Cryptography and Network Security Chapter 20

Fifth Edition

by William Stallings

Chapter 20– Intruders

They agreed that Graham should set the test for Charles Mabledene. It was neither more nor less than that Dragon should get Stern's code. If he had the 'in' at Utting which he claimed to have this should be possible, only loyalty to Moscow Centre would prevent it. If he got the key to the code he would prove his loyalty to London Central beyond a doubt.

—*Talking to Strange Men,* Ruth Rendell

Εισβολεις (Intruders)

- Ενα σημαντικο θεμα για τα δικτυακα συστηματα ειναι η εχθρικη ή ανεπιθυμητη προσβαση
- Ειτε μεσω δικτυου, ειτε τοπικα
- Μπορουμε να καταταξουμε τους Intruders στις εξης κατηγοριες:
  - **Μεταμφιεσμενος (Masquerader):** Ενα άτομο που δεν ειναι εξουσιοδοτημενο να χρησιμοποιησει τον υπολογιστη και διαπερνα τον ελεγχο προσβασης του συστηματος για να εκμεταλλευτει το λογαρισμο ενος νομιμου χρηστη. Είναι συνηθως outsider.
  - **Παρανομος (Misfeasor):** Ενας νομιμος χρηστης που προσπελαυνει δεδομενα, προγραμματα ή πορους που δεν ειναι εξουσιοδοτημενος να προσπελασει ή ειναι εξουσιοδοτημενος για αυτην την προσβαση, αλλα καταχραται τα προνομια του. Ειναι συνηθως insider.
  - **Κρυφος Χρηστης (Clandestine user):** Ενα ατομο που παιρνει ελεγχο του συστηματος και τον χρησιμοποιει για να αποφυγει ή να καταστειλει τον ελεγχο προσβασης. Μπορει να ειναι είτε insider, είτε outsider.

Intruders

- Η σοβαροτητα της απειλης απο εναν intruder ποικιλει.
  - Benign (καλοηθης): εξερευνα, ωστοσο ξοδευει πορους του συστηματος
  - Serious (σοβαρη): προσπεκλαυνει ή/και τροποποιει δεδομενα, διαταρασσουν το συστημα
- Η υπαρξη των intruders έχει οδηγησει στην αναπτυξη των CERTs (Computer Emergency Response Teams)
- Οι τεχνικες των intruder & και τα προτυπα συμπεριφορας τους σταθερα αλλαζουν, εχουν ομως καποια κοινα χαρακτηριστικα

Παραδείγματα Εισβολης (Examples of Intrusion)

- remote root compromise
- web server defacement
- guessing / cracking passwords
- copying viewing sensitive data / databases
- running a packet sniffer
- distributing pirated software
- using an unsecured modem to access net
- impersonating a user to reset password
- using an unattended workstation

Hackers

- υποκινούνται από συγκίνηση της πρόσβασης και του κυρους
  - Στην κοινοτητα του hacking επικρατει απολυτη αξιοκρατια
  - Το κυρος καθοριζεται απο το επιπεδο ικανοτητας του καθενος
- Καλοηθεις intruders μπορει να ειναι ανεκτοι
  - Καταναλωνουν πορους και μπορει να υποβαθμισουν την συμπερφορα του συστηματος
  - Δεν μπορουμε να ξερουμε απο την αρχη αν ειναι καλοηθεις ή κακοηθεις
- Τα IDS / IPS / VPNs μπορουν να βοηθησουν
- Η επαγρυπνηση που πρεπει να υπαρχει κατα παρεισακτων οδηγησε στην αναπτυξη των CERTs
  - Συλλεγουν και διαδιδουν πληροφορια τρωσιμοτητας του σθυστηματος

Παραδείγματα συμπεριφορας Hacker

1. Επιλέγει το στοχο χρησιμοποιωντας IP lookup tools
2. Χαρτογραφει το δικτυο αναζητωντας προσβασιμες υπηρεσιες
3. Προσδιοριζει δυνητικα τρωσιμες υπηρεσιες
4. Σαρωνει ή «μαντευει» τα passwords
5. Εγκαθιστα remote administration tool
6. Περιμενει τον Admin να κανει log on και υποκλεπτει το password του
7. Χρησιμοποιει το password για να προσπελασει το δικτυο

