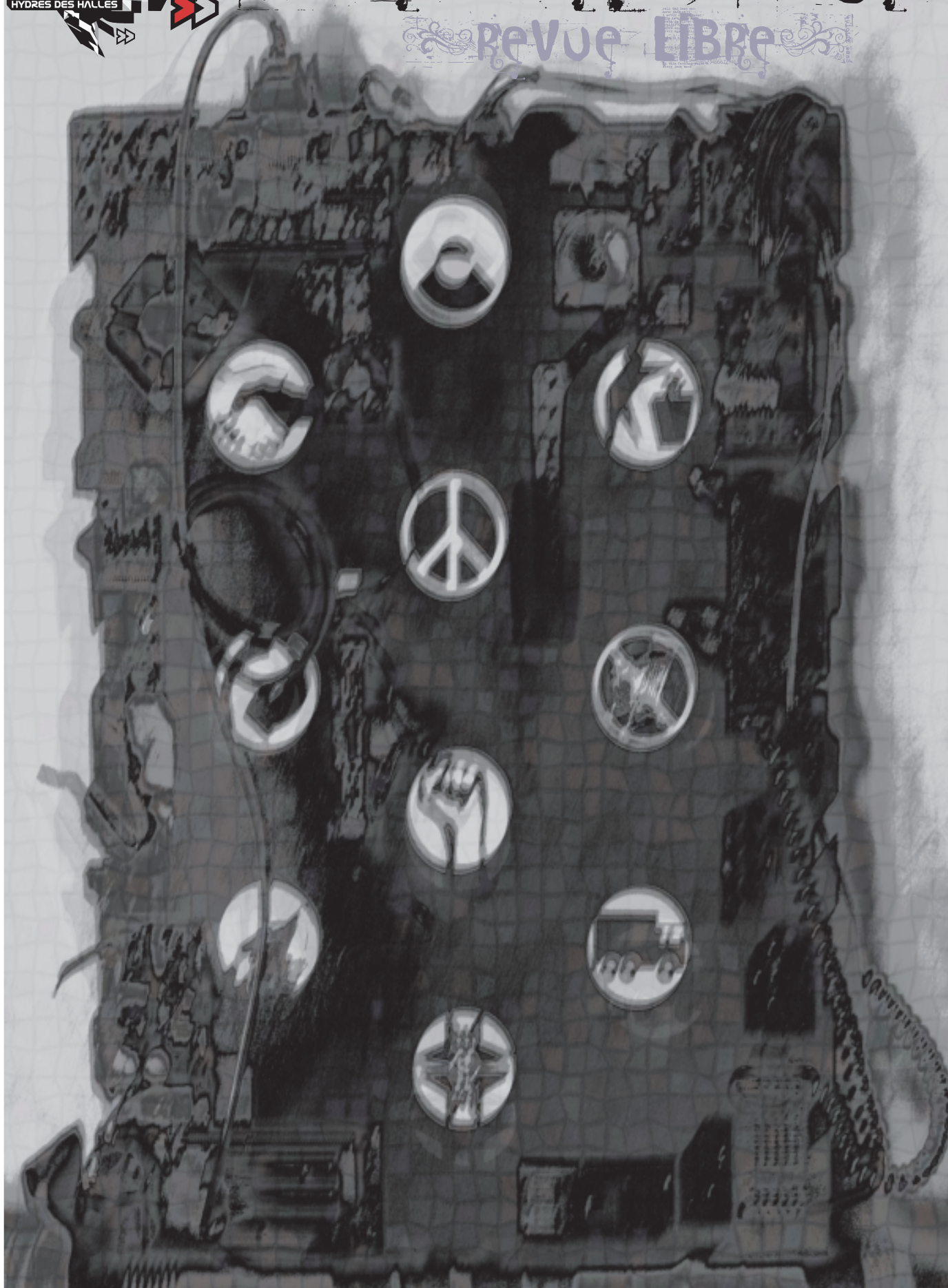




HYDRES DES HALLES

REVUE LIBRE



HYDRES DES HAILES

REVUE LIBRE



Crédits : hdh_kms, hdh_sc, hdh_hln, hdh_plonk, hrtk_stalker, nokos de NostraScein, bobardkor, bendabadmotherfucker, 6tek_falcom, hdh_lta.

Ce zine a été réalisé en utilisant majoritairement des logiciels libres (que vous trouverez facilement sous linux et qui sont fournis sur le cd pour windows) sous Ubuntu Linux. Citons parmi eux : Scribus pour la mise en page et GIMP pour l'édition d'images.

