

8.3.2 Επεξήγηση Ορολογίας

Πριν προχωρήσουμε στις διάφορες τεχνικές ασφάλειας και μεθόδους παραβίασης, θα κάνουμε μια σύντομη αναφορά στην ορολογία που χρησιμοποιείται. Κάποιοι από τους όρους που θα παρουσιάσουμε εδώ, εξηγούνται καλύτερα παρακάτω σε συνδυασμό με τον αντίστοιχο τρόπο χρήση τους.

Οι πιο βασικοί όροι σε θέματα ασφάλειας πληροφοριακών συστημάτων είναι οι παρακάτω:

- **Κρυπτογράφηση (Encryption):** Η κρυπτογράφηση είναι η διαδικασία με την οποία μετατρέπονται τα αρχικά δεδομένα (γνωστά και ως *plaintext*) σε μορφή (κρυπτόγραμμα) η οποία δεν μπορεί πλέον να γίνει κατανοητή χωρίς να αποκρυπτογραφηθεί. Η κρυπτογράφηση γίνεται με τη βοήθεια αλγορίθμου, το αποτέλεσμα του οποίου μπορεί να αντιστραφεί ώστε να παράγει ξανά τα αρχικά δεδομένα εισόδου. Για την κρυπτογράφηση και την αποκρυπτογράφηση χρησιμοποιείται το κλειδί.
- **Αποκρυπτογράφηση (Decryption):** Προφανώς η αντίστροφη διαδικασία της κρυπτογράφησης. Ο αλγόριθμος δέχεται ως είσοδο τα κρυπτογραφημένα δεδομένα (κρυπτόγραμμα) και με τη βοήθεια του κλειδιού (το οποίο προφανώς είναι διαθέσιμο μόνο σε εξουσιοδοτημένα άτομα) τα μετατρέπει ξανά στα κανονικά δεδομένα. Τα δεδομένα πλέον δεν είναι κωδικοποιημένα και μπορούν να χρησιμοποιηθούν κανονικά.
- **Κλειδί (Key):** Στο πεδίο της κρυπτογράφησης, το κλειδί είναι ένας ψηφιακός κωδικός (ένας αριθμός από bits) ο οποίος χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση της πληροφορίας. Προφανώς το κλειδί φυλάσσεται σε ασφαλές μέρος και είναι διαθέσιμο μόνο στα μέρη που επιτρέπεται να έχουν πρόσβαση στα δεδομένα.
- **Δημόσιο Κλειδί (Public Key):** Στην *ασυμμετρική* κρυπτογράφηση, χρησιμοποιούνται για κάθε χρήστη δύο κλειδιά, το δημόσιο και το ιδιωτικό. Η βασική ιδέα είναι ότι το δημόσιο το γνωρίζει καθένας, ενώ το ιδιωτικό μόνο ο χρήστης. Το δημόσιο κλειδί χρησιμοποιείται για να “κλειδώσει” (κρυπτογραφεί) ενώ το ιδιωτικό ξεκλειδώνει. Όποιος θέλει να μας στείλει κρυπτογραφημένα δεδομένα, χρησιμοποιεί το δημόσιο μας κλειδί για να τα κλειδώσει. Μετά από αυτό η αποκρυπτογράφηση γίνεται μόνο με το δικό μας ιδιωτικό κλειδί. Γενικά η ασυμμετρική κρυπτογράφηση θεωρείται πιο ασφαλής από τη συμμετρική, καθώς δεν γνωρίζει κανείς άλλο το ιδιωτικό μας κλειδί. (Στη συμμετρική κρυπτογράφηση χρησιμοποιείται το ίδιο κλειδί και για τις δύο λειτουργίες, άρα πρέπει να το έχουν και τα δύο μέρη της επικοινωνίας)
- **Ιδιωτικό Κλειδί (Private Key):** Το ιδιωτικό κλειδί χρησιμοποιείται στην ασυμμετρική κρυπτογράφηση για να αποκρυπτογραφεί και να υπογράψει δε-

δομένα. ΠΡΟΣΟΧΗ: το σχολικό βιβλίο γράφει λανθασμένα ότι το ιδιωτικό κλειδί κρυπτογραφεί και ελέγχει υπογραφές - αυτά τα κάνει το δημόσιο κλειδί. Το ιδιωτικό κλειδί συνδυάζεται πάντα (σαν ζεύγος) με ένα αντίστοιχο δημόσιο. Η πλήρης διαδικασία εξηγείται σε επόμενη ενότητα.

- **Μυστικό Κλειδί (Secret Key):** Ψηφιακός κωδικός που είναι γνωστός και στα δύο μέρη προκειμένου να τον χρησιμοποιήσουν σε ανταλλαγή δεδομένων με χρήση κρυπτογράφησης / αποκρυπτογράφησης.
- **Λειτουργία (Συνάρτηση) Κατατεμαχισμού (Hash Function):** Μαθηματική συνάρτηση της οποίας η έξοδος δεν μπορεί με αντιστροφή (με κανένα τρόπο) να μας παράγει την αρχική είσοδο. Προφανώς δεν μπορεί να χρησιμοποιηθεί για κρυπτογράφηση, καθώς δεν μπορούμε μετά να αποκρυπτογραφήσουμε το κείμενο, αλλά χρησιμοποιείται για την παραγωγή συνόψεων (digests).
- **Σύνοψη Μηνύματος (Message Digest):** Η σύνοψη ενός μηνύματος είναι το αποτέλεσμα (έξοδος) της συνάρτησης κατατεμαχισμού. Η σύνοψη δεν είναι το ίδιο μέγεθος (αλλά συνήθως μικρότερη) από το αρχικό μήνυμα – κάτι το οποίο έχει νόημα, γιατί όπως εξηγήσαμε δεν μπορούμε έτσι και αλλιώς να ξαναγαυρίσουμε στο αρχικό μήνυμα. Οι αλγόριθμοι κατατεμαχισμού είναι φτιαγμένοι με τέτοιο τρόπο ώστε μια μικρή μεταβολή στα δεδομένα εισόδου (π.χ. ένα μόνο γράμμα ή ακόμα και ένα μόνο bit) να προκαλεί ολοκληρωτική αλλαγή στην έξοδο (πλήρης αλλαγή της σύνοψης). Για το λόγο αυτό η σύνοψη χρησιμοποιείται πολύ συχνά για να ελέγξουμε την ακεραιότητα κάποιου αρχείου που κατεβάσαμε π.χ. από το Internet. Σε μεγάλα downloads, μπορούμε συνήθως να κατεβάσουμε και ένα αρχείο CHECKSUM (αθροίσματος ελέγχου) που περιέχει μέσα την σύνοψη του μεγάλου αρχείου. Εκτελώντας τη συνάρτηση κατατεμαχισμού στο δικό μας μηχάνημα, μπορούμε να συγκρίνουμε τις συνόψεις: αν είναι ίδιες το αρχείο έχει κατέβει σωστά.
- **Ψηφιακή Υπογραφή (Digital Signature):** Η ψηφιακή υπογραφή είναι τυπικά ένας αριθμός από bit που προστίθεται στο τέλος κάποιου αρχείου και εξασφαλίζει την αυθεντικότητα (“το έστειλε πράγματι ο χρήστης Α”) και την ακεραιότητα (“το έχουμε λάβει σωστά”) ενός μηνύματος.

8.3.3 Μέθοδοι Παραβίασης

Σε κάθε δίκτυο υπολογιστών μπορεί να υπάρχουν εμπιστευτικές πληροφορίες. Τυπικά αυτές θα είναι αποθηκευμένες σε διάφορα αποθηκευτικά μέσα (σκληροί δίσκοι κλπ) ενώ κατά τη διάρκεια της επεξεργασίας τους θα βρίσκονται και στην κύρια μνήμη (RAM) των υπολογιστών. Επίσης μεταδίδεται στο δίκτυο με τη μορφή πακέτων. Η ύπαρξη πληροφοριών σε αυτές τις καταστάσεις μπορεί να απειληθεί με

διάφορους τρόπους από ενέργειες χρηστών τόσο του εσωτερικού δικτύου όσο και του Internet (εφόσον υπάρχει σύνδεση σε αυτό). Στην ενότητα αυτή θα αναφερθούμε στους συνηθισμένους τρόπους επιθέσεων που χρησιμοποιούνται για την παραβίαση της ασφάλειας ενός δικτύου υπολογιστών.

