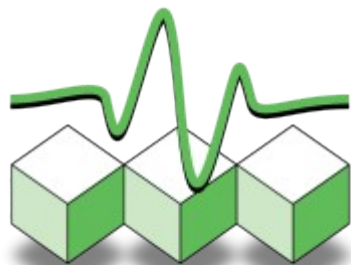


LINAGORA

Formations



Administration et sécurité



Glossaire sécurité

Auteurs :

- LINAGORA *Formations*
formations@linagora.com




Licence

Paternité - Pas d'Utilisation Commerciale - Partage des Conditions Initiales à l'Identique 2.0 France

Vous êtes libres :

- de reproduire, distribuer et communiquer cette création au public,
- de modifier cette création.

Selon les conditions suivantes :

-  Paternité. Vous devez citer le nom de l'auteur original.
-  Pas d'Utilisation Commerciale. Vous n'avez pas le droit d'utiliser cette création à des fins commerciales.
-  Partage des Conditions Initiales à l'Identique. Si vous modifiez, transformez ou adaptez cette création, vous n'avez le droit de distribuer la création qui en résulte que sous un contrat identique à celui-ci.

À chaque réutilisation ou distribution, vous devez faire apparaître clairement aux autres les conditions contractuelles de mise à disposition de cette création.

Chacune de ces conditions peut être levée si vous obtenez l'autorisation du titulaire des droits.

Ce qui précède n'affecte en rien vos droits en tant qu'utilisateur (exceptions au droit d'auteur : copies réservées à l'usage privé du copiste, courtes citations, parodie...)

Pourquoi Linagora met ce support sous licence Creative Commons

- Volonté de contribuer activement à l'essor du logiciel libre
- Promouvoir l'échange et favoriser l'émulation communautaire
- Assurer la pérennité de l'industrie logiciel libre et ne comptabiliser que la Valeur Ajoutée (le formateur)
- Partager le savoir et la connaissance à une vaste échelle

Linagora croit au Libre !

