

Ε Κ Δ Ο Σ Ε Ι Σ Κ Λ Ε Ι Δ Α Ρ Ι Θ Μ Ο Σ

# ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ

## ΑΡΧΕΣ ΚΑΙ ΠΡΑΚΤΙΚΕΣ

3η αμερικανική έκδοση



William Stallings • Lawrie Brown



# Κεφάλαιο 8

Ανιχνευση εισβολών

# Κατηγορίες εισβολέων – Κυβερνοεγκληματίες

- Μεμονωμένα άτομα ή μέλη του οργανωμένου εγκλήματος, των οποίων ο απώτερος στόχος είναι το οικονομικό κέρδος
- Δραστηριότητες :
  - Κλοπή ταυτότητας
  - Κλοπή χρηματοπιστωτικών διαπιστευτηρίων
  - Εταιρική κατασκοπεία
  - Κλοπή δεδομένων
  - Είσπραξη λύτρων για αποκρυπτογράφηση δεδομένων
- Συνήθως έχουν νεαρή ηλικία, προέρχονται από την ανατολική Ευρώπη, τη Ρωσία, ή τη νοτιοανατολική Ασία, και εκτελούν τις συναλλαγές τους μέσω του Ιστού
- Συναντιούνται σε μυστικά φόρουμ για να ανταλλάξουν συμβουλές και δεδομένα και να συντονίσουν τις επιθέσεις τους

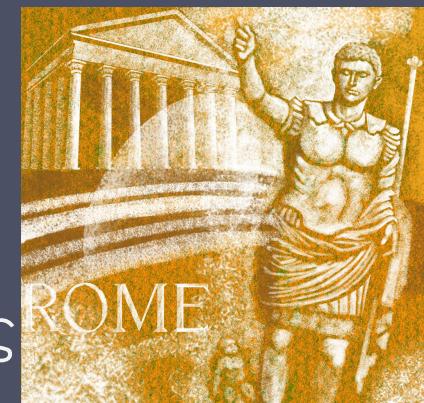


# Κατηγορίες εισβολέων – Ακτιβιστές

- Πρόκειται για μεμονωμένα άτομα, τα οποία συνήθως δουλεύουν εκ των ίσων, ή μέλη μιας μεγαλύτερης ομάδας παρείσακτων-επιτιθέμενων, με κίνητρα που παραπέμπουν σε κοινωνικούς ή πολιτικούς αγώνες
- Γνωστοί και ως «χακτιβιστές»
  - Το επίπεδο των δεξιοτήτων τους συχνά είναι αρκετά χαμηλό
- Ο σκοπός των επιθέσεών τους είναι να προάγουν και να διαφημίσουν τον αγώνα τους, συνήθως μέσα από:
  - Βανδαλισμό ιστότοπων
  - Επιθέσεις άρνησης εξυπηρέτησης
  - Κλοπή και διανομή δεδομένων που οδηγεί σε αρνητική δημοσιότητα ή παραβίαση των στόχων τους

# Κατηγορίες εισβολέων – Οργανισμοί χρηματοδοτούμενοι από κυβερνήσεις κρατών

- Ομάδες χάκερ που χρηματοδοτούνται από διάφορες κυβερνήσεις και επιδίδονται σε δραστηριότητες κατασκοπείας ή δολιοφθοράς
- Τέτοιες δραστηριότητες είναι γνωστές και ως Προηγμένες Μόνιμες Απειλές (APT) λόγω της κρυφής και μόνιμης (για παρατεταμένα χρονικά διαστήματα) φύσης πολλών από τις επιθέσεις αυτής της κατηγορίας
- Ευρύτατα διαδεδομένη υιοθέτηση τέτοιων δραστηριοτήτων από διάφορες χώρες –όπως η Κίνα, οι Η.Π.Α. και το Ηνωμένο Βασίλειο– και τις μυστικές υπηρεσίες των συμμάχων τους

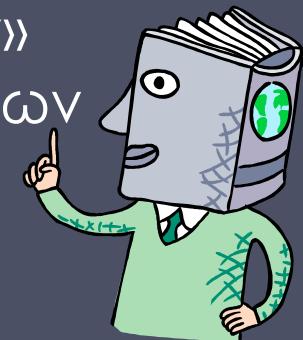


# Κατηγορίες εισβολέων – Λοιποί

- Χάκερ με κίνητρα διαφορετικά από αυτά που έχουν αναφερθεί
- Σε αυτούς περιλαμβάνονται χάκερ ή «σπάστες» με μοναδικό κίνητρο τις τεχνικές προκλήσεις ή την αναγνώριση και εκτίμηση που θα κερδίσουν από τους ομοϊδεάτες τους
- Στα μέλη της συγκεκριμένης κατηγορίας θα μπορούσαμε να κατατάξουμε πολλούς από τους χάκερ που κατάφεραν να ανακαλύψουν νέες κατηγορίες ευπαθειών υπερχείλισης περιοχών προσωρινής αποθήκευσης
- Με δεδομένη την ευρεία διαθεσιμότητα των κιτ επίθεσης, υπάρχει μια μεγάλη μερίδα «χάκερ από χόμπι» που χρησιμοποιούν τέτοια κιτ για να τεστάρουν την ασφάλεια συστημάτων και δικτύων

# Επίπεδο δεξιοτήτων εισβολέων – Μαθητευόμενοι

- Χάκερ με ελάχιστες τεχνικές δεξιότητες οι οποίοι συνήθως χρησιμοποιούν υπάρχοντα κιτ επίθεσης
- Αποτελούν τη μεγάλη πλειοψηφία των επιτιθέμενων, και σε αυτούς περιλαμβάνονται πολλοί εγκληματίες και ακτιβιστές
- Επειδή στηρίζονται σε υπάρχοντα, γνωστά εργαλεία, είναι πιο εύκολο να τους αντιμετωπίσει κανείς με επιτυχία
- Είναι επίσης γνωστοί ως «παιδιά των σεναρίων» (script-kiddies) επειδή κάνουν χρήση υπαρχόντων σεναρίων (εργαλείων)



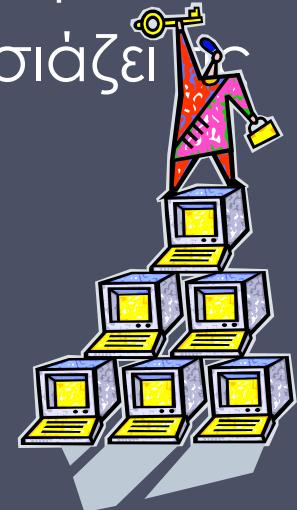
# Επίπεδο δεξιοτήτων εισβολέων – Μετρίων ικανοτήτων

- Χάκερ με επαρκείς τεχνικές δεξιότητες οι οποίοι μπορούν να τροποποιήσουν και να επεκτείνουν τα κιτ επίθεσης ώστε να χρησιμοποιούν ευπάθειες που έχουν ανακαλυφθεί ή «αγοραστεί» πρόσφατα
- Ενδέχεται να είναι σε θέση να εντοπίζουν νέες ευπάθειες προς εκμετάλλευση οι οποίες είναι παρόμοιες με ήδη γνωστές ευπάθειες
- Σε όλες τις κατηγορίες εισβολέων που παρατίθενται παραπάνω είναι πιθανό να βρείτε αρκετούς χάκερ με τέτοιες δεξιότητες
- Προσαρμόζουν εργαλεία για χρήση από άλλους



# Επίπεδο δεξιοτήτων εισβολέων – Εξπέρ

- Χάκερ με εξαιρετικές τεχνικές δεξιότητες, ικανοί να ανακαλύπτουν εντελώς νέες κατηγορίες ευπαθειών
- Δημιουργούν νέα πανίσχυρα κιτ επίθεσης
- Ορισμένοι από τους πιο γνωστούς κλασικούς χάκερ ανήκουν σε αυτό το επίπεδο
- Μερικοί χρηματοδοτούνται από κυβερνήσεις κρατών
- Η άμυνα κατά των επιθέσεων αυτών παρουσιάζει μεγαλύτερες δυσκολίες



# Παραδείγματα εισβολών

- Απομακρυσμένη παραβίαση και απόκτηση δικαιωμάτων υπερχρήστη (root)
- Βανδαλισμός διακομιστών Ιστού
- Τυχαία εύρεση και «σπάσιμο» κωδικών πρόσβασης
- Αντιγραφή βάσεων δεδομένων που περιέχουν αριθμούς πιστωτικών καρτών
- Προβολή ευαίσθητων δεδομένων χωρίς εξουσιοδότηση
- Εκτέλεση λογισμικού ανίχνευσης πακέτων (packet sniffer)
- Διανομή πειρατικού λογισμικού
- Χρήση μη ασφαλούς μόντεμ και απόκτηση πρόσβασης στο εσωτερικό δίκτυο
- Άτομα που παριστάνουν τα στελέχη για να πάρουν πληροφορίες
- Χρήση ανεπιτήρητου σταθμού εργασίας