Επιθέσεις στους Κωδικούς Πρόσβασης (Password Attacks)

Οι κωδικοί πρόσβασης είναι ένας από τους πλέον συνηθισμένους μεθόδους ελέγχου πρόσβασης σε υπολογιστικά συστήματα. Γενικά υπάρχουν δύο είδη κωδικών:

- **Τα επαναχρησιμοποιούμενα passwords:** Πρόκειται για τον πλέον συνηθισμένο τύπο κωδικού πρόσβασης. Μπορεί να χρησιμοποιηθεί πολλές φορές για την εξακρίβωση των στοιχείων του χρήστη.
- **Τα passwords μια χρήσης, OTP (One Time Password):** Τα passwords αυτά αλλάζουν συνεχώς, καθένα είναι έγκυρο για μια και μοναδική χρήση.

Στα περισσότερα είδη λειτουργικών συστημάτων, όπως το UNIX και τα Windows υποστηρίζεται η χρήση επαναχρησιμοποιούμενων κωδικών πρόσβασης. (Στο UNIX υποστηρίζονται και τα OTP, αλλά το βιβλίο σας ντρέπεται να το πει)

Με την εξέλιξη της τεχνολογίας (αλλά και με την άνοδο των τεχνικών “ψαρέματος” των χρηστών) η προστασία ενός υπολογιστικού συστήματος μόνο με τη χρήση κωδικών (και ειδικά επαναχρησιμοποιούμενων) θεωρείται πολύ ασθενής.

Για την παραβίαση κωδικών πρόσβασης υπάρχουν προγράμματα που σε μικρό χρονικό διάστημα μπορούν να δοκιμάσουν πολύ μεγάλο συνδυασμό χαρακτήρων και γραμμάτων (brute force attack). Ένας άλλος τρόπος παραβίασης είναι η παρακολούθηση των πλήκτρων (key stroke monitoring) με τη βοήθεια κάποιου προγράμματος (keylogger) που καταγράφει τα πλήκτρα που πρίζονται, ενδεχομένως σε κάποιο αρχείο. Προφανώς το πρόγραμμα αυτό πρέπει να εγκατασταθεί εν αγνοία του αρχικού χρήστη του συστήματος. Με την ανάλυση των στοιχείων που έχουν καταγραφεί στο αρχείο μπορεί να αποκαλυφθεί ο κωδικός πρόσβασης (και ενδεχομένως και άλλες εμπιστευτικές πληροφορίες, π.χ. αριθμοί πιστωτικών καρτών κλπ).

Ένας άλλος ιδιαίτερα συνηθισμένος στις μέρες μας τρόπος ανάκτησης κωδικών πρόσβασης αναφέρεται ως *social engineering* και επικεντρώνει στην παραπλάνηση των χρηστών για την απόκτηση πληροφοριών. Για παράδειγμα, φανταστείτε ότι σας καλεί στο τηλέφωνο κάποιος που υποτίθεται ότι ανήκει στο τεχνικό τμήμα του παροχέα σας υπηρεσιών Internet (ISP) και σας ζητάει να του δώσετε τον κωδικό σας γιατί θέλουν να κάνουν κάποιες αλλαγές ρυθμίσεων στα συστήματά τους. Πάρα πολλοί χρήστες το πιστεύουν αυτό και πραγματικά δίνουν τους κωδικούς τους. Γιατί άραγε ένας τεχνικός του ISP σας να θέλει τον κωδικό σας; Ο διαχειριστής ενός συστήματος έχει πλήρη πρόσβαση σε όλα τα στοιχεία και τους λογαριασμούς και δεν χρειάζεται

ποτέ κανένα κωδικό χρήστη! Στην ίδια κατηγορία εντάσσεται και η δυνατότητα να δούμε τυχαία (shoulder surfing) τον κωδικό πρόσβασης ενός χρήστη την ώρα που τον πληκτρολογεί (αρκεί να περνάμε δίπλα του εκείνη τη στιγμή).

