0000 0000 0000 0000 0000 0000            ..............
02/10/2003 19:18:18.775317 66.45.25.71.53 > 172.16.1.7.49921:  23864 NXDomain
0/1/0 (130) (DF)
0x0000   4500 009e f1ab 4000 f011 9017 422d 1947        E.....@.....B-.G
0x0010   ac10 0107 0035 c301 008a aea1 5d38 8183        .....5......]8..
0x0020   0001 0000 0001 0000 0331 3238 0131 0231        .........128.1.1
0x0030   3603 3137 3207 696e 2d61 6464 7204 6172        6.172.in-addr.ar
0x004   7061 0000 0c00 01c0 1200 0600 0100 0028        pa.............(
0x0050   9c00 4b04 7862 7275 0262 7202 6e73 0765        ..K.xbru.br.ns.e
0x0060   6c73 2d67 6d73 0361 7474 036e 6574 000d        ls-gms.att.net..
0x0070   726d 2d68 6f73 746d 6173 7465 7203 656d        rm-hostmaster.em
0x0080   7303 6174 7403 636f 6d00 0000 0001 0000        s.att.com.......
0x0090   0708 0000 0384 0009 3a80 0009 3a80            ........:...:.
02/10/2003 19:18:21.250143 172.16.1.7.49922 > 66.45.25.71.53:  23865+ PTR?
128.1.16.172.in-addr.arpa. (43)
```

ΔΗΜΙΟΥΡΓΙΑ SESSION DATA ΜΕ TCPTRACE

Μερικές φορές, είναι χρήσιμο να προσδιοριστούν οι διαφορετικές σύνοδοι TCP που περιλαμβάνονται μέσα σε ένα μεγάλο δυαδικό αρχείο. Αυτό είναι μια εργασία για το tcptrace. Μπορείτε να εκτελέσετε το αρχείο καταγραφής μέσω tcptrace, να αποθηκεύσετε τα αποτελέσματά της σε ένα αρχείο ,και στη συνέχεια να δείτε

τα περιεχόμενα αυτού του αρχείου . Το βοηθητικό πρόγραμμα tcptrace έχει πολλά να προσφέρει (πατώντας -h tcptrace εμφανίζετε βοήθεια).

- Το -n "λέει" στο tcptrace να μην επιλύσει θέματα με τις ip και τα ports
- Το -u ζητάει να εμφανιστούν τα udp αρχεία

ΧΡΗΣΗ SNORT ΓΙΑ ΕΞΑΓΩΓΗ ΣΤΟΙΧΕΙΩΝ

Αφότου έχουμε προσδιορίσει κάποια ύποπτη δραστηριότητα, πρέπει να ψάξουμε τα στοιχεία του περιστατικού της σε όλα τα δυαδικά μας συλλεγμένα αρχεία Για να εξάγουμε στοιχεία σαν αυτά πρέπει να δημιουργήσουμε μια γεννήτρια γεγονότων που να ταυτοποιεί τις υπογραφές που ικανοποιούν τα κριτήρια μας. Το snort αποτελεί μια ελεύθερη γεννήτρια γεγονότων που παρέχει έναν αποτελεσματικό τρόπο επεξεργασίας των binary αρχείων.

ΕΛΕΓΧΟΣ ΓΙΑ ΠΑΚΕΤΑ SYN

Για παράδειγμα, ο ακόλουθος Snort κανόνας θα ελέγξει για SYN πακέτα που αποστέλλονται από τον web διακομιστή μας (172.16.1.7)
alert tcp 172.16.1.7 any -> any any (msg: "Outbound connection attempt from Web server"; flags: S;)
Χρησιμοποιώντας τον κανόνα αυτό , μπορούμε εύκολα να μελετήσουμε τα gigabytes των πληροφοριών που έχουν συλλεχθεί. Εφαρμόζουμε τον έλεγχο αυτό με τη ακόλουθη εντολή:
snort -r sample1.lpc -b -l sample_log -c snort.conf

ΕΠΑΝΑΣΥΝΑΡΜΟΛΟΓΗΣΗ SESSION ΜΕ TCPFLOW

Ένα άλλο χρήσιμο εργαλείο είναι tcpflow , το οποίο καταγράφει τα δεδομένα που διαβιβάζονται στο πλαίσιο των συνόδων TCP (flows). Το βοηθητικό πρόγραμμα tcpflow αναδομεί τα πραγματικά ρεύματα δεδομένων και αποθηκεύει κάθε ροή (flow) σε ένα ξεχωριστό αρχείο για μετέπειτα ανάλυση. Κατανοεί αριθμούς ακολουθίας και θα ανακατασκευάσει σωστά ροές δεδομένων , ανεξάρτητα από αναμεταδόσεις. Χρησιμοποιεί ίδια φίλτρα με το tcpdumb πράγμα που το καθιστά εύκολο στη χρήση. Το βοηθητικό αυτό εργαλείο δεν καταλαβαίνει IP διευθύνσεις επομένως τα sessions που περιλαμβάνουν IP δεν θα καταγραφούν σωστά.

ΕΣΤΙΑΖΟΝΤΑΣ ΣΤΑ FTP SESSIONS

Στο ακόλουθο παράδειγμα θα δημιουργήσουμε ένα αρχείο ροής για τα ftp sessions που όπως προσδιορίσαμε προέρχονται από τον server του δικτύου μας .Η ακόλουθη γραμμή εντολών χρησιμοποιεί tcpflow για να ανακατασκευάσει όλο το traffic της θύρας 21

ΠΑΡΑΔΕΙΓΜΑ FTP SESSION

 # tcpflow -v -r sample1.lpc port 21
tcpflow[6502]: tcpflow version 0.20 by Jeremy Elson <jelson@circlemud.org>
tcpflow[6502]: looking for handler for datalink type 1 for interface sample1.lpc
tcpflow[6502]: found max FDs to be 20 using OPEN_MAX
tcpflow[6502]: 198.082.184.028.00021-172.016.001.007.49160: new flow

tcpflow[6502]: 198.082.184.028.00021-172.016.001.007.49160: opening new output file
tcpflow[6502]: 172.016.001.007.49160-198.082.184.028.00021: new flow
tcpflow[6502]: 172.016.001.007.49160-198.082.184.028.00021: opening new output file
tcpflow[6502]: 130.094.149.162.00021-172.016.001.007.49161: new flow
tcpflow[6502]: 130.094.149.162.00021-172.016.001.007.49161: opening new output file
tcpflow[6502]: 172.016.001.007.49161-130.094.149.162.00021: new flow
tcpflow[6502]: 172.016.001.007.49161-130.094.149.162.00021: opening new output file

ΕΡΜΗΝΕΙΑ TCPFLOW OUTPUT

Σε αυτό το παράδειγμα και τρέχοντας το tcpflow για το αρχείο sample1.lpc δημιουργούνται 4 αρχεία:

- 172.016.001.007.49161-130.094.149.162.00021
- 130.094.149.162.00021-172.016.001.007.49161
- 172.016.001.007.49160-198.082.184.028.00021
- 198.082.184.028.00021-172.016.001.007.49160

Κάθε ένα από αυτά τα αρχεία αντιπροσωπεύει μια πλευρά μιας συνομιλίας μιας σύνδεσης FTP. Πρέπει να αναθεωρήσετε όλα αυτά τα αρχεία για να λάβετε τις ενδείξεις σχετικά με τη φύση αυτών των συνόδων FTP.

Για να δείτε τα δεδομένα που αποστέλλονται από τον web server (172.16.1.7) στο διακομιστή FTP (198.82.184.28),

θα δείτε το αρχείο 172.016.001.007.49161-130.094.149.162.00021:

 # cat 172.016.001.007.49160-198.082.184.028.00021

USER anonymous

PASS anon@

QUIT

Αυτό το αρχείο δείχνει μια καταγραφή χρήστη ως ανώνυμη στον απομακρυσμένο διακομιστή FTP, εισάγουμε την εντολή anon @, και στη συνέχεια, για την περάτωση της συνόδου FTP την εντολή QUIT.

Για να δούμε τα δεδομένα που αποστέλλονται από τον διακομιστή FTP (198.82.184.28) στον web server(172.16.1.7), ανοίγουμε το αρχείο 198.082.184.028.00021-172.016.001.007.49160:
cat 198.082.184.028.00021-172.016.001.007.49160
220 raven.cslab.vt.edu FTP server (Version wu-2.6.2(1) Sun Mar 10 20:00:40 GMT
2002) ready.
331 Guest login ok, send your complete e-mail address as password.
530-
530- Sorry, there are too many users using the system at this time.
530- There is currently a limit of 50 users. Please try again later.
530-
530 Login incorrect.
221 Goodbye.
Το περιεχόμενο αυτού του αρχείου μας δείχνει ότι υπήρχαν πάρα πολλοί χρήστες στο διακομιστή FTP 198.82.184.28. Ως εκ τούτου, το πρόσωπο που ξεκίνησε την FTP συνεδρία δεν ήταν σε θέση να συνδεθεί στο σύστημα 198.82.184.28.
Για να δείτε τα δεδομένα που αποστέλλονται από τον web server (172.16.1.7) στο διακομιστή FTP (130.94.149.162),θα δείτε τα περιεχόμενα του αρχείου 172.016.001.007.49161-198.082.184.028.00021:
#cat 172.016.001.007.49161-130.094.149.162.00021

USER anonymous
PASS anon@
SYST
FEAT
PWD
EPSV
LIST
CWD pub
PWD
EPSV
LIST -al
CWD FreeBSD
PWD
EPSV
LIST -al
TYPE I
SIZE dir.sizes
EPSV
RETR dir.sizes
MDTM dir.sizes
QUIT

Με την αναθεώρηση αυτού του αρχείου, μπορούμε να διαπιστώσουμε ότι κάποιος κατέβασε ένα αρχείο με το όνομα "Dir.sizes" για τον web server από το διακομιστή FTP 198.82.184.28. Αυτή η συνεδρία FTP, ξεκίνησε για τον web server (172.16.1.7) από κάποιον χρήστη του δικτύου ή από κάποιον εισβολέα. Για να δούμε τα δεδομένα που αποστέλλονται από το 130.94.149.162 πίσω στον web server 172.16.1.7, πρέπει να αναθεωρήσουμε τα περιεχόμενα του αρχείου 130.094.149.162.00021-172.016.001.007.49161:

 # cat 130.094.149.162.00021-172.016.001.007.49161

220 ftp2.freebsd.org FTP server (Version 6.00LS) ready.
331 Guest login ok, send your email address as password.
230 Guest login ok, access restrictions apply.
215 UNIX Type: L8 Version: BSD-199506
500 'FEAT': command not understood.
257 "/" is current directory.
229 Entering Extended Passive Mode (|||61883|)
150 Opening ASCII mode data connection for '/bin/ls'.
226 Transfer complete.
250 CWD command successful.
257 "/pub" is current directory.
229 Entering Extended Passive Mode (|||61888|)
150 Opening ASCII mode data connection for '/bin/ls'.
226 Transfer complete.
250 CWD command successful.
257 "/pub/FreeBSD" is current directory.
229 Entering Extended Passive Mode (|||61897|)
150 Opening ASCII mode data connection for '/bin/ls'.
226 Transfer complete.
200 Type set to I.
213 15803
229 Entering Extended Passive Mode (|||61904|)
150 Opening BINARY mode data connection for 'dir.sizes' (15803 bytes).

226 Transfer complete.
213 20030209155213
221 Goodbye.
Αυτά τα δύο αρχεία 172.016.001.007.49161-198.082.184.028.00021 και 130.094.149.162.00021-172.016.001.007.49161, αποτελούν τη μια πλευρά της επικοινωνίας.
Μπορούμε χειροκίνητα να ανακατασκευάσουμε το tcp session και να παράγουμε τα ακόλουθα :

Υπάρχουν εργαλεία που θα αναδημιουργήσουν ολόκληρα τα αρχεία,συμπεριλαμβανομένων των πακέτων που προέρχονται και από τα δύο ρεύματα και από τον αποστολέα αλλά και από τον παραλήπτη. Είναι μια απο τις δυνατότητες του Ethereal. Μπορεί να επαναλάβει ολόκληρη τη συνεδρία ή απλώς τη μία πλευρά της συνόδου. Ως εκ τούτου,σπάνια πρέπει να επαναλάβουμε χειροκίνητα την πλήρη συνεδρία συνδυάζοντας πολλαπλά αρχεία από τις εξόδους του tcpflow.
220 ftp2.freebsd.org FTP server (Version 6.00LS) ready.
USER anonymous
331 Guest login ok, send your email address as password.
PASS anon@
230 Guest login ok, access restrictions apply.
SYST
215 UNIX Type: L8 Version: BSD-199506
FEAT
500 'FEAT': command not understood.
PWD
257 "/" is current directory.
EPSV
229 Entering Extended Passive Mode (|||61883|)
LIST
229 Entering Extended Passive Mode (|||61897|)
LIST -al
150 Opening ASCII mode data connection for '/bin/ls'.
226 Transfer complete.
TYPE I
200 Type set to I.
SIZE dir.sizes
213 15803
EPSV
229 Entering Extended Passive Mode (|||61904|)
RETR dir.sizes
150 Opening BINARY mode data connection for 'dir.sizes' (15803 bytes).
226 Transfer complete.
MDTM dir.sizes
213 20030209155213
QUIT
221 Goodbye.

ΥΠΟΣΗΜΕΙΩΣΗ :

Συμπερασματικά λοιπόν παρατηρούμε ότι ο web server (172.16.1.7) ξεκίνησε μια σύνδεση με τη θύρα FTP στο σύστημα 130.94.149.162. Η σύνδεση αποκαλύπτει ότι η 130.94.149.162 έχει το hostname ftp2.freebsd.org. Επίσης, σημειώστε ότι οι εντολές list, list-all και cwd δεν λειτουργούν στον ftp server έτσι οι εντολές που πραγματικά μαρτυρούν το τι συμβαίνει είναι οι control channel commands (ls –al

= LIST –al, bin = TYPE I) . Εάν αυτή η δραστηριότητα είναι ή όχι κανονική εξαρτάται από το εάν είναι ή όχι αποδεκτά αυτά τα είδη των εξερχόμενων συνδέσεων FTP για τον κεντρικό web server σας .

ΒΕΛΤΙΣΤΟΠΟΙΗΣΗ ΦΙΛΤΡΩΝ TCPDUMP

Τις περισσότερες φορές όσοι έχουν πέσει θύμα κάποιας επίθεσης στο δίκτυό τους αναρωτιούνται πως κατάφεραν οι εισβολείς να αποκτήσουν πρόσβαση και είναι δύσκολο να το αντιμετωπίσουν καθώς δεν γνωρίζουν τις μεθόδους που χρησιμοποιούν οι επιτιθέμενοι. Αυτό αποτελεί μια πρόκληση καθώς εάν δεν ξέρουμε τις μεθόδους που χρησιμοποιούν οι επιτιθέμενοι πως είμαστε ικανοί να ξεκινήσουμε έλεγχο της ασφάλειας του δικτύου μας; Ως εκ τούτου χρησιμοποιούμε δικτυακό έλεγχο που που δεν έχει φίλτρα κατά τη διάρκεια των πρώτων ημερών που εμφανίστηκε η επίθεση. Ωστόσο αποκτώντας σιγά σιγά γνώση της τακτικής του επιτιθέμενου προσθέτουμε φίλτρα για να συλλέξουμε τα δεδομένα που μας αφορούν. Στο συγκεκριμένο σενάριο και κατά τη διάρκεια παρακολούθησης του δικτύου με την συνηθισμένη μέθοδο συλλέξαμε πληροφορίες από και προς τον web server μας.

Τώρα λοιπόν που λάβαμε πληροφορίες σχετικά με τις κινήσεις του επιτιθέμενου θέλουμε να αποβάλουμε τον "θόρυβο" (white noise) προσπαθώντας να επικεντρωθούμε στη συλλογή δεδομένων ύποπτης δραστηριότητας. Μπορούμε λοιπόν να ρυθμίσουμε τα φίλτρα μας να συλλέγουν τις IP διευθύνσεις που επικοινώνησαν με το δίκτυο μας τροποποιώντας τα dcpdump φίλτρα με τον εξής τρόπο :

host 172.16.1.7 or net 69.192.1 or host 130.94.149.162 or host 198.82.184.28
Τώρα κάνοντας επανεκκίνηση το dcpdump για να δούμε τι θα συλλέξουμε. Εάν κάποιο άλλο σύστημα στο δίκτυο μας συνδέετε με μηχανές στο 69.192.1.0/24 netblock ή με FTP server στο 130.94.149.162 ή το 198.82.184.28 ίσως να βρήκαμε στοιχεία που αποδεικνύουν παραβίαση του συστήματός μας.

ΣΥΜΠΕΡΑΣΜΑΤΙΚΑ

Δεν είναι καθόλου εύκολο να εξετάσεις τα δισεκατομμύρια αρχεία που περιλαμβάνονται σε ένα δίκτυο έτσι ώστε να εντοπίσεις και να προσδιορίσεις τα ύποπτα αρχεία. Ωστόσο , υπάρχουν μερικά ελεύθερα διαθέσιμα εργαλεία (tcptrace, Snort, tcpflow,Ethereal) που μπορούν να σε βοηθήσουν να αποκτήσεις πιο γρήγορα μια εικόνα της κίνησης του δικτύου σας. Αυτά τα εργαλεία σας βοηθούν να συλλέξετε αλλά και να ερμηνεύσετε τυχόν επιθέσεις.

ΕΡΩΤΗΣΕΙΣ

Ο οργανισμός σας πιστεύει ότι ένα σύστημα με IP 172.16.4.31 έχει παραβιαστεί από έναν υπολογιστή με IP 172.16.3.61 . Δεν είσαι σίγουρος για το πώς το σύστημα μπορεί να έχει παραβιαστεί. Ωστόσο , ξέρεις ότι τα αρχεία καταγραφής του συστήματος για την 172.16.4.31 έχουν διαγραφεί , και ότι κανένα πρόσωπο δεν ήταν συνδεδεμένο στο σύστημα σε τοπικό επίπεδο όταν διαγράφηκαν τα αρχεία . Τι φιλτράρισμα θα εκτελέσεις για την ελαχιστοποίηση υποκλοπής στο traffic του δικτύου;

ΚΕΦΑΛΑΙΟ 12

ΕΡΕΥΝΩΝΤΑΣ ΤΑ ΕΡΓΑΛΕΙΑ ΕΝΟΣ HACKER

Κατά τη διάρκεια των ερευνών για εγκλήματα πληροφορικής, ιδίως για εισβολές σε υπολογιστές, θα συναντήσετε φακέλους των επιτιθέμενων με άγνωστο σκοπό. Ξέρετε ότι το αρχείο αυτό κάνει κάτι που ο επιτιθέμενος θέλει, αλλά το μόνο που έχετε είναι ένα δυαδικό αρχείο και ίσως μερικές θεωρίες σχετικά με το τι κάνει αυτό το αρχείο. Η ανάλυση θα ήταν πολύ πιο εύκολη αν οι εισβολείς άφηναν τον πηγαίο κώδικα πίσω. Αλλά οι περισσότεροι επιτιθέμενοι έχουν κάτι κοινό με τη Microsoft, προστατεύουν τον πηγαίο κώδικα τους.
Σε αυτό το κεφάλαιο, περιγράφουμε μια καλή επιστημονική προσέγγιση για την εκτέλεση της ανάλυσης εργαλείων. Θα μάθετε πώς να λαμβάνετε ένα εκτελέσιμο αρχείο με μια άγνωστη λειτουργία και να εκτελείτε λειτουργίες
για να αποκτήσετε γνώση του σκοπού του φακέλου.

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΣΤΟΙΧΟΙ ΑΝΑΛΥΣΗΣ ΤΩΝ ΕΡΓΑΛΕΙΩΝ

Εάν είστε τυχεροί, τα εργαλεία χάκερ έχουν ονόματα αρχείων που δίνουν πολλές ενδείξεις σχετικά με τη λειτουργία τους. Ένα αρχείο που ονομάζεται sniffer ή esniff είναι πιθανό να είναι ένα εργαλείο sniffer. Ωστόσο, είναι πιο πιθανό οι εισβολείς να μετονομάσουν τον κώδικα σε κάποιο αβλαβές όνομα αρχείου συστήματος όπως xterm ή d.1. Αυτά τα ονόματα προσφέρουν πληροφορίες σχετικά με τη λειτουργία ενός κακόβουλου προγράμματος . Επομένως, θα πρέπει να αναλύσετε αυτά τα εργαλεία για να επιτύχετε τους ακόλουθους στόχους:

- Αποτρέψτε παρόμοιες επιθέσεις στο μέλλον
- Αξιολογήστε το επίπεδο δεξιοτήτων ή απειλών ενός επιτιθέμενου
- Προσδιορίστε την έκταση της παραβίασης
- Προσδιορίστε εάν έχουν προκληθεί ζημιές
- Προσδιορίστε τον αριθμό και τον τύπο των εισβολέων
- Ετοιμάστε τον εαυτό σας για μια επιτυχημένη συνέντευξη στο θέμα, αν πιάσετε τον επιτιθέμενο
- Προσδιορίστε τους στόχους του επιτιθέμενου

ΠΩΣ ΜΕΤΑΓΛΩΤΤΙΖΟΝΤΑΙ ΤΑ ΑΡΧΕΙΑ

Ένας μεταγλωττιστής, όπως ο μεταγλωττιστής GNU C, διαβάζει ένα ολόκληρο πρόγραμμα γραμμένο σε γλώσσα υψηλού επιπέδου, όπως C ή Pascal, και το μετατρέπει σε αντικειμενικό κώδικα, ο οποίος καλείται συχνά κώδικας μηχανής, δυαδικός κώδικας ή εκτελέσιμος κώδικας. Σκεφτείτε τους μεταγλωττιστές ως προγράμματα που μεταφράζουν την ανθρώπινη αναπαράσταση πηγαίου κώδικα στη γλώσσα του μηχανήματος που κατανοεί ένα σύστημα. Υπάρχουν πολλοί τρόποι για τους επιτιθέμενους να συντάξουν τον πηγαίο κώδικα τους. Ορισμένες μέθοδοι σύνταξης καθιστούν την ανάλυση εργαλείων ευκολότερη από άλλες. Είναι κοινή λογική ότι όσο μεγαλύτερο είναι το δυαδικό αρχείο τόσες περισσότερες πληροφορίες μπορούν να λάβουν κατά την εκτέλεση της ανάλυσης του αρχείου οι ερευνητές. Στις επόμενες ενότητες, εξηγούμε τους διαφορετικούς τρόπους που μπορεί να συνταχθεί ένα πρόγραμμα και τον τρόπο με τον οποίο το καθένα επηρεάζει το ποσό των πληροφοριών που είναι διαθέσιμες στον ερευνητή κατά τη διάρκεια του εργαλείου ανάλυσης.

ΣΤΑΤΙΚΩΣ ΣΥΝΔΕΔΕΜΕΝΑ ΠΡΟΓΡΑΜΜΑΤΑ

Ένα στατικά συνδεδεμένο εκτελέσιμο αρχείο περιέχει όλο τον απαραίτητο κώδικα για την επιτυχή εκτέλεση της εφαρμογής. Συνήθως δεν έχει εξαρτήσεις. Αυτό σημαίνει ότι το πρόγραμμα θα λειτουργεί χωρίς να βασίζεται σε συγκεκριμένη έκδοση ενός λειτουργικού συστήματος. Ορισμένες εμπορικές εφαρμογές που μπορείτε να κάνετε λήψη από το Internet, μπορεί να γίνει στατικές ώστε να μην εξαρτώνται από τις βιβλιοθήκες του συστήματός σας. Για παράδειγμα, το StarOffice της Sun Microsystems διανέμεται ως στατικώς συνδεδεμένη συσκευασία. Η Sun διανέμει το StarOffice σε αυτή τη μορφή για να ξεπεράσει τις διαφορές στις διάφορες κατανομές του λειτουργικού συστήματος Linux. Ακολουθεί ένα παράδειγμα μιας εντολής για τη στατική καταγραφή ενός προγράμματος μέσα στο λειτουργικό σύστημα Linux χρησιμοποιώντας τον μεταγλωττιστή GNU: **gcc -static zap.c -o zapstatic**

- Ο πηγαίος κώδικας zap.c συντάχθηκε για να δημιουργήσει ένα στατικά συνδεδεμένο αντικείμενο αρχείο που ονομάζεται zapstatic.

ΔΥΝΑΜΙΚΑ ΣΥΝΔΕΔΕΜΕΝΑ ΠΡΟΓΡΑΜΜΑΤΑ

Σχεδόν όλα τα σύγχρονα λειτουργικά συστήματα υποστηρίζουν τη χρήση κοινών βιβλιοθηκών, οι οποίες περιέχουν συνήθεις λειτουργίες. Συντάσσοντας ένα πρόγραμμα για τη χρήση των κοινόχρηστων βιβλιοθηκών, ένας προγραμματιστής μπορεί να παραπέμπεται κάπου στη μνήμη όταν το πρόγραμμα χρειάζεται να χρησιμοποιήσει αυτές τις λειτουργίες αντί να ενσωματώσει όλο αυτό τον κώδικα στην ίδια την εφαρμογή. Αυτό μειώνει το μέγεθος του εκτελέσιμου αρχείου, εξοικονομεί μνήμη συστήματος και επιτρέπει ενημερώσεις στις κοινόχρηστες βιβλιοθήκες χωρίς να χρειάζεται να αλλάξει οποιοδήποτε από τα αρχικά προγράμματα. Τα προγράμματα που χρησιμοποιούν κοινόχρηστες βιβλιοθήκες είναι συνταγμένα δυναμικά. Χρησιμοποιώντας τον μεταγλωττιστή GNU, η ακόλουθη γραμμή εντολών αποδίδει ένα εκτελέσιμο αρχείο που έχει δημιουργηθεί δυναμικά: **gcc zap.c -o zap_out**

- **Η προεπιλεγμένη συμπεριφορά του μεταγλωττιστή GNU δημιουργεί ένα δυναμικά συνδεδεμένο εκτελέσιμο αρχείο**

ΠΡΟΓΡΑΜΜΑΤΑ ΜΕ ΕΠΙΛΟΓΕΣ ΕΝΤΟΠΙΣΜΟΥ ΣΦΑΛΜΑΤΩΝ 1/2

Σε σπάνιες περιπτώσεις, θα είστε αρκετά τυχεροί να συναντήσετε εργαλεία hacker που έχουν συνταχθεί σε λειτουργία εντοπισμού σφαλμάτων. Οι συλλογές εντοπισμού σφαλμάτων χρησιμοποιούνται συνήθως από προγραμματιστές λογισμικού κατά τα πρώτα στάδια της ανάπτυξης του προγράμματος για να τους βοηθήσουν να επιλύσουν προβλήματα και να βελτιστοποιήσουν τον κώδικα τους. Όταν είναι

ενεργοποιημένες οι επιλογές εντοπισμού σφαλμάτων, ο μεταγλωττιστής θα περιλαμβάνει πολλές πληροφορίες σχετικά με το πρόγραμμα και τον πηγαίο κώδικα του. Η ακόλουθη γραμμή εντολών δείχνει πώς θα χρησιμοποιούσατε τον μεταγλωττιστή GNU για να μεταγλωττίσετε το αρχείο πηγαίου κώδικα zap.c με ενεργοποιημένες τις επιλογές εντοπισμού σφαλμάτων. Παρατηρήστε ότι αυτό επιτυγχάνεται προσθέτοντας την επιλογή -g στη γραμμή εντολών:

* **gcc -g zap.c -o zapdebug**

ΠΡΟΓΡΑΜΜΑΤΑ ΜΕ ΕΠΙΛΟΓΕΣ ΕΝΤΟΠΙΣΜΟΥ ΣΦΑΛΜΑΤΩΝ 2/2

Το ακόλουθο είναι μια λίστα ενός καταλόγου που περιέχει το εργαλείο καταγραφής zap που δημιουργήθηκε δυναμικά, στατικά και με επιλογές αποσφαλμάτωσης. Παρατηρήστε το μέγεθος κάθε έκδοσης. Το δυναμικά μεταγλωττισμένο zap είναι 13,217 bytes και το στατικό zap 1,587,273 bytes σε μέγεθος. Το static zap binary αρχείο είναι περισσότερο από 120 φορές μεγαλύτερο από το δυναμικό συνημμένο αρχείο. Η έκδοση εντοπισμού σφαλμάτων περιέχει επιπλέον δεδομένα, καθιστώντας το σχεδόν διπλάσιο από το μέγεθος του δυναμικά καταρτισμένου zap.