# Συμπεριφορά εισβολέων

Προσδιορισμός  
στόχων και  
συλλογή  
πληροφοριών

Αρχική  
πρόσβαση

Αύξηση  
προνομίων

Συλλογή  
πληροφοριών ή  
εκμετάλλευση  
συστήματος

Διατήρηση  
πρόσβασης

Απόκρυψη ιχνών

#### (α) Προσδιορισμός στόχων και συλλογή πληροφοριών

- Εξερεύνηση εταρικού ιστότοπου με σκοπό την εύρεση πληροφοριών για την εταρική δομή, το προσωπικό, τα βασικά συστήματα, καθώς και λεπτομέρειες για τον συγκεκριμένο διακομιστή Ιστού και το λειτουργικό σύστημα που χρησιμοποιείται.
- Συλλογή πληροφοριών στο δίκτυο-στόχο με χρήση εργαλείων αναζήτησης DNS (DNS lookup) όπως τα dig, host και άλλα: υποβολή ερωτημάτων στη βάση δεδομένων WHOIS.
- Χαρτογράφηση των προσπελάσματων υπηρεσιών του δικτύου με χρήση εργαλείων όπως το NMAP.
- Αποστολή διερευνητικού μηνύματος ηλεκτρονικού ταχυδρομείου στη σχετική ηλεκτρονική διεύθυνση της εξυπηρέτησης πελατών, εξέταση της απάντησης για εύρεση πληροφοριών σχετικά με τα προγράμματα πελάτη και διακομιστή ηλεκτρονικού ταχυδρομείου και το λειτουργικό σύστημα που χρησιμοποιούνται, καθώς και στοιχείων για τον συντάκτη της απάντησης.
- Προσδιορισμός δυνητικά ενυπάρχων υπηρεσιών, π.χ., ευπαθές σύστημα διαχείρισης περιεχομένου (content management system, CMS) του Ιστού.

#### (β) Αρχική πρόσβαση

- Τυχαία είρεση με «ωμή βίᾳ» (εξαντλητική αναζήτηση/δοκιμή) του κωδικού πρόσβασης ενός χρήστη στο σύστημα διαχείρισης περιεχομένου (CMS) του Ιστού.
- Εκμετάλλευση ευπάθειας στη συνδέσμενη υπομονάδα (plugin) CMS του Ιστού ώστε να αποκτηθεί πρόσβαση στο σύστημα.
- Αποστολή μηνύματος ηλεκτρονικού «κακαμάκωματος» σε άτομα-κλειδιά, το οποίο θα περιέχει έναν σύνδεσμο που θα οδηγεί στην ευπάθεια του φυλλομετρητή ιστού.

#### (γ) Ανάηση προνομίων

- Σάρωση συστήματος για εφαρμογές με τοπική εκμετάλλευση ευπαθειών.
- Εκμετάλλευση τυχόν ευπαθών εφαρμογών ώστε να αποκτηθούν αυξημένα προνόμια.
- Εγκατάσταση προγραμμάτων ανίχνευσης πακέτων (sniffers) με σκοπό την υποκλοπή των κωδικών πρόσβασης του διαχειριστή.
- Χρήση του κλεμμένου κωδικού πρόσβασης του διαχειριστή για την απόκτηση πρόσβασης σε προστατευμένες πληροφορίες.

#### (δ) Συλλογή πληροφοριών ή εκμετάλλευση αδυναμιών του συστήματος

- Σάρωση αρχείων για τις επιθυμητές πληροφορίες.
- Μεταφορά πολλών εγγράφων σε εξωτερικό «αποθετήριο».
- Χρήση κωδικών πρόσβασης που έχουν βρεθεί τυχαία ή υποκλαπεί για την απόκτηση πρόσβασης σε άλλους διακομιστές του δικτύου.

#### (ε) Διατήρηση πρόσβασης

- Εγκατάσταση εργαλείου απομακρυσμένης διαχείρισης ή κιτ υπερχρήστη με κερκόπορτα για μελλοντική πρόσβαση.
- Χρήση του κωδικού πρόσβασης του διαχειριστή για μελλοντική πρόσβαση στο δίκτυο.
- Τροποποίηση ή απενεργοποίηση προγραμμάτων προστασίας από ιούς ή προγραμμάτων IDS τα οποία εκτελούνται στο σύστημα.

#### (στ) Απόκρυψη ιχνών

- Χρήση κιτ υπερχρήστη για την απόκρυψη αρχείων που έχουν εγκατασταθεί στο σύστημα
- Επεξεργασία αρχείων καταγραφής για τη διαγραφή καταχωρίσεων που έχουν παραχθεί κατά τη διάρκεια της εισβολής.

## Πίνακας 8.1

# Παραδείγματα συμπεριφοράς εισβολέων

(Ο πίνακας βρίσκεται στις σελ. 305-306 του βιβλίου.)

# Ορισμοί από το RFC 2828

(Γλωσσάρι ασφαλειας Διαδικτύου)



**Παραβίαση ασφαλείας:** Συμβάν ασφαλείας, ή συνδυασμός πολλών συμβάντων ασφαλείας, το οποίο συνιστά περιστατικό ασφαλείας κατά το οποίο ένας εισβολέας αποκτά, ή επιχειρεί να αποκτήσει, πρόσβαση σε ένα σύστημα (ή πόρο συστήματος) χωρίς να έχει σχετική εξουσιοδότηση.

**Ανίχνευση εισβολών:** Μια υπηρεσίας ασφαλείας η οποία παρακολουθεί και αναλύει συμβάντα ασφαλείας με σκοπό τον εντοπισμό, και την παροχή σχετικών προειδοποιήσεων σε πραγματικό ή σχεδόν πραγματικό χρόνο, οποιασδήποτε απόπειρας να αποκτηθεί πρόσβαση σε πόρους του συστήματος με μη εξουσιοδοτημένο τρόπο.

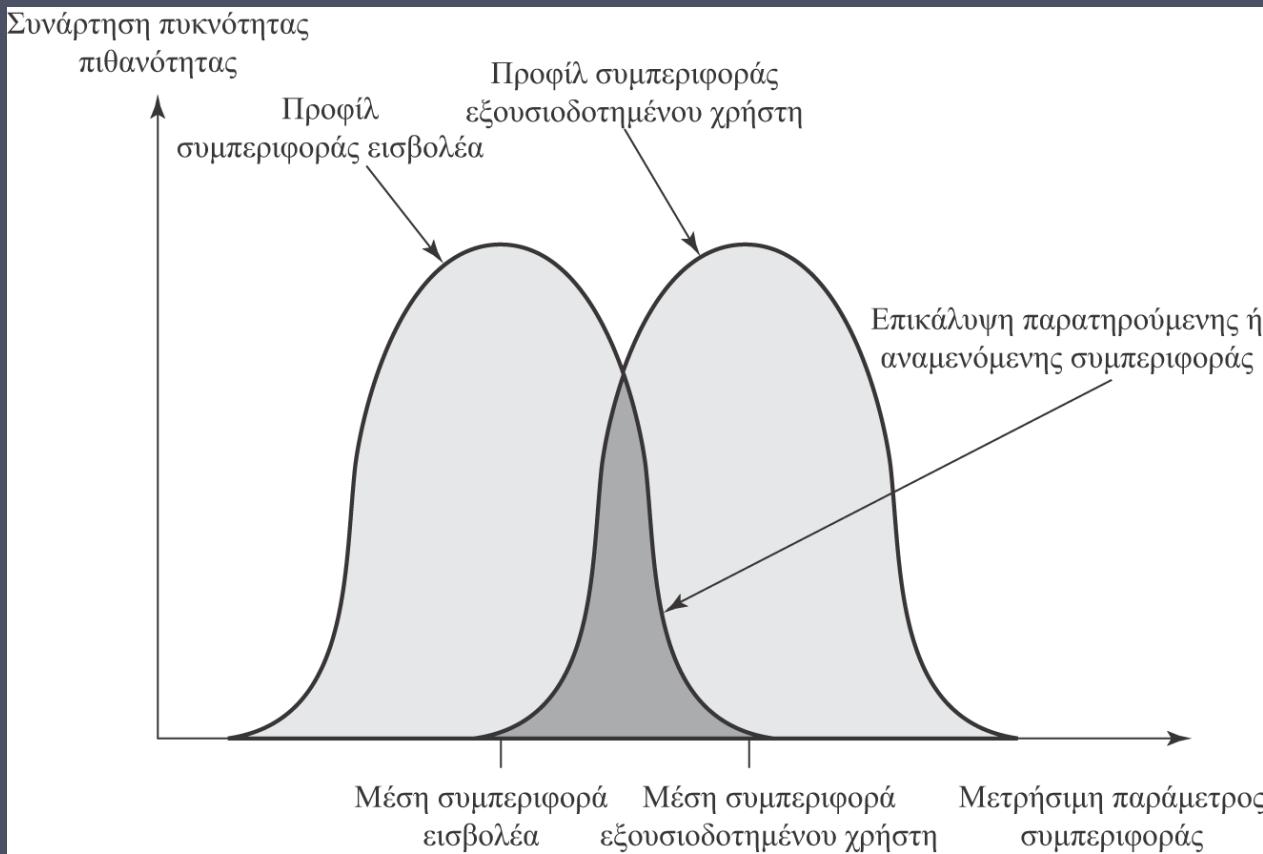
# Σύστημα ανίχνευσης εισβολών (IDS)

- IDS βασισμένο σε υπολογιστή υπηρεσίας (HIDS)
  - Παρακολουθεί τα χαρακτηριστικά ενός μόνο υπολογιστή υπηρεσίας για ύποπτη δραστηριότητα
- IDS βασισμένο σε δίκτυο (NIDS)
  - Παρακολουθεί την κυκλοφορία δικτύου και αναλύει τα πρωτόκολλα δικτύου, μεταφοράς, και εφαρμογών προκειμένου να αναγνωρίσει τυχόν ύποπτη δραστηριότητα
- Κατανεμημένο ή υβριδικό IDS
  - Συνδυάζει πληροφορίες από πολλούς αισθητήρες, συχνά βασισμένους και σε υπολογιστές υπηρεσίας και σε δίκτυα, σε έναν κεντρικό αναλυτή ο οποίος είναι σε θέση να αναγνωρίζει πιο εύκολα και να αποκρίνεται σε δραστηριότητες εισβολής



**Αποτελείται από τρεις λογικές υπομονάδες:**

- **Αισθητήρες – συλλογή δεδομένων**
- **Αναλυτές – εξακρίβωση τυχόν εισβολής**
- **Διασύνδεση χρήστη – προβολή της εξόδου ή έλεγχος της συμπεριφοράς του συστήματος**



Εικόνα 8.1 Προφίλ συμπεριφοράς εισβολέων και εξουσιοδοτημένων χρηστών

# Απαιτήσεις ενός IDS

Συνεχής λειτουργία

Ανεκτικότητα  
στα σφάλματα

Ανθεκτικότητα  
σε συγκεκαλυμμένες  
τροποποιήσεις

Πρόκληση ελάχιστης  
επιβάρυνσης  
στο σύστημα

Διευθέτηση  
σύμφωνα με τις  
πολιτικές ασφαλείας  
του συστήματος

Προσαρμογή  
σε αλλαγές του  
συστήματος και  
της συμπεριφοράς  
των χρηστών

Προσαρμογή  
μεγέθους για  
παρακολούθηση  
μεγάλου αριθμού  
συστημάτων

Παροχή ομαλής  
υποβάθμισης της  
εξυπηρέτησης

Δυνατότητα  
δυναμικής  
επαναδιευθέτησης

# Τεχνικές ανάλυσης

## Ανίχνευση ανωμαλιών

- Περιλαμβάνει τη συλλογή δεδομένων που σχετίζονται με τη συμπεριφορά έγκυρων χρηστών για κάποιο χρονικό διάστημα
- Η παρατηρούμενη συμπεριφορά αναλύεται ώστε να προσδιοριστεί αν αντιστοιχεί σε έγκυρο χρήστη ή σε εισβολέα

## Ανίχνευση υπογραφών/ ευρετική ανίχνευση

- Χρησιμοποιεί ένα σύνολο από γνωστές, κακόβουλες ακολουθίες δεδομένων ή κανόνες επίθεσης, τα οποία συγκρίνει με την τρέχουσα συμπεριφορά
- Γνωστή και ως ανίχνευση αθέμιτης χρήσης
- Μπορεί να αναγνωρίσει μόνο γνωστές επιθέσεις για τις οποίες διαθέτει ακολουθίες ή κανόνες

# Ανίχνευση ανωμαλιών

Χρησιμοποιούνται διάφορες μέθοδοι ταξινόμησης :

## Στατιστικές

- Αναλύουν την παρατηρούμενη συμπεριφορά χρησιμοποιώντας μονομεταβλητά ή πολυμεταβλητά μοντέλα, ή μοντέλα χρονοσειρών των παρατηρούμενων μετρικών

## Βασισμένες σε γνώσεις

- Χρησιμοποιούν ένα έμπειρο σύστημα που ταξινομεί την παρατηρούμενη συμπεριφορά σύμφωνα με ένα σύνολο κανόνων που μοντελοποιούν την έγκυρη συμπεριφορά

## Μηχανικής μάθησης

- Προσδιορίζουν αυτόματα ένα κατάλληλο μοντέλο ταξινόμησης από τα δεδομένα εκπαίδευσης χρησιμοποιώντας τεχνικές εξόρυξης δεδομένων

# Ανίχνευση υπογραφών ή ευρετική ανίχνευση

## Μέθοδοι βασισμένες σε υπογραφές



Συγκρίνουν μια μεγάλη συλλογή από γνωστές ακολουθίες κακόβουλων δεδομένων με δεδομένα που είναι αποθηκευμένα σε ένα σύστημα ή διέρχονται από ένα δίκτυο



Οι υπογραφές πρέπει να είναι αρκετά μεγάλες ώστε να ελαχιστοποιείται το ποσοστό ψευδών συναγερμών, επιτρέποντας ταυτόχρονα την ανίχνευση ενός επαρκώς υψηλού ποσοστού κακόβουλων δεδομένων



Χρησιμοποιούνται ευρέως σε προϊόντα προστασίας από ιούς, σε μεσολαβητές σάρωσης δικτυακής κυκλοφορίας και σε συστήματα NIDS

## Βασισμένη σε κανόνες ευρετική ταυτοποίηση



Περιλαμβάνει τη χρήση κανόνων για την ταυτοποίηση γνωστών εισβολών ή εισβολών που θα εκμεταλλεύονται γνωστές αδυναμίες



Μπορούν επίσης να οριστούν κανόνες οι οποίοι αναγνωρίζουν ύποπτες συμπεριφορές, ακόμα και όταν αυτές βρίσκονται εντός των ορίων των καθιερωμένων μοτίβων χρήσης



Συνήθως οι κανόνες που χρησιμοποιούνται έχουν οριστεί ειδικά για κάποιο σύστημα



To SNORT αποτελεί παράδειγμα συστήματος NIDS το οποίο βασίζεται σε κανόνες

# Ανίχνευση εισβολών βασισμένη σε υπολογιστές υπηρεσίας (HIDS)

- Προσθέτει ένα εξειδικευμένο επίπεδο λογισμικού ασφαλείας σε ευπαθή ή ευαισθητά συστήματα
- Μπορεί να χρησιμοποιεί είτε μεθόδους βασισμένες σε ανωμαλίες είτε μεθόδους βασισμένες σε υπογραφές και ευρετικά κριτήρια
- Παρακολουθεί τη δραστηριότητα προκειμένου να ανιχνεύει ύποπτες συμπεριφορές
  - Ο κύριος σκοπός του είναι να ανιχνεύει εισβολές, να καταγράφει ύποπτα συμβάντα, και να στέλνει προειδοποιήσεις
  - Μπορεί να ανιχνεύει και εξωτερικές και εσωτερικές εισβολές



# Πηγές δεδομένων και αισθητήρες



Βασική υπομονάδα της ανίχνευσης εισβολών είναι ο αισθητήρας συλλογής δεδομένων

Στις δημοφιλείς πηγές δεδομένων περιλαμβάνονται:

- Ίχνη κλήσεων συστήματος
- Εγγραφές διαχειριστικής παρακολούθησης (αρχεία καταγραφής)
- Αθροίσματα ελέγχου ακεραιότητας αρχείων
- Πρόσβαση στο μητρώο