Υπάρχει προφανώς η πιθανότητα απόκτησης ενός κωδικού πρόσβασης και με τη χρήση φυσικής βίας. Οι περιπτώσεις φυσικής βίας μπορούν να ενταχθούν σε δύο κατηγορίες: στην εξωτερική και στην εσωτερική βία. Είναι προφανές ότι με την εξωτερική βία, ο χρήστης του οποίου απειλείται η σωματική ακεραιότητα θα αποκαλύψει ενδεχομένως τον κωδικό του. Με την εσωτερική βία, αναφερόμαστε στην περίπτωση όπου κάποιος αντιγράφει (νόμιμα η παράνομα) κρυπτογραφημένα passwords και στη συνέχεια χρησιμοποιεί κάποιο πρόγραμμα crack για να προσπαθήσει να τα αποκρυπτογραφήσει.

Οι κωδικοί πρόσβασης δεν αποθηκεύονται απευθείας σε ένα σύστημα. Αντίθετα, περνούν από λειτουργία κατατεμαχισμού και αποθηκεύεται η σύνοψη τους (digest). Για τον έλεγχο έπειτα του κωδικού που εισάγει ο χρήστης, γίνεται ξανά η ίδια διαδικασία: παράγεται το digest και συγκρίνεται με το αποθηκευμένο. Αν είναι ίδιο, ο κωδικός που δίνει ο χρήστης είναι ο σωστός. Από τα παραπάνω, μπορούμε να αντιληφθούμε ότι δεν είναι δυνατόν να πάρουμε με κάποιο τρόπο τον αρχικό κωδικό με αποκρυπτογράφηση του αποθηκευμένου, καθώς έχει προέλθει από λειτουργία κατατεμαχισμού (που δεν αντιστρέφεται).

Ένα πρόγραμμα τύπου crack χρησιμοποιεί μια απλή μέθοδο: αν έχουμε αποκτήσει τα digests των κωδικών πρόσβασης (γνωστά και ως hashes) και γνωρίζουμε τον αλγόριθμο κατατεμαχισμού που έχει χρησιμοποιηθεί για την παραγωγή τους, μπορούμε να αρχίζουμε να δοκιμάζουμε τυχαίους συνδυασμούς γραμμάτων, μέχρι να παράγουμε το ίδιο digest. Τότε θα έχουμε βρει τον κωδικό πρόσβασης. Η μέθοδος αυτή είναι γνωστή ως *brute force attack*.

Τα πράγματα γίνονται πιο εύκολα αν αναλογιστούμε ότι οι περισσότεροι χρήστες (για ευκολία τους) χρησιμοποιούν μάλλον απλές λέξεις ως κωδικούς πρόσβασης. Έτσι, αντί να ψάχνουμε τυχαία γράμματα μπορούμε να ψάχνουμε για λέξεις. Τα περισσότερα προγράμματα crack διαθέτουν ένα λεξικό αγγλικών (συνήθως) λέξεων τις οποίες δοκιμάζουν. Ένα γνωστό τέτοιο πρόγραμμα για UNIX είναι το Jack the Ripper, το οποίο χρησιμοποιούν και οι διαχειριστές για να ελέγξουν αν ο κωδικός κάποιου χρήστη είναι “ασθενής”.

Να σημειώσουμε βέβαια ότι πρόσβαση στο αρχείο των κρυπτογραφημένων κωδικών σε ένα UNIX σύστημα έχει μόνο ο διαχειριστής (root) και τα προγράμματα που εξασφαλίζουν την είσοδο των χρηστών και την αλλαγή των κωδικών (login και passwd αντίστοιχα). Αν το αρχείο αυτό έχει πέσει στα χέρια κάποιου άλλου, τα προβλήματα μας είναι συνήθως πολύ πιο σοβαρά από την απλή παραβίαση κωδικών...