```
root@conan zap]# ls -al
mtotal 1604
drwxr-xr-x   2 root     root         1024 Mar 22 08:10 .
drwxr-xr-x   3 root     root         1024 Mar 22 08:06 ..
-rwxr-xr-x   1 root     root         1972 Mar 22 08:05 zap.c
-rwxr-xr-x   1 root     root        25657 Mar 22 08:06 zapdebug
-rwxr-xr-x   1 root     root        13217 Mar 22 08:08 zapdynamic
-rwxr-xr-x   1 root     root      1587273 Mar 22 08:05 zapstatic
```

STIRPPED ΠΡΟΓΡΑΜΜΑΤΑ 1/2

Το strip είναι μια λειτουργία που απορρίπτει όλα τα σύμβολα από τον κώδικα αντικειμένου για να κάνει ένα αρχείο πολύ μικρότερο και ίσως πιο βέλτιστο για εκτέλεση. Δεδομένου ότι τα απογυμνωμένα, δυναμικά συνταγμένα προγράμματα έχουν ως αποτέλεσμα το μικρότερο εκτελέσιμο μέγεθος επομένως είναι πιο δύσκολο για έναν ερευνητή να τα αναλύσει όταν χρησιμοποιεί τεχνικές εξαγωγής συμβολοσειρών (strings) και συμβόλων. Για παράδειγμα, εάν το αρχείο δεν έχει απογυμνωθεί και περιέχει σύμβολα και strings θα τα εμφανιστεί η εντολή nm. Αντίθετα, η εντολή strip θα αφαιρέσει αυτές τις πληροφορίες. Η ακόλουθη γραμμή εντολών επιδεικνύει τη χρήση της έκδοσης GNU strip και δείχνει πόσο μικρότερη γίνεται η σύγκριση της δυναμικά μεταγλωττισμένης, απογυμνωμένης εκδοχής του zap στα αρχεία που δημιουργήθηκαν:

STIRPPED ΠΡΟΓΡΑΜΜΑΤΑ 2/2

Παρατηρήστε ότι η απογύμνωση του δυναμικά συνδεδεμένου προγράμματος zap (zapdynamic) συρρικνώνει το μέγεθος του αρχείου από το αρχικό του μέγεθος 13.217 byte (όπως είδαμε σε προηγούμενο παράδειγμα) σε 4.400 byte.