# Πίνακας 8.2

Παρακολουθούμενες  
κλήσεις συστήματος  
Linux και βιβλιοθήκες  
DLL των Windows

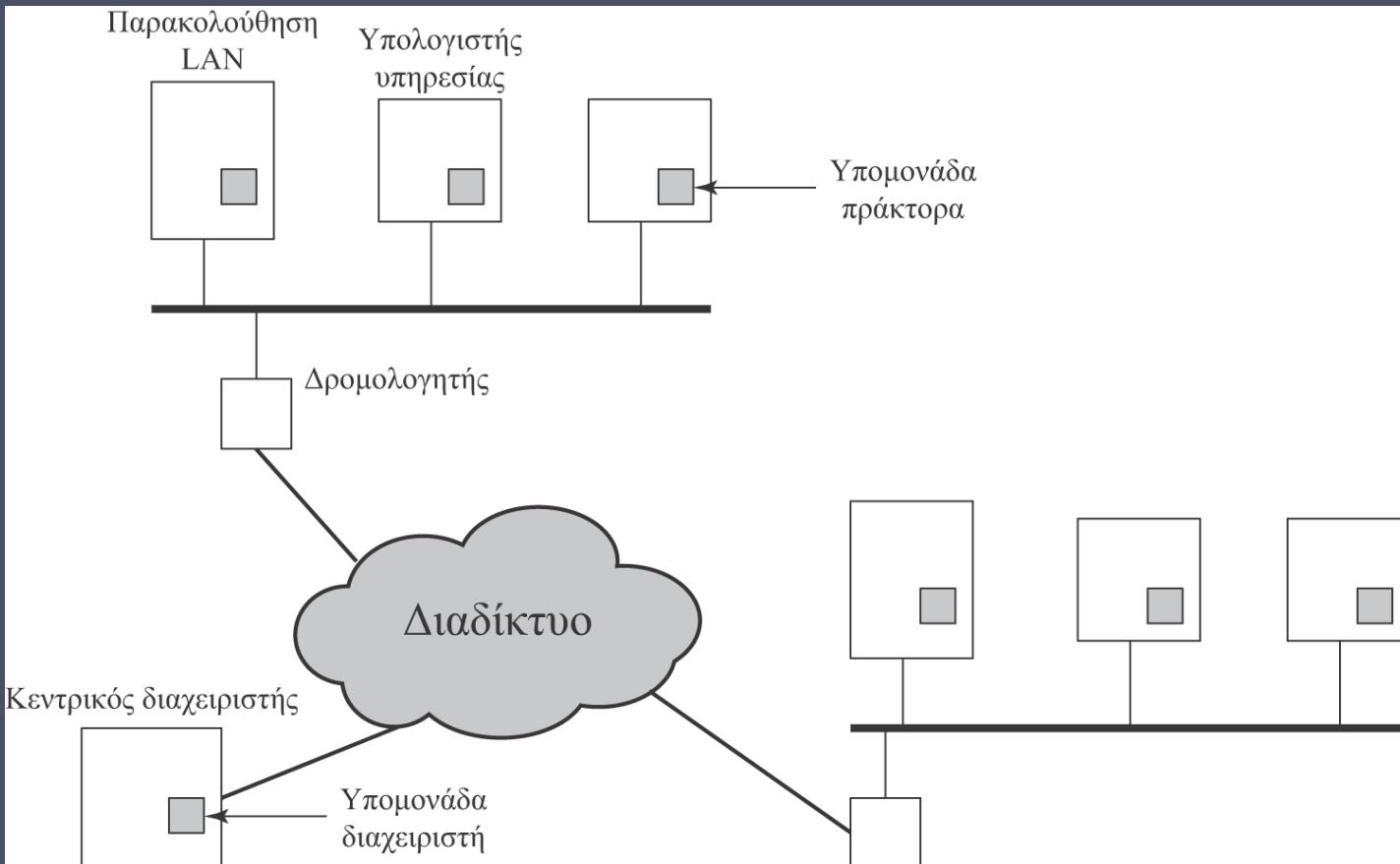
## (α) Κλήσεις συστήματος Ubuntu Linux

accept, access, acct, adjtime, aiocancel, aioread, aiowait, aiowrite, alarm, async\_daemon, auditsys, bind, chdir, chmod, chown, chroot, close, connect, creat, dup, dup2, execv, execve, exit, exportfs, fchdir, fchmod, fchown, fchroot, fcntl, flock, fork, fpathconf, fstat, fstatfs, fsync, ftime, ftruncate, getdents, getdirent, getdomainname, getopt, getdtsize, getfh, getgid, getgroups, gethostid, gethostname, getitimer, getmsg, getpagesize, getpeername, getpgrp, getpid, getpriority, getrlimit, getrusage, getsockname, getsockopt, gettimeofday, getuid, gtty, ioctl, kill, killpg, link, listen, lseek, lstat, madvise, mctl, mincore, mkdir, mknod, mmap, mount, mount, mprotect, mpxchan, msgsys, msync, munmap, nfs\_mount, nfssvc, nice, open, pathconf, pause, pcfs\_mount, phys, pipe, poll, profil, ptrace, putmsg, quota, quotactl, read, readlink, ready, reboot, recv, recvfrom, recvmsg, rename, resuba, rfssys, rmdir, sbreak, sbrk, select, semsys, send, sendmsg, sendto, setdomainname, setdopt, setgid, setgroups, sethostid, sethostname, setitimer, setpgid, setpgrp, setquota, setregid, setreuid, setrlimit, setsid, setsockopt, gettimeofday, setuid, shmsys, shutdown, sigblock, sigpause, sigpending, sigsetmask, sigstack, sigsys, sigvec, socket, socketaddr, socketpair, sstk, stat, stat, statfs, stime, stty, swapon, symlink, sync, sysconf, time, times, truncate, umask, umount, uname, unlink, unmount, ustata, utime, utimes, vadvise, vfork, vhangup, vlimit, vpixsys, vread, vtimes, vtrace, vwrite, wait, wait3, wait4, write, writev

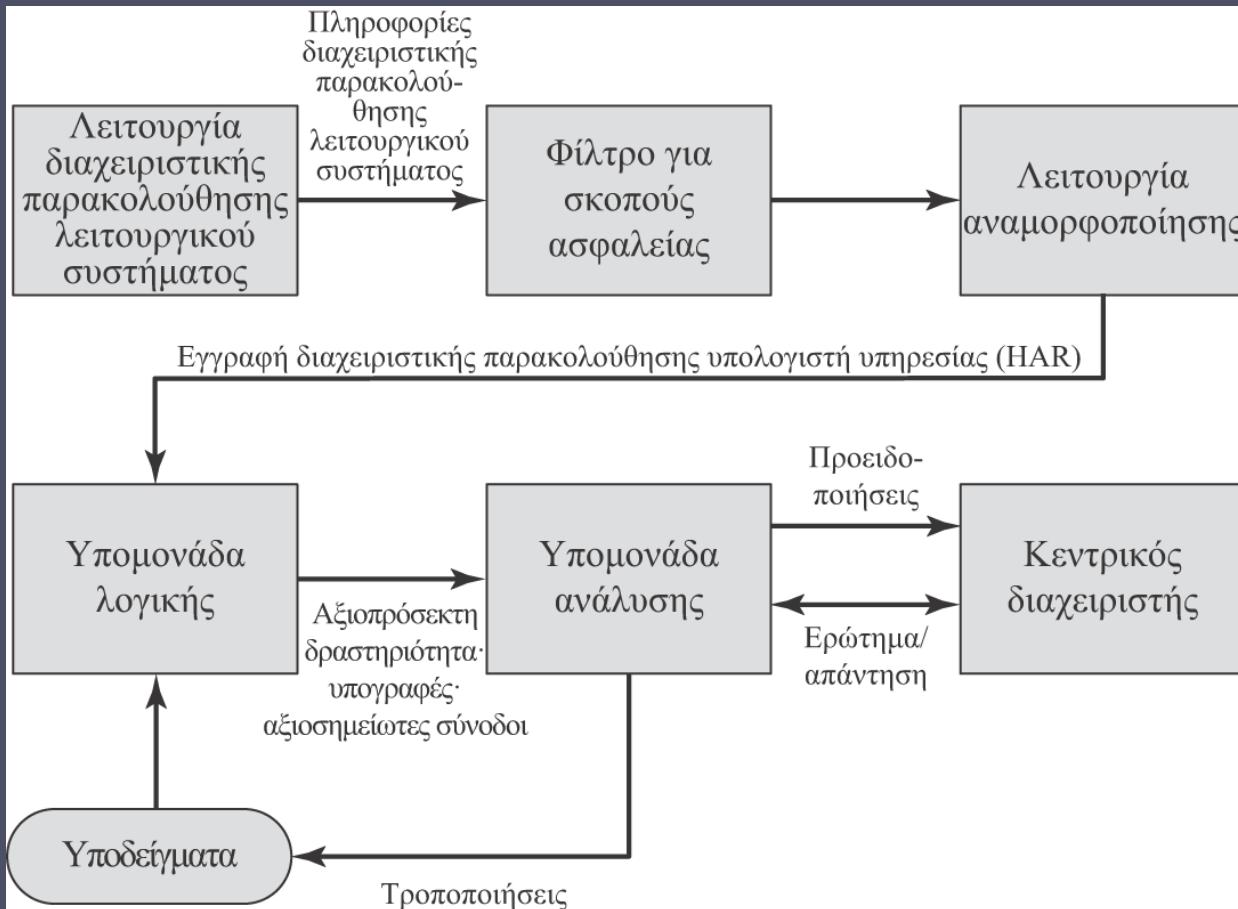
## (β) Βασικές βιβλιοθήκες DLL και εκτελέσιμα αρχεία των Windows

comctl32  
kernel32  
msvcpp  
msvcrt  
mswsock  
ntdll  
ntoskrnl  
user32  
ws2\_32

(Ο πίνακας βρίσκεται  
στη σελ. 314 του βιβλίου)