Criminal Enterprise

- Οργανωμενες ομαδες απο hackers έιναι πλεον μια σημαντικη απειλη
  - Βρισκονται σε εταιριες,κυβερνητικους οργανισμους και σε συμμοριες
  - Ειναι συνηθως νεοι
  - Συχνα ειναι Ανατολικοευρωπαιοι ή Ρωσοι
  - Συχνα στοχευουν στους αριθμους πιστωτικων καρτων σε servers ηλεκτρονικου εμποριου
- Οι εγκληματιες hackers συνηθως εχουν συγκεκριμενους στοχους
- Απο τη στιγμη που θα διεισδυσουν ενεργουν γρηγορα και φευγουν
- Τα συστηματα IDS / IPS βοηθουν, αλλα δεν ειναι παντα αποτελεσματικα
- Τα ευαισθητα δεδομενα χρειαζονται ισχυρη προστασια

Criminal Enterprise Behavior

1. Ενεργουν γρηγορα και με ακριβεια για να καταστησουν δυσκολοτερη την ανιχνευση τους
2. Διευσδυουν στην περιμετρο μεσω τρωτων ports
3. Χρησιμοποιουν trojan horses (hidden software) για να αφησουν back doors ωστε να μπορουν να ξαναμπουν
4. Χρησιμοποιουν sniffers για να υποκλεψουν τα passwords
5. Δεν παραμενουν μεχρι να εντοπιστουν
6. Κανουν λιγα η καθολου λαθη

Επιθεσεις απο Insiders

- Ειναι απο τις πιο δυσκολες στο να ανιχνευτουν και να προληφθουν
- Οι υπαλληλοι εχουν προσβαση και γνωση των συστηματων
- Μπορει να εχουν ως κινητρο την εκδικηση ή την υποκλοπη στοιχειων
  - Οταν τερματιζεται η εργασιακη σχεση
  - Ή για να υποκλεψουν αρχεια πελατων οταν μετακινουνται σε ανταγωνιστικη εταιρια
- Τα IDS / IPS μπορει να βοηθησουν αλλα επισης χρειαζονται:
  - Να υιοθετηθει η αρχη των Ελαχιστων Προνομιων (least privilege), logs παρακολουθησης, ισχυρη πιστοποιηση αυθεντικοτητας, διαδικασιες τερματισμου για να μπλοκαρουν την προσβαση και mirror data

Παραδειγμα συμπεριφορας Insider

1. Δημιουργουν λογαριασμους δικτυου για τους εαυτους τους και τους φιλους τους
2. Προσπελαυνουν λογαριασμους και εφαρμογες που κανονικα δεν θα χρησιμοποιουσαν για τις συνηθεις δουλειες τους
3. Στελνουν e-mail σε πρωην και μελλοντικους εργοδοτες
4. Επιδιδονται κρυφα σε instant-messaging chats
5. Επισκεπτονται web sites που απευθυνονται σε δυσαρεστημενους υπαλληλους
6. Εκτελουν μεγαλα downloads και αντιγραφες αρχειων
7. Προσπελαυνουν το δικτυο κατα τη διαρκεια ωρων μη-αιχμης.

Τεχνικες Εισβολης

- Αποσκοπουν στο να αποκτησουν προσβαση ή/και να αυξησουν τα προνομια σε ενα συστημα
- Συχνα χρησιμοποιουν τα τρωτα σημεια του συστηματος και του λογισμικου
- Ο βασικος στοχος ειναι συχνα να υποκλεψουν τα passwords
  - και στη συνεχεια να ασκησουν τα δικαιωματα του ιδιοκτητη τους
- Βασικη μεθοδογια επιθεσης
  - Προσκτηση στοχων και ληψη πληροφοριων
  - Αρχικη προσβαση
  - Αυξηση των προνομιων
  - Καλυψη Ιχνων

«Μαντεμα» του Password (Password Guessing)

- Μια απο τις πιο συχνες επιθεσεις
- Ο επιτιθεμενος γνωριζει ενα login (απο email/web page, κλπ)
- Και στη συνεχεια προσπαθει να «μαντεψει» το password για το συγκεκριμενο login
  - defaults, μικρα passwords, κοινες λεξεις
  - πληροφοριες του χρηστη (variations on names, birthday, phone, common words/interests)
  - Εξαντλητικη αναζητηση ολων των δυνατων passwords
- Πολλες φορες χρησιμοποιουνται κλεμμενα password files
- Η επιτυχια εξαρταται απο το password που θα επιλεγει απο το χρηστη
- Μελετες δειχνουν οτι πολλοι χρηστες επιλεγουν ευκολα passwords

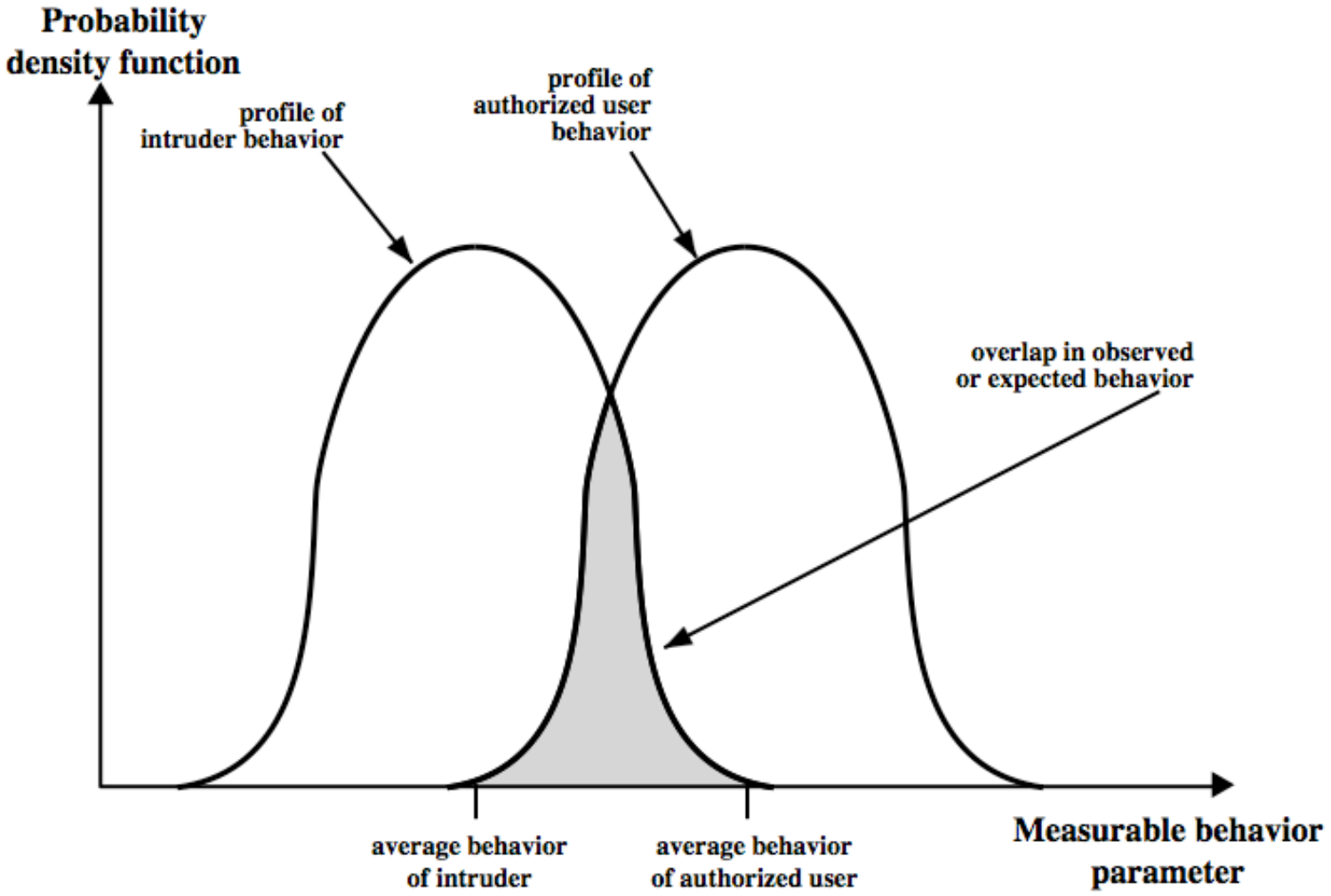
Υποκλοπη του Password (Password Capture)

- Ενα άλλο είδος επίθεσης βασίζεται στην υποκλοπη του password. Η υποκλοπη γίνεται με τους εξης τροπους:
  - Παρακολουθηση καποιου την ωρα που πληκτρολογει το password του
  - Χρησιμοποιηση ενος trojan horse για τη συλλογη του password
  - Παρακολουθηση ενος μη-ασφαλους network login
    - eg. telnet, FTP, web, email
  - Εξαγωγη καταγεγραμμενης πληροφοριας μετα απο επιτυχημενο login (web history/cache, last number dialed etc)
- Χρησιμοποιωντας το υποκλαπεν password μπορουν να παραστησουν καποιον αλλον χρηστη
- Οι χρηστες πρεπει να εκπαιδευονται για να παιρνουν τα καταλληλα μετρα ωστε να αποφευγουν την υποκλοπη του password τους

Ανιχνευση Εισβολής (Intrusion Detection)

- Ειναι βεβαιο οτι θα υπαρχουν αποτυχιες τους συστηματος ασφαλειας
- Συνεπως, χρειαζεται να ανιχνευονται οι εισβολες, ετσι ωστε:
  - Να την ανιχνευτουν γρηγορα και να να μπλοκαριστουν.
  - Να υπαρξει αποτροπή τους
  - Να συλλεγουν πληροφοριες που θα χρησιμοποιηθουν για τη βελτίωση της ασφάλειας
- Υποθετουμε οτι ενας εισβολεας θα συμπεριφερθει διαφορετικα απ’οτι ενας νομιμος χρηστης
  - Αλλα η διακριση μεταξυ των δυο δεν ειναι ακριβης

Intrusion Detection



Προσεγγισεις της Ανιχνευσης Εισβολης

- **Ανιχνευση στατιστικων ανωμαλιων (statistical anomaly detection):** Συλλέγονται δεδομενα για τη συμπεριφορα των νομιμων χρηστων σε μια χρονικη περιοδο. Στη συνεχεια εφαρμοζονται στατιστικοι ελεγχοι, στην παρατηρουμενη συμπεριφορα, ωστε να αξιολογηθει αν ειναι ή οχι συμπεριφορα νομιμου χρηστη.

  α) Ανιχνευση βασισμενη σε Κατωφλια (Threshold detection): Οριζονται κατωφλια, αναξαρτητως χρηστη για τη συχνοτητα εμφανισης διαφορων γεγονοτων. Οταν το κατωφλι ξεπεραστει, τοτε ανιχνευεται εισβολη.

  β) Ανιχνευση βασισμενη σε Προφιλ (Profile based): Αναπτυσσεται για καθε χρηστη ενα προφιλ δραστηριοτητας. Ετσι ανιχνευονται αλλαγες στην συμπεριφορα του καθε account.

- **Ανιχνευση βασισμενη σε κανονες (rule-based detection):** Χρησιμοποιουνται κανονες, προκειμενου να ανιχνευτει αν μια συμπεριφορα ειναι νομιμου χρηστη ή οχι.

  α) Ανιχνευση Ανωμαλιων (Anomaly detection): Αναπτυσσονται κανονες για να ανιχνευτει αποκλιση απο τα προηγουμενα προτυπα χρησης.

  β) Αναγνωρθση Διεισδυσης (Penetration identification): Η προσεγγιση αυτη βασιζεται στη χρηση εμπειρου συστηματος (expert system) που αναζητα υποπτη συμπεριφορα.

Εγγραφες Παρακολουθησης (Audit Records)

- Ειναι ενα βασικο εργαλειο για ανιχνευση εισβολης
- Εγγενεις εγγραφες παρακολουθησης (native audit records)
  - Μερος ολων των πολυχρηστικων λειτουργικων συστηματων
  - Ειναι ηδη παροντα και ετοιμα για χρηση
  - Μπορει ομως να μην υπαρχει η πληροφορια που απαιτειται ή να μην ειναι στην επιθυμητη μορφη
- Εγγραφες παρακολουθησης ειδικα για την ανιχνευση (detection-specific audit records)
  - Δημιουργουνται ειδικα για να συλλεγουν επιθυμητη πληροφορια
  - Προσθετουν επιπλεον overhead στο συστημα