Rien ni personne n'a été blessé (physiquement) durant la réalisation de ce zine.

E L I T O R I A L

Que de plaisir de vous accueillir en ces pages, j'espère de tout coeur qu'il sera pleinement partagé. Nous avons l'immense joie de vous présenter l'Hydre des Halles numéro 0. Dans celui-ci vous pourrez trouver une version préliminaire du manifeste d'Hydres des Halles, lequel pose les fondements de l'action que nous souhaitons mener avec vous. Vous trouverez, à cheval sur le cd et sur le zine "La Piste" de Stalker, un essai qui présente de nombreuses relations avec le présent magazine. Dans ces lignées, nous avons essayé de fournir un contenu culturel et artistique sur le CD et dans le magazine, aussi varié que le temps de réalisation nous l'a permis. L'intention mérité d'être explicitée, nous avons tenté de montrer toute l'ouverture des orientations du magazine. A terme nous aimerions développer différentes sous-sections : hiphop, rock, ska, par exemple, ainsi qu'étendre les disciplines présentes dans ce magazine : nouvelles, plus de type d'essais, pièces de theatre, techniques musicales, jeux de rôle, bricolages, ou tout ce que en quoi vous croyez sincèrement et êtes prêts à nous proposer. Nous imposons cependant certains critères : l'individu de doit pas prendre plus de place que la création d'une part, d'autre part l'ouverture, le respect, l'humanisme et la recherche de la liberté, affirmés comme nos valeurs fondamentales, ne doivent pas être baffoués dans les travaux que vous nous soumettez. Pour conclure je vous invite à prendre contact avec nous si le zine vous plaît afin de participer à l'élaboration du manifeste d'hdh version finale.

Bonne lecture =), Ita

SOMMAIRE

- Le Manifeste preliminaire d'Hydres des Halles.
- La meditation.
- Essai : La Piste de Stalker
 - Manifeste pour une techno alternative qui se survit a elle meme.
- Poesie.
- Jongle : l'asso NostraScein.
- Photo.
- Encyclopedie symbolique .
- OS-Hacker rockstar-life

HYDRES DES HALLES

MANIFESTE

préliminaire

Préface :

Voici la version préliminaire du manifeste d'Hydres des Halles. Celle-ci est incomplète pour plusieurs raisons :

- Ce manifeste n'est que le fruit des réflexions d'un groupuscule et mériterait de recevoir un consensus plus large parmi les artistes qui sont cibles par la revue, pour cette raison il constitue un appel à sa propre remise en cause. J'invite par la présente toutes les personnes qui se sentent touchées à prendre contact pour participer à une plus large réflexion sur le sujet dans la mesure où elles sont prêtes à s'investir dans la réalisation des numéros à venir.

- Hydres des Halles est un projet vieux de plusieurs années mais attendant la réalisation du premier point, rien ne s'en était produit. Il s'est donc produit un sursaut il y a quelques temps afin de ne pas laisser plus longtemps ce projet au stade végétatif. Cette version a donc été réalisée relativement hâtivement, et dans l'attente que plus de contributeurs nous rejoignent le manifeste vous est présenté en l'état.

Manifeste :

La culture est une essence humaine,
l'art en est sa conscience sereine.



Si la première partie nous caractérise indubitablement, la deuxième n'a pas la pleine vigueur que l'on pourrait lui souhaiter. Dans l'émergence de nouvelles communautés, réunies par un même paradigme idéologique, les hommes génèrent de leur communication, de leurs rapports en tout genre cette petite ombre, ce petit fantôme qui donne l'impression de n'être pas là par hasard, qui vous donne l'impression

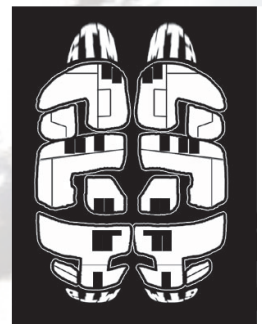
d'exister pour une sphère du monde en laquelle vous avez foi intrinsèquement, qui nous donne l'impression de l'existence d'un "Nous". Cette petite connexion spirituelle n'est rien d'autres que l'accumulation ectoplasmique des bons (et mauvais) moments que nous avons passés ensemble. Substrat de ce que nous avons à nous donner,

récolte de cette part de nos âmes qui peut se libérer durant ces soirées, ces nuits, ces jours ... Tout cela n'est autre que notre culture, Cette capacité a tous nous connaître mieux qu'aucun sans jamais s'être vu. Et puis ... Comme toutes