Εικόνα 8.2 Αρχιτεκτονική για κατανεμημένη ανίχνευση εισβολών



Εικόνα 8.3 Αρχιτεκτονική πράκτορα



# IDS βασισμένο σε δίκτυο (NIDS)

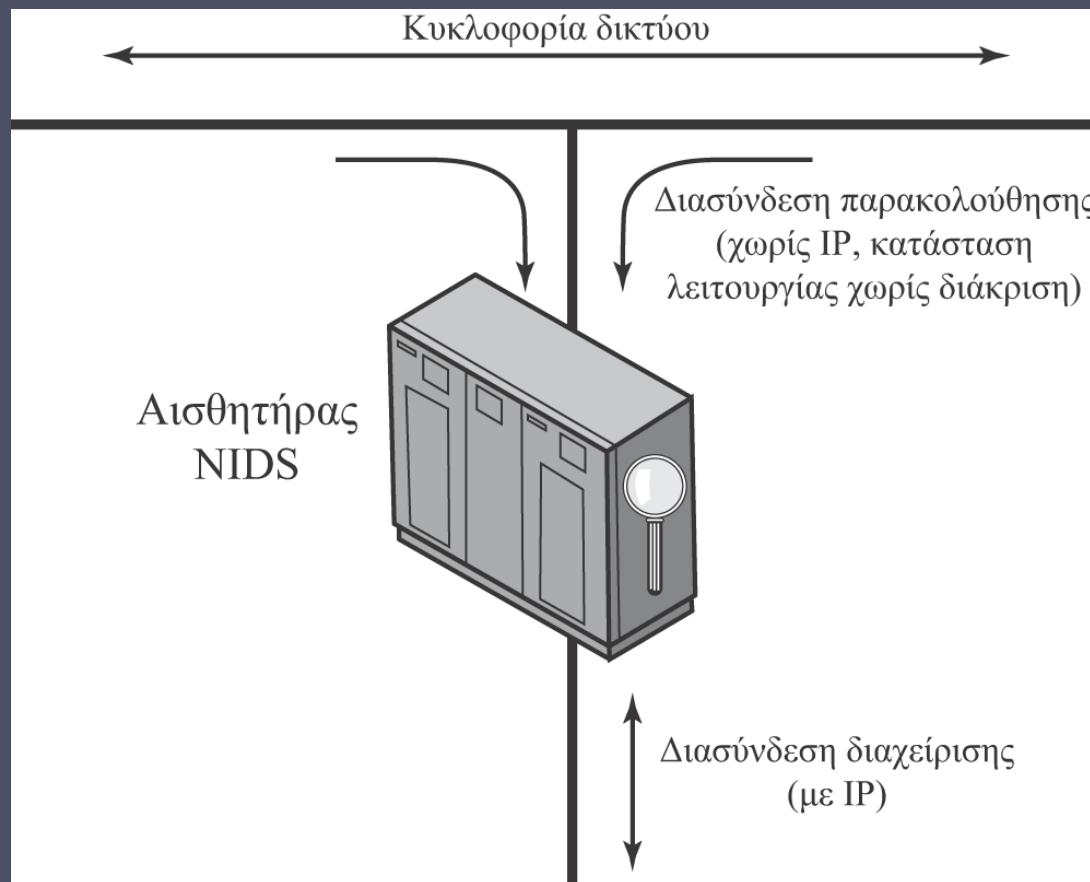
Παρακολουθεί την κυκλοφορία δεδομένων σε επιλεγμένα σημεία ενός δικτύου

Εξετάζει κάθε πακέτο της κυκλοφορίας ξεχωριστά σε πραγματικό, ή σχεδόν σε πραγματικό, χρόνο

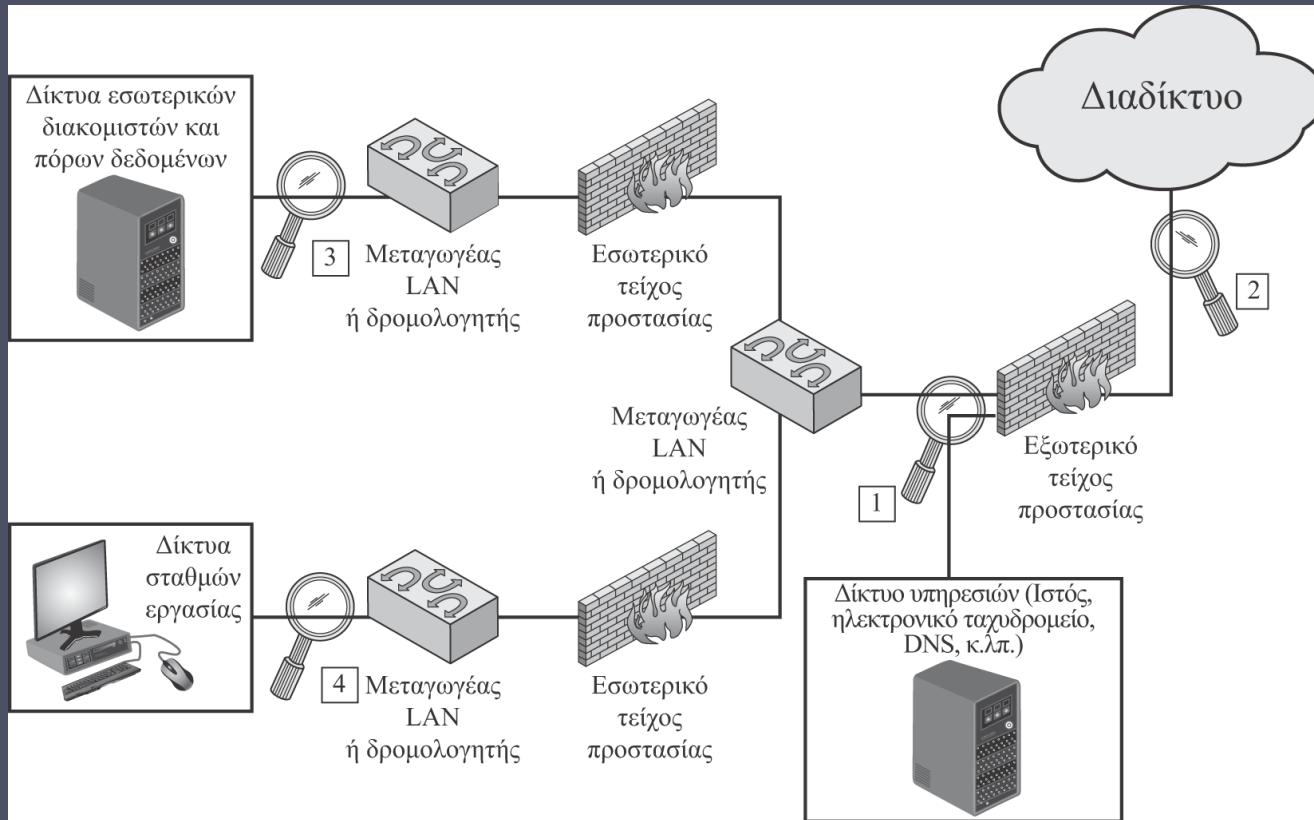
Ενδέχεται να εξετάζει τη δραστηριότητα σε επίπεδο πρωτοκόλλου μεταφοράς ή/και εφαρμογών

Περιλαμβάνει αρκετούς αισθητήρες, έναν ή περισσότερους διακομιστές για λειτουργίες διαχείρισης του NIDS, καθώς και μία ή περισσότερες κονσόλες διαχείρισης για τη διασύνδεση με ανθρώπους

Η ανάλυση των μοτίβων κυκλοφορίας μπορεί να πραγματοποιείται στον αισθητήρα, στον διακομιστή διαχείρισης, ή κάποιον συνδυασμό και των δύο



Εικόνα 8.4 Παθητικός αισθητήρας NIDS



Εικόνα 8.5 Παράδειγμα τοποθέτησης αισθητήρα NIDS

# Τεχνικές ανίχνευσης εισβολών

Επιθέσις κατάλληλες για  
ανίχνευση υπογραφών

- Αναγνώριση και επιθέσεις επιπέδου εφαρμογών
- Αναγνώριση και επιθέσεις επιπέδου μεταφοράς
- Αναγνώριση και επιθέσεις επιπέδου δικτύου
- Μη αναμενόμενες υπηρεσίες εφαρμογών
- Παραβιάσεις πολιτικής

Επιθέσις κατάλληλες για  
ανίχνευση ανωμαλιών

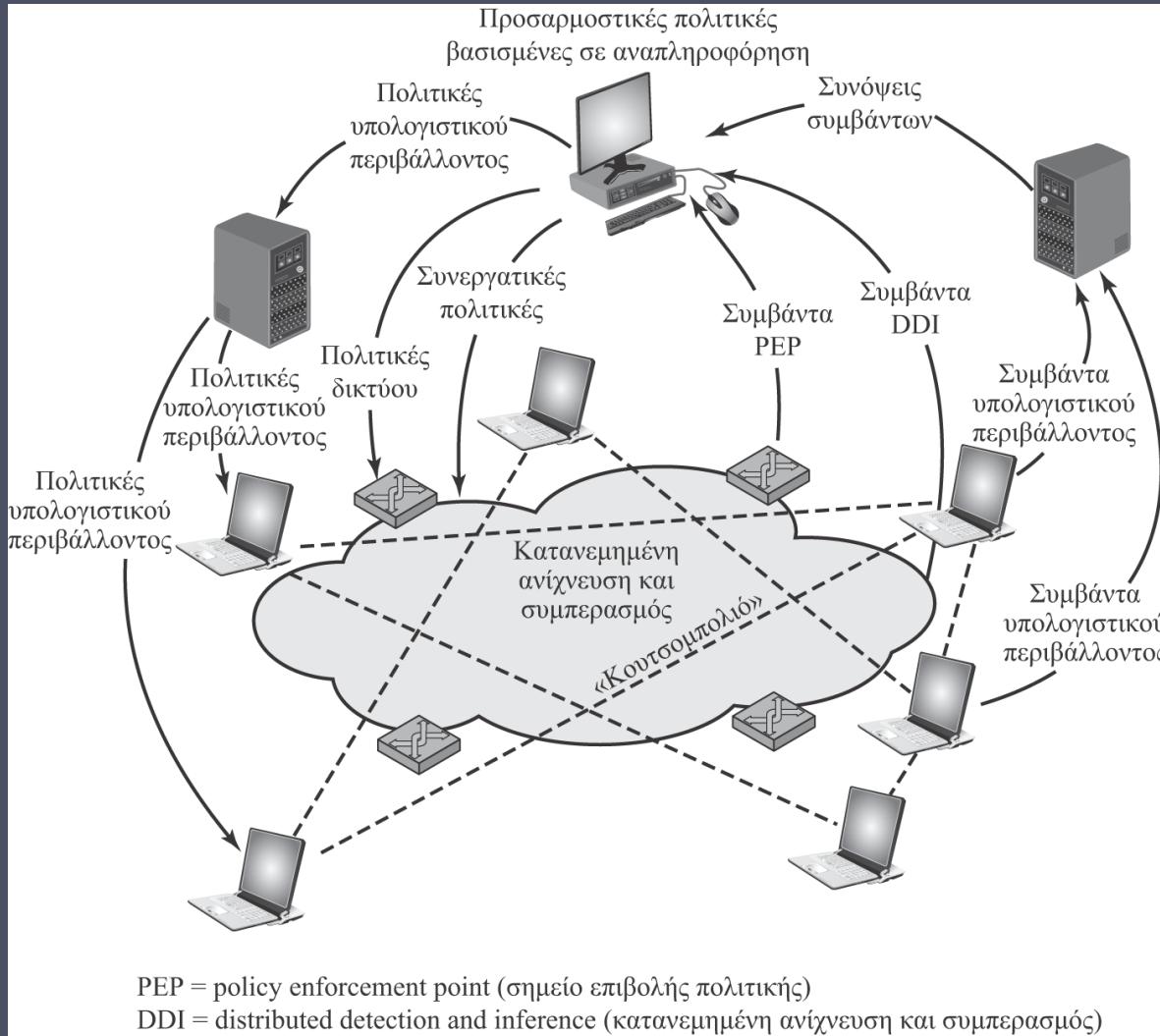
- Επιθέσεις άρνησης εξυπηρέτησης (DoS)
- Σάρωση
- Σκουλήκια

