Τεχνολογίες & Εφαρμογές Πληροφορικής

Ενότητα 10: Ασφάλεια στο Διαδίκτυο

Ανδρέας Βέγλης, Αναπληρωτής Καθηγητής
Τμήμα Δημοσιογραφίας και ΜΜΕ

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Άδειες Χρήσης

- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.
- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «Ανοικτά Ακαδημαϊκά Μαθήματα στο Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

ΑΡΙΣΤΟΤΕΛΕΙΟ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΕΣΣΑΛΟΝΙΚΗΣ

Ανδρέας Βέγλης,
Αναπληρωτής Καθηγητής

Ασφάλεια στο Διαδίκτυο

Το πρόβλημα

- Καθημερινά διάφοροι κακόβουλοι χρήστες του διαδικτύου προσπαθούν να εκμεταλλευτούν τις μικρές ή μεγάλες ατέλειες της πλατφόρμας λογισμικού και των πρωτοκόλλων του διαδικτύου για διάφορους λόγους.

Χάκερ

- Προγραμματιστής.
- Ενδιαφέρεται έντονα για τις μυστικές και απόκρυφες λειτουργίες οποιουδήποτε λειτουργικού συστήματος υπολογιστή.
- Προσπαθεί να ανακαλύψει τα κενά στα συστήματα υπολογιστών καθώς και τους λόγους ύπαρξης αυτών των κενών.
- Αναζητεί πρόσθετη γνώση, μοιράζονται ελεύθερα ότι έχουν ανακαλύψει και ποτέ δεν καταστρέφουν δεδομένα σκοπίμως.

Κράκερ

- Είναι εκείνος που διεισδύει ή διαφορετικά παραβιάζει την ακεραιότητα συστήματος απομακρυσμένων μηχανημάτων, με κακή πρόθεση.
- Καταστρέφει σημαντικά δεδομένα, αποτρέπουν την εξυπηρέτηση των νόμιμων χρηστών ή προξενούν σοβαρά προβλήματα στα θύματά τους.
- Χαρακτηρίζονται γενικά από κακόβουλες πράξεις.

Τύποι επιθέσεων

- Επιθέσεις σε διακομιστές και εταιρικά δίκτυα.
- Μη εξουσιοδοτημένη πρόσβαση.
- Ιοί, σκουλήκια, δούρειοι ίπποι.
- Παρακολούθηση e-mails.
- Παρακολούθηση πληκτρολόγησης.

Επιθέσεις σε διακομιστές και εταιρικά δίκτυα

- **Προέλευση:** Κράκερ από το διαδίκτυο .
- **Στόχος:** διακομιστές.
- **Επικινδυνότητα:** υψηλή (απώλεια δεδομένων, διακοπή υπηρεσιών).
- **Αντιμετώπιση:** εγκατάσταση firewall, χρήση κωδικών πρόσβασης, επιτήρηση λογισμικού.

Μη εξουσιοδοτημένη πρόσβαση

- **Προέλευση:** Τοπικό δίκτυο, διαδίκτυο.
- **Στόχος:** Όλοι οι χρήστες.
- **Επικινδυνότητα:** υψηλή (Κατάληψη μηχανημάτων, παραβίαση του απορρήτου, μηχανήματα εκτίθενται στο τοπικό δίκτυο).
- **Αντιμετώπιση:** εγκατάσταση firewall, με μέτρο χρήση των κοινόχρηστων φακέλων και εκτυπωτών, χρήση κατάλληλων κωδικών πρόσβασης.

Ιοί, σκουλήκια, δούρειοι ίπποι

- **Προέλευση:** Ηλεκτρονική αλληλογραφία, λογισμικό που κατεβάζουμε από το διαδίκτυο.
- **Στόχος:** Όλοι οι χρήστες.
- **Επικινδυνότητα:** μέτρια - υψηλή (Παρακολούθηση ενεργειών, απώλεια δεδομένων).
- **Αντιμετώπιση:** χρήση αντιβιοτικών και firewall.