Ανιχνευση Στατιστικων Ανωμαλιων

- **Ανιχνευση βασισμενη σε Κατωφλια (Threshold detection)**
  - Μετρα τις εμφανισεις ενος συγκεκριμενου γεγονοτος στο χρονο
  - Αν υπερβαινουν μια συγκεκριμενη τιμη τοτε υποθετουμε οτι προκειται για εισβολη
  - Απο μονη της ειναι μια καπως «χοντροκομμενη» και αναποτελεσματικη μεθοδος ανιχνευσης
- **Ανιχνευση βασισμενη σε Προφιλ (Profile based):**
  - Χαρακτηριζει την προηγουμενη συμπεριφορα των χρηστων
  - Ανιχνευει αποκλισεις απο αυτην
  - Το προφιλ του χρηστη ειναι συνηθως πολυπαραμετρικο

Αναλυση εγγραφων παρακολουθησης (Audit Record Analysis)

- Ειναι η βαση των στατιστικων προσεγγισεων
- Αναλυονται οι εγγραφες για να παρουμε μετρικες ως προς το χρονο
  - counter, gauge, interval timer, resource use
- Χρησιμοποιουμε διαφορα tests πανω σε αυτες τις μετρικες για να προσδιορισουμε αν η τρεχουσα συμπεριφορα ειναι αποδεκτη
  - mean & standard deviation, multivariate, markov process, time series, operational
- Το κυριο πλεονεκτημα ειναι οτι δε χρησιμοποιειται προτερη γνωση

Ανιχνευση Εισβολων Βασισμενη σε Κανονες (Rule-Based Intrusion Detection)

- Παρατηρουνται τα συμβαντα στο συτημα και στη συνεχεια εφαρμοζονται κανονες για να αποφασιστει αν η δραστηριοτητα αυτη ειναι υποπτη ή όχι.
- Ανιχνευση Ανωμαλιων Βασισμενη σε Κανονες (rule-based anomaly detection)
  - Αναλυση ιστορικων εγγραφων παρακολουθησης για να προσδιοριστουν τα προτυπα χρησης και να δημιουργησουν αυτοματα κανονες για αυτα
  - Στη συνεχεια παρατηρειται η τρεχουσα συμπεριφορα και ελεγχεται συμφωνα με κανονες ωστε να δουμε αν τους πληρει
  - Οπως και η στατιστικη ανιχνευση πληροφοριας, δε χρειαζεται προτερη γνωση των αδυναμιων της ασφαλειας του συστηματος

Ανιχνευση Εισβολων Βασισμενη σε Κανονες

- Αναγνωριση διεισδυσης βασισμενη σε κανονες
  - Χρησιμοποιει τεχνολογια εμπειρων συστηματων
  - Οι κανονες αναγνωριζουν γνωστες μορφες διεισδυσης, προτυπα αδυναμιων ασφαλειας ή υποπτη συμπεριφορα
  - Συγκρινονται οι εγγραφες παρακολουθησης με τους κανονες
  - Οι κανονες ειναι συνηθως ειδικοι για ενα συγκεκριμενο υπολογιστη και ενα συγκεκριμενο λειτουργικο συστημα
  - Δημιουργουνται απο ειδικους που αξιοποιουν τη γνωση των διαχειριστων ασφαλειας συζητωντας μαζι τους

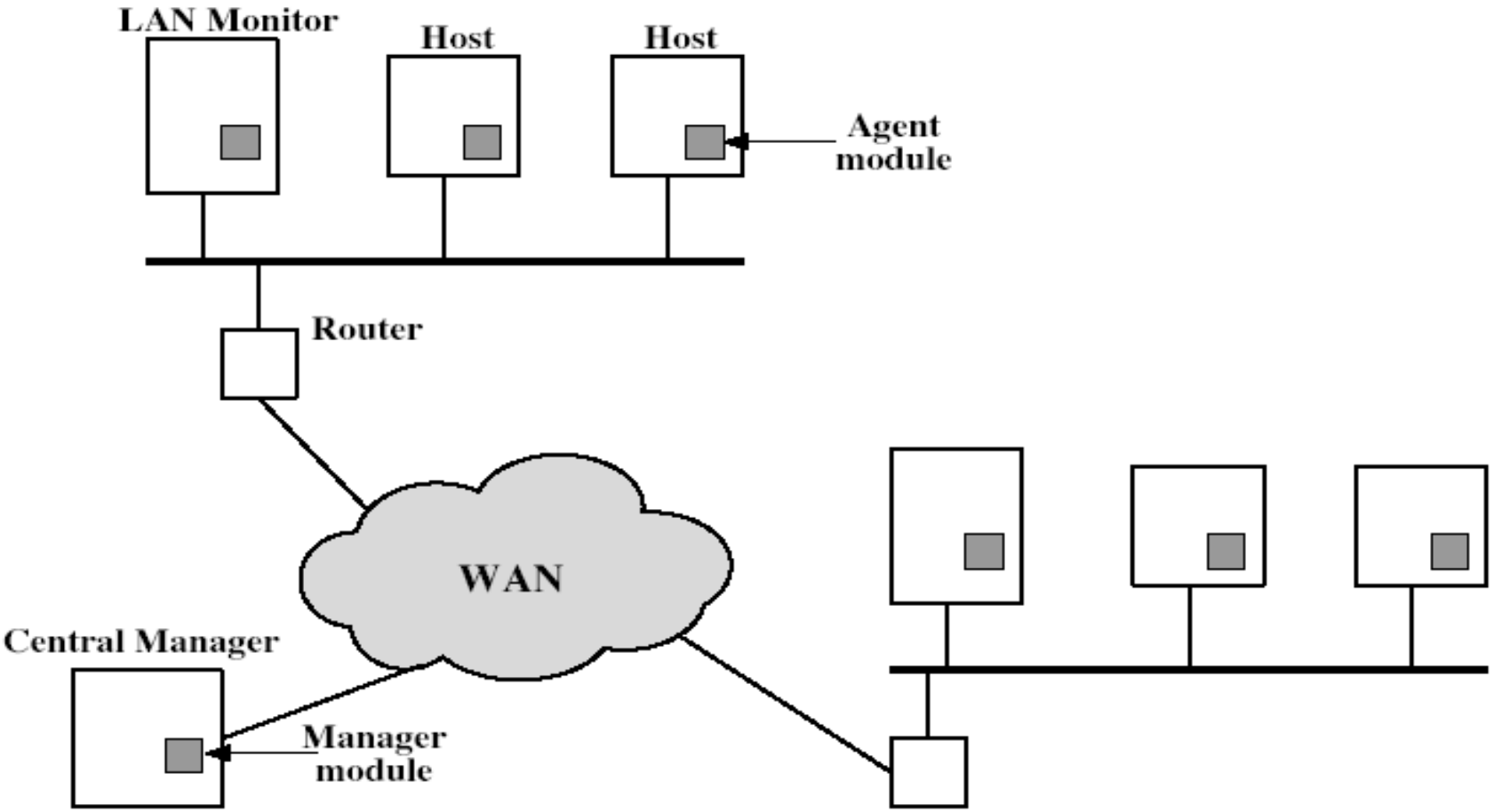
Πλανη του Βασικου Ποσοστου

- Πρακτικα ενα συστημα ανιχνευσης εισβολης χρειαζεται να ανιχνευει ενα μεγαλο ποσοστο των εισβολων με οσο το δυνατο λιγοτερους λανθασμενους συναγερμους (false alarms)
  - Αν ανιχνευονται πολυ λιγες εισβολες τοτε υπαρχει προβλημα στην ασφαλεια
  - Αν υπαρχουν πολλοι λαθος συναγερμοι τοτε ειτε οι χρήστες θα αρχισουν να τους αγνοουν, ειτε θα χανεται ασκοπα χρονος για τη διερευνηση τους
- Αυτο ειναι πολυ δυσκολο να γινει
- Τα υπαρχοντα συστηματα δεν το επιτυγχανουν ικανοποιητικα

Κατανεμημενη Ανιχνευση Εισβολης (Distributed Intrusion Detection)

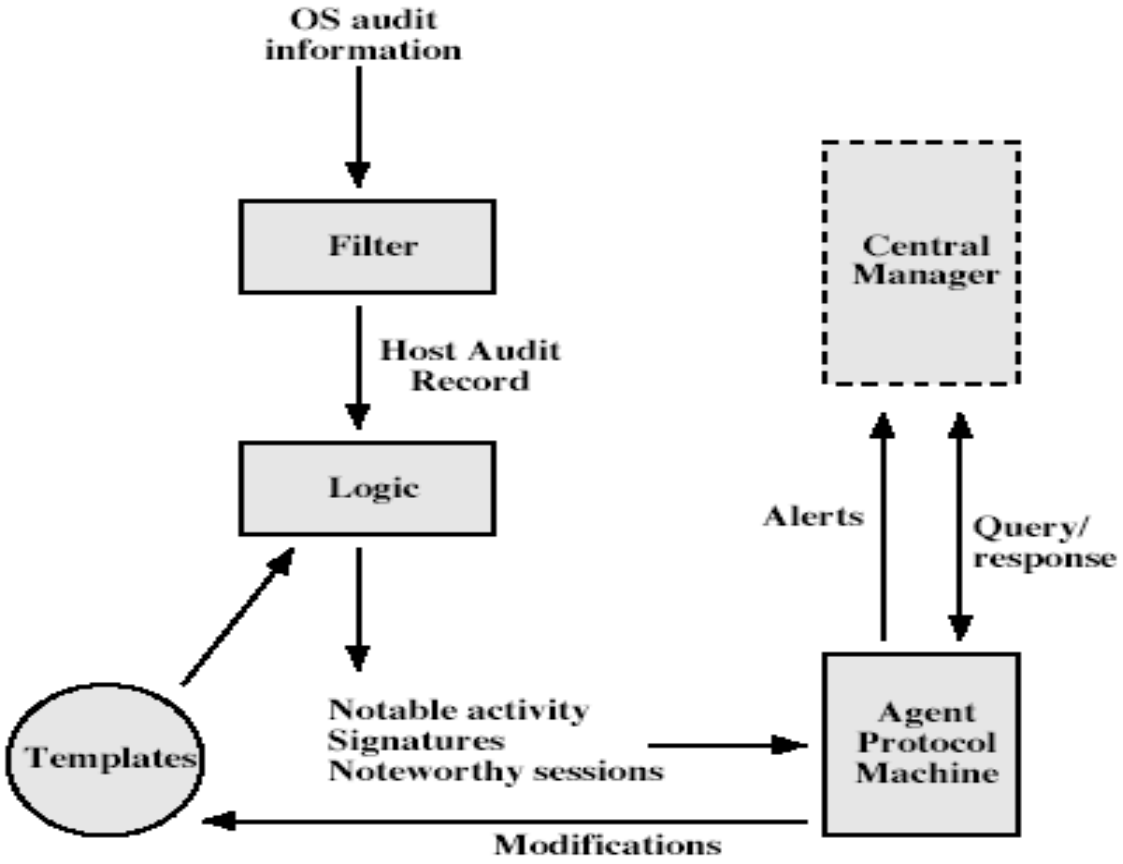
- Μεχρι τωρα η ερευνα στα συστηματα ανιχνευσης εισβολων εστιαζοταν σε αυτονομες εγκαταστασεις ενος μονο συστηματος
- Ωστοσο, συνηθως οι οργανισμοι χρειαζεται να υπερασπιστουν μια κατανεμημενη συλλογη υπολογιστων.
- Ειναι πιο αποτελεσματικο να συνεργαζονται τα συστηματα ανιχνευσης ολων αυτων των κατανεμημενων υπολογιστων
- Σημαντικα Θεματα:
  - Το οτι σε ενα ετερογενες περιβαλλον, οι εγγραφες παρακολουθησης εχουν διαφορετικα format.
  - Η ακεραιοτητα και η εμπιστευτικοτητα των δικτυωμενων δεδομενων
  - Το αν θα επιλεγει κεντρικη ή αποκεντρωμενη αρχιτεκτονικη

Αρχιτεκτονικη για κατανεμημενη ανιχνευση εισβολων



Κατανεμημενη ανιχνευση εισβολων

Αρχιτεκτονικη πρακτορα



Δολώματα (Honeypots)