# Καταστασιακή ανάλυση πρωτοκόλλων (SPA)

- Υποσύνολο της ανίχνευσης ανωμαλιών, το οποίο συγκρίνει την παρατηρούμενη κυκλοφορία του δικτύου με προκαθορισμένα, οικουμενικά προφίλ αβλαβούς κυκλοφορίας πρωτοκόλλων τα οποία παρέχονται από τους κατασκευαστές
  - Αυτό το χαρακτηριστικό διαφοροποιεί τη συγκεκριμένη μέθοδο από τεχνικές ανίχνευσης ανωμαλιών οι οποίες εκπαιδεύονται με προφίλ κυκλοφορίας εξειδικευμένα για κάθε οργανισμό
- Κατανοεί και παρακολουθεί καταστάσεις πρωτοκόλλων δικτύου, μεταφοράς και εφαρμογών ώστε να διασφαλίσει ότι εξελίσσονται κατά τον αναμενόμενο τρόπο
- Ένα βασικό μειονέκτημα είναι η αυξημένη χρήση πόρων που απαιτεί

# Καταγραφή προειδοποίησεων

- Στις τυπικές πληροφορίες τις οποίες καταγράφει ένας αισθητήρας NIDS περιλαμβάνονται τα εξής:
  - Χρονοσφραγίδα
  - Αναγνωριστικό σύνδεσης ή συνόδου
  - Τύπος συμβάντος ή προειδοποίησης
  - Χαρακτηρισμός
  - Πρωτόκολλα επιπέδου δικτύου, μεταφοράς και εφαρμογών
  - Διεύθυνσεις IP προέλευσης και προορισμού
  - Θύρες TCP ή UDP προέλευσης ή προορισμού, ή τύποι και κωδικοί ICMP
  - Πλήθος των byte που μεταδίδονται μέσω της σύνδεσης
  - Αποκωδικοποιημένα δεδομένα φορτίου (payload), όπως αιτήσεις και απαντήσεις εφαρμογών
  - Πληροφορίες σχετικές με την κατάσταση



Εικόνα 8.6 Γενική αρχιτεκτονική ενός συστήματος αυτόνομης εταιρικής ασφάλειας

# Ομάδας Εργασίας Ανίχνευσης Εισβολών της IETF

- Ο σκοπός της είναι να ορίζει μορφές δεδομένων και διαδικασίες ανταλλαγής για την κοινή χρήση πληροφοριών μεταξύ συστημάτων ανίχνευσης και αντιμετώπισης εισβολών, καθώς και συστημάτων διαχείρισης τα οποία ενδέχεται να πρέπει να αλληλεπιδράσουν με αυτά
- Το 2007 η ομάδα εργασίας εξέδωσε τις ακόλουθες Αιτήσεις για σχόλια (RFC):

## Απαιτήσεις ανταλλαγής μηνυμάτων ανίχνευσης εισβολών (RFC 4766)

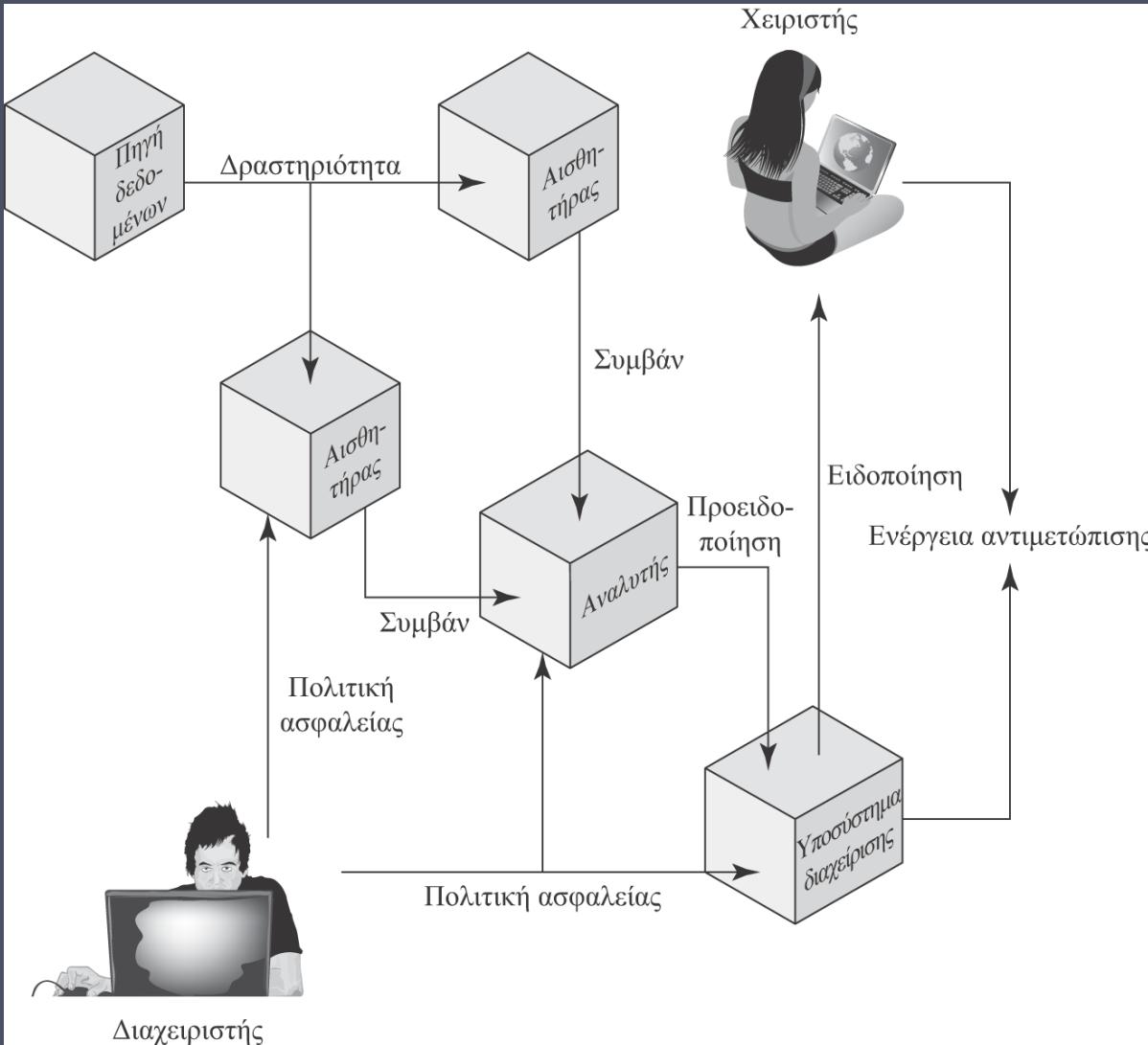
- Ορίζει απαιτήσεις για τη Μορφή Ανταλλαγής Μηνυμάτων Ανίχνευσης Εισβολών (Intrusion Detection Message Exchange Format, IDMEF)
- Επίσης καθορίζει απαιτήσεις για ένα πρωτόκολλο επικοινωνίας σχετικό με τη μετάδοση μηνυμάτων IDMEF

## Η μορφή ανταλλαγής μηνυμάτων ανίχνευσης εισβολών (RFC 4765)

- Περιγράφει ένα μοντέλο δεδομένων για την αναπαράσταση πληροφοριών που εξάγονται από συστήματα ανίχνευσης εισβολών, και εξηγεί τη λογική της χρήσης του μοντέλου
- Επίσης παρουσιάζει μια υλοποίηση του μοντέλου δεδομένων με την Επεκτάσιμη Γλώσσα Σήμανσης (Extensible Markup Language, XML), αναπτύσσει έναν Όρισμό Τύπου Εγγράφου (Document Type Definition, DTD) σε XML, και παραθέτει διάφορα παραδείγματα

