

## Formation Linux Sécurité



La sécurité informatique est devenue une préoccupation essentielle des entreprises et donc des responsables informatiques. La sécurisation de Linux est paradoxale : d'un côté, c'est un système qui peut être extrêmement hermétique (à l'exception peut-être d'Unix BSD) et d'un autre côté, il est souvent très vulnérable compte tenu des nombreuses possibilités de configuration offertes

### Objectifs

- Comprendre comment bâtir une sécurité forte autour de Linux
- Acquérir un niveau d'expertise plus élevé sur Linux
- Savoir mettre en place la sécurité d'une application Linux
- Comprendre les fondements de la sécurité informatiques et notamment de la sécurité réseau
- Savoir sécuriser les échanges réseaux en environnement hétérogène grâce à Linux

### Public concerné

- Administrateurs systèmes expérimentés
- Administrateurs réseaux expérimentés

### Pré requis

- Stage LAN1 : "Linux - Administration niveau 1" ou connaissances équivalentes.
- Stage LAN2 : "Linux - Administration niveau 2".

### Une formation de 4 jours

Caractéristiques
<b>Tarif : 1960 € HT par personne</b>
<b>Numéro de formateur : 11753687675</b>
<b>Nombre d'heures : 28</b>
<b>Référence : LIN2</b>
<b>Contact : Loic LE FUR</b>
<b>Telephone : 01.48.12.93.40</b>
<b>Email : <a href="mailto:contact@anaska.com">contact@anaska.com</a></b>

Paris
<b>15/12/2008</b>

## Description des modules

num	Module
<b>1</b>	<b>Les enjeux de la sécurité</b>
<b>Détails</b>	<ul style="list-style-type: none"><li>- Les attaques, les techniques des hackers</li><li>- Panorama des solutions</li><li>- La politique de sécurité ou l'épine dorsale de la stratégie de défense</li></ul>
<b>2</b>	<b>La cryptologie ou la science de base de la sécurité</b>
<b>Détails</b>	<ul style="list-style-type: none"><li>- Les concepts de protocoles et d'algorithmes cryptographiques</li><li>- Les algorithmes symétriques et asymétriques (à clé publique), les fonctions de hachage</li><li>- La signature numérique, les certificats X-509, la notion de PKI</li></ul>
<b>3</b>	<b>Les utilisateurs et les droits</b>
<b>Détails</b>	<ul style="list-style-type: none"><li>- Rappels sur la gestion des utilisateurs et des droits, les ACLs</li><li>- La dangerosité des droits d'endossement (SUID, SGID)</li><li>- La sécurité de connexion, le paquetage SHADOW</li></ul>
<b>4</b>	<b>Les bibliothèques PAM</b>
<b>Détails</b>	<ul style="list-style-type: none"><li>- L'architecture du système PAM, les fichiers de configuration</li><li>- L'étude des principaux modules</li></ul>
<b>5</b>	<b>Le système SELinux ou la sécurité dans le noyau</b>
<b>Détails</b>	<ul style="list-style-type: none"><li>- L'architecture du système SELinux</li><li>- Modifier les règles de comportement des exécutable</li></ul>
<b>6</b>	<b>Les principaux protocoles cryptographiques en client/serveur</b>
<b>Détails</b>	<ul style="list-style-type: none"><li>- SSH, le protocole et les commandes ssh</li><li>- SSL, l'utilisation de SSL et des certificats X-509 dans Apache et stunnel</li><li>- Kerberos et les applications kerbérorisées</li></ul>
<b>7</b>	<b>Les pare-feu</b>
<b>Détails</b>	<ul style="list-style-type: none"><li>- Panorama des techniques pare-feu : bastion, DMZ, routeur filtrant, proxy, masquerading</li><li>- L'architecture Netfilter/Iptables, la notion de chaîne, la syntaxe d'iptables</li><li>- La bibliothèque tcpd ou l'enveloppe de sécurité, la sécurisation via xinetd</li><li>- Mise en place d'un routeur filtrant, du masquerading et d'un bastion avec iptables</li><li>- Le proxy SQUID</li></ul>
<b>8</b>	<b>Les VPN</b>
<b>Détails</b>	<ul style="list-style-type: none"><li>- Panorama des techniques tunnels et VPN</li><li>- Le logiciel OpenVPN</li></ul>
<b>9</b>	<b>La sécurisation des applications</b>
<b>Détails</b>	<ul style="list-style-type: none"><li>- Principes généraux</li><li>- sécurisation du Web (Apache), du email (Sendmail, Postfix), du DNS (bind), du FTP</li></ul>
<b>10</b>	<b>Les techniques d'audit</b>
<b>Détails</b>	<ul style="list-style-type: none"><li>- L'audit des systèmes de fichiers avec AIDE et Tripwire</li><li>- Les outils d'attaque réseau : le scanner nmap, le simulateur d'intrusion nessus</li><li>- La détection des attaques avec snort, lire et écrire des règles snort</li></ul>