# Ασφάλεια με ανοιχτό λογισμικό / φιλοσοφία και εφαρμογές

Μαμαλάκης Γιώργος
Ευστρατίου Παναγιώτης
Καραμήτας Χαρίτων

# Εισαγωγή

- ΕΛΛΑΚ – τί είναι και η φιλοσοφία του
- Σύγκριση ΕΛΛΑΚ και κλειστού λογισμικού
- ΕΛΛΑΚ και ασφάλεια
- Υποδομή του ΤΗΜΜΥ / ασφάλεια

# Τι είναι το ΕΛΛΑΚ ?

- Το ΕΛΛΑΚ είναι λογισμικό το οποίο διανέμεται ελεύθερα από τους κατασκευαστές του προς το κοινό για ελεύθερη χρήση. Παρέχεται στο χρήστη με τον πηγαίο κώδικά του για μελέτη, αντιγραφή, ανάπτυξη και διανομή.

# Φιλοσοφία του ΕΛΛΑΚ

- Η Ελευθερία να χρησιμοποίειται το πρόγραμμα για οποιοδήποτε λόγο.
- Η Ελευθερία να μελετά κανείς το πώς λειτουργεί το πρόγραμμα και να το προσαρμόζει στις ανάγκες του (προϋπόθεση για αυτό είναι η πρόσβαση στον πηγαίο κώδικα του προγράμματος)
- Η Ελεύθερη διακίνηση αντιγράφων του προγράμματος.
- Η Ελευθερία να μπορεί να αναπτύξει και να βελτιώσει κανείς ένα πρόγραμμα και να διανέμει τις βελτιώσεις αυτές στο κοίνο

# Το ΕΛΛΑΚ από άποψη ασφάλειας

+ Δωρεάν & Ελεύθερο

+ Δυνατότητες τροποποίησης & προσαρμογής.

+ Τεκμηρίωση

+ Συμβατότητα με τα περισσότερα πρώτυπα

- Χαλαρά χρονικά πλαίσια στην έκδοση patches.

- Δυσχρηστία (σε επίπεδο configuration)

- Ανοιχτός κώδικας = (ίσως) μεγαλύτερη πιθανότητα δημιουργείας exploits

# Κλειστό λογισμικό και ασφάλεια

+ Άμεση ανταπόκριση σε προβλήματα

+ Support σε επίπεδο configuration

+ Μεγάλη γκάμα εφαρμογών

- Δεν παρέχονται αρκετές πληροφορίες με εύκολο τρόπο για το σύστημα και τα προγράμματά του

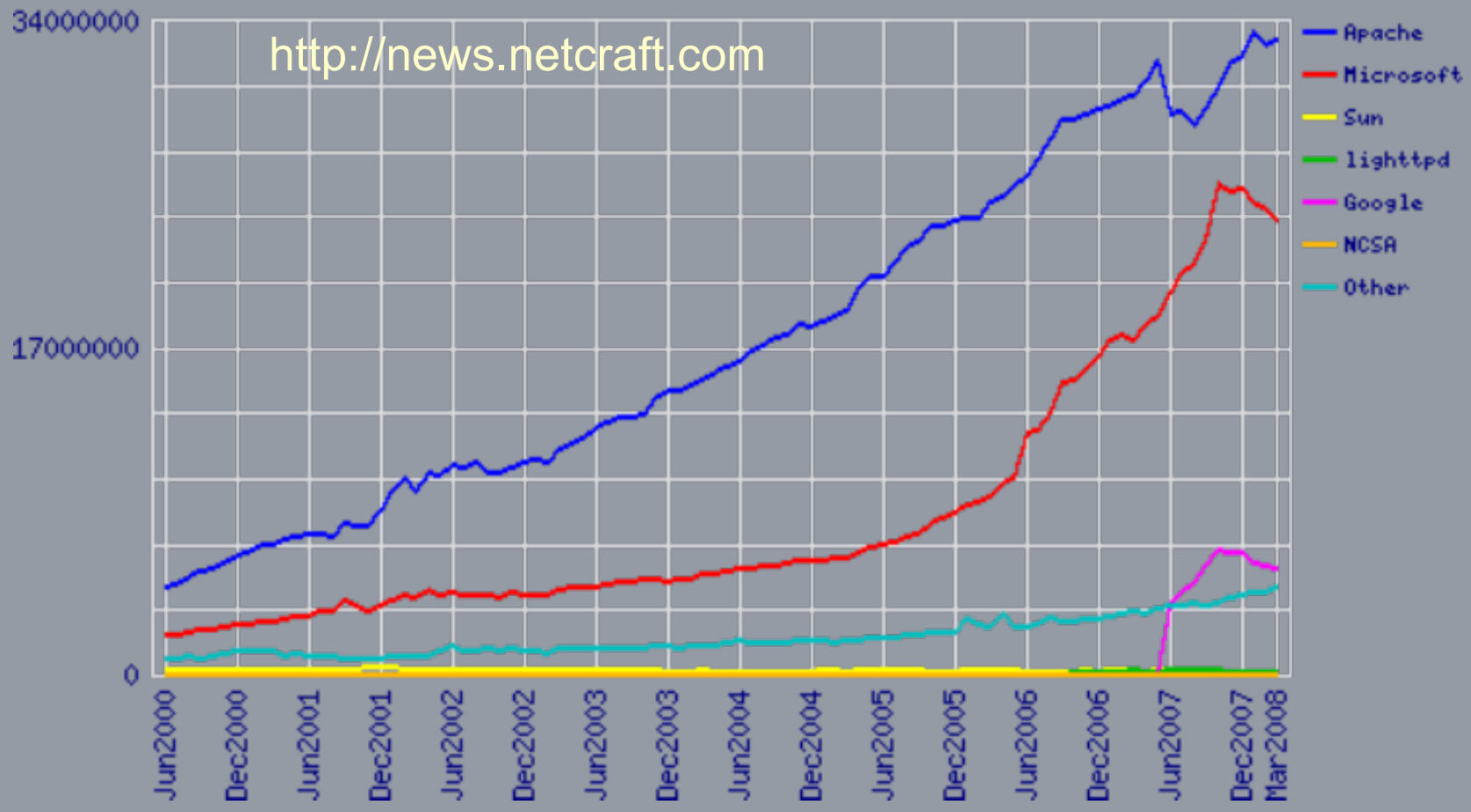
- Κλειστά πρότυπα (έλειψη τεκμηρίωσης, ασυμβατότητα)

- Ψευδαίσθηση ασφάλειας (για κάποιους ισχύει assembly = πηγαίος

# Γενικά Στατίστικα Χρήσης ΕΛΛΑΚ

Υπηρεσίες web (στατιστικά Μαρτίου 2008) :

| Server | Active Sites | Percentage |
|---|---|---|
| Apache | 33,011,740 | 49.38% |
| MS IIS | 23,533,801 | 35.20% |

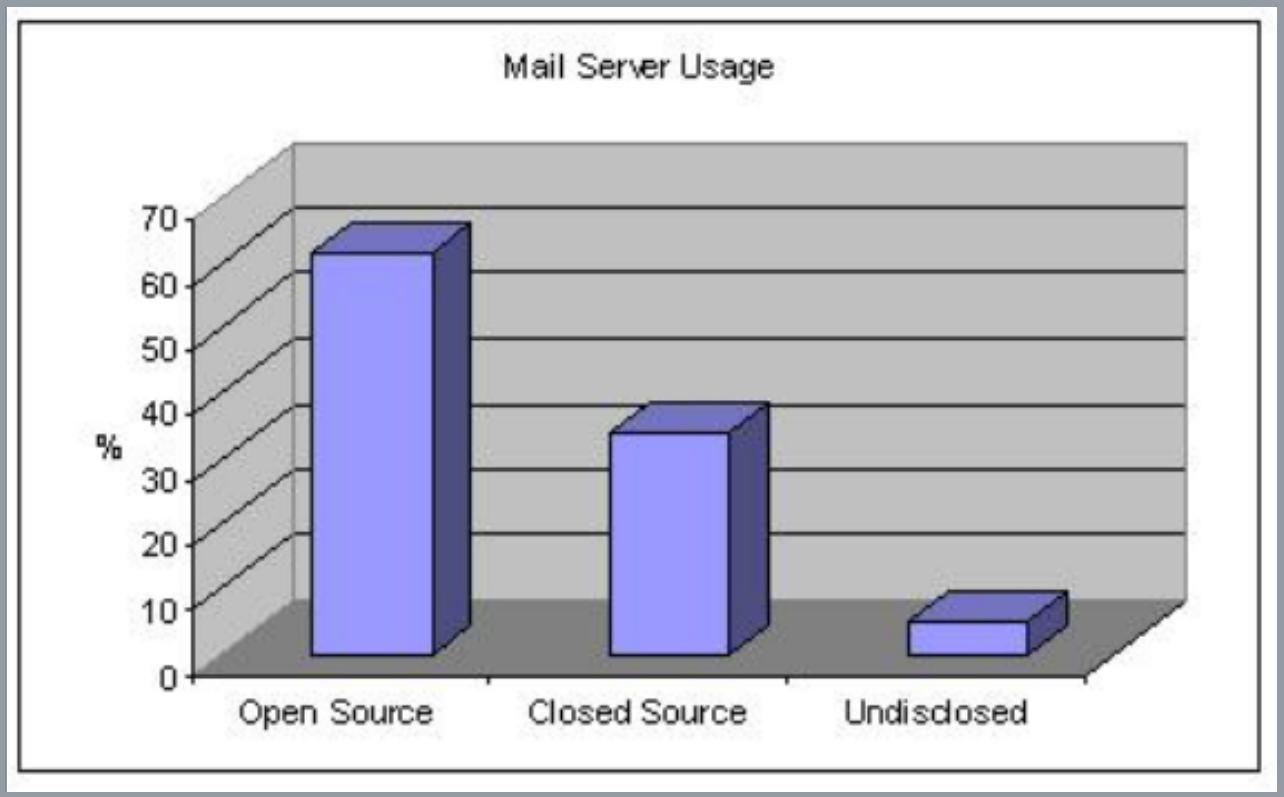


# Γενικά Στατίστικα Χρήσης ΕΛΛΑΚ

Υπηρεσίες mail (στατιστικά Μαρτίου 2008) :

Total Servers : 2,818,895

Open Source : 61%
Closed Source : 34%
Undisclosed : 5%

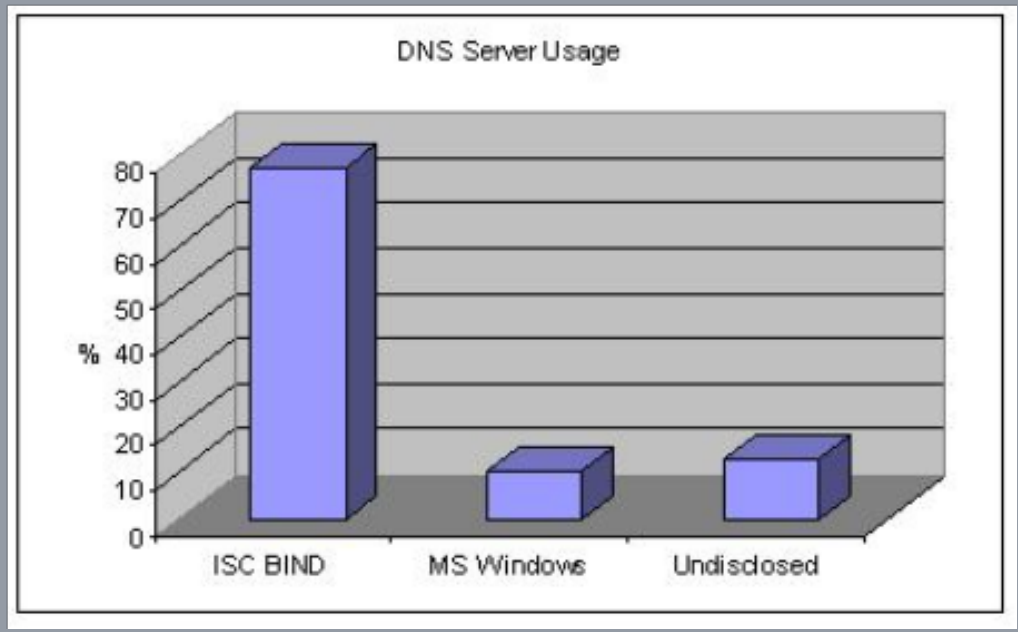



http://www.mailradar.com/mailstat/

# Γενικά Στατίστικα Χρήσης ΕΛΛΑΚ

Υπηρεσίες DNS (στατιστικά Απριλίου-Ιουνίου 2005) :

Total : 1,300,000
ISC BIND (Various Versions) : 77%
Microsoft Windws (2000 & 2003) : 10%
Undisclosed : 13%




http://dns.measurement-factory.com/surveys/sum1.html

# Weak & Default passwords

- Η πρώτη προσπάθεια για την διείσδυση σε ένα δίκτυο ή σύστημα
- Σε αρχείο περίπου 50.000 χρηστών ένας στους πέντε είχε κωδικό 1234, 12345 ή 123456!
- Περίπου 2000 χρήστες είχαν πολύπλοκο κωδικό!

- Αυστηρό password policy
- Συχνή αλλαγή κωδικών
- CrackLib
- John the ripper

http://sourceforge.net/projects/cracklib

# Web Attacks

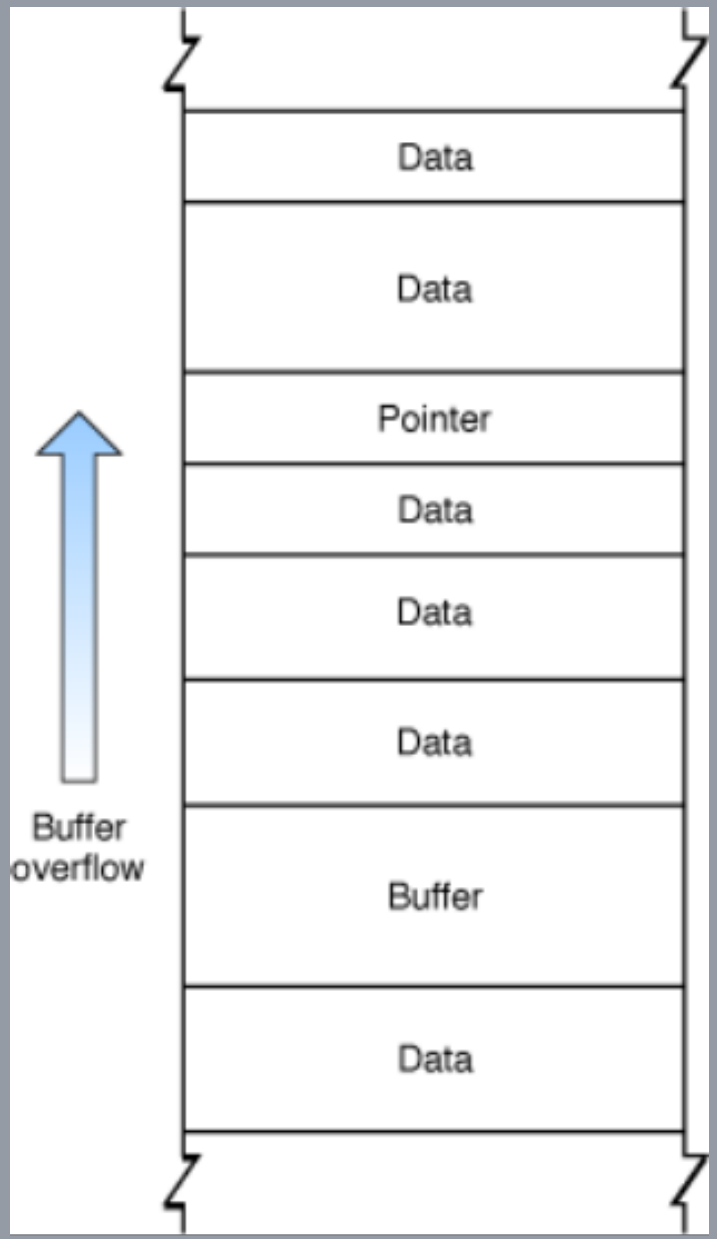
- Δεύτερη απόπειρα για διείσδυση σε ένα σύστημα
- Πολλά & Εκμεταλλέυσημα με εύκολο τρόπο

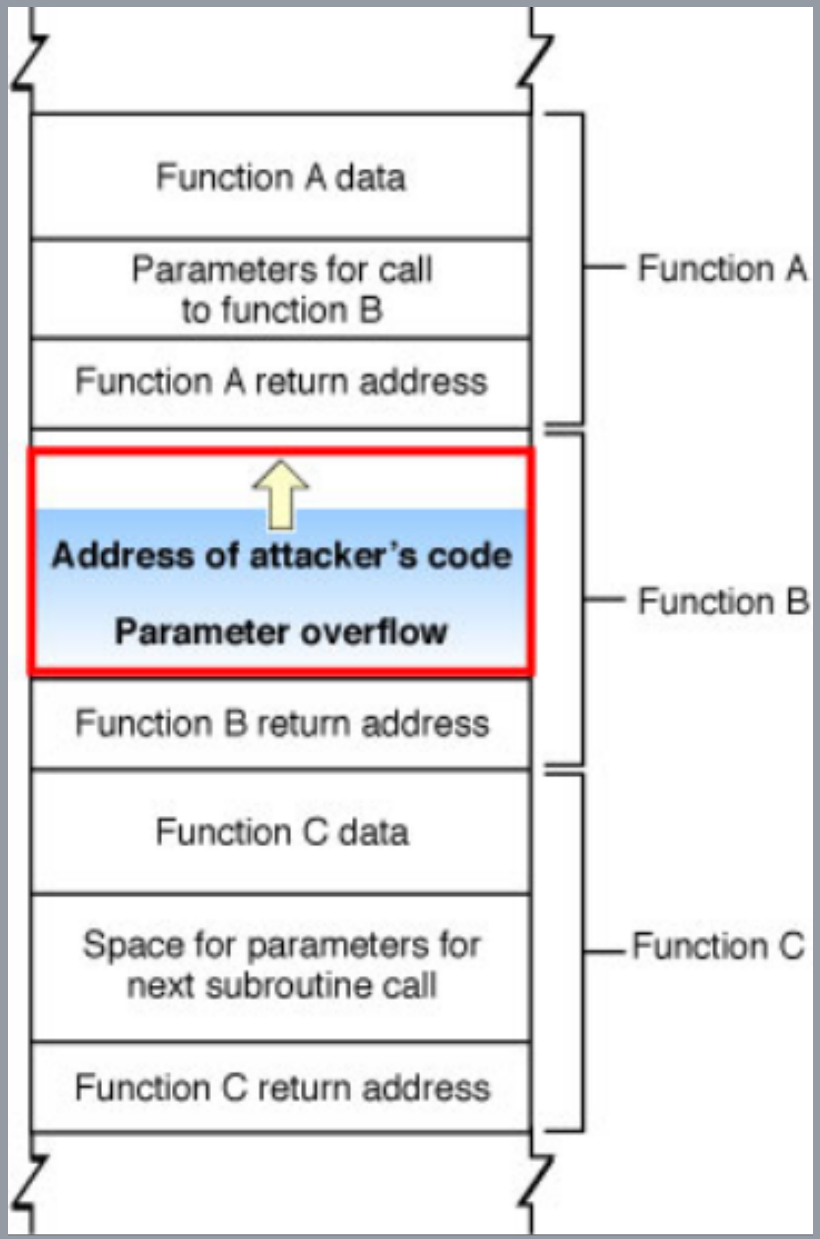
Κατηγορίες:

- SQL injections (MSSQL, MySQL, PostgreSQL κ.α)
- Client side attacks (Phising, XSS, CSRF k.a)
- Remote command execution (κυρίως σε CGIs)
- File upload & File inclusion attacks (PHP, ASP, Java Servlets κ.α)

http://en.wikipedia.org/wiki/SQL_injection
http://en.wikipedia.org/wiki/Cross-site_request_forgery
http://en.wikipedia.org/wiki/Cross-site_scripting
http://en.wikipedia.org/wiki/Remote_File_Inclusion
http://project.honeynet.org/papers/webapp/

# Buffer overflows



# Race conditions & Symlink attacks

- Κάποιο πρόγραμμα ανοίγει ένα αρχείο χωρίς να ελέγχει:
  1. Τον χρήστη στον οποίο ανήκει το αρχείο
  2. Αν το αρχείο είναι link (δλδ. δείχνει σε άλλο αρχείο)
  3. Αν το όνομα κάποιου προσωρινού αρχείου που χρησιμοποιεί είναι προβλέψιμο

- Apple Mac OS X Internet Connection Privilege Escalation

http://secunia.com/advisories/12157/

http://en.wikipedia.org/wiki/Symlink_race

# Leaked file descriptors

- Κάποιο πρόγραμμα ανοίγει ένα αρχείο με ευαίσθητες πληροφορίες (π.χ κωδικοί) και δεν το κλείνει πριν καλέσει κάποιο άλλο πρόγραμμα ή κομμάτι κώδικα.
- PHP / mod_php File Descriptor Leakage Vulnerability

http://secunia.com/advisories/10507/

# Bad design

- Προβλήματα σε επίπεδο πρωτοκολλου (SMTP, NFS, NIS κ.α)
- Προβλήματα στο implementation (Timming Attacks / Sidechannel attacks)
- Αποτέλεμα:
  1. Φανέρωση ευαίσθητων πληροφοριών
  2. Προβλεψιμότητα πηγαίου κώδικα / υλοποίησης
  3. Προβλεψιμότητα κρυπτογραφικών κλειδιών!

# Decoy attacks

- Κάνουμε τον χρήστη να πιστεύει ότι δίνει τα στοιχεία του σε κάποιο έμπιστο πρόγραμμα!
- Γνωστό παράδειγμα: /bin/login σε διάφορα Unix based OSes ;-)
- Οι επιθέσεις αυτές στο internet αναφέρονται ως Phising (Decoy attack είναι πιο παλιός όρος).

http://project.honeynet.org/papers/phishing/

# 0days!

- Ο όρος είναι αστεϊσμός του zero hour!
- Πρόκειται για προγράμματα που εκμεταλλεύονται software vulnerabilities σε προγράμματα (exploits) με τη διαφορά ότι τα συγκεκριμένα vulnerabilities δεν δημοσιεύονται ποτέ!
- Αποτέλεσμα:
  1. Διαιώνιση των τρωτών σημείων από έκδοση σε έκδοση
  2. Compromise καινούριων συστημάτων
  3. "Knowledge shared is power lost" -- Aleister Crowley
- Πρόσβαση σε αυτά έχουν μόνο τα έμπιστα μέλη διάφορων ομάδων

# Προστασία από software vulnerabilities

- Auditing του κώδικα για τρωτά σημεία (το πιο σημαντικό!)
- Συχνά updates & patches (μόνο όταν χρειάζονται! Extra features = Extra bugs)
- Ενημέρωση από sites & mailing lists σχετικές με ασφάλεια
- Ενημέρωση χρηστών για πιθανούς κινδύνους (ημερίδες και mailing lists)
- Έλεγχος υποδομής από τρίτα άτομα με εμπειρία, penetration tests!
- Μεγάλη προσοχή στις πληροφορίες που πετάμε ακόμα και στα σκουπίδια
- Φυσική ασφάλεια των υπολογιστών (ειδικά δωμάτια ή έπιπλα με κλειδαριές κ.α)
- Σχεδόν καμία εταιρεία/ίδρυμα δεν εφαρμοζει αυτόν τον κανόνα!

# Ποιούς πρέπει να αντιμετωπίσουμε;

- Hackers Wannabe's & Script kiddies

Απλά ακολουθήστε τους κανόνες που περιγράψαμε προηγουμένως ;-)

- Ευτυχώς ή δυστυχώς υπάρχουν άνθρωποι που ξέρουν καλά τι κάνουν. Δεν υπάρχει και δε θα υπάρξει ποτέ πανάκεια!
- Στη δεύτερη περίπτωση -- Compromised σύστημα + hacker = οικοσύστημα.

- Παραβίαση ισορροπίας καταλήγει σε προβλήματα και για τον διαχειριστή του συστήματος αλλά και για την αντίπαλη πλευρά! Ας κάνουν καλύτερα και οι δύο τη δουλειά τους :-)

# Εμείς στο ΤΗΜΜΥ..

- Η ασφάλεια είναι ένα πολύπλευρο ζήτημα
- Υπηρεσίες κυρίως δικτυακές (smtp, web, SSH, radius, WIFI, SMB/CIFS)
- Λογικός διαχωρισμός τρωτών σημείων
- Κατηγοριοποίηση:
  - Επίπεδο δικτύου
    - Layer 2 (VLANs, WPA2)
    - Layer 3
  - Επίπεδο συστήματος
    - Ασφάλεια Λ/Σ
    - Ασφάλεια εφαρμογών

# Ασφάλεια δικτύου (1)

- Firewalls
  - Επίπεδο ενεργού στοιχείου (router)
  - Επίπεδο εξυπηρετητή (host)
  - Πλήρης έλεγχος εισερχόμενων-εξερχόμενων πακέτων
  - Έλεγχος ροής πληροφορίας από και προς τους εξυπηρετητές
  - Κανονικοποίηση πακέτων (κατακερματισμός)
  - Layer 3 antispoofing
  - Προστασία από DoS/DDoS attacks
  - Fault tolerance, load balancing, traffic shaping

# Ασφάλεια Δικτύου (2)

- Proxies
  - Traffic normalization (backdoor prevention)
  - Traffic shaping (caching)
  - “Content” filtering
  - Acls (IP based, time based, content based)
  - Εφαρμογή λογικής bastion host
    - Single point of traffic flow
    - Εύκολος τρόπος διασφάλισης ενός εξυπηρετητή
    - Μπορούν να εφαρμοστούν διαδικασίες αυθεντικοποίησης/εξουσιοδότησης

# Ασφάλεια Εξυπηρετητή (1)

- Επιλογή χώρου
  - Κλειδωμένοι χώροι
  - Κλειδωμένα racks
  - UPS
- Επιλογή Server
  - Raid – hot swap HDDs
  - Hot swap τροφοδοτικά
  - Αξιοπιστία μηχανήματος
- Επιλογή Λ/Σ
  - OpenBSD για firewall/router
  - FreeBSD για εξυπηρετητές
- Επίπεδο χρήστη
  - Cracklib
  - Strong password hashing (blowfish)
  - Password policies
  - One time passwords where applicable
  - Resource limits
  - Restricted shell access (no shell access καλύτερα ☺)

# Ασφάλεια Εξυπηρετητή (2)

- Επίπεδο Λ/Σ
  - Updates
  - BSD Security levels
    - Filesystem remounting not possible
    - Unix extended attributes (system binaries, logfiles)
    - No time readjustment
    - No Firewall ruleset reconfiguration
  - auditing
  - ntpd
  - Privilege separation
  - Jails/chroots
  - Αφαίρεση Suid/gid και executable flags από προγράμματα που δεν τα χρειάζονται
- Επίπεδο Συστήματος αρχείων
  - Read only filesystem mounting
  - Noexec, nodev, nosuid flags where possible
  - Encrypted swap filesystem
  - Encrypted partitions containing sensitive information

# Ασφάλεια Εξυπηρετητή (3)

- Επίπεδο εφαρμογών
  - Updated services
  - Security focused services' configuration - installation
  - Privilege separation
  - Chrooted/jailed services
  - Resource limited services
  - Antispam filters
  - Antivirus filters
  - Encrypted services (SSH, https, imaps, pops)

# Μελλοντικά...

- NIDS
- Kerberos
- LDAP
- Secure Loghost
- Honeypots / honeynets

# Ευχαριστούμε !

Ερωτήσεις?