```
[root@conan zap]# strip zapdynamic
[root@conan zap]# ls -al
total 1595
drwxr-xr-x   2 root     root        1024 Mar 22 08:10 .
drwxr-xr-x   3 root     root        1024 Mar 22 08:06 ..
-rwxr-xr-x   1 root     root        1972 Mar 22 08:05 zap.c
-rwxr-xr-x   1 root     root       25657 Mar 22 08:06 zapdebug
-rwxr-xr-x   1 root     root        4400 Mar 22 08:10 zapdynamic
-rwxr-xr-x   1 root     root     1587273 Mar 22 08:05 zapstatic
```

ΠΡΟΓΡΑΜΜΑΤΑ ΜΕ UPX

Το UPX(Ultimate Packer για eXecutables) είναι ένα αποτελεσματικό εργαλείο συμπίεσης για εκτελέσιμα αρχεία. Ίσως ένας άλλος λόγος για τη δημοτικότητά του είναι ότι οι επιτιθέμενοι μπορούν να το χρησιμοποιήσουν για να αποκρύψουν τα παράνομα προγράμματα τους από IDS με βάση την υπογραφή. Το UPX θα συμπιέσει και θα αποσυμπιέσει εφαρμογές Linux και Win32, καθώς και αρχεία εκτελέσιμων αρχείων DOS 16 bit και .com, αρχεία COF DOS 32 bit, εκτελέσιμα αρχεία DOS 32 bit και εκτελέσιμα αρχεία Atari TOS / MiNT. Μια ανασκόπηση των string με μορφή ASCII μέσα στον κώδικα των επιτιθέμενων θα δείξει εάν το UPX χρησιμοποιήθηκε για τη συμπίεση του εκτελέσιμου. Αν βρείτε ένα εκτελέσιμο με UPX, θα πρέπει να το αποσυμπιέσετε χρησιμοποιώντας το UPX για να μπορέσετε να ελέγξετε τις συμβολοσειρές που περιέχονται στο κανονικό εκτελέσιμο αρχείο. Μπορείτε να ελέγξετε τις συμβολοσειρές σε ένα αρχείο χρησιμοποιώντας την εντολή strings όπως θα δούμε παρακάτω.

ΣΤΑΤΙΚΗ ΑΝΑΛΥΣΗ ΕΡΓΑΛΕΙΟΥ HACKER

Η στατική ανάλυση είναι η ανάλυση εργαλείων που εκτελείται χωρίς να εκτελείται ο κακόβουλος κώδικας. Επειδή δεν σκοπεύετε να εκτελέσετε τον κακόβουλο κώδικα κατά τη διάρκεια της στατικής ανάλυσης, μπορείτε να εκτελέσετε στατική ανάλυση σε οποιοδήποτε λειτουργικό σύστημα, ανεξάρτητα από τον τύπο του αντικειμενικού κώδικα. Για παράδειγμα, μπορείτε να χρησιμοποιήσετε το λειτουργικό σύστημα Solaris για να εκτελέσετε στατική ανάλυση μιας Win32 εφαρμογής. Η γενική προσέγγιση της στατικής ανάλυσης περιλαμβάνει τα ακόλουθα βήματα:

- Προσδιορίστε τον τύπο του αρχείου που εξετάζετε.
- Ελέγξτε τις συμβολοσειρές ASCII και Unicode που περιέχονται στο δυαδικό αρχείο.
- Εκτελέστε έρευνα στο διαδίκτυο για να διαπιστώσετε αν το εργαλείο είναι διαθέσιμο στο κοινό στις τοποθεσίες ασφάλειας υπολογιστών ή hacker.
- Εκτελέστε αναθεώρηση πηγαίου κώδικα εάν έχετε είτε τον πηγαίο κώδικα είτε πιστεύετε ότι έχετε εντοπίσει τον πηγαίο κώδικα μέσω online έρευνας

ΠΡΟΣΔΙΟΡΙΣΤΕ ΤΟΝ ΤΥΠΟ ΤΟΥ ΑΡΧΕΙΟΥ

Αφού εντοπίσετε τα εκτελέσιμα αρχεία που απαιτούν ανάλυση εργαλείων, ακολουθήστε το επόμενο βήμα για να καθορίσετε τον τρόπο υπολογισμού των εκτελέσιμων αρχείων, καθώς και το εγγενές λειτουργικό σύστημα και την αρχιτεκτονική τους. Υπάρχουν πολλοί διαφορετικοί τύποι εκτελέσιμων αρχείων που μπορεί να συναντήσετε. Ευτυχώς, το Unix και τα Windows παρέχουν μια εντολή που ανακτά τις απαραίτητες πληροφορίες.

ΧΡΗΣΙΜΟΠΟΙΩΝΤΑΣ ΤΗΝ ΕΝΤΟΛΗ ΑΡΧΕΙΟΥ UNIX

Η τυπική εντολή για τον προσδιορισμό ενός τύπου αρχείου σε συστήματα Unix είναι αρχείο. Το ακόλουθο παράδειγμα δείχνει τα αποτελέσματα της χρήσης της εντολής αρχείου σε διάφορους τύπους εκτελέσιμων προγραμμάτων:

```
[root@conan zap] file *
rinetd.exe:  MS-DOS executable (EXE), OS/2 or MS Windows
zap.c:       C program text
zapdebug:    ELF 32-bit LSB executable, Intel 80386, version 1,
dynamically linked (uses shared libs), not stripped
zapdynamic:  ELF 32-bit LSB executable, Intel 80386, version 1,
dynamically linked (uses shared libs), not stripped
zapstatic:   ELF 32-bit LSB executable, Intel 80386, version 1,
statically linked, not stripped
zapstripped: ELF 32-bit LSB executable, Intel 80386, version 1,
dynamically linked (uses shared libs), stripped
```

ΑΝΑΣΚΟΠΗΣΗ ΤΩΝ ASCII STRINGS

Η βασική στατική ανάλυση του κώδικα αντικειμένου περιλαμβάνει την εξέταση των συμβολοσειρών με μορφή ASCII του δυαδικού αρχείου. Προσδιορίζοντας τις λέξεις-κλειδιά, τα επιχειρήματα της γραμμής εντολών και τις μεταβλητές, θα αποκτήσετε κάποια εικόνα για τον σκοπό του προγράμματος. Η εντολή που χρησιμοποιείται για την εξαγωγή συμβολοσειρών ASCII είναι strings. Η εντολή συμβολοσειρών είναι στάνταρ στις περισσότερες παραλλαγές Unix και είναι διαθέσιμη για Windows από την ιστοσελίδα Sysinternals. Η εντολή συμβολοσειρών έχει την ακόλουθη σύνταξη**: strings -a filename**

Αυτή η γραμμή εντολών θα εμφανίσει όλες τις συμβολοσειρές ASCII που περιέχονται στον κώδικα αντικειμένου που είναι τέσσερις ή περισσότεροι χαρακτήρες. Παρατηρήστε την επιλογή -a. Αν παραλειφθεί αυτή η επιλογή, η παραλλαγή Unix θα σαρώσει μόνο τμήματα του δυαδικού αρχείου.

ΑΝΑΣΚΟΠΗΣΗ ΤΩΝ UNICODE STRINGS

Σε εκτελέσιμα αρχεία με βάση τα Windows, είναι σημαντικό να εκτελέσετε επίσης αναζήτηση Unicode Strings. Τα Windows βασίζονται στο Unicode και πολλές εφαρμογές που βασίζονται στα Windows χρησιμοποιούν το Unicode. Το βοηθητικό πρόγραμμα συμβολοσειρών που είναι διαθέσιμο για τα Windows είναι προεπιλεγμένο για εκτέλεση μιας αναζήτησης Unicode όταν χρησιμοποιείται μόνο με το όνομα αρχείου ως το όρισμα της γραμμής εντολών. Το Unicode είναι ένα τυποποιημένο σύνολο χαρακτήρων που χρησιμοποιεί τιμές 2 byte για να αντιπροσωπεύει έναν χαρακτήρα. Επειδή το Unicode χρησιμοποιεί 16 bits για να αντιπροσωπεύει ένα μόνο χαρακτήρα, υπάρχουν περισσότεροι από 65.000 χαρακτήρες διαθέσιμοι, οι οποίοι το καθιστούν ικανό να κωδικοποιεί χαρακτήρες από πολλές διαφορετικές γλώσσες.

ΥΠΟΣΗΜΕΙΩΣΗ ASCII ΚΑΙ UNICODE STRINGS

Όταν εξετάζετε τις συμβολοσειρές στον κώδικα αντικειμένου, αναζητήστε τα ακόλουθα στοιχεία:

- Το όνομα των αρχείων πηγαίου κώδικα πριν η εφαρμογή συνταχθεί.
- Ο ακριβής μεταγλωττιστής που χρησιμοποιήθηκε για τη δημιουργία του αρχείου.
- Τα strings "βοηθείας" στο εργαλείο.
- Τα μηνύματα σφάλματος που εμφανίζει το πρόγραμμα.
- Την τιμή των στατικών μεταβλητών.

ΕΚΤΕΛΕΣΗ ONLINE ΕΡΕΥΝΑΣ

Η γνώση ύπαρξης άλλων επιθέσεων που περιλαμβάνουν τα ίδια εργαλεία που έχετε ανακαλύψει είναι πολύ χρήσιμη. Μπορείτε να εκτελέσετε την εντολή συμβολοσειρών σε κακόβουλα εκτελέσιμα αρχεία για να προσδιορίσετε τον μεταγλωττιστή που χρησιμοποιήθηκε για τη δημιουργία του εκτελέσιμου αρχείου. Αν βρείτε ένα ηλεκτρονικό εργαλείο που φαίνεται να έχει παρόμοια λειτουργία, μπορείτε να μεταγλωττίσετε τον πηγαίο κώδικα που είναι διαθέσιμος στο κοινό με τον ίδιο μεταγλωττιστή που χρησιμοποιήθηκε από τον επιτιθέμενο και να εξετάσετε το μέγεθος του αρχείου που προκύπτει. Το μέγεθος μπορεί να υποδηλώνει ότι τα εργαλεία είναι παρόμοια. Εάν τα εργαλεία έχουν το ίδιο μέγεθος, τότε μόλις βρήκατε τον πηγαίο κώδικα στο εργαλείο που χρησιμοποιεί ο hacker.

ΕΚΤΕΛΕΣΗ ΑΝΑΘΕΩΡΗΣΗΣ ΠΗΓΑΙΟΥ ΚΩΔΙΚΑ

Με τον πηγαίο κώδικα που έχετε στη διάθεσή σας για έλεγχο, θα είστε σε θέση να καθορίσετε ακριβώς τι κάνει ένα αδίστακτο πρόγραμμα. Επομένως, η απόκτηση του πηγαίου κώδικα είναι ίσως το καλύτερο μέτρο για την εκτέλεση εκτενούς στατικής ανάλυσης ενός προγράμματος. Η διεξαγωγή ανασκόπησης πηγαίου κώδικα απαιτεί γνώση της γλώσσας προγραμματισμού που χρησιμοποιείται για τη δημιουργία του εργαλείου.

ΔΥΝΑΜΙΚΗ ΑΝΑΛΥΣΗ ΕΡΓΑΛΕΙΟΥ HACKER

Η δυναμική ανάλυση ενός εργαλείου λαμβάνει χώρα όταν εκτελείτε τον κακόβουλο κώδικα και ερμηνεύετε την αλληλεπίδρασή του με το λειτουργικό σύστημα υποδοχής. Αυτό μπορεί να είναι επικίνδυνο, διότι όποια ασθένεια επιφέρει ο κακόβουλος κώδικας μπορεί να λάβει χώρα στον εγκληματολογικό σταθμό εργασίας σας. Ωστόσο, αυτή είναι συχνά η πιο διαφωτιστική μορφή ανάλυσης εργαλείων. Η μεθοδολογία μας περιλαμβάνει τα ακόλουθα:

- Παρακολουθήστε τις σφραγίδες ώρας / ημερομηνίας για να προσδιορίσετε τα αρχεία που επηρεάζουν ένα εργαλείο.
- Εκτελέστε το πρόγραμμα για να υποκλέψετε τις κλήσεις του συστήματος.
- Εκτελέστε παρακολούθηση δικτύου για να προσδιορίσετε εάν δημιουργείται οποιαδήποτε κίνηση δικτύου.
- Ελέγξτε πώς αλληλεπιδρούν τα εκτελέσιμα αρχεία με το μητρώο με βάση τα Windows

ΔΥΝΑΜΙΚΗ ΑΝΑΛΥΣΗ ΣΕ ΣΥΣΤΗΜΑ UNIX

Οι περισσότερες εφαρμογές εκτελούνται σε μια περιοχή μνήμης που ορίζεται ως χώρος χρήστη. Οι εφαρμογές χώρου χρηστών απαγορεύονται τυπικά να έχουν άμεση πρόσβαση στο hardware και τους πόρους του υπολογιστή.. Αυτοί οι πόροι ελέγχονται από τον πυρήνα για να επιβάλουν την ασφάλεια, να διατηρήσουν μη συνεχή χρήση και να παρέχουν σταθερότητα στο λειτουργικό σύστημα. Οι εφαρμογές χρηστών έχουν πρόσβαση σε αυτούς τους πόρους ζητώντας από τον πυρήνα να εκτελεί τις πράξεις για λογαριασμό του. Η εφαρμογή χρήστη κάνει αυτά τα αιτήματα στον πυρήνα μέσω κλήσεων συστήματος. Το Unix διαθέτει ένα εργαλείο που εντοπίζει τη χρήση κλήσεων συστήματος από μια εκτελεσθείσα διαδικασία. Αυτό το εργαλείο, που ονομάζεται strace (System trace), είναι ουσιαστικά μια υποκλοπή μεταξύ ενός προγράμματος και του λειτουργικού συστήματος. Η εντολή strace εμφανίζει πληροφορίες σχετικά με την πρόσβαση στο αρχείο, την πρόσβαση στο δίκτυο, την πρόσβαση μνήμης και πολλές άλλες κλήσεις συστήματος που κάνει ένα αρχείο όταν εκτελείται.

ΔΥΝΑΜΙΚΗ ΑΝΑΛΥΣΗ ΣΕ ΣΥΣΤΗΜΑΤΑ WINDOWS

Η δυναμική ανάλυση μιας εφαρμογής που βασίζεται στα Windows είναι λίγο διαφορετική από την ανάλυση των εργαλείων που βασίζονται στο Unix, αλλά οι βασικές έννοιες είναι οι ίδιες. Εκτελείτε τον ύποπτο κώδικα και χρησιμοποιείτε βοηθητικά προγράμματα για να παρακολουθήσετε πώς αλληλεπιδρά η διαδικασία αθέμιτων ενεργειών με το σύστημα αρχείων, το μητρώο, τις διεπαφές προγραμματισμού εφαρμογών (API) και το λειτουργικό σύστημα. Για τη δυναμική ανάλυση των εφαρμογών των Windows, χρησιμοποιούμε τα εργαλεία Filemon, Regmon, ListDLLs, Fport και PsList.

ΠΕΡΑΙΤΕΡΩ ΑΝΑΛΥΣΗ ΣΤΑ WINDOWS

Τα εργαλεία που περιγράφονται σε αυτό το κεφάλαιο παρέχουν το πρώτο επίπεδο ανάλυσης. Ωστόσο, όπως και με την ανάλυση Unix, είναι διαθέσιμες πιο ολοκληρωμένες τεχνικές για την ανάλυση των Windows. Η αποσυμπίεση και η αποσφαλμάτωση είναι τα επόμενα βήματα. Μερικά εξαιρετικά εργαλεία σε αυτόν τον τομέα είναι το IDA Pro (ένας διαδραστικός αποσυναρμολογητής) και το SoftICE (ένα πρόγραμμα εντοπισμού σφαλμάτων σε επίπεδο πηγής). Το IDA Pro παρέχει δυνατότητες αποσυναρμολόγησης για μια μεγάλη ποικιλία λειτουργικών συστημάτων και μορφών αρχείων. Το λογισμικό SoftICE παρέχει δυνατότητες εντοπισμού σφαλμάτων για συστήματα Windows.

ΣΥΜΠΕΡΑΣΜΑΤΙΚΑ

Η σωστή ανάλυση εργαλείων μπορεί να βοηθήσει στην πρόληψη μελλοντικών επιθέσεων, να καθορίσει την έκταση της επίθεσης και να καθορίσει τον αριθμό και τον τύπο των εισβολέων. Βοηθά δραματικά κατά τη διάρκεια των συνεντεύξεων του θέματος. Χρησιμοποιήσαμε ανάλυση εργαλείων για τον εντοπισμό ομάδων hacker, τη συσχέτιση διαφορετικών επιθέσεων και την αξιολόγηση του επιπέδου δεξιοτήτων ή απειλών ενός εισβολέα. Η σωστή ανάλυση εργαλείων είναι εξαιρετικά χρήσιμη κατά τη φάση περιορισμού και καθαρισμού της απόκρισης σε περιστατικά. Αφού εντοπίσετε τον τύπο, τα ονόματα και την τοποθεσία των εργαλείων, μπορείτε να σαρώσετε το δίκτυο για άλλες εμφανίσεις του ίδιου εργαλείου.

ΕΡΩΤΗΣΕΙΣ

- Ποιο είδος binary είναι πιο δύσκολο να αναλυθεί: δυναμικά ή στατικά συνταγμένο και γιατί;
- Πώς μπορούν να ληφθούν τα εργαλεία χάκερ όταν δεν υπάρχει αποθηκευμένο εκτελέσιμο αρχείο στο σύστημα αρχείων;
- Είναι σημαντικό το συγκεκριμένο λειτουργικό σύστημα που χρησιμοποιεί ο εγκληματολογικός ερευνητής κατά τη στατική ανάλυση; Γιατί ή γιατί όχι;
- Περιγράψτε τους κρίσιμους παράγοντες που απαιτούνται για τη δυναμική ανάλυση

ΚΕΦΑΛΑΙΟ 13

ΕΡΕΥΝΩΝΤΑΣ ΤΟΥΣ ROUTERS

Τα routers παίζουν πολλούς και διαφορετικούς ρόλους κατά τη διάρκεια ενός περιστατικού. Αποτελούν στόχο και πέρασμα για τους επιτιθέμενους αλλά και εργαλείο για τους ερευνητές της επίθεσης. Παρέχουν ποικιλία πληροφοριών και αποδεικτικών στοιχείων που επιτρέπουν στους ερευνητές να επιλύσουν περίπλοκα περιστατικά του δικτύου. Τα routers είναι πιο πιθανό να αποτελέσουν αφετηρία για τους επιτιθέμενους κατά τη διάρκεια της διείσδυσής τους στο δίκτυο. Οι πληροφορίες όπως κωδικοί, πίνακες δρομολόγησης κ.α αποθηκεύονται στους δρομολογητές καθιστώντας τους έτσι πολύτιμο πρώτο βήμα για τους επιτιθέμενους. Σε αυτό το κεφάλαιο θα αναλύσουμε τις πληροφορίες που αποθηκεύει ένα router καθώς και το πως αυτές οι πληροφορίες βοηθούν τους επιτιθέμενους αλλά και τους ερευνητές.

ΑΠΟΚΤΗΣΗ ΕΥΜΕΤΑΒΛΗΤΩΝ ΣΤΟΙΧΕΙΩΝ

Όπως πάντα, ξεκινάμε τη διαδικασία ανταπόκρισης σε ένα περιστατικό αποκτώντας πρώτα τα πιο ευμετάβλητα στοιχεία. Η σειρά της μεταβλητότητας δηλώνει ότι οι πληροφορίες στη μνήμη είναι πιο ασταθής , ενώ οι πληροφορίες που αποθηκεύονται στο σκληρό δίσκο ή σε μη ευμετάβλητη μνήμη RAM (NVRAM) είναι σχετικά σταθερές. Αναλόγως, εάν οποιαδήποτε από τις πληροφορίες στη μνήμη μπορεί να είναι σημαντική για την έρευνα , θα πρέπει να σωθεί πριν να απενεργοποιήσετε ή να μεταβληθεί η κατάσταση του δρομολογητή. Με τους δρομολογητές , οι πληροφορίες στη μνήμη είναι σχεδόν πάντα σημαντικές , επειδή οι δρομολογητές έχουν μια μικρή ικανότητα αποθήκευσης δεδομένων. Τα μόνα πραγματικά δεδομένα που είναι σωμένα στη NVRAM είναι η διαμόρφωση του ίδιου του δρομολογητή, και αυτή η διαμόρφωση δεν είναι ακριβώς ίδια με τις ρυθμίσεις που έχει ο δρομολογητής ενώ βρίσκεται σε λειτουργία,ειδικά εάν ο δρομολογητής έχει αποτελέσει αντικείμενο επίθεσης χάκερ. Η κατάσταση του συστήματος και οι πληροφορίες που υπάρχουν στην μνήμη , όπως οι τρέχοντες κωδικοί πρόσβασης ή οι πίνακες δρομολόγησης θα χαθούν εάν ο δρομολογητής απενεργοποιηθεί ή επανεκκινηθεί.

ΥΠΟΣΗΜΕΙΩΣΗ

Τα βήματα που θα αναλυθούν είναι πολύ σημαντικά για τα routers που έχουν υποστεί παραβίαση και επίθεση. Οι πληροφορίες από αυτά τα βήματα διερεύνησης θα σας επιτρέψουν να καθορίσετε εάν η ρύθμιση του δρομολογητή δεν είναι η αναμενόμενη , υποδεικνύοντας μια συμβιβαστική λύση. Οι πληροφορίες σχετικά με τη διαμόρφωση του δρομολογητή θα παράσχουν επίσης μια σαφή εικόνα για το πως δρομολογούνται τα πακέτα εντός του δικτύου. Ανάλογα με τις λεπτομέρειες μιας συγκεκριμένης επίθεσης, αν υποψιάζεστε ας πούμε ότι ο δρομολογητής αποτελεί ενεργό μέρος της επίθεσης ή απλώς σκαλοπάτι, μπορείτε να επιλέξετε να παραλείψετε ή να αλλάξετε τη σειρά ορισμένων βημάτων.

ΔΗΜΙΟΥΡΓΙΑ ΣΥΝΔΕΣΗΣ ROUTER

Πριν κάνετε οτιδήποτε, HP πρέπει να δημιουργήσετε μια σύνδεση με το router. Ο καλύτερος τρόπος για να αποκτήσετε πρόσβαση στο router είναι απευθείας στη θύρα console. Αν η πρόσβαση κονσόλας δεν είναι διαθέσιμη, μια dial up σύνδεση ή ένα κρυπτογραφημένο πρωτόκολλο όπως το Secure Shell (SSH) είναι μια καλύτερη επιλογή από telnet.

ΥΠΟΣΗΜΕΙΩΣΗ

Οι περισσότεροι δρομολογητές απαιτούν εξειδικευμένο εξοπλισμό για την πρόσβαση κονσόλας . Για τους περισσότερους δρομολογητές Cisco , θα χρειαστείτε ένα RJ - 45 καλώδιο rollover (διαφορετικό από το crossover) και ένα RJ - 45 σε -DB - 9 θηλυκό DTE προσαρμογέα (οι προσαρμογείς κανονικά βρίσκονται με την ένδειξη " Terminal") Θα χρειαστείτε επίσης ένα laptop ή έναν σταθερό H/Y με εγκατεστημένο το κατάλληλο λογισμικό (π.χ Hyperterminal software).Κατά την εγκατάσταση μιας σύνδεσης στο δρομολογητή, σιγουρευτείτε ότι θα καταγράψετε ολόκληρη τη σύνοδο. Με το Hyperterminal επιλέξτε Transfer | Capture Text για να καταγράψετε τα όσα θέλετε. Η γλώσσα εντολής λειτουργικών συστημάτων της Cisco Internetwork (IOS) έχει πολλά modes όπως (initial setup, login prompt, basic command, enable, configuration, and interface configuration)

ΚΑΤΑΓΡΑΦΗ ΩΡΑΣ ΣΥΣΤΗΜΑΤΟΣ

Ένα από τα πρώτα σας βήματα θα πρέπει να είναι να καταγράψει την ώρα του συστήματος. Τα επιμέρους συστήματα συχνά έχουν διαφορετικές ρυθμίσεις του χρόνου . Χρησιμοποιήστε την εντολή show clock για να λάβετε το χρόνο του συστήματος (enable, or privileged, level access is not required).

- e.g :
- cisco_router>show clock
- 03:13:21.511 UTC Tue Mar 2 2003

ΠΡΟΣΔΙΟΡΙΣΤΕ ΠΟΙΟΙ ΕΙΝΑΙ ΣΥΝΔΕΔΕΜΕΝΟΙ 1/2

Το επόμενο βήμα είναι να δείτε ποιοι άλλοι είναι συνδεδεμένοι στο router. Χρησιμοποιείστε την εντολή show users ή την εντολή systat για να λάβετε στοιχεία όπως τα εξής :