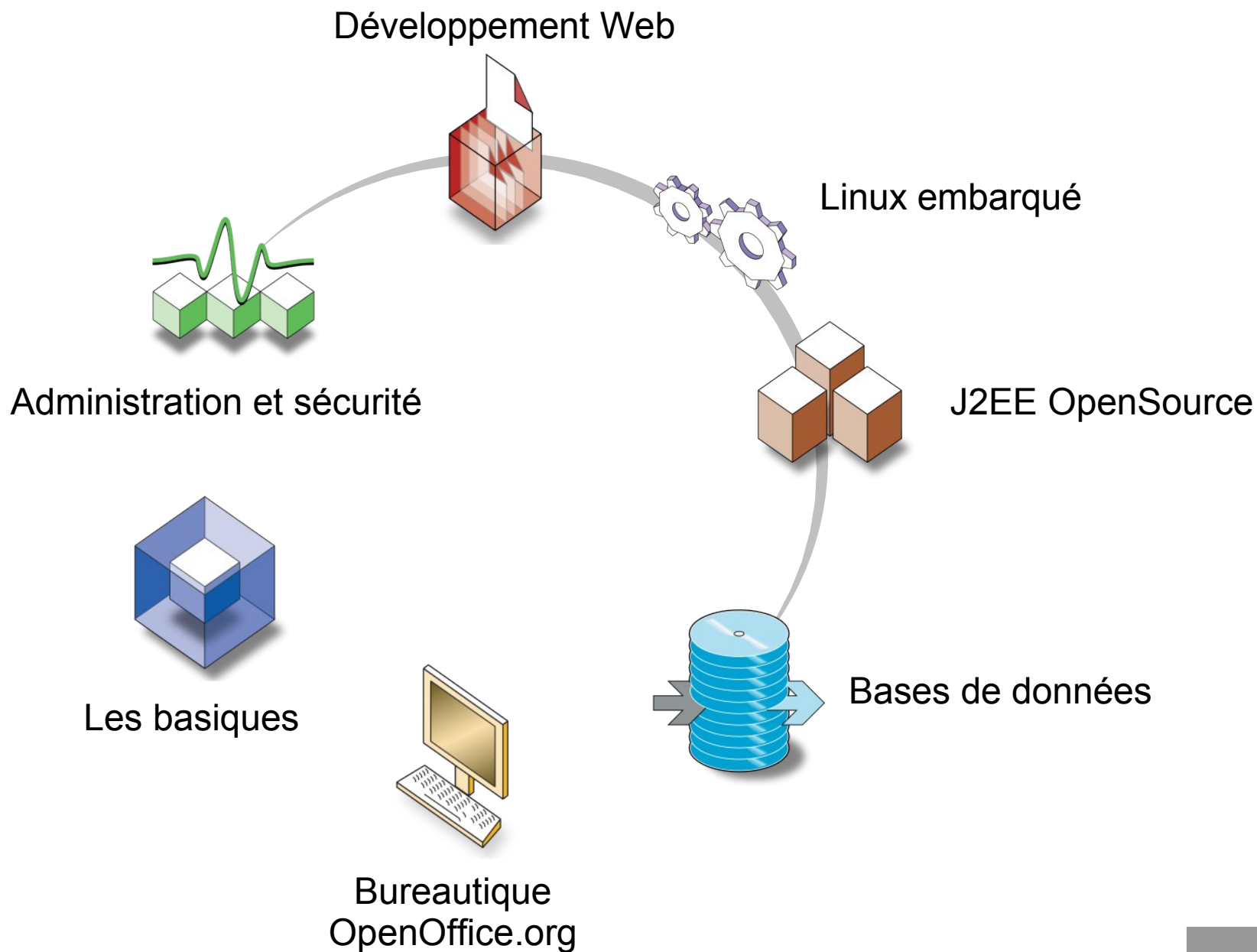
LINAGORA, premier EOS

- Créateur des concepts SS2L (Société de Services en Logiciels Libres) et TM2L (Tierce Maintenance Logiciel Libre), LINAGORA se définit désormais comme un Éditeur Orienté Service (EOS).
- LINAGORA propose une **Open Source Software Assurance** (OSSA) sur 150 logiciels libres :
 - Prêts à l'industrialisation, sur une plate-forme unique : le 08000LINUX.com.
 - Avec garantie de service contractuelle : en cas de bug, LINAGORA s'engage au résultat sur des délais de résolution.
 - Gestion de la feuille de route du logiciel pour le compte du client et s'engage au reversement des développements.
- LINAGORA apporte également son expertise sur toute une gamme de **services professionnels** et de **formations** au travers de **LINAGORA Formations** à **Paris** et à **Lyon**.

LINAGORA Formations

- **7 années d'expérience**, au service des technologies libres et Open Source
- **40 modules** de formation répartis au travers de **7 filières**
- Un cadre agréable, au coeur de Paris
- Deux salles de formation climatisées pouvant accueillir jusqu'à 10 stagiaires.
- **2006 : Plus de 150 stages** effectués
- **2006 : Plus de 900 stagiaires**
- **Une satisfaction** moyenne client de **18/20**
- **Une note moyenne formateur** de **16,27/20**

Filières de formations



Organisation générale et planning

09h30 : début des cours

10h30 : pause du matin

10h45 : reprise des cours

12h00 : pause déjeuner

13h00 : reprise des cours

15h00 : pause de l'après-midi

15h15 : reprise des cours

17h30 : fin de journée

17h30 : libre discussion avec le formateur

Jour 1 :

-

Jour 2 :

-

Jour 3 :

-

Jour 4 :

-

Jour 5 :

-

Glossaire réseau

- fingerprint / fingerprinting
 - Le terme fingerprint se traduit par empreinte
 - On entend par fingerprinting la capacité de déterminer une information en fonction de différentes empreintes. Cette analyse peut être aussi bien passive qu'active (envoi de stimuli et analyse des réponses)
 - Par exemple, on fait souvent référence à l'OS fingerprinting pour des techniques permettant de déterminer le type de système d'exploitation d'une machine donnée.
- handshake TCP
 - Le terme handshake se traduit par poignée de main
 - Par handshake TCP, on désigne l'échange SYN, SYN ACK, ACK nécessaire à l'ouverture d'une session TCP

Glossaire réseau

- firewall stateless / statefull
 - Un firewall statefull (a contrario d'un firewall stateless) maintient une table d'état des connexions actives, rendant ainsi possible une politique de filtrage basée sur l'état de la connexion (NEW, ESTABLISHED, RELATED)
- Man in the Middle (MitM)
 - Terme générique désignant une attaque par substitution. Ce type d'attaque fait intervenir 3 acteurs, A, B et l'attaquant. Le but pour l'attaquant est de se faire passer pour B auprès de A, et vice versa.
- sniffing
 - Opération consistant à récupérer l'ensemble du trafic réseau d'une machine. Ne pas oublier que la majorité des protocoles (dans leurs versions non sécurisées) comme POP3, IMAP font transiter les mots de passe en clair

Glossaire sécurité système

- buffer overflow
 - Attaque consistant à utiliser une faille d'une application dans sa gestion de la mémoire. Ces types d'attaques permettent d'exécuter du code arbitraire, généralement pour obtenir un shell (voir shellcode)
- exploit
 - On désigne par exploit une faille applicative, et une (petite) application qui utilise celle-ci
- shellcode
 - On désigne par shellcode une toute petite (en général une quarantaine d'octets) application binaire permettant l'obtention d'un shell.
- rootkit
 - Ensemble de logiciels permettant généralement d'obtenir les droits administrateurs sur une machine, et d'installer une porte dérobée (backdoor). Un rootkit contient également les logiciels nécessaires à l'effacement des traces de la compromission (suppression des logs, des logiciels du rootkit)

Glossaire sécurité

- virus / ver
 - Programme malicieux dont le premier but est la propagation. Certains virus sont inoffensifs pour le système d'exploitation et les données (mais pas pour le réseau) alors que d'autres vont détruire des données
- trojan / cheval de troie
 - Programme à apparence légitime qui exécute des routines nuisibles à l'insu de l'utilisateur
- spyware / logiciel espion
 - Programme visant à collecter des informations personnelles sur l'utilisateur
- keylogger / enregistreur de frappe
 - Programme collectant l'ensemble des frappes claviers de l'utilisateur (et donc par définition tous les mots de passe qu'il va taper)

Glossaire sécurité, authentification

- AAA (Authorization, Authentication, Accounting)
 - Terme générique désignant trois opérations différentes
 - Authentication : valider un couple identifiant / mot de passe
 - Authorization : valider que le client est habilité à utiliser un service
 - Accounting : assurer la traçabilité des actions effectuées par un utilisateur
- SSO (Single Sign On)
 - Ensemble d'applications (et généralement d'agents) permettant à un utilisateur de s'authentifier une seule fois **mais**
- NSS (Name Service Switch)
 - Bibliothèque d'abstraction permettant la mise à disposition des informations sur un utilisateur au sens Unix (login, mot de passe, UID, GID, home directory, etc.)
 - L'intérêt de cette couche d'abstraction est de pouvoir utiliser différentes sources (fichiers, LDAP, NIS) pour les utilisateurs par configuration plutôt que par changement de code

Glossaire sécurité, authentification

- PAM (Pluggable Authentication Module)
 - Bibliothèque d'authentification (et uniquement d'authentification) permettant aux développeurs d'application de ne pas se soucier de la manière effective dont sera authentifié un utilisateur
 - Il existe de très nombreux modules PAM
 - unix (utilisation des fonctions fournies par la couche NSS)
 - ldap (utilisation d'un annuaire LDAP)
 - mysql (utilisation d'une base données MySQL)
 - postgresql (utilisation d'une base de données PostgreSQL)
 - radius (utilisation d'un serveur radius)
 - PAM, en plus de l'authentification, permet d'assurer quelques autres fonctionnalités
 - Vérification de la force d'un mot de passe à son changement

Glossaire sécurité application Web

- XSS (Cross Site Scripting)
 - Attention à ne pas confondre avec CSS (Cascade Style Sheet), d'où l'utilisation d'un X pour la première lettre
 - Technique consistant à injecter des données arbitraires dans un site et qui sera exécuté par celui-ci, typiquement du javascript
 - Pour vérifier si un site est sensible
- SQL Injection / Injection SQL
 - Technique consistant à injecter du code SQL dans les champs utilisateurs
 - Par exemple, une application (ne vérifiant pas les données fournies par l'utilisateur) qui utilise la commande SQL « `SELECT login FROM users WHERE login = $login AND password = $PASSWORD` » pour vérifier si un utilisateur est valide ou non est sensible aux Injection SQL.

En effet, il suffira à un attaquant de fournir « `OR 1` » comme mot de passe pour être connecté à l'application

Glossaire PKI

- PKI, Public Key Infrastructure (en français, IGC ou ICP)
- X509, Norme définissant la structure des certificats du groupe de travail PKIX
- CRL, Certificate Revocation List (en français, LCR)
- OCSP, Online Certificate Status Protocol
- SCEP, Simple Certificate Enrollment Protocol