choses, une culture a son apogée, un point culminant où la somme des esprits pleinement reliés à la toile culturelle bat son plein, sans en remettre en cause l'intégrité. Simplement la conscience ou l'inconscience d'un instant au soleil dans le calme et la paix dans ce milieu qui vous est cher. C'est en cet instant idéal que devrait naître... autre chose. Les quelques grains de sable du temps qui ont l'entière valeur du sablier devraient voir apparaître l'émancipation de cette culture qui veut rejaillir dans l'intemporel au travers de l'art inaltérable et entier. Art et cultures sont liés par une double relation d'intergénération et d'interdépendance. Un art qui se morfond peut nager dans la culture et se ressourcer en inspiration fraîche, en idée mouvante. La culture qui s'éparpille peut tirer de l'art un regard sur elle-même si précieux, et perdurer au delà de son propre milieu de prolifération, l'Homme.

Toujours distants,
ils semblent pour()tant
le son et le caisson.

Séparés par ce qu'ils sont,
par delà tout restants,
leurs pourquoi et leurs comment.



Beaucoup sont ceux qui voient cette seconde mystique comme un passé si lointain qu'ils en ont oublié la douce caresse. Beaucoup sont ceux qui pleurent la mort, qui pleurent la corruption, qui crient l'indignation qui rôde dans leur coeur, mais qu'ont ils fait ? Leurs esprits auront raison de cette question. Le point culminant est-il passé depuis tant d'année que plus rien ne puit arriver ? Est-il trop tard ? NON ! Car je l'ai décidé ! ... Quel prétention ! Mais qui est donc cet être, sage parmi les sages, puissant parmi les puissants, pour avoir d'un replis de sa volonté balayé les traces de tout passé ? Eh bien, cet être n'est pas, et souhaitons le, ne sera jamais ! Simplement, la véracité de mes dires ne sera que dans la férocité de VOTRE décision. Et je dis bien votre décision car de vous seul dépend cet avenir. Il est facile de penser que d'autres feront ce choix, mais si ce n'était pas le cas ?

(...)

Cela se passe entre toi et elle, seuls sous le ciel. Face à ce qui t'es cher, comme le dernier chevalier pour sauver la Terre. Les autres sont une dimension qui n'existe pas, reste à savoir ce que tu vas faire toi.

Tant de ceux que j'ai eu l'occasion de rencontrer on oublié la valeur et la puissance de l'engagement. Aujourd'hui, je vous demande de le réapprendre, je vous demande de goûter de nouveau au risque d'avoir tort, je vous demande de reprendre le droit d'exister. Requête pesée. Il n'est aisé de remuer la lourde poussière qui recouvre la vision d'un monde figé dans lequel nous ne sommes que des grains. La vision d'un univers vissé sur des rails orientés vers le malheur et la souffrance sont tout ce en quoi tant croient. La poussière fut jadis pierre, nous ne sommes pas que des molécules que l'on manipule. Ce qui fut défait nous pouvons le refaire, la force de nos idées nous véhicule. Le bon moment sera-t-il demain, est aujourd'hui ou bien est-ce trop tard ? La réponse est dans la force de l'art, comme moyen de cohésion, comme cristallisation d'idéaux. Soyons aujourd'hui, soyons demain, hier... Mais surtout allons remuer ce qui flotte dans l'air.

Nous sommes un courant idéologique fort et pluriel, mais dispersé (ô, pas dans la pluralité) victimes de l'érosion du temps, subissant les assauts du consumérisme, et de cet éparpillement.

Folie ou embellie ? Votre seule arme est le choix ... Une sorte de Fight club ? N'acquiescent-ils pas en un temps l'apparence d'un essor vers la liberté de l'esprit, intense et sereine à la fois ?

Une suggestion, mais quelle est-elle donc ? De celle-ci nous allons explorer 3 aspects fondamentaux et distincts : le fond, la forme et le dessin.

[Le fond]

De quoi donc les hydres des halles se veulent-elles constituées ?

Car, je l'ai dit, elles se veulent, multiples et indéterminées, troublantes à en désirer, idéales en vérité.

Les hydres des halles sont nous et vous incarnées dans le monde des idées, nos âmes seulement se rencontrent le plus souvent et nous voilà séant une communauté avec ses maux à combattre, des arches à inventer et assouvir, en idée et en créativité. Voilà ce monde que l'on doit bâtir, et ce n'est pas faute de bâtisseurs ... Vous pouvez errer sur le net jusqu'à point d'heures -n'en riez pas le lieu est propice, il y a des pages que l'on ne trouve jamais à moins que l'on ne vous les offre, ce qui fait l'essence de nombreuses communautés sur le net autour de divers peer to peer ou sites, des plus connus, malgré tout, aux plus profondes abîmes là où aucun robot-brasseur d'un moteur de recherche ne s'aventure jamais. Il est parmi toutes ces pages de nombreuses araignées artistes



aimant à tisser leurs toiles mystiques, et comme dirait un frère, de nombreuses cartes retournées. Il est fourmillant sur le net et dans le monde "réel" tant d'artistes aveugles au-delà de la liberté qu'ils recherchent et de la quête qu'ils mènent en leur sein.

Ce sont les hydres de ces halles brumeuses et fantomatiques qui sont le fond de ce projet. Il faut montrer à tant qu'elles existent, leur permettre de se rassembler. Il faut les faire sortir des cercles enfumés des intellectuels et les offrir à un plus grand nombre.

À l'heure actuelle, les cultures sont souvent définies principalement par la musique qui les rassemble (freetekno, hiphop, trance, ...). Or il est bien des cas où la musique prend une telle place qu'elle étouffe les autres arts et rites de cette culture. Et/Ou d'autres circonstances où la musique semble souffrir de la faible présence des autres arts dans les cultures où elle s'enracine. Hdh souhaite donc permettre à ces autres arts de se rencontrer et d'être plus présents. Hdh se veut être à la peinture, au dessin, à la littérature, à la photo, à la sculpture, à la philosophie, à la jungle, à la danse, (...(...)) ce qu'un label est à la musique. Son orientation se veut, à terme, expérimentale.

Bien sur, la musique n'est pas exclue, mais nous souhaitons lui redonner sa place : un art parmi d'autres. Nous souhaitons de plus en plus l'aborder le plus possible sous l'angle de son interpénétration avec les autres arts.

[La forme]

(Cette section est quasiment vide, car elle nécessite une importante réflexion de groupe)

Ce premier numéro est présenté sous une forme très classique, mais les suivants auront un mode de rédaction plus développé et un format plus novateur. Ainsi qu'il est énoncé plus haut, si vous êtes intéressés par le projet, je vous invite à prendre contact rapidement pour participer à cette réflexion.

[Le dessin]

(Cette section sera mieux définie dans le numéro 2, mais les grandes lignes sont évoquées ci-dessous)

Hdh poursuit plusieurs objectifs, il s'agit dans un premier temps de permettre aux artistes et performers de disposer d'un lieu d'expression et de collaboration. Il permettra d'accéder "plus facilement" à différents univers créatifs et expressifs. Cet engendrement sera de plus fixé dans le temps et entière. Il s'agit de placer régulièrement ces points fixes afin, d'une part de manifester l'existence de certains courants de pensées, et d'autre part de constater leur évolution. Se souvenir d'où l'on vient n'est pas inutile lorsque l'on cherche à savoir où l'on va. Dans un deuxième temps, nous souhaitons inciter nos lecteurs à la création sous toutes ses formes, en poursuivant l'idéal humaniste de la Renaissance.

Nicolas Flamel

tout se passe dans la tête

"Ne cherchez pas la Voie chez les autres
Dans un endroit éloigné,
La Voie se trouve sous vos pieds."

- Maître Tosan (807 - 869), fondateur du Zen Soto -

Les états modifiés de conscience.

L'état d'éveil, dans lequel nous passons le plus clair de nos journées, n'est que l'un des nombreux états que nous puissions connaître. Durant l'éveil, les ondes qui parcourent en permanence notre cerveau sont principalement de deux types différents: alpha et bêta. Ce sont ces fréquences qui constituent la "normale" de notre encéphale. Vient ensuite le sommeil profond, et avec lui les ondes Delta, lentes et amples, témoins d'une activité particulière des nombreuses zones qui constitue le cerveau. Puis vient le rêve, le sommeil paradoxal, qui comme son nom l'indique, sème la panique dans l'analyse, car les ondes dans notre tête semblent être celles de l'éveil, et pourtant, notre paralysie est complète. Ce phénomène, découvert en 1959 par Michel Jouvet, a depuis été étudié de toutes parts durant près d'un demi siècle. Pourtant, il aura fallu attendre le nouveau millénaire pour voir apparaître les recherches concernant la méditation. Une recherche effectuée en 2004 sur huit pratiquants de la méditation, d'origines différentes a révélé que le cerveau a une activité particulière lorsque l'on médite. L'onde la plus importante à ce moment est dite "gamma".

Les ondes gamma

"Les différentes régions du cerveau sont spécialisées dans certaines fonctions comme les émotions, le goût, l'odorat, la mémoire. Elles doivent se synchroniser entre elles. La présence d'ondes gamma reflète la coordination à travers le cerveau de ces différentes régions." En effet l'augmentation exceptionnelle des rythmes gamma dans le cortex frontal, observée chez les méditants expérimentés, indique que ces régions jouent un rôle important dans la génération de cet état. "Ce n'est pas surprenant, puisque ces régions sous-tendent des fonctions mentales complexes, comme la pensée abstraite, la capacité d'apprentissage mais aussi les actions volontaires", commente Antoine Lutz, docteur en neurosciences cognitives, responsable de la recherche. "Mais ce n'est pas la seule zone concernée, l'étude montre une activation d'un grand nombre de régions et notamment des aires pariétales. Suggérant ainsi une synchronisation à longue distance entre ces zones. La méditation générerait donc une forte coordination entre plusieurs régions du cerveau."

La méditation, c'est quoi finalement?

Dans notre quotidien occidental, nous avons dénaturé ou oublié le sens du mot "méditation". Dans l'imagerie populaire, on y associe les moines qui lévitent, les postures non-chalantes des sixties. Pourtant, la pratique de la vraie méditation n'a rien à voir, n'y a avec une quelconque appartenance religieuse, ni avec un "super pouvoir" inaccessible. Elle a du reste été pratiquée sous diverses formes à travers les âges et les continents, des soufistes, moines mystiques musulmans, à l'Inde à travers le yoga, la Chine à travers le Taoïsme, ou au Japon avec l'arrivée du bouddhisme. Il s'agit d'un autre état de conscience, mais nous pouvons en maîtriser les états, à travers la pratique assidue et quotidienne. Il ne s'agit de rien d'autre que de ne penser à rien, avec une approche bien particulière qui assure que l'on ne tombe pas dans le sommeil, et que l'on arrive effectivement à se débarrasser de ses pensées.

Nombreuses sont les anecdotes comme celle qui suit à travers l'histoire du Tao ou du Bouddhisme.. Maître Dogen, qui rapporta le Zen au Japon vers le XIIIème siècle, alla en Chine trouver les racines du Bouddhisme. A son arrivée, il rencontra un vieux moine cuisinier (tenzo) venu lui acheter des marchandises. Lors d'une conversation avec ce tenzo, Dogen demanda "Quel est le sens de la lettre ? De quelle manière doit-on lire les sutras ?

-1-2-3-4-5, lui répond le cuisinier.

-Mais comment faire pour étudier la Voie ? Le vrai Bouddhisme?

-Nulle part la voie n'est dissimulée.

-Comment faire pour étudier les sutras ? Le vrai Bouddhisme?

-1-2-3-4-5, rétorque enfin le cuisinier."

C'est en effet l'esprit du geste de méditation qui est important. La méditation n'est pas un exercice intellectuel, ni un exercice physique. L'on ne doit pas chercher à avoir un satori, sorte de "révélation" qui correspond à un stade élevé de concentration, ni à trouver des réponses concrètes. Les images n'ont plus de sens. Il ne faut plus regarder dehors, mais dedans. Il ne faut plus voir par les yeux, plus entendre par les oreilles, il faut vivre par le souffle. Yeux ouverts, dans une pièce calme, il faut se concentrer sur la respiration, jusqu'à la sentir emporter toute substance de pensée. Puis viendra le calme, le dharma, la paix intérieure, et avec lui la vraie compréhension et la vraie perception de la réalité.

Que faire?

Différentes approches existent. Aucune n'est meilleure qu'une autre, les moines tibétains en pratique par exemple plusieurs formes.

(...)

On peut citer :

- fixer un point vague dans le vide,
- fixer la flamme d'un bougie,
- se focaliser sur son souffle.

La pratique quotidienne de la méditation, et surtout l'acceptation de cet idéal dans la vie quotidienne, a bien d'autres vertus que celle d'apporter le calme. Les moines bouddhistes eux mêmes voient avant tout essentiellement le fait de "muscler" son cerveau, de l'entraîner, de le discipliner. Ceci permet assez vite des grands progrès et une meilleure qualité de la vie, une bonne concentration, la possibilité de contrôler ses pulsions, ses envies, de comprendre les instincts. De regarder vers l'intérieur.

// Ce qui suit est le dernier passage, c est une situation de "le trésor du zen", texte de maître Dogen commenté par maître Teisen Deshimaru

"A l'endroit où vous avez l'habitude de vous asseoir, étendez une natte épaisse et placez un coussin dessus. Asseyez vous en lotus ou en demi-lotus. Dans pose du lotus, vous placez d'abord votre pied droit sur votre cuisse gauche et votre pied gauche sur votre cuisse droite. Dans la pose du demi lotus vous vous contentez de presser votre pied gauche contre votre cuisse droite. Veillez à desserrer vos vêtements et votre ceinture. Arrangez les convenablement. Placez alors votre

main droite sur votre jambe gauche, et votre main gauche tournée vers le haut sur votre main droite. Les extrémités des pouces se touchent. Asseyez vous bien droit dans l'attitude corporelle correcte. Ni penché à gauche ni penché à droite, ni en avant ni en arrière. Assurez vous que vos oreilles sont dans le même plan que vos épaules et que votre nez se trouve sur la même ligne verticale que votre nombril. Placez la langue en avant contre le palais; la bouche est fermée, les dents se touchent. Les yeux doivent rester toujours ouverts. Vous devez respirer doucement par le nez. Quand vous avez pris la posture correcte, respirez profondément une fois, inspirez et expirez. Inclinez votre corps de droite et de gauche et immobilisez vous dans une position assise stable. Pensez à ne pas penser. Comment pense-t-on à ne pas penser? Non-pensée (hishiryo). Cela en soit est l'art essentiel du zazen."

Attention: Pour arriver à l'état de méditation, il faut absolument éviter d'occuper le cerveau par un processus d'imagerie mentale, comme imaginer des chiffres qui s'écrivent puis s'effacent, ou encore s'imaginer en train de descendre une échelle. En effet, du fait des zones différentes que ces pensées occupent, elles conduisent à un autre état modifié de conscience : la transe légère, également appelé "hypnose Ericksonienne". Mais ceci est une autre histoire...

hdh kms



ESSAI

Dans ce numéro, nous publions le superbe essai de Stalker : "La piste". Vous voudrez bien trouver l'essai sur le CD, à côté du magazine, sous le nom "stalker_la_piste.pdf". si vous utiliser Windows vous devez installer Adobe Acrobat Reader. Si vous utilisez Linux ou MacOS, un programme permettant de visionner le format PDF est inclus en standard. Ce pdf, piètrement mis-en-page --vous m'en excuserez-- est issu du site de Stalker (<http://skarlet.heretik.org>).

Ce texte, publié en 2003, a été complété en 2006 par le texte ci-dessous, nous vous le livrons tel quel, sans commentaires, ni avertissement, bien que le texte y invite. Nous vous invitons à y réfléchir et à nous soumettre votre point de vue et vos suggestions, nous ferons de même et publierons le résultat de nos travaux lors d'un prochain numéro.

Manifeste pour une techno alternative qui survit à elle-même.

ETHIQUE et développement durable des soirées alternatives de musique digitale et autres free parties:

1- Ce rassemblement ouvert à tous est à vocation artistique. Dans un souci de découverte et de diversité, avant garde sonore et histoire du son sont respectées car elles sont intimement liées. Un large champ d'ouverture sur toutes formes de musiques ou d'images animées est donc laissé ouvert.

2 - L'ordre d'apparition des musiques jouées en direct est négligeable, et ce toujours dans un souci d'équité, ainsi que pour marquer et "faire" les différences. La danse n'est pas une priorité. Si le caractère festif est secondaire, c'est pour en assurer sa survie face aux pouvoirs publics. En effet l'histoire nous a montré qu'un laisser-aller festif au détriment de l'artistique provoquait des dérives et de fait, la repression et l'empêchement du mouvement alternatif.

3 - La confidentialité est garantie par les deux premières propositions. Elles limitent le caractère non-engagé du rassemblement (porte ouverte à l'oisiveté ou la surconsommation) tout en laissant le champ libre à la jouissance des sens au travers de l'art, de la sensibilité et du partage des sources et du savoir.

4 - Les artistes invités sont issus de scènes et d'influences diverses, pour garantir la diversité musicale, avec si possible des artistes venus de l'étranger. Les échanges sont nécessaires pour éviter une consanguinité musicale et un formatage de l'écoute au niveau local.

5 - Le prix d'entrée doit être le moins cher possible pour faciliter l'accès aux plus démunis, et toutes actions pour financer les frais logistiques, techniques, ou de déplacement des artistes et techniciens sont recherchés (participation aux frais, donations, subventions, co-

productions).

6 - Le but n'est pas d'avoir le plus de monde possible, ni le plus de sonorisation possible. Le but est de proposer une alternative aux clubs et discothèques, ainsi qu'à la culture de masse imposée par les médias majoritaires, au travers d'une recherche esthétique particulière. Ce positionnement est donc politique, et se doit d'être clairement démontré et rappelé à chaque événement.

7 - Si une des 5 premières propositions n'est pas possible à mettre en place, l'association avec d'autres artistes ou collectifs sera alors nécessaire.

8 - Sur le terrain, les diversités artistiques et écologiques sont des priorités incompressibles. Leur préservation aussi. La transmission d'un savoir acquis est dès lors nécessaire avec les nouveaux arrivants, et ce de quelque manière que ce soit (parole, imprimés, net, et tout support musical).

9 - La recherche artistique doit garantir la sérénité du rassemblement, et ainsi éviter les phénomènes d'agglomération de masse débilante et l'appauvrissement du son qui en résulte.

note d'intention et explication préalables au débat:

Le mouvement free party est mort en France pour différentes raisons, les principales étant paradoxalement ce qui s'avère être les fondements de la rave party:

1- la danse,

2 - la foule

3 - l'envie de ne pas réfléchir de manière rationnelle.

C'est ultra-polémique (nous sommes sur un forum de discussion). Je m'explique:

(...)

1 - la danse. ça veut dire les règles de la danse, règles qui empêchent de donner libre cours à la création digitale tout azimut. règles de la régularité, périodes de modes, refus des musiques non dansantes, donc pas open to all du tout...)

2 - La foule. La foule, comme chacun sait, est une entité un peu bizarre qui génère ses propres modes de pensée. L'individu se perd dans la foule, il s'y adapte, il perd son libre abriter. Ainsi pour rester "dans le coup", un dj, un label, un shop, un sound system, ou un teuffer, préférera s'adapter à l'évolution constante et impersonnelle de la foule. Les publicitaires provoquent ça. Pour la free, ça se fait tout seul. Nul n'est plus responsable qu'un autre...mouton. La foule, c'est aussi le trop grand nombre de touristes venu se défoncer au lieu de vivre de vrais moments alternatifs culturels (ce qui rejoint ce troisième point:)

3- L'envie de ne plus réfléchir de manière rationnelle. Cela veut dire: on veut se droguer tranquillement, sans qu'on vienne nous faire chier tous les quatres matins avec une intellectualisation ou des principes de réalités que je fuis, justement (comme: la recherche de la vérité, l'art, l'équité, la politique, et le plus difficile d'entre tous les principes de réalité, qui rejoint le second et précédent point: la recherche de soi). Cela veut dire aussi : c'est la porte ouverte à tous les abrutis de la planète (encore qu'il faut bien qu'ils aient un endroit à eux, mais est-ce le but?).

Ainsi, il faudrait poser les bases d'un manifeste qui ciblerait les priorités éthiques et artistiques, pour qu'un mouvement alternatif ne dérive pas vers l'armée des petits pois, et un consumérisme amer.

A vous de faire des propositions, de proposer des améliorations, de faire des critiques.

je voudrai brièvement rappeler quelques points.

Ce texte n'est pas là pour rameuter les foules, ni pour faire acte de loi, on n'impose rien à personne.

Simplement il serait, je dis bien il serait, une prise de conscience théorique, un résumé pratique, pour poser les bases d'une synthèse. Cette synthèse serait la juste mesure des problèmes artistiques et humains qui ont conduit la free party à devenir plutôt sordide, et délaissée, puis interdite, car montrée du doigt.

ces problèmes auraient pu, à mon sens, être évités, si

l'intérêt des sounds systems et des DJ's s'était porté sur autre chose que de donner à la foule ce qu'elle veut soit disant entendre. En gros, éviter de reproduire le schéma de la culture de masse imposée par les médias. Ils nous disent que la demande entraine l'offre, alors que tout le monde sait bien aujourd'hui que c'est l'offre qui entraine la demande (par effet de matraquage, comme le ferait une radio à coup de promotion, de publicité. Les esprits s'habituent à ce qu'on leur impose, et ils finissent même par le défendre...).

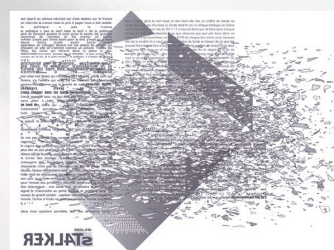
Ainsi ce texte tente de définir humblement ce qu'il serait utile de poser sur le papier pour que tout le monde se mette d'accord sur les priorités.