## Το πρωτόκολλο ανταλλαγής ανίχνευσης εισβολών (RFC 4767)

- Περιγράφει το Πρωτόκολλο Ανταλλαγής Ανίχνευσης Εισβολών (Intrusion Detection Exchange Protocol, IDXP), ένα πρωτόκολλο επιπέδου εφαρμογών για την ανταλλαγή δεδομένων μεταξύ οντοτήτων ανίχνευσης εισβολών
- Το IDXP υποστηρίζει την αμοιβαία πιστοποίηση ταυτότητας, την ακεραιότητα και την εμπιστευτικότητα μέσω ενός συνδεσμικού πρωτοκόλλου

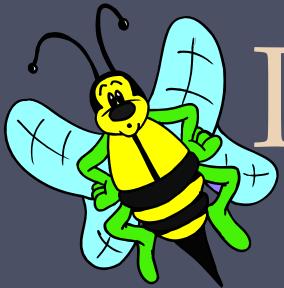


Εικόνα 8.7 Μοντέλο για ανταλλαγή μηνυμάτων ανίχνευσης εισβολών

# Παγίδες εισβολών



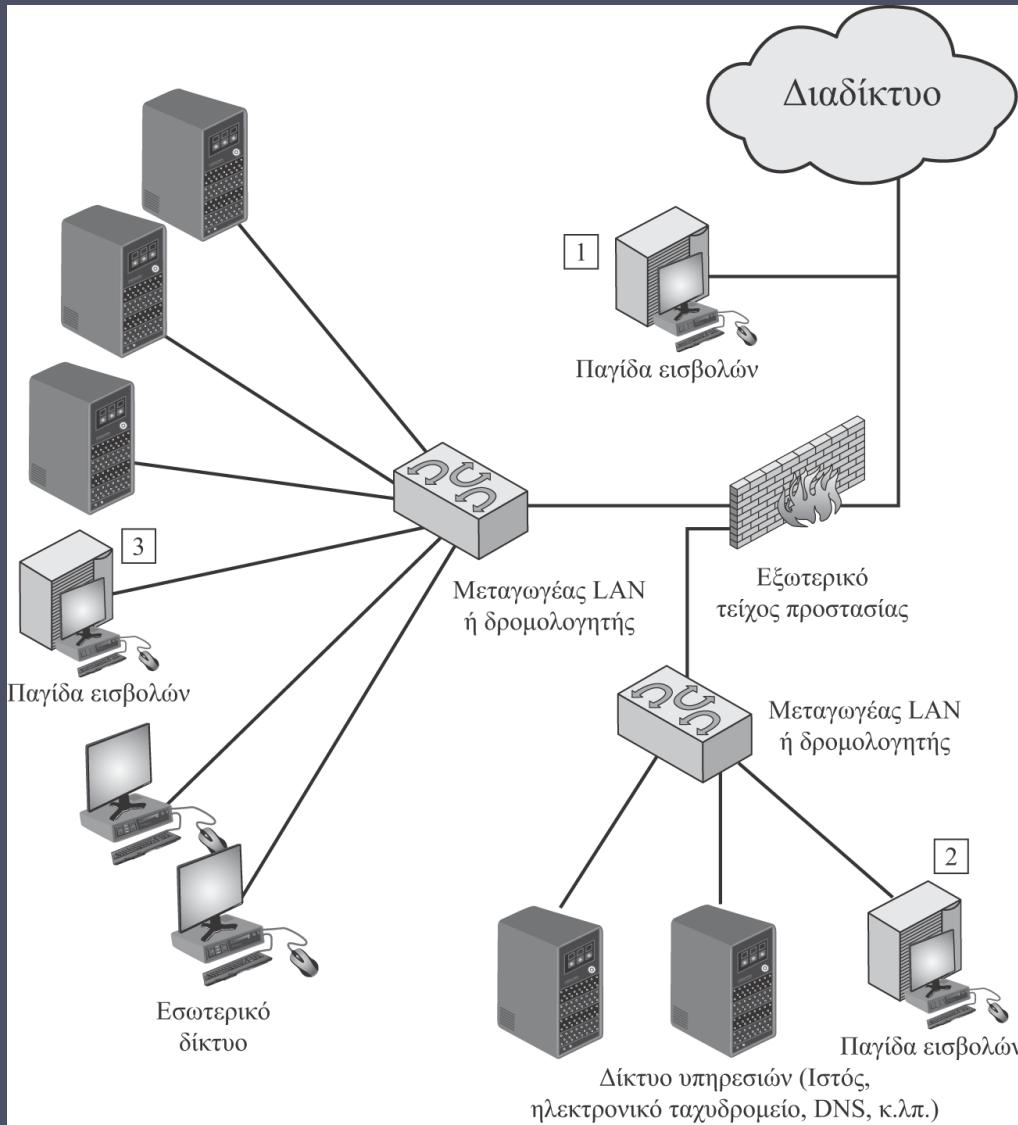
- Συστήματα-δολώματα σχεδιασμένα
  - Να παρασύρουν τους επιτιθέμενους μακριά από κρίσιμα συστήματα
  - Να συλλέγουν πληροφορίες για τη δραστηριότητα του επιτιθέμενου
  - Να παροτρύνουν τον επιτιθέμενο να παραμείνει στο σύστημα για αρκετό χρονικό διάστημα, δίνοντας έτσι τη δυνατότητα στους διαχειριστές να αντιδράσουν εγκαίρως
- Τα συστήματα αυτά είναι γεμάτα με πλαστές πληροφορίες τις οποίες δεν θα προσπέλαζε ένας έγκυρος χρήστης του συστήματος
- Πόροι χωρίς παραγωγική αξία
  - Επομένως, οποιαδήποτε εισερχόμενη επικοινωνία είναι πιθανόν μια απόπειρα ανίχνευσης, σάρωσης, ή επίθεσης
  - Αν παρατηρηθεί εξερχόμενη επικοινωνία από μια παγίδα εισβολών, τότε το σύστημα έχει μάλλον εκτεθεί