Παρακολούθηση Δικτύου (Network Monitoring ή Network Packet Sniffing)

Όπως είναι γνωστό, τα δεδομένα μέσα σε ένα δίκτυο μεταφέρονται μεταξύ υπολογιστών με τη μορφή πακέτων. Σε αρκετές εφαρμογές (για παράδειγμα το telnet και το ftp για τα οποία έχουμε ήδη μιλήσει) τα δεδομένα αλλά και οι ίδιοι οι κωδικοί πρόσβασης μεταφέρονται με μορφή απλού κειμένου, χωρίς κανένα είδος κρυπτογράφησης (clear text). Είναι φανερό, ότι κάποιος με τα κατάλληλα τεχνικά μέσα και γνώσεις μπορεί να λάβει τα πακέτα, να τα συναρμολογήσει και να παράγει έτσι το σύνολο των πληροφοριών που παρέχονται σε αυτά, συμπεριλαμβανομένων και τυχόν κωδικών.

Τα προγράμματα που κάνουν ανίχνευση πακέτων (packet sniffing) χρησιμοποιούν την κάρτα δικτύου του υπολογιστή σε κατάσταση λειτουργίας promiscuous. Στο promiscuous mode η κάρτα δικτύου λαμβάνει όλα τα πακέτα που κυκλοφορούν στο δίκτυο, και όχι μόνο αυτά που απευθύνονται σε αυτήν. Τα προγράμματα για packet sniffing μπορούν να χρησιμοποιηθούν για επίλυση προβλημάτων δικτύου από τους διαχειριστές συστημάτων, αλλά αποτελούν και ένα πολύ ισχυρό εργαλείο για επίδοξους εισβολείς. Τα προγράμματα αυτά μπορούν να συλλέξουν εμπιστευτικές πληροφορίες την ώρα που διέρχονται μέσα από τις γραμμές του δικτύου και πιθανόν και κωδικούς που μεταδίδονται σε μορφή κειμένου. Η αποκάλυψη passwords με αυτό τον τρόπο είναι γνωστή και ως επίθεση *Man-in-the-Middle*. Είναι φανερό ότι η παρακολούθηση δικτύου μπορεί να χρησιμοποιηθεί και για την παραβίαση κωδικών πρόσβασης.

Μεταμφίεση (Masquerade)

Η επίθεση με μεταμφίεση παρατηρείται όταν ο επιτιθέμενος που βρίσκεται σε δίκτυο έξω από το δικό μας, προσποιείται ότι βρίσκεται στο δικό μας. Ειδικά για τα πρωτόκολλα TCP/IP, το παραπάνω είναι γνωστό και ως *IP Spoofing* καθώς ο επιτιθέμενος αλλάζει την διεύθυνση IP των πακέτων του ώστε να φαίνεται ότι προέρχονται από το εσωτερικό μας δίκτυο (ότι ανήκουν δηλ. στο εύρος των δικών μας IP διευθύνσεων). Η μέθοδος αυτή χρησιμοποιείται κυρίως για να ξεγελάσει ο επιτιθέμενος το firewall που συνδέει το εσωτερικό μας δίκτυο με τον έξω κόσμο (το Internet), γενικά με δίκτυο που δεν θεωρείται έμπιστο (trusted). Τυπικά, το IP spoofing περιορίζεται στο να εισάγει δεδομένα ή εντολές σε υπάρχον πακέτο δεδομένων σε επικοινωνίες τύπου client – server ή σημείου προς σημείο (point to point).

Για να είναι δυνατή η αμφίδρομη επικοινωνία (τη στιγμή που η διεύθυνση αφετηρίας δεν είναι η πραγματική του εισβολέα), θα πρέπει ο εισβολέας να έχει αλλάξει κατάλληλα τους πίνακες δρομολόγησης που δείχνουν προς τη διεύθυνση που έχει προσποιηθεί ότι βρίσκεται, ώστε να κατευθύνουν τα δεδομένα προς την πραγματική του διεύθυνση. Έτσι θα λαμβάνει όλα τα πακέτα που κατευθύνονται προς την

“ψεύτικη” διεύθυνση. Στην περίπτωση αυτή, ενδέχεται να λάβει και πακέτα που περιέχουν κωδικούς πρόσβασης. Μπορεί επίσης να στέλνει emails προς το εσωτερικό μας δίκτυο, στους πελάτες ή τους συνεργάτες μας και να χρησιμοποιήσει τεχνικές social engineering που αναφέραμε προηγουμένως για να ανακτήσει κωδικούς.