Παρακολούθηση e-mails

- **Προέλευση:** κράκερ από το διαδίκτυο ή το τοπικό δίκτυο.
- **Στόχος:** Όλοι οι χρήστες.
- **Επικινδυνότητα:** μέτρια - υψηλή (Μη εξουσιοδοτημένοι χρήστες μπορούν να διαβάζουν το e-mail από ενδιάμεσους διακομιστές).
- **Αντιμετώπιση:** κρυπτογράφηση μηνυμάτων, χρήση κατάλληλων κωδικών, περιορισμός της φυσικής πρόσβασης σε μηχανήματα.

Παρακολούθηση πληκτρολόγησης

- **Προέλευση:** δούρειοι ίπποι, χρήστες που έχουν φυσική πρόσβαση στο μηχάνημα.
- **Στόχος:** Όλοι οι χρήστες.
- **Επικινδυνότητα:** υψηλή (παρακολουθείται οτιδήποτε πληκτρολογείται, έτσι γίνονται γνωστοί διάφοροι κωδικοί πρόσβασης).
- **Αντιμετώπιση:** χρήση προγραμμάτων για τον εντοπισμό δούρειων ίππων, έλεγχος της φυσικής πρόσβασης).

Μέθοδοι επίθεσης από το διαδίκτυο

- **DoS (Denial of Service attacks):** χρησιμοποιείται από τους κράκερς για να θέτουν εκτός λειτουργίας διακομιστές. Ο υπολογιστής θύμα για ένα χρονικό διάστημα δεν είναι σε θέση να εξυπηρετεί αιτήσεις από άλλους χρήστες, εξαιτίας του τεράστιου πλήθους κίβδηλων αιτήσεων από δέχεται από τον επιτιθέμενο.
- Υπάρχουν πολλά είδη επιθέσεων **DoS:**

Ping of Death, Smurf Attack, SYN Flood Attack, Teardrop Attack

Ping of Death

- Περιλαμβάνει μία αίτηση PING προς τον υπολογιστή στόχο, με άκυρο μέγεθος πακέτου στην κεφαλή του τελευταίου (>64Kb).
  - Τέτοια παράτυπα πακέτα μπορούν να κρεμάσουν υπολογιστές που τρέχουν λειτουργικά συστήματα ανίκανα να τα μεταχειριστούν.

Smurf Attack

- Περιλαμβάνει αιτήσεις PING σε μία διεύθυνση εκπομπής στο υπό επίθεση δίκτυο ή σε κάποιο άλλο ενδιάμεσο.
  - Η διεύθυνση επιστροφής πλαστογραφείται ώστε να είναι ίδια με αυτήν του υπολογιστή στόχου.
  - Επειδή μία διεύθυνση εκπομπής αντιστοιχεί σε όλα τα μηχανήματα ενός υποδικτύου, η αίτηση λειτουργεί ενισχυτικά και δημιουργείται μεγάλος όγκος άχρηστων πακέτων.

SYN Flood Attack

- Περιλαμβάνει την κακή χρήση της εγκαθίδρυσης συνεδρίας (επικοινωνίας) με έναν διακομιστή.
  - Ένας κράκερ μπορεί με αυτό τον τρόπο να υπερφορτώσει ένα διακομιστή.
  - Κατά τη διάρκεια της επίθεσης ο κράκερ παραποιεί την IP διεύθυνσή του, κρύβοντας έτσι τα ίχνη του.