- Ειναι σχεδιασμενα για να προσελκυουν τους δυνητικα επιτιθεμενους.
  - Μακρυα απο την προσβαση κρισιμων συστηματων
  - Να συλλεγουν πληροφοριες για τις δραστηριοτητες τους
  - Να ενθαρρυνει τους επιτιθεμενους να παραμενουν στο συστημα ωστε να προλαβει ο διαχειριστης να απαντησει στην επιθεση
- Αυτα τα συστηματα ειναι γεματα με κατασκευασμενες πληροφοριες που ειναι φτιαγμενες να μοιαζουν πολυτιμες
- Εφαρμοζονται σε ενα ή σε πολλα δικτυωμενα συστηματα

Διαχειριση Συνθηματικων (Password Management)

- Ειναι η πρωτη γραμμη αμυνας απεναντι στους εισβολεις
- Οι χρηστες προμηθευονται:
  - login – καθοριζει τα προνομια του χρηστη
  - password – για την πιστοποιηση οτι το ατομο που χρησιμοποιησε το login ειναι πραγματι αυτος στον οποιο ανηκει το login
- Τα passwords συνηθως αποθηκευονται κρυπτογραφημενα
  - Το Unix χρησιμοποιει πολλαπλο DES (μια παραλλαγη του)
  - Τα πιο συγχρονα συστηματα χρησιμοποιουν κρυπτογραφικη hash function
- Φυσικα, το αρχειο των συνθηματικων (password file) πρεπει να προστατευεται στο συστημα

Στρατηγικες επιλογης συνθηματικου

- Μπορει να χρησιμοποιηθουν πολιτικες και καλη εκπαιδευση των χρηστων
- Πρεπει να εκπαιδευτουν στην σημαντικοτητα των καλων passwords
- Πρεπει να δινονται οδηγιες για το ποια ειναι καλα passwords
  - Ελαχιστο μηκος (>6)
  - Απαιτειται ενα μειγμα κεφαλαιων και μικρων γραμματων, αριθμων και σημειων στιξης
  - Δεν πρεπει να ειναι λεξεις που υπαρχουν στο λεξικο
- Ειναι ομως πιθανο οι οδηγιες αυτες να αγνοηθουν απο πολλους χρηστες

Παραγομενα απο υπολογιστη συνθηματικα

- Αφηνουμε τον υπολογιστη να δημιουργησει τα passwords
- Αν ειναι τυχαια, ειναι πιθανο να μην μπορουν οι χρηστες να τα απομνημονευσουν. Ετσι θα τα γραψουν σε χαρτι και μπορει να τους τα υποκλεψουν
- Ακομα κι αν μπορουν να προφερθουν δεν μπορουν να απομνημονευτουν
- Η εμπειρια εχει δειξει οτι οι χρηστες δεν τα αποδεχονται
- Το FIPS PUB 181 οριζει μια απο τις πιο καλοσχεδιασμενες γεννητριες συνθηματικων.
  - Περιλαμβανει τοσο περιγραφη, οσο και ενδεικτικο κωδικα.
  - Δημιουργει λεξεις ενωνοντας τυχαιες συλλαβες που μπορουν να προφερθουν

Αντιδραστικος Ελεγχος Συνθηματικων (Reactive Checking)

- Το ιδιο το συστημα εκτελει προγραμμα σπασιματος συνθηματικων για να εντοπισει τα αδυναμα συνθηματικα
- Τα συνθηματικα που σπαζουν απενεργοποιουνται
- Η μεθοδος ειναι εξαιρετικα δαπανηρη σε πορους
- Τα ασχημα επιλεγμενα συνθηματικα ειναι τρωτα, μεχρι να βρεθουν

Προληπτικος Ελεγκτης Συνθηματικων

- Ειναι η πιο πολλα υποσχομενη προσεγγιση για βελτιωση της ασφαλειας των συνθηματικων
- Επιτρεπει στους χρηστες να επιλεξουν το δικο τους συνθηματικο
- Αλλα το συστημα επιβεβαιωνει αν το συνθηματικο που επελεξαν ειναι αποδεκτο
- Το ζητημα με τον προληπτικο ελεγκτη ειναι η ισορροπια μεταξυ της αποδοχης απο τον χρηστη και της ισχυος του συνθηματικου

Συνοψη

- Εξετασαμε:
  - Το προβλημα της εισβολης
  - Την ανιχνευση εισβολης
  - Τη διαχειριση συνθηματικων