```
cisco_router>show users
Line User Host(s) Idle Location
* 0 con 0  idle 00:29:46
1 vty   0    idle 00:00:00 10.0.2.71
2 vty   1 10.0.2.18 00:00:36 172.16.1.1
```

ΠΡΟΣΔΙΟΡΙΣΤΕ ΠΟΙΟΙ ΕΙΝΑΙ ΣΥΝΔΕΔΕΜΕΝΟΙ 2/2

Το προηγούμενο αποτέλεσμα μας δείχνει πως 3 χρήστες είναι συνδεδεμένοι:

- Η πρώτη καταχώρηση δείχνει ότι κάποιος είναι συνδεδεμένος σε κονσόλα (con) . Ο αστερίσκος (*) στα αριστερά δείχνει ότι αυτή είναι η σύνδεσή μας.
- Η δεύτερη είσοδος είναι μια VTY , ή εικονική γραμμή τερματικού. Αυτό δείχνει ότι κάποιος είναι συνδεδεμένος στο δρομολογητή από ξενιστή με τη διεύθυνση IP 10.0.2.71
- Η τελική σύνδεση VTY δείχνει ότι κάποιος έχει συνδεθεί από διεύθυνση IP 172.16.1.1 , και το ίδιο πρόσωπο έχει καθιερώσει μια σύνδεση από το δρομολογητή στον κεντρικό υπολογιστή με διεύθυνση IP 10.0.2.18
- **Όπως μπορείτε να δείτε, αυτές είναι χρήσιμες πληροφορίες κατά τη διερεύνηση περιστατικών.**

ΧΡΟΝΟΣ ΛΕΙΤΟΥΡΓΙΑΣ ROUTER

Η χρονική περίοδος που το σύστημα ήταν ενεργό μέχρι το τελευταίο reboot είναι πολύ σημαντική. Χρησιμοποιείστε την εντολή show version για να συλλέξετε τις εξής πληροφορίες :

```
cisco_router>show version
Cisco Internetwork Operating System Software
IOS (tm) 1600 Software (C1600-Y-M), Version 11.3(5)T, RELEASE      SOFTWARE (fc1)
Copyright (c) 1986-1998 by cisco Systems, Inc.
Compiled Wed 12-Aug-98 04:57 by ccai
Image text-base: 0x02005000, data-base: 0x023C5A58
ROM: System Bootstrap, Version 11.1(12)XA, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)
```

ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΤΩΝ SOCKETS ΠΟΥ "ΑΚΟΥΝ"

Οι routers έχουν περιορισμένη λειτουργικότητα , σε σύγκριση με άλλες τεχνολογίες , καθιστώντας πιο δύσκολο για τους επιτιθέμενους να εισάγουν τον κώδικα Trojan που εξυπηρετεί την παράνομη πρόσβασή τους .Ωστόσο , οι δρομολογητές παρέχουν μια σειρά από υπηρεσίες που επιτρέπουν απομακρυσμένες συνδέσεις . Το Telnet είναι το πιο γνωστό , αλλά υπάρχουν και άλλα. Ένας τρόπος για να ανακαλύψετε εάν υπάρχουν προσβάσιμες διαδρομές σε ένα router είναι να προσδιορίσετε ποιες θύρες (sockets) "ακούνε" (είναι ενεργές και προσβάσιμες) στο δρομολογητή σας. Για να προσδιορίσετε ποιες υπηρεσίες τρέχουν στο δρομολογητή , χρησιμοποιήστε έναν εξωτερικό σαρωτή πορτών (port scanner) ή εξετάστε το αρχείο ρυθμίσεων. Ένα παράδειγμα σάρωσης όλων των TCP και UDP θυρών με χρήση του ScanLine είναι το εξής :

```
C:\ScanLine>sl -p -t 1-65535 -u 1-65535 10.0.2.244
ScanLine (TM) 1.01
Copyright (c) Foundstone, Inc. 2002
http://www.foundstone.com
Scan of 1 IP started at Sat May 17 14:21:04 2003
```

ΑΠΟΘΗΚΕΥΣΗ ΤΗΣ ΔΙΑΜΟΡΦΩΣΗΣ ΤΟΥ ROUTER

Οι ρυθμίσεις του δρομολογητή είναι γενικά απλές. Όλες οι πληροφορίες διαμόρφωσης για Cisco δρομολογητές είναι αποθηκευμένες σε ένα ενιαίο αρχείο ρυθμίσεων. Αυτή η διαμόρφωση καθοδηγεί όλες τις πτυχές της συμπεριφοράς του δρομολογητή , και αποθηκεύεται σε NVRAM .Ο δρομολογητής χρησιμοποιεί αυτή την αποθηκευμένη διαμόρφωση κατά την εκκίνησή του . Ωστόσο , μπορείτε να αλλάξετε τη ρύθμιση παραμέτρων του δρομολογητή χωρίς τροποποίηση του αρχείου ρυθμίσεων που είναι αποθηκευμένο στη NVRAM. Αντ 'αυτού , οι αλλαγές στη διαμόρφωση γίνονται στη μνήμη RAM , και αποθηκεύονται σε NVRAM μόνο με διοικητική εντολή (admin command).Έτσι , θα πρέπει να αποθηκεύσετε τη ρύθμιση που είναι στη μνήμη RAM , καθώς και τη διαμόρφωση NVRAM. Για να

αποθηκεύσετε τα αρχεία ρυθμίσεων , θα πρέπει να έχετε επιτρέψει (privileged) επίπεδο πρόσβασης στον δρομολογητή.

cisco_router#show running-config

Χρησιμοποιείστε την εντολή show startup-config ή show config για να δείτε τη διαμόρφωση στη NVRAM.

cisco_router#show startup-config

ΕΠΑΝΕΞΕΤΑΣΗ ΤΟΥ ΠΙΝΑΚΑ ΔΡΟΜΟΛΟΓΗΣΗΣ

Ο πίνακας δρομολόγησης περιέχει το προσχέδιο για το πώς το router προωθεί πακέτα . Εάν ένας εισβολέας μπορεί να χειριστεί τον πίνακα δρομολόγησης, μπορεί και να αλλάξει το που αποστέλλονται τα πακέτα. Κατανοούμε λοιπόν ότι η χειραγώγηση ενός πίνακα δρομολόγησης θέτει σε κίνδυνο το router. Ο πίνακας δρομολόγησης μπορεί να αλλοιωθεί μέσω εντολών (command-line access) καθώς και μέσω κακόβουλων πακέτων σε περίπτωση update του router. Σε κάθε περίπτωση, ο πίνακας δρομολόγησης θα απεικονίσει τις αλλαγές. Για να δείτε τον πίνακα δρομολόγησης, χρησιμοποιήστε την εντολή show ip route :

```
cisco_router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B – BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

ΕΛΕΓΧΟΣ ΔΙΑΜΟΡΦΩΣΗΣ ΔΙΕΠΑΦΩΝ (INTERFACES)

Οι πληροφορίες διαμόρφωσης των interfaces είναι διαθέσιμες με την εντολή show ip interface. Παρόλο που αυτές οι πληροφορίες υπάρχουν στο αποθηκευμένο αρχείο διαμόρφωσης η εντολή αυτή κάνει τις πληροφορίες που μας αφορούν πιο ευανάγνωστες.

* e.g :

```
cisco_router#show ip interface
Ethernet0 is up, line protocol is up
Internet address is 10.0.2.244/24
Broadcast address is 255.255.255.255
Address determined by non-volatile memory
MTU is 1500 bytes
Helper address is not set
```

ΕΞΕΤΑΣΗ ΤΗΣ ARP CACHE

Το Address Resolution Protocol (ARP) χαρτογραφεί τις IP και MAC διευθύνσεις. Σε αντίθεση με τις IP διευθύνσεις (που ανήκουν στο επίπεδο διευθύνσεων δικτύου) , οι MAC διευθύνσεις είναι φυσικές διευθύνσεις (layer 2 στο πρότυπο OSI) και δεν δρομολογούνται εκτός των τομέων μετάδοσης (broadcast domains). Οι δρομολογητές αποθηκεύουν τις MAC διευθύνσεις από οποιαδήποτε συσκευή σε ένα τοπικό τομέα μετάδοσης(broadcast domain) μαζί με τις IP διευθύνσεις στην μνήμη ARP. Οι επιτιθέμενοι κατά καιρούς παραποιούν τις IP ή τις MAC διευθύνσεις εξαπατώντας τον έλεγχο ασφαλείας, όπως τις λίστες ελέγχου προσπέλασης (ACLs access control lists) , τους κανόνες των firewalls ή αλλάζουν την τοποθέτηση των ports. Συνεπώς η μνήμη ARP είναι χρήσιμη για την εξέταση επιθέσεων τέτοιου τύπου. Από τη στιγμή που είναι εύκολο να καταστρέψεις είναι εύκολο και να σώσεις χρήσιμες πληροφορίες χρησιμοποιώντας απλά την εντολή ip arp μπορείς να δεις τη μνήμη arp.

ΒΡΙΣΚΟΝΤΑΣ ΑΠΟΔΕΙΞΕΙΣ

Τώρα που έχεις συλλέξει τα περισσότερα από τα στοιχεία που χρειάζεσαι ποιο είναι το επόμενο βήμα; Η απάντηση φυσικά εξαρτάται ανάλογα τον τύπο του συμβάντος με βάση την αρχική έρευνα. Εδώ θα δούμε τις απαντήσεις διαφόρων τύπων συμβάντων που περιλαμβάνουν routers. Ταξινομούμε τους τύπους συμβάντων ως εξής:

- Άμεση διακύβευση
- Χειρισμός πίνακα δρομολόγησης
- Κλοπή πληροφοριών
- Άρνηση υπηρεσιών

ΧΕΙΡΙΣΜΟΣ ΣΥΜΒΑΝΤΩΝ ΑΜΕΣΗΣ ΕΚΘΕΣΗΣ ΣΕ ΚΙΝΔΥΝΟ

Η άμεση έκθεση του δρομολογητή σε κίνδυνο, είναι οποιοδήποτε γεγονός κατά το οποίο ένας επιτιθέμενος κερδίζει δικαίωμα εισόδου στον router. Έτσι ο επιτιθέμενος έχει τον έλεγχο του δρομολογητή αλλά και των πληροφοριών που αποθηκεύονται σε αυτόν. Η άμεση πρόσβαση στο δρομολογητή είναι διαθέσιμη με έναν εκπληκτικά μεγάλο αριθμό τρόπων συμπεριλαμβανομένου Telnet, console, web, SNMP, TFTP. Η διαχειριστική πρόσβαση ακόμη και αν δεν είναι ευνοϊκή είναι επικίνδυνη λόγω της λειτουργικότητας του router. Οποιοσδήποτε αποκτήσει τέτοιου είδους πρόσβαση μπορεί να χρησιμοποιήσει το router για να εντοπίσει και να επιτεθεί σε άλλους εξυπηρετητές (hosts) μέσω διαθέσιμων χρηστών. Αυτό είναι ιδιαίτερα επικίνδυνο καθώς ο router επιτρέπει συχνά τη πρόσβαση σε εσωτερικά δίκτυα, ακόμα και αν υπάρχει firewall μου εμποδίζει κάποια άλλη πρόσβαση στα εσωτερικά δίκτυα.

ΕΡΕΥΝΩΝΤΑΣ ΕΝΑ ΣΥΜΒΑΝ ΑΜΕΣΟΥ ΚΙΝΔΥΝΟΥ

Ανάλογα με το πώς ειδοποιηθήκατε για το γεγονός, μπορείτε να έχετε κάποια ιδέα για το πώς αποκτήθηκε η διαχειριστική πρόσβαση. Παραδείγματος χάριν, ένα IDS μπορεί να παρουσιάσει σύνδεση Telnet από μια διεύθυνση IP. Σε άλλες περιπτώσεις θα πρέπει να βρείτε τις απαντήσεις κατά τη διάρκεια της έρευνας. Με τις πληροφορίες που έχετε συλλέξει ήδη και ειδικά το αρχείο διαμόρφωσης και η λίστα των ενεργών ports η έρευνα ξεκινάει δυναμικά.