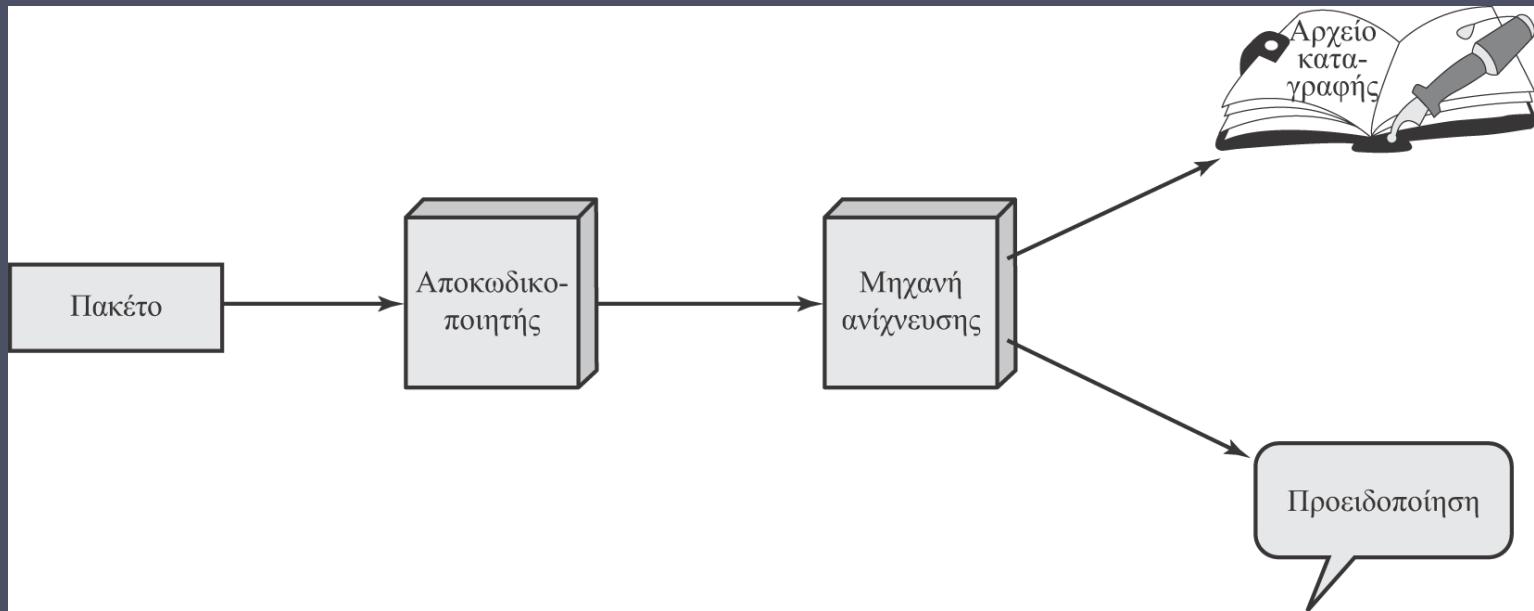
# Παγίδες εισβολών – Ταξινόμηση



- Παγίδα εισβολών χαμηλής αλληλεπίδρασης
  - Αποτελείται από ένα πακέτο λογισμικού το οποίο εξομοιώνει συγκεκριμένες υπηρεσίες ή συστήματα ΙΤ με αρκετά πειστικό τρόπο ώστε να παρέχει μια ρεαλιστική αρχική αλληλεπίδραση, χωρίς όμως να εκτελεί την πλήρη έκδοση αυτών των υπηρεσιών ή συστημάτων
  - Παρέχει λιγότερο ρεαλιστικό στόχο
  - Είναι συχνά αρκετή, όταν χρησιμοποιείται ως υπομονάδα ενός κατανεμημένου συστήματος IDS, ώστε να προειδοποιεί για επικείμενες επιθέσεις
- Παγίδα εισβολών υψηλής αλληλεπίδρασης
  - Πραγματικό σύστημα με πλήρες λειτουργικό σύστημα, υπηρεσίες και εφαρμογές, που έχουν εγκατασταθεί και χρησιμοποιούνται σε σημεία στα οποία μπορούν να προσπελαστούν από επιτιθέμενους
  - Αποτελεί πιο ρεαλιστικό στόχο, ο οποίος μπορεί να κρατήσει έναν επιτιθέμενο απασχολημένο για μεγαλύτερο χρονικό διάστημα
  - Ωστόσο απαιτεί σημαντικά περισσότερους πόρους
  - Αν παραβιαστεί, θα μπορούσε να χρησιμοποιηθεί ως αφετηρία για επιθέσεις εναντίον άλλων συστημάτων



Εικόνα 8.8 Παράδειγμα τοποθέτησης παγίδων εισβολών



Εικόνα 8.9 Αρχιτεκτονική του Snort

Ενέργεια	Πρωτόκολλο	Διεύθυνση IP προέλευσης	Θύρα προέλευσης	Κατεύθυνση	Διεύθυνση IP προορισμού	Θύρα προορισμού
(α) Κεφαλίδα κανόνα						
Λέξη-κλειδί επιλογής	Ορίσματα επιλογής	...				
(β) Επιλογές						

Εικόνα 8.10 Μορφές κανόνων του Snort

# Πίνακας 8.3

## Ενέργειες κανόνων του Snort

Ενέργεια	Περιγραφή
alert	Παράγει μια προειδοποίηση με χρήση της επιλεγμένης μεθόδου και στη συνέχεια καταγράφει το πακέτο.
log	Καταγράφει το πακέτο.
pass	Αγνοεί το πακέτο.
activate	Προειδοποιεί και κατόπιν ενεργοποιεί κάποιον άλλο δυναμικό κανόνα.
dynamic	Παραμένει σε αδράνεια μέχρι να ενεργοποιηθεί από κάποιον κανόνα, και έπειτα λειτουργεί ως κανόνας καταγραφής.
drop	Αναγκάζει το πρόγραμμα iptables να απορρίψει το πακέτο, και καταγράφει το πακέτο.
reject	Αναγκάζει το πρόγραμμα iptables να απορρίψει το πακέτο, και καταγράφει το πακέτο. Έπειτα, αν το πρωτόκολλο είναι το TCP, στέλνει εντολή επαναφοράς (reset) του TCP· αν το πρωτόκολλο είναι το ICMP, στέλνει ένα μήνυμα απροσπέλαστης θύρας (port unreachable) του ICMP.
sdrop	Αναγκάζει το πρόγραμμα iptables να απορρίψει το πακέτο, αλλά δεν το καταγράφει.

(Ο πίνακας βρίσκεται στη σελ. 332 του βιβλίου.)

### μεταδεδομένα

<b>msg</b>	Ορίζει το μήνυμα που πρέπει να αποσταλεί όταν ένα πακέτο προκαλεί ένα συμβάν.
<b>reference</b>	Ορίζει έναν σύνδεσμο προς κάποιο εξωτερικό σύστημα αναγνώρισης επιθέσεων, το οποίο παρέχει πρόσθετες πληροφορίες.
<b>classtype</b>	Υποδεικνύει τον τύπο της επίθεσης που επιχείρησε να πραγματοποιήσει το πακέτο.
<b>φορτίο</b>	
<b>content</b>	Επιτρέπει στο Snort να εκτελεί αναζήτηση με διάκριση πεζών-κεφαλαίων για συγκεκριμένο περιεχόμενο (σε μορφή κειμένου ή/και δυαδική μορφή) στο φορτίο του πακέτου.
<b>depth</b>	Καθορίζει μέχρι ποιο σημείο του πακέτου πρέπει να εκτελέσει το Snort την αναζήτηση για τη συγκεκριμένη ακολουθία. Η επιλογή depth (βάθος) λειτουργεί ως παράμετρος για την προηγούμενη λέξη-κλειδί της επιλογής content (περιεχόμενο) στον κανόνα.
<b>offset</b>	Καθορίζει από ποιο σημείο του πακέτου πρέπει να ξεκινήσει η αναζήτηση για μια ακολουθία. Η επιλογή offset (σχετική απόσταση) λειτουργεί ως παράμετρος για την προηγούμενη λέξη-κλειδί της επιλογής content στον κανόνα.
<b>nocase</b>	Το Snort πρέπει να αναζητήσει τη συγκεκριμένη ακολουθία αγνοώντας τη διάκριση πεζών-κεφαλαίων. Η επιλογή nocase λειτουργεί ως παράμετρος για την προηγούμενη λέξη-κλειδί της επιλογής content στον κανόνα.
<b>δεδομένα εκτός φορτίου</b>	
<b>ttl</b>	Ελέγχει την τιμή του πεδίου time-to-live (χρόνος ζωής) του IP. Η επιλογή αυτή προοριζόταν για χρήση στην ανίχνευση αποπειρών με το πρόγραμμα traceroute.
<b>id</b>	Ελέγχει το πεδίο ID του IP για συγκεκριμένη τιμή. Μερικά εργαλεία (προγράμματα εκμετάλλευσης ευπαθειών, προγράμματα σάρωσης, και άλλα περίεργα προγράμματα) ορίζουν αυτό το πεδίο συγκεκριμένα για διάφορους σκοπούς: για παράδειγμα, η τιμή 31337 τυγχάνει μεγάλης απήχησης από κάποιους χάκερ.
<b>dsizze</b>	Ελέγχει το μέγεθος του φορτίου του πακέτου. Μπορεί να χρησιμοποιηθεί για τον έλεγχο πακέτων με υπέρμετρο μέγεθος. Σε πολλές περιπτώσεις, είναι χρήσιμο για την ανίχνευση υπερχειλίσεων περιοχών προσωρινής αποθήκευσης.
<b>flags</b>	Ελέγχει τις σημαίες του TCP για συγκεκριμένες ρυθμίσεις.
<b>seq</b>	Ψάχνει για συγκεκριμένο αριθμό ακολουθίας στην κεφαλίδα του TCP.
<b>icmp-id</b>	Ελέγχει το πεδίο ID του ICMP για συγκεκριμένη τιμή. Αυτό μπορεί να αποδειχθεί χρήσιμο επειδή μερικά προγράμματα συγκεκαλυμμένων καναλιών χρησιμοποιούν στατικά πεδία ICMP όταν επικοινωνούν. Η συγκεκριμένη επιλογή αναπτύχθηκε για την ανίχνευση του πράκτορα stacheldraht σε επιθέσεις DDoS.
<b>μετα-ανίχνευση</b>	
<b>logto</b>	Καταγράφει πακέτα που ταιριάζουν με τον κανόνα στο αρχείο με το καθορισμένο όνομα.
<b>session</b>	Εξάγει δεδομένα χρηστών από συνόδους TCP. Υπάρχουν πολλές περιπτώσεις στις οποίες είναι πολύ χρήσιμο να βλέπει κανείς τι πληκτρολογούν οι χρήστες σε συνόδους telnet, rlogin, ftp, ή ακόμα και του Ιστού.

# Πίνακας 8.4

## Παραδείγματα επιλογών για κανόνες του Snort

(Ο πίνακας βρίσκεται στη σελ. 333 του βιβλίου.)

# Σύνοψη

- Εισβολείς
  - Συμπεριφορά εισβολέων
- Ανίχνευση εισβολών
  - Βασικές αρχές
  - Η πλάνη του βασικού ποσοστού
  - Απαιτήσεις
- Τεχνικές ανάλυσης
  - Ανίχνευση ανωμαλιών
  - Ανίχνευση υπογραφών ή ευρετική ανίχνευση
- Κατανεμημένη ή υβριδική ανίχνευση εισβολών
- Μορφή ανταλλαγής ανίχνευσης εισβολών
- Παγίδες εισβολών
- Ανίχνευση εισβολών βασισμένη σε υπολογιστές υπηρεσίας
  - Πηγές δεδομένων και αισθητήρες
  - HIDS βασισμένα σε ανωμαλίες
  - HIDS βασισμένα σε υπογραφές ή ευρετικά κριτήρια
  - Κατανεμημένα HIDS
- Ανίχνευση εισβολών βασισμένη σε δίκτυα
  - Τύποι δικτυακών αισθητήρων
  - Χρήση αισθητήρων NIDS
  - Τεχνικές ανίχνευσης εισβολών
  - Καταγραφή προειδοποιήσεων
- Παράδειγμα συστήματος: Snort
  - Αρχιτεκτονική του Snort
  - Κανόνες του Snort