Αρνηση Παροχής Υπηρεσίας (Denial of Service)

Αυτή η κατηγορία επιθέσεων διαφοροποιείται από αυτές που έχουμε περιγράψει ως τώρα, καθώς δεν προσπαθεί να αποσπάσει τους κωδικούς από το δίκτυο μας, αλλά έχει ως στόχο την *διαθεσιμότητα* των δεδομένων μας. Σκοπός μιας τέτοιας επίθεσης είναι να φτάσει το δικτυακό εξοπλισμό (ή την υπολογιστική ισχύ) στα όρια της, ώστε να μην μπορεί να εξυπηρετήσει πλέον τους νόμιμους χρήστες του δικτύου. Η επίθεση γίνεται συνήθως με εξάντληση των ορίων των πόρων του δικτύου (π.χ. μέγιστος αριθμός πακέτων ανά δευτερόλεπτο που μπορεί να αντέξει το δίκτυο μας, μέγιστος αριθμός πακέτων ανά δευτ. σε κάποιο δρομολογητή ή και μέγιστος αριθμός διεργασιών κάποιου εξυπηρετητή κλπ).

Οι επιθέσεις του παραπάνω τύπου είναι διαδεδομένες ειδικά σε γνωστά και μεγάλα sites στο Internet (Yahoo, CNN, twitter κλπ). Επειδή δεν είναι γενικά δυνατόν να παράγονται και να αποστέλλονται όλα αυτά τα πακέτα της επίθεσης από ένα μόνο υπολογιστή, τυπικά χρησιμοποιούνται μηχανήματα γνωστά ως *zombies* που ανήκουν σε κάποιο *botnet*.

Σημείωση: Ένας υπολογιστής που έχει μολυνθεί με κατάλληλο κακόβουλο πρόγραμμα (malware) μπορεί να δίνει τη δυνατότητα σε κάποιον να τον κατευθύνει από μακριά. Ένας τέτοιος υπολογιστής ονομάζεται *zombie*. Πολλοί υπολογιστές που έχουν μολυνθεί από το ίδιο πρόγραμμα και τους χειρίζεται το ίδιο άτομο ταυτόχρονα, αποτελούν ένα *botnet*. Ο “χειριστής” του botnet μπορεί να στείλει εντολή σε όλα τα zombies που το αποτελούν να αρχίσουν να στέλνουν πακέτα προς μια συγκεκριμένη διεύθυνση δικτύου δημιουργώντας έτσι μια επίθεση τύπου Denial Of Service. Μάλιστα, επειδή η επίθεση αυτή δεν προέρχεται από ένα μόνο μηχανήμα και διεύθυνση IP (ένα botnet μπορεί να περιέχει υπολογιστές σε κάθε σημείο του κόσμου), η συγκεκριμένη επίθεση είναι κατανεμημένη (Distributed Denial of Service Attack, ή DDOS) και είναι αρκετά πιο δύσκολο να αντιμετωπιστεί από το απλό Denial of Service.

Σε σχέση με τις άλλες επιθέσεις που αναφέραμε, οι τεχνικές τύπου Denial of Service δεν απαιτούν ειδικές γνώσεις. Είναι πάντως πιο αποτελεσματικές αν υπάρχει γνώση της εσωτερικής δομής του δικτύου στο οποίο πρόκειται να γίνει η επίθεση.

Επιθέσεις στο Επίπεδο Εφαρμογών (Application-Layer Attacks)

Ορισμένες εφαρμογές όπως το HTTP, ActiveX, Telnet, FTP κλπ. παρουσιάζουν αδυναμίες σε συγκεκριμένα σημεία της ασφάλειας τους, που οφείλονται πολλές φορές σε αδυναμίες στον κώδικα τους (γνωστές και ως τρύπες, holes). Οι γνώστες αυτών των αδυναμιών μπορούν να τις εκμεταλλευθούν για να αποκτήσουν πρόσβαση στο σύστημα με απώτερο σκοπό τη δημιουργία προβλημάτων ή τη συλλογή πληροφοριών.