ΑΝΑΚΑΜΨΗ ΑΠΟ ΣΥΜΒΑΝΤΑ ΑΜΕΣΟΥ ΚΙΝΔΥΝΟΥ

Μετά απο ένα τέτοιο συμβάν θα πρέπει να ληφθούν όλα τα μέτρα αποκατάστασης ενώ το router είναι offline. Η αποκατάσταση πρέπει να είναι ανάλογη της επίθεσης. Για τυχόν αμφιβολίες μπορείτε να λάβετε και παραπάνω μέτρα ασφαλείας. Παραδείγματος χάριν:

* Κατάργηση όλων των περιττών υπηρεσιών.
* Επιτρέψτε την απομακρυσμένη πρόσβαση μόνο μέσω κρυπτογραφημένων πρωτοκόλλων.
* Μην επιτρέπετε την πρόσβαση SNMP ή την πρόσβαση μόνο για ανάγνωση
* Μην χρησιμοποιείτε τον κωδικό πρόσβασης SNMP για οποιαδήποτε άλλη πρόσβαση
* Αλλάξτε όλους τους κωδικούς
* Εφαρμόστε ACLs έτσι ώστε να έχουν πρόσβαση στο router μόνο αξιόπιστοι εξυπηρετητές
* Αναβαθμίστε το λειτουργικό σας στην τελευταία έκδοση

ΧΕΙΡΙΣΜΟΣ ΠΙΝΑΚΩΝ ΔΡΟΜΟΛΟΓΗΣΗΣ ΧΕΙΡΑΓΩΓΗΣΗΣ ΣΥΜΒΑΝΤΩΝ

Οι router μπορούν να χρησιμοποιήσουν ποικιλία πρωτοκόλλων για την ενημέρωση των πινάκων δρομολόγησης, συμπεριλαμβανομένων των εξής: RIP, OSPF, EIGRP, IGRP, BGP. Τα πρωτόκολλα διαβιβάζουν τις πληροφορίες για τη βέλτιστη διαδρομή μεταξύ γειτονικών router και έχουν διάφορους βαθμούς ασφαλείας. Μερικά πρωτόκολλα όπως το RIP κάνουν ενημερώσεις χωρίς να δίνουν τη δυνατότητα επιβεβαίωσης των ενημερώσεων. Κάποια άλλα πρωτόκολλα δίνουν δυνατότητα ύπαρξης κωδικού

επαλήθευσης αλλά είναι θέμα του διαχειριστή εάν επιθυμεί την ύπαρξη κωδικού ασφαλείας. Οι επιθέσεις αφορούν τη λειτουργικότητα ενός router μέσω των πινάκων δρομολόγησης και όχι αυτό καθεαυτό το router.

ΔΙΕΡΕΥΝΗΣΗ ΣΥΜΒΑΝΤΩΝ ΧΕΙΡΑΓΩΓΗΣΗΣ ΠΙΝΑΚΩΝ ΔΡΟΜΟΛΟΓΗΣΗΣ

Ο καθορισμός του τρέχοντος πίνακα δρομολόγησης είναι τόσο απλός όσο η επανεξέταση των αποτελεσμάτων της εντολής ip route. Ωστόσο, οι πληροφορίες του δικτύου είναι απαραίτητες για να κατανοήσουμε αν υπάρχουν αντιφάσεις. Εάν τα πακέτα εμφανίζονται να δρομολογούνται από απομακρυσμένα δίκτυα τότε απαιτείται προσεκτική έρευνα. Εάν στον πίνακα δρομολόγησης εμφανίζονται άγνωστες στατικές διαδρομές τότε ίσως ο δρομολογητής να έχει υποστεί άμεσο κίνδυνο.

ΑΝΑΚΑΜΨΗ ΜΕΤΑ ΤΑ ΣΥΜΒΑΝΤΑ ΣΤΟΥΣ ΠΙΝΑΚΕΣ ΔΡΟΜΟΛΟΓΗΣΗΣ

Η ανάκαμψη των παραβιασμένων πινάκων δρομολόγησης είναι απλή, αφαιρείτε τις ανεπιθύμητες στατικές διαδρομές και κάνετε επανεκκίνηση το router. Ωστόσο η αποτροπή μελλοντικών επιθέσεων είναι λίγο πιο δύσκολη. Οι ACLs μπορούν να περιορίσουν τα updates του router επιτρέποντας μόνο αναγνωρισμένες διευθύνσεις. Ωστόσο επειδή πολλά πρωτόκολλα δρομολόγησης είναι UDP αυτές οι διευθύνσεις μπορεί να πλαστογραφηθούν. Υπάρχουν ACLs που περιορίζουν την πλαστογράφηση αλλά δεν είναι αλάνθαστες. Το πρωτόκολλο δρομολόγησης που επιλέγεται πρέπει να επιτρέπει τον έλεγχο ταυτότητας και ο έλεγχος ταυτότητας πρέπει να είναι ενεργοποιημένος.

ΧΕΙΡΙΣΜΟΣ ΚΛΟΠΗΣ ΠΛΗΡΟΦΟΡΙΩΝ

Η κλοπή δεδομένων από δρομολογητή είναι δύσκολη καθώς λίγα δεδομένα ανήκουν στο router. Ο επιτιθέμενος δεν θα βρει τη βάση δεδομένων μισθοδοσίας ή κάποιο άλλο μυστικό σε ένα router. Οι πληροφορίες που βρίσκονται στο router είναι σχετικές με την τοπολογία του δικτύου πρόσβασης και ελέγχου. Οι τυπικές πληροφορίες που μπορεί να υποκλέψει ο επιτιθέμενος περιλαμβάνουν κωδικό, τη δρομολόγηση και πληροφορίες που αφορούν την τοπολογία. Για να ανακάμψετε από μια τέτοια κλοπή θα πρέπει να αλλάξετε κωδικούς, να μην επαναχρησιμοποιηθεί κάποιος κωδικός και να περιοριστεί η δυνατότητα ενός επιτιθέμενου να αποκτήσει ευαίσθητες πληροφορίες.

ΧΕΙΡΙΣΜΟΣ ΕΠΙΘΕΣΕΩΝ DoS (Denial of Service)

Οι επιθέσεις DoS συχνά στοχεύουν τους δρομολογητές. Εάν ένας επιτιθέμενος μπορεί να αναγκάσει τη διακοπή μετάδοσης των πακέτων επιτυγχάνει όλοι οι χρήστες του router να βγουν εκτός λειτουργίας. Οι επιθέσεις DoS διακρίνονται στις εξής βασικές κατηγορίες:

- Καταστροφής : Είναι επιθέσεις οι οποίες έχουν την ικανότητα να καταστρέψουν τη λειτουργικότητα του router, διαγράφοντας τις πληροφορίες διαμόρφωσης του ή να σταματήσουν τη τροφοδοσία του.
- Πόροι κατανάλωσης: Είναι επιθέσεις που υποβαθμίζουν την ικανότητα του router να λειτουργήσει, ανοίγοντας ταυτόχρονα πολλές συνδέσεις.
- Κατανάλωση εύρους ζώνης (bandwith): Επιθέσεις που καταλαμβάνουν τη χωρητικότητα του εύρους ζώνης του δικτύου του router.

ΕΡΕΥΝΑ ΕΠΙΘΕΣΕΩΝ DoS

Ο καθορισμός του τύπου επίθεσης DOS πρέπει να είναι το ευκολότερο μέρος της έρευνας. Εάν ο δρομολογητής δεν λειτουργεί καθόλου, είναι πιθανώς μια επίθεση καταστροφής. Ελέγξτε τα προφανή προβλήματα πρώτα: τροφοδοσία, καλώδια, και διαμόρφωση. Το router κάνει επανεκκίνηση (reboot)

σποραδικά ή πέφτει σταδιακά η απόδοσή του;Μια σποραδική επανεκκίνηση δηλώνει απευθείας επίθεση στο δρομολογητή. Μια σταδιακή πτώση της απόδοσης του router μπορεί να είναι μια απευθείας επίθεση στην κατανάλωση του εύρους ζώνης (bandwidth). Σε κάθε περίπτωση μια έρευνα στο δίκτυο θα αποκαλύψει λεπτομέρειες. Ψάξτε για πακέτα που αποστέλλονται απευθείας στο δρομολογητή ή περίσσεια πακέτα που δεν προέρχονται από το συγκεκριμένο δίκτυο. Την απόδοση του δρομολογητή μπορεί να επηρεάσει επίσης και μια υπερχείλιση πακέτων. Εάν τα ports του router είναι ενεργά μια αφθονία SYN ή άλλων πακέτων ρίχνουν την απόδοση του. Εναλλακτικά, ακόμα κι αν ο δρομολογητής δεν έχει κανέναν ανοικτό port, μια πλημμύρα πακέτων μπορεί να επηρεάσει το δρομολογητή ή να χρησιμοποιήσει το bandwidth έτσι ώστε η απόδοση του δικτύου να υποβιβαστεί. Οι επιθέσεις DoS αφορούν ως συνήθως επιθέσεις στο bandwidth. Αν και αυτός ο τύπος επίθεσης δεν κατευθύνεται απαραιτήτως σε έναν router, μπορεί να χρησιμοποιηθεί για να μετριάσει το αποτελέσματα της επίθεσης.

ΑΝΑΚΑΜΨΗ ΑΠΟ ΕΠΙΘΕΣΕΙΣ DoS

Ενώ οι επιθέσεις DoS έχουν σοβαρές επιπτώσεις στα δίκτυα, είναι ένα από τα ευκολότερα επεισόδια για επίλυση. Συνήθως επιθέσεις DoS δεν συνεπάγονται διακύβευση του router μάλλον αποτελούνται από ανεπιθύμητα πακέτα που αποστέλλονται προς ή μέσω του router. Η ανάκαμψη αποτελείται συνήθως από τα ακόλουθα μέτρα :

- Εξάλειψη των υπηρεσιών που "ακούνε"
- Αναβάθμιση του λογισμικού στην τελευταία έκδοση
- Χρήση ACLs για περιορισμό πρόσβασης στις υπηρεσίες που "ακούνε"
- Χρήση ACLs για να περιοριστεί η κακόβουλη κίνηση

ΧΡΗΣΙΜΟΠΟΙΗΣΗ ΤΩΝ ΔΡΟΜΟΛΟΓΗΤΩΝ ΩΣ ΕΡΓΑΛΕΙΑ ΑΠΟΚΡΙΣΗΣ

Οι δρομολογητές έχουν πολλές χρήσεις κατά τη διάρκεια της αντίδρασης σε συμβάντα, ειδικά κατά τη διάρκεια της αποκατάστασης. Μερικά από τα πιο χρήσιμα χαρακτηριστικά ενός router είναι οι ACLs. Επιπλέον, εκεί είναι συγκεκριμένες ενέργειες που μπορούν να ληφθούν στους δρομολογητές για να μετριάσουν τα αποτελέσματα των επιθέσεων DOS. Για το υπόλοιπο αυτού του κεφαλαίου, θα συζητήσουμε αυτές τις δυνατότητες και τον τρόπο εφαρμογής τους.

ΚΑΤΑΝΟΗΣΗ ΛΙΣΤΩΝ ΕΛΕΓΧΟΥ ΠΡΟΣΒΑΣΗΣ (ACLs)

Οι ACLs είναι μηχανισμοί που περιορίζουν την κίνηση στους δρομολογητές. Πακέτα μπορούν να περιοριστούν βάση μιας ποικιλίας χαρακτηριστικών :

- Πρωτόκολλο
- Πηγή ή προορισμός IP διεύθυνσης
- Πηγή ή προορισμός TCP ή UDP port
- TCP flag
- Τύπος μηνύματος ICMP
- Ώρα της ημέρας
- Κανονικά οι ACLs χρησιμοποιούνται για την εφαρμογή πολιτικών ασφαλείας. Ένα καλά διαμορφωμένο router μπορεί να παρέχει πολλές από τις δυνατότητες των εμπορικών firewalls και συχνά χρησιμοποιούνται για να συμπληρώσουν τα τείχη προστασίας.