Teardrop Attack

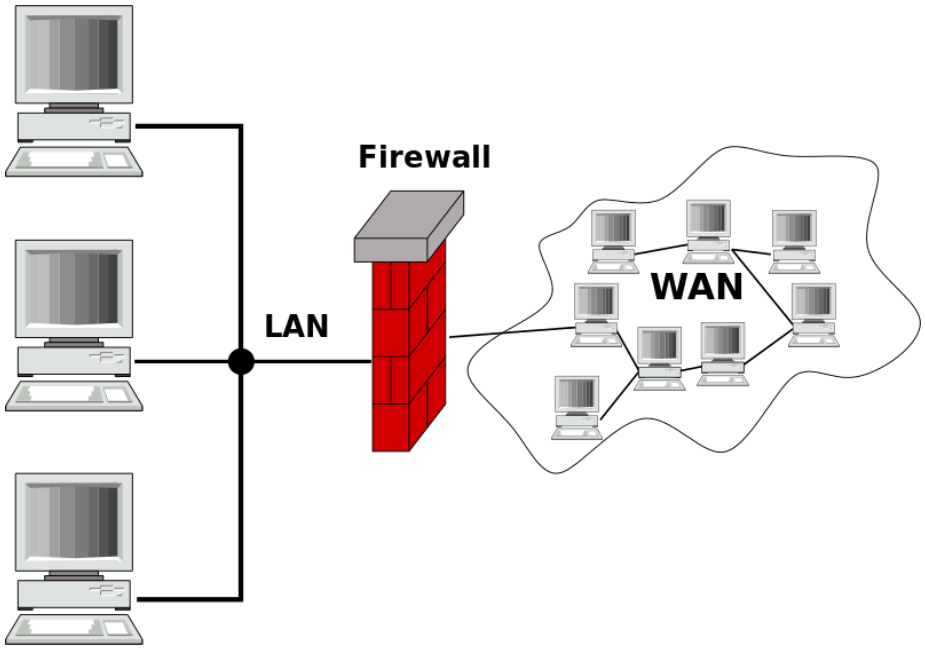
- Όταν ένα πακέτο αποστέλλεται στο διαδίκτυο ενδέχεται να χωριστεί σε επιμέρους μικρότερα τμήματα. Κάθε τμήμα περιλαμβάνει στην κεφαλή του ένα πεδίο όπου εκεί περιγράφεται η θέση του στο αρχικό, «μεγάλο» πακέτο IP. Ο κράκερ χρησιμοποιεί ένα πρόγραμμα με όνομα Teardrop το οποίο τεμαχίζει πακέτα IP σε τμήματα με λανθασμένες πληροφορίες στο συγκεκριμένο πεδίο.
- Όταν ο υπολογιστής στόχος προσπαθήσει να συναρμολογήσει τα παραπλανητικά αυτά τμήματα, θα κολλήσει ή θα επανεκκινήσει.

Distributed Denial of Service

- Σε αυτή την περίπτωση στις επιθέσεις συμμετέχουν περισσότερα του ενός μηχανήματα. Στις επιθέσεις είναι δυνατό να συμμετέχουν και PC χωρίς να το γνωρίζουν οι χρήστες τους. Ο κράκερ κατορθώνει με κάποιο τρόπο να βάλει ένα μικρό πρόγραμμα σε καθένα από τα μηχανήματα που θα συμμετάσχουν εν αγνοία των χρηστών τους στην επίθεση.
- Την στιγμή που ξεκινάει την επίθεση στέλνει μία ειδοποίηση σε ένα από αυτά. Τότε αυτό ειδοποιεί καθένα από τα άλλα και αρχίζουν όλα να στέλνουν πλαστές αιτήσεις στο στόχο.

Firewall

- Ένα πρόγραμμα Firewall σε τοπικό δίκτυο ή σε έναν υπολογιστή ελέγχει όλες τις εισερχόμενες και εξερχόμενες διαδικτυακές επικοινωνίες.



Εικόνα 1

Απόπειρα κατάλυσης του διαδικτύου

- Επί 3 ημέρες στα τέλη του Οκτωβρίου του 2002 βρισκόταν σε εξέλιξη επίθεση (Distributed DoS) στους 13 βασικούς διακομιστές (DomainName root servers) του διαδικτύου. Για τρεις ώρες στις 21/10/02 επτά από τους 13 διακομιστές απόδοσης διευθύνσεων σε δικτυακούς τόπους με καταλήξεις .com, .org, .uk διέκοψαν την λειτουργία τους.
- Αν η επίθεση πετύχαινε να διακόψει την λειτουργία σε 8-10 διακομιστές η καθυστέρηση στη πρόσβαση στο διαδίκτυο θα ήταν σημαντική.

Αναφορές εικόνων

1. Gateway firewall https://commons.wikimedia.org/wiki/File%3AGateway_firewall.svg By Harald Muhlbock [GFDL (http://www.gnu.org/copyleft/fdl.html) or CC-BY-SA-3.0 (http://creativecommons.org/licenses/by-sa/3.0/)], via Wikimedia Commons from Wikimedia Commons

Τέλος Ενότητας

Επεξεργασία: Γιομελάκης Δημήτριος

Θεσσαλονίκη, Εαρινό εξάμηνο 2012-13

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης