Εξέταση 102 – Μάθημα 19

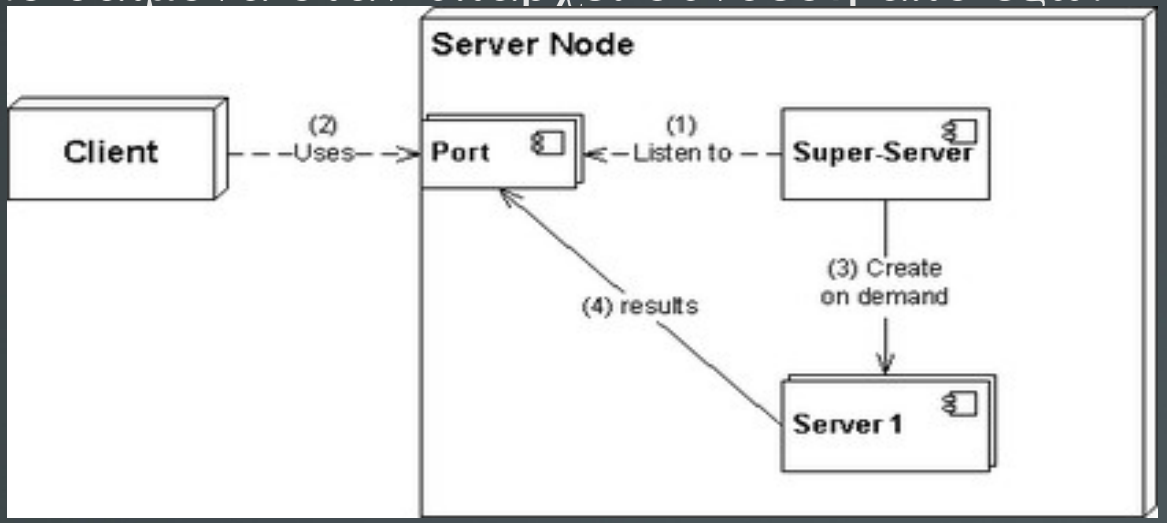
110.2 Οργάνωση ασφάλειας διακομιστή

Οι υπερδιακομιστές (superservers) *inetd* και *xinetd*

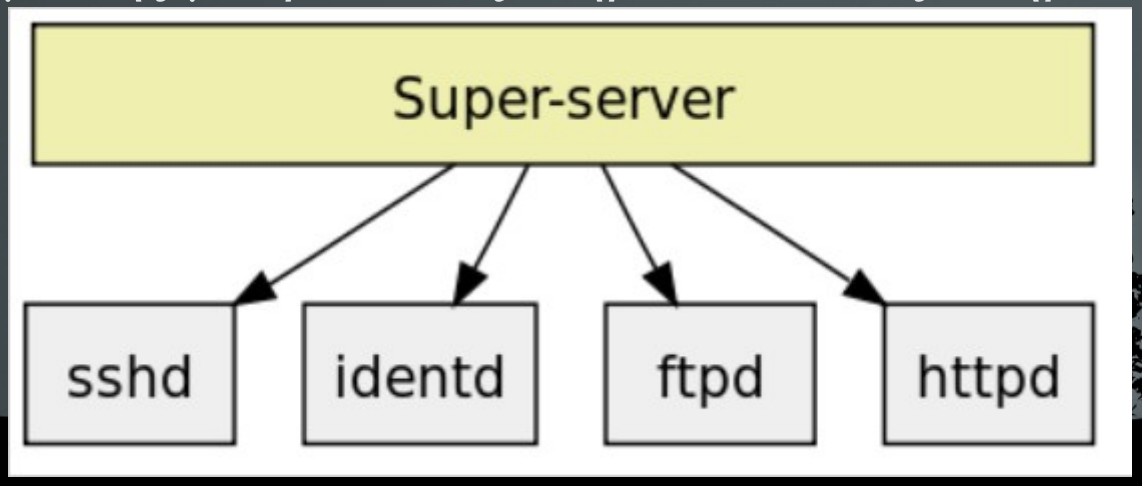
- Οι δαιμονες **inetd** και **xinetd** είναι υπηρεσίες που αναμένουν συνδέσεις σε θύρες **TCP** και **UDP** και αναλόγως των ρυθμίσεων τους ξεκινούν διάφορες εφαρμογές πχ, ssh, ftp, http κτλ
- Το πλεονέκτημα του να τρέχεις υπηρεσίες όπως την ssh, telnet, ftp, tftp, μέσω υπερδιακομιστή αντί του του δικού της αυτόνομου δαίμονα, είναι ότι έχεις μόνο μια διεργασία που ακούει σε πολλές θύρες και έτσι έχεις λιγότερες διεργασίες στο σύστημα
- Με τον υπερδιακομιστή μπορείς επίσης να μετατρέψεις σε υπηρεσίες εφαρμογές οι οποίες δεν έχουν τον δικό τους δαίμονα πχ tftp, cvs, rsync κτλ
- Το μειονέκτημα της χρήσης υπερδιακομιστή είναι η καθυστέρηση που προκαλείται μέχρι αυτός να καλέσει την άλλη υπηρεσία και έτσι δεν συστήνεται να χρησιμοποιείται σε υπηρεσίες με μεγάλο όγκο δικτυακών δεδομένων

Οι υπερδιακομιστές (superservers) *inetd* και *xinetd*

- Ένας υπερδιακομιστής ακούει σε μια θύρα και την εκχωρεί σε κάποιο άλλο δαίμονα όταν υπάρχει σύνδεση από έξω:



- Ένας υπερδιακομιστής μπορεί να εξυπηρετεί πολλές υπηρεσίες ταυτόχρονα:



Ο υπερδιακομιστής *inetd*

- Ο υπερδιακομιστής **inetd** ήταν ιστορικά ένα από τα πρώτα προγράμματα με αυτή την δυνατότητα.
- **# apt-get install inetutils-inetd | openbsd-inetd** # εγκατάσταση σε Debian
- Τα αρχεία ρυθμίσεως του είναι το **/etc/inetd.conf** και όλα τα αρχεία κάτω από τον κατάλογο **/etc/inetd.d/**. Η μορφή του αρχείου ρυθμίσεων είναι ως εξής:

 # <service_name> <sock_type> <proto> <flags> <user> <server_path> <args>

Το αρχείο ρυθμίσεως */etc/inetd.conf*

- **service_name**: πρέπει να είναι ένα όνομα από το αρχείο **/etc/services**
- **socket_type**: μπορεί να έχει τιμές όπως **stream**, **dgram**, **raw** κα. Για TCP χρησιμοποιείται το stream και για UDP το dgram
- **proto**: κάποιο πρωτόκολλο από το αρχείο **/etc/protocols**. Συνήθως TCP ή UDP
- **flags**: Οι τιμές είναι **wait** ή **nowait**. Το **wait** χρησιμοποείται σε περιπτώσεις όπου ο **inetd** πρέπει να περιμένει το καλούμενο διακομιστή να τελειώσει πριν ανακαταλάβει την θύρα αναμονής
- **user**: ο χρήστης που θα ξεκινά την υπηρεσία. Συνήθως **root**
- **server_path**: Η διαδρομή όπου βρίσκεται ο καλούμενος δαίμονας
- **args**: παράμετροι που πρέπει να περάσουν στους δαίμονες. Η τιμή είναι **internal** για εσωτερικές υπηρεσίες του **inetd**

Το αρχείο ρυθμίσεως */etc/inetd.conf*

- Ένα παράδειγμα ρυθμίσεων στο **/etc/inetd.conf**:

```
#discard      stream  tcp     nowait  root    internal
#discard      dgram   udp     wait    root    internal
#daytime      stream  tcp     nowait  root    internal
#time         stream  tcp     nowait  root    internal
talk          dgram   udp     wait    root    /usr/sbin/talkd
telnet        stream  tcp     wait    root    /usr/sbin/telnetd
```

- Μετά την επανεκκίνηση του δαίμονα **inetd**:

```
# netstat -lnptu | grep inet
tcp   0    0.0.0.0 :23     0.0.0.0:*  LISTEN  13463/inetutils-ine
udp   0    0 0.0.0.0:517   0.0.0.0:*          13463/inetutils-ine
```

- **# /etc/init.d/inetutils-inetd restart** # επανεκκίνηση **inetutils-inetd**
- **# /etc/init.d/openbsd-inetd restart** # επανεκκίνηση **openbsd-inetd**

Ο υπερδιακομιστής *xinetd*

- Ο υπερδιακομιστής **xinetd** είναι μεταγενέστερος του **inetd** και παρέχει περισσότερες δυνατότητες.
- Είναι προεγκατεστημένος σε RedHat συστήματα
- **# apt-get install xinetd** # εγκατάσταση **xinetd** σε Debian
- Τα αρχεία ρυθμίσεως του είναι το **/etc/xinetd.conf** και όλα τα αρχεία κάτω από τον κατάλογο **/etc/xinetd.d/**. Η μορφή του αρχείου ρυθμίσεων είναι ως εξής:

```
service rsync{
    disable yes  # no για ενεργοποίηση
    socket_type = stream  # dgram, raw άλλες πιθανές επιλογές
    wait = no  # yes για ενεργοποίηση
    user = root # χρήστης που θα τρέχει το καλούμενο δαίμονα
    server = /usr/bin/rsync # διαδρομή του καλούμενου δαίμονα
    server_args = --daemon# παράμετροι του καλούμενου δαίμονα
}
```

Ενεργοποίηση υπηρεσιών σε xinetd

- Αν στο αρχείο **/etc/xinetd.d/rsync** αλλάξουμε τη παράμετρο **disable** σε **no** η υπηρεσία **rsync** θα ενεργοποιηθεί στην επόμενη επανεκκίνηση του δαίμονα **xinetd**
- **# /etc/rc.d/init.d/xinetd restart** # επανεκκίνηση σε RedHat
- **# /etc/init.d/xinetd restart** # επανεκκίνηση σε Debian
- Έλεγχος αν είναι εντάξει:

```
# netstat -lnptu | grep inet
tcp   0    0.0.0.0:873     0.0.0.0:*  LISTEN  24950/xinetd
```

Τα αρχεία */etc/passwd* και */etc/shadow*

- Τα συνθηματικά των χρηστών παραδοσιακά υπήρχαν στο αρχείο **passwd**. Αυτό ήταν σοβαρό πρόβλημα ασφάλειας γιατί αν και κρυπτογραφημένα (hashed) μπορούσαν να διαβαστούν από όλους διότι το **passwd** έχει άδειες χρήσης **644**. Αυτό συμβαίνει γιατί πρέπει να διαβάζεται από όλους τους χρήστες
- Για να λυθεί το πρόβλημα αυτό δημιουργήθηκε το σύστημα των σκιωδών συνθηματικών (shadow passwords). Στην θέση της στήλης συνθηματικών εμφανίζεται ένα "**x**" και το μοναδικό και κρυπτογραφημένο (salted and hashes) συνθηματικό εμφανίζεται στο αρχείο **/etc/shadow**
- Οι αλγόριθμοι μονόδρομης κρυπτογράφησης που χρησιμοποιούνται συνήθως είναι ο MD5 και πιο πρόσφατα ο SHA1

Ασφάλεια στο */etc/inittab*

- Αρκετοί οδηγοί ασφάλειας σε Linux συστήνουν την απενεργοποίηση του **Ctrl-Alt-Del** και την εισαγωγή συνθηματικού ακόμη για για λειτουργία μοναδικού χρήστη (**single user mode**). Αυτά μπορούμε να τα ρυθμίσουμε στο **/etc/inittab**
- **~~:S:wait:/sbin/sulogin** # προτροπή για συνθηματικό ακόμη και στην λειτουργία μοναδικού χρήστη. Αυτό θα πρέπει να συνδυαστεί με συνθηματικό στο **boot loader** (grub ή lilo)
- **# ca::ctrlaltdel:/sbin/shutdown -r now**# η γραμμή στο **inittab** που επιτρέπει την λειτουργία επανεκκίνησης με **Ctrl-Alt-Del** θα πρέπει να απενεργοποιηθεί προσθέτοντας ένα "**#**" για να μετατραπεί σε σχόλιο. Ή να διαγραφεί εντελώς

Ανίχνευση και απενεργοποίηση αχρείαστων υπηρεσιών

- Χρησιμοποιώντας τις εντολές **netstat -lnptu** ή **lsof -i** μπορούμε να εντοπίσουμε τις υπηρεσίες πίσω από τις ανοικτές θύρες. Αν βρούμε υπηρεσίες που δεν χρειάζεται να υπάρχουν θα πρέπει να απενεργοποιηθούν.
- Για απενεργοποίηση υπηρεσιών κατά την εκκίνηση σε **System V init** θα πρέπει οι συμβολικοί σύνδεσμοι των υπηρεσιών στους καταλόγους **rc[1-6].d**, και που παραπέμπουν στο κατάλογο **/etc/init.d**, να μετονομαστούν με **K** μπροστά πχ:
  /etc/rc3.d/S19postgresql -> ../init.d/postgresql σε
  /etc/rc3.d/K19postgresql -> ../init.d/postgresql
  Αυτό μπορεί να γίνει και με τις εντολές **chkconfig** σε RedHat και **update.rc-d** σε Debian
- Θα πρέπει επίσης να απενεργοποιηθούν αν είναι ήδη ενεργές με
  # /etc/init.d/postgresql stop
- Οι υπηρεσίες που ενεργοποιούνται από τους υπερδιακομιστές **inetd** και **xinetd** θα πρέπει να απενεργοποιηθούν από τα αρχεία ρυθμίσεως τους

Απενεργοποίηση της εισόδου κοινών χρηστών στο σύστημα με */etc/nologin*

- Πολλές φορές κάποιος διαχειριστής θα πρέπει να προβεί σε εργασίες συντήρησης στο σύστημα και δεν θέλει να μπορούν οι χρήστες να συνδεθούν με το σύστημα
- Σε αυτή την περίπτωση ο διαχειριστής πρέπει να δημιουργήσει το αρχείο **/etc/nologin**. Η παρουσία του θα εμποδίσει στους χρήστες να συνδεθούν είτε τοπικά είτε απομακρυσμένα και θα τους εμφανίσει σαν μήνυμα τα περιεχόμενα του
- **# echo "Out of order for maintenace" > /etc/nologin** # απενεργοποίηση σύνδεσης όλων πλην του **root** και εμφάνιση μηνύματος επεξήγησης
- **# rm /etc/nologin** # μην ξεχάσετε να το διαγράψετε όταν τελειώσουν οι εργασίες!

Περιορισμοί δικτυακής πρόσβασης με *TCP Wrapper*

- Το σύστημα **TCP Wrapper** είναι ένα σύστημα Λιστών Ελέγχου Πρόσβασης (Access Control Lists – ACL) και μπορεί να εμποδίσει δικτυακές συνδέσεις σε υπηρεσίες που το υποστηρίζουν.
- Οι υπηρεσίες που το χρησιμοποιούν έχουν μεταγλωττιστεί απέναντι στη βιβλιοθήκη **libwrap**. Αυτό μπορούμε να το δούμε με **ldd**:
  # ldd /usr/sbin/sshd | grep libwrap
  libwrap.so.0 => /lib/x86_64-linux-gnu/libwrap.so.0 (0x00007f2262807000)
- Το σύστημα χρησιμοποιεί τα αρχεία **/etc/hosts.allow** και **/etc/hosts.deny** για καθορισμό των δικτύων, κόμβων και υπηρεσιών όπου επιτρέπεται η πρόσβαση.
- Εννοείται ότι τα αρχεία αυτά έχουν αποτέλεσμα μόνο σε εφαρμογές που χρησιμοποιούν την βιβλιοθήκη **libwrap**

Τα αρχεία */etc/hosts.allow* και */etc/hosts.deny*

- Η σειρά με την οποία δουλεύουν τα αρχεία **/etc/hosts.allow** και **/etc/hosts.deny** είναι η εξής:
  - Αν υπάρχει κάποιο δίκτυο, τομέας, IP ή όνομα στο **/etc/hosts.allow** επιτρέπεται η πρόσβαση σε αυτό
  - Αν υπάρχει κάποιο δίκτυο, τομέας, IP ή όνομα στο **/etc/hosts.deny** απαγορεύεται η πρόσβαση σε αυτό
  - Σε όσα δεν υπάρχουν σε κανένα από τα δύο επιτρέπεται η πρόσβαση
- Αν θέλουμε να απαγορεύσουμε την πρόσβαση σε όλους, και να επιτρέπουμε την πρόσβαση μόνο σε ορισμένους, θα πρέπει να ρυθμιστεί το **hosts.deny** ως **ALL: ALL** και να βάλουμε τους επιτρεπόμενους στο **hosts.allow**

Τα αρχεία */etc/hosts.allow* και */etc/hosts.deny*

- **# cat /ets/hosts.deny**

  ALL: ALL # απαγορεύεται η πρόσβαση σε όλες τις υπηρεσίες από παντού
- **# cat /etc/hosts.allow**

  sshd: 10.0.1.0/24 EXCEPT 10.0.1.64/26 # επιτρέπεται η πρόσβαση στην υπηρεσία **sshd** για το δίκτυο **10.0.1.0/24** με εξαίρεση το υποδίκτυο **10.0.1.64/26**

  ALL EXCEPT tftpd: .example.com EXCEPT vpn.example.com # επιτρέπεται η πρόσβαση σε όλες τις υπηρεσίες (εκτός tftpd) από όλο τον τομέα **example.com** (προσοχή στην αρχική τελεία!) εκτός από τον κόμβο **vpn.example.com**

  mysqld: LOCAL, @netgroup # επιτρέπεται τοπική πρόσβαση και πρόσβαση από ομάδα **netgroup** σε **mysqld**

  telnetd: 10.0.1.0/24, .example.com EXCEPT 10.0.1.23 # επιτρέπεται η πρόσβαση στην υπηρεσία **telnetd** για το δίκτυο **10.0.1.0/24** και τον τομέα **example.com** αλλά απαγορεύεται η πρόσβαση στο IP **10.0.1.23**