ΔΙΑΜΟΡΦΩΣΗ ΜΙΑΣ ACL

Μια ACL μπορεί να χρησιμοποιηθεί κατά τη διάρκεια απόκρισης για να εξαλείψει την κυκλοφορία στο δίκτυο. Για την εφαρμογή αυτού του κανόνα σε ένα Cisco router η διαμόρφωση ξεκινάει ως εξής:

cisco_router#config t
Enter configuration commands, one per line. End with CNTL/Z.
cisco_router(config)#
Μετά δημιουργήστε μια ACL που να απορρίπτει την κυκλοφορία από το δίκτυο (200.200.200.0/24 σε αυτό το παράδειγμα) προς το δίκτυο σας
cisco_router(config)#access-list 101 deny ip 200.200.200.0 0.0.0.255 any
cisco_router(config)#access-list 101 permit ip any any

ΑΠΟΤΡΟΠΗ ΠΛΑΣΤΟΓΡΑΦΗΣΗΣ IP ΔΙΕΥΘΥΝΣΗΣ

Η πλαστογραφία ip διευθύνσεων είναι η πιο παλιά και από τις πιο επικίνδυνες τεχνικές που χρησιμοποιούν οι επιτιθέμενοι. Εάν ο επιτιθέμενος προσποιηθεί με μια ασφαλή διεύθυνση δικτύου τα πακέτα του θα καταφέρουν να εξαπατήσουν το σύστημα-θύμα. Οι δρομολογητές παίζουν ένα σημαντικό ρόλο στην πρόληψη αυτών των επιθέσεων. Κάθε interface σε ένα router πρέπει να απαγορεύει πακέτα που λογικά δεν θα μπορούσαν να προέρχονται από την εν λόγω διασύνδεση δικτύου.

ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΜΕΣΩ ROUTER

Κατά τη διάρκεια των γεγονότων, είναι συχνά χρήσιμο να ελεγχθεί η κυκλοφορία του δικτύου. Οι δρομολογητές μπορούν να χρησιμοποιηθούν για αυτό το στόχο, και μπορούν να αποδειχθούν ανεκτίμητοι σε πολλές περιπτώσεις. Το αρχείο καταγραφής διαμορφώνεται μέσω ACLs και διαμορφώνει ποιες κινήσεις επιτρέπονται ή ποιες κινήσεις απορρίπτονται και γενικά όλη την κυκλοφορία στο δίκτυο. Για παράδειγμα πέστε οτι θέλετε να καταγράψετε όλα τα πακέτα που προήλθαν από το απαγορευμένο δίκτυο όπως περιγράψαμε και σε προηγούμενο κεφάλαιο εφαρμόζουμε το εξής:

access-list 101 deny ip 200.200.200.0 0.0.0.255 any log

Η προσθήκη της λέξης κλειδιού βοηθάει να καταγραφούν τα πακέτα που ταιριάζουν σε αυτή. Από τη στιγμή που οι router δεν είναι το ιδανικό μέσο για να δείτε τα αποτελέσματα του ελέγχου μπορείτε να ρυθμίσετε το router να καταγράφει τα αποτελέσματα αυτά σε ένα syslog server όπως είδαμε σε προηγούμενο κεφάλαιο.

ΑΝΤΑΠΟΚΡΙΣΗ ΕΠΙΘΕΣΕΩΝ DDoS 1/2

Ο όρος DDoS εισήλθε στο λεξιλόγιο των επαγγελματιών ασφαλείας στα τέλη του 1999.Αυτές οι πανούργες επιθέσεις χρησιμοποίησαν συστήματα γύρω από το Διαδίκτυο για να στείλουν ταυτόχρονα πακέτα που θα αυξήσουν την κυκλοφορία στα site-θύματα. Μεταγενέστερες επιθέσεις έχουν επεκταθεί στο θέμα, με την ενίσχυση του traffic, χρησιμοποιώντας τεχνικές που ήταν ικανές να υποβιβάσουν την απόδοση των μεγαλυτέρων ιστοτόπων. Οι επιδράσεις αυτών των επιθέσεων δεν μπορούν ποτέ να αποφευχθούν εντελώς. Εάν αρκετό traffic πλήττει ταυτόχρονα ένα site-θύμα τότε το site δεν μπορεί να ανταποκριθεί σε όλα τα αιτήματα. Εντούτοις, υπάρχουν μερικές συγκεκριμένες ενέργειες που μπορούν να ληφθούν για να μετριάσουν τα αποτελέσματα αυτών των επιθέσεων και να μειώσουν τη δυνατότητά τους να αρνηθούν την υπηρεσία.

ΑΝΤΑΠΟΚΡΙΣΗ ΕΠΙΘΕΣΕΩΝ DDoS 2/2

Οι DDoS επιθέσεις είναι επιθέσεις πολλαπλών πρωτοκόλλων. ICMP, UDP και TCP πακέτα είναι μέρος της επίθεσης. Επιθέσεις που αφορούν ICMP και UDP πακέτα μπορούν να μετριαστούν γρήγορα με την παρεμπόδιση ICMP και UDP πακέτων. Τα περισσότερα δίκτυα δεν έχουν καμία ανάγκη για αυτά τα πρωτόκολλα που επιτρέπονται μέσα από το Διαδίκτυο (εκτός από UDP 53, DNS), εισάγετε έτσι ACLs που

αρνείται όλη την κυκλοφορία ICMP και όλο UDP εκτός από DNS κυκλοφορία στο συγκεκριμένο DNS κεντρικό υπολογιστή.
Για να μειωθεί η πιθανότητα των επιθέσεων ενίσχυσης της κυκλοφορίας στα ανυποψίαστα θύματα, μπορείτε να εξετάσετε επίσης την έξοδο των φίλτρων, τα οποία περιορίζουν αυτά τα πρωτόκολλα. Οι επιθέσεις TCP είναι λίγο δυσκολότερο να μετριαστούν. Η κυκλοφορία TCP είναι απαραίτητη, εκτός αν δεν λαμβάνετε email ή δεν επισκέπτεστε κάποιο ιστότοπο ή δεν συνδέεστε με οποιονδήποτε άλλο τρόπο στο διαδίκτυο. Οι βασισμένες σε TCP πακέτα επιθέσεις DoS χωρίζονται σε δυο βασικές κατηγορίες σε προσαρμοσμένη άμεση σύνδεση ή χωρίς σύνδεση.

ΑΝΤΑΠΟΚΡΙΣΗ ΣΤΙΣ ΕΠΙΘΕΣΕΙΣ TCP

Οι προσανατολισμένες ως προς τη σύνδεση επιθέσεις ολοκληρώνουν την τριπλή χειραψία (three-way handshake) TCP για να εγκαταστήσουν μια σύνδεση. Επειδή η τριπλή χειραψία ολοκληρώνεται, η διεύθυνση προέλευσης της επίθεσης είναι ουσιαστικά σίγουρη (Είναι εξαιρετικά δύσκολο να εξαπατήσουν την IP της πηγής και να ολοκληρωθεί η λειτουργία three-way handshake, λόγω του αριθμού ακολουθίας TCP). Οι προσανατολισμένες ως προς τη σύνδεση επιθέσεις είναι γνωστές συχνά ως επιθέσεις κατανομής πινάκων(process table) ή επιθέσεις κατανομής πόρων (resource allocation) και προέρχονται από καθορισμένη διεύθυνση, έτσι το φιλτράρισμα παραβατικών διευθύνσεων είναι δυνατό με τη χρήση ACL. Το ατυχές μέρος είναι ότι με το φιλτράρισμα μπορείτε να φιλτράρετε μόνο τη διεύθυνση πηγής, μετά εντοπίζετε τον δράστη μέσω αρχείων καταγραφής ή παρακολουθώντας το δίκτυο.

ΑΝΤΑΠΟΚΡΙΣΗ ΣΤΗΝ ΧΩΡΙΣ ΣΥΝΔΕΣΗ ΕΠΙΘΕΣΗ TCP 1/2

Οι χωρίς σύνδεση επιθέσεις TCP αρχίζουν τις συνδέσεις TCP με την αποστολή μόνο των πακέτων SYN,ποτέ ολοκληρώνοντας τη χειραψία. Με αυτές τις επιθέσεις η παραποίηση της πηγής της IP είναι ασήμαντη δεδομένου ότι ο αριθμός ακολουθίας δεν παίζει κανένα ρόλο. Αυτές οι επιθέσεις είναι δυσκολότερες ως προς την ανταπόκριση του φιλτραρίσματος γιατί κάθε πακέτο μπορεί να έχει διαφορετική διεύθυνση πηγής οι οποίες δεν είναι πραγματικές διευθύνσεις. Το θετικό είναι πως οι χωρίς σύνδεση επιθέσεις δεν είναι τόσο καταστροφικές όπως αυτές που έχουν πραγματοποιήσει σύνδεση. Για να μειώσετε τα αποτελέσματα των χωρίς σύνδεση επιθέσεων, θα πρέπει να εφαρμόσετε το φιλτράρισμα ποσοστού TCP. Η βασική ιδέα του φιλτραρίσματος ποσοστού είναι βασισμένη στα χαρακτηριστικά της κανονικής κυκλοφορίας εναντίον της κυκλοφορίας που εμφανίζεται κατά τη διάρκεια της υπερχείλισης SYN πακέτων.

ΑΝΤΑΠΟΚΡΙΣΗ ΣΤΗΝ ΧΩΡΙΣ ΣΥΝΔΕΣΗ ΕΠΙΘΕΣΗ TCP 2/2

Στις κανονικές συνδέσεις το πακέτο SYN απαιτείται να σταλεί μόνο κατά την πρώτη φορά που πραγματοποιείται σύνδεση. Το ποσοστό που περιορίζει τον αριθμό πακέτων SYN στο δίκτυο θα αποτρέψει το ποσό νέων εισερχόμενων συνδέσεων κατά τη διάρκεια της κανονικής λειτουργίας. Η σημαντικότητα του περιορισμού αυτού έρχεται όταν εμφανίζεται υπερχείλιση πακέτων SYN και οι ρυθμιστικές δικλείδες του router απορρίπτουν τα πλαστά πακέτα που φτάνουν σε αυτό.

ΣΥΜΠΕΡΑΣΜΑΤΙΚΑ

Οι δρομολογητές είναι υψίστης σημασίας συσκευές του δικτύου που μπορούν να παίξουν πολλούς ρόλους στις επιθέσεις του δικτύου. Μπορούν να είναι τα εργαλεία στο έγκλημα, το θύμα, ή ένας πολύτιμος σύμμαχος κατά τη διάρκεια της ανταπόκρισης σε ένα συμβάν. Για τον ερευνητή το σημαντικότερο είναι να κατανοήσει την ποικιλία λειτουργιών του router. Κατανοώντας πλήρως την πολυλειτουργικότητα του router έχετε ένα χρήσιμο εργαλείο για να να ερευνήσετε και να ανταποκριθείτε σε ένα περιστατικό.

ΕΡΩΤΗΣΕΙΣ

- Ποια η διαφορά εκκίνησης και διαχείρισης αρχείων διαμόρφωσης σε έναν router;
- Πώς θα εντοπίσετε μια στατική διαδρομή και γιατί θα πρέπει να την εξετάσετε;
- Πως θα αποτρέψετε εξερχόμενα πακέτα ICMP;
- Πως θα καταγράψετε την απόπειρα εξερχόμενων πακέτων ICMP σε έναν κεντρικό διακομιστή αρχείων καταγραφής (syslog server);

ΒΙΒΛΙΟΓΡΑΦΙΑ

INCIDENT RESPONSE AND COMPUTER FORENSICS

SECOND EDITION

Kevin Mandia, Chris Prosise & Matt Pepe

Computer crime experts from Foundstone, Inc.