Et là s'en trouve la subtilité : ce n'est pas une charte, ni un truc pompeux à appliquer. Ce n'est qu'une tentative de trouver un terrain d'entente commun, basé sur LES musiques, et non sur une uniformisation du son. Les points essentiels sur des valeurs de partage, d'entraide, de collaboration, et de respect de l'environnement, sont pour moi secondaires, car ils tombent sous le sens. C'est normal. Le mec qui laisse la clairière propre ne doit pas se prendre pour un héros (encore que...). Non, les point importants sont ceux qui n'ont pas l'air évidents: une diversité musicale radicale, pour donner à penser aux participants, pour sortir grandi d'un rassemblement, et non épuisé et déprimé, violenté par l'absurde des choses. Et ne me dites pas que vous n'avez jamais connu ça. Je vous parle de premières expériences, dans une période fragile 16/25 an. Et je ne parle pas de ne pas faire la fête ou de jouer des trucs intello, non. Je parle d'insufler une force, une intelligence. C'est une utopie théorique. Ce ne sont que des IDEES.

Voilà.

Le résultat de ces discussion ne servira à RIEN. Rien, si ce n'est avoir trouvé un truc qui définirait de manière très SOUPLE, ce qui devrait ne pas se reproduire : la merde fashion, la lobotomie, la consumérisme drogue/musique vide, le laisser aller, et la perte d'une certaine liberté de mouvement.

Le résultat serait de définir les choses, et de les valider. Puis de les échanger.



Stalker

Lta

G33K

#N0uS 3T!onz kuElQueZ l33t_h4cK3rZ
1 package s3RRé 2 g33Kz
A noU Fr4gg3R d4ns D 6unKerz
eT nOuS r3venD!K4nt d'Un1X

h3l4s, L3 T3mPs, c tro p4 kool
1L f0rM4t c: n0s Bra1nz
eR4ze n0s c0nSc1enCes, r0ule
n0s t3tes de l3cTuRe, en ch4iN3z

Et c0m 1 conN3x1oN r00t
m4rke l'4v3NeM3Nt d'l prog
t0uT l3s syst-Mz ke j3 reb00t
0nT l3 parf1 de m3s vieu log
./

BOBARDKOR





JONGLE



NOSTRA SCEÏN QUAND LE FEU RENCONTRE LE SON



QUOI ?

Avec plus d'une trentaine de prestations à leur actif, les jongleurs de Nostra Sceïn se produisent dans toutes sortes d'endroits. Très présents dans le monde des free parties et autres teknivals, ils participent également à des fêtes de quartier, des festivals et des soirées organisées sans oublier le carnaval de Paris. L'association propose deux types de spectacle : l'un chorégraphié et orchestré, l'autre plus « free style ».

Nostra Sceïn organise aussi des ateliers d'initiation au jonglage destinés aux enfants comme aux adultes. Ils fabriquent et vendent également leur propre matériel de jonglage enflammé.

Quand aux photographes ils effectuent de nombreux clichés exploitant allègrement les thèmes du jonglage et du feu.

COMMENT ?

Autogestion, et système D sont les maîtres mots de Nostra Sceïn. Cette asso qui ne rentre dans aucune case se finance entièrement par elle-même. Pas de subventions ni de cachets

exorbitants ! Ils sont là avant tout pour s'amuser et se réunir autour de la flamme, rythmée par la musique qu'ils affectionnent. Les jongleurs de Nostra Sceïn participent à des événements qu'ils aiment et ne font pas « du commercial » comme le souligne Antoine leur président.

POURQUOI ?

Des valeurs qui leur sont propres réunissent les jongleurs autour de leurs passions communes, le feu et la musique techno underground. Le partage et les rencontres rythment la vie de l'association dont les membres sont des acteurs à part entière du mouvement des free party. Ils souhaitent d'ailleurs améliorer l'image de cet univers, souvent décrié mais très peu connu.

Promoteurs de la culture libre, les jongleurs de Nostra Sceïn ne cessent de s'entraîner dans une synergie créative.

QUI ?

Issue du mouvement des free parties, l'association Nostra Sceïn regroupe une vingtaine de jongleurs, sans oublier les 3 photographes de talent qui les suivent au quotidien. L'aventure commence en mars 2005 à l'initiative de deux jongleuses. Leur objectif, développer les arts du feu au sein de la culture techno. Au fil du temps et des rencontres, de nouveaux membres se joignent à elles.

Certains s'en vont, d'autres arrivent mais l'asso continue d'avancer.

[hdh_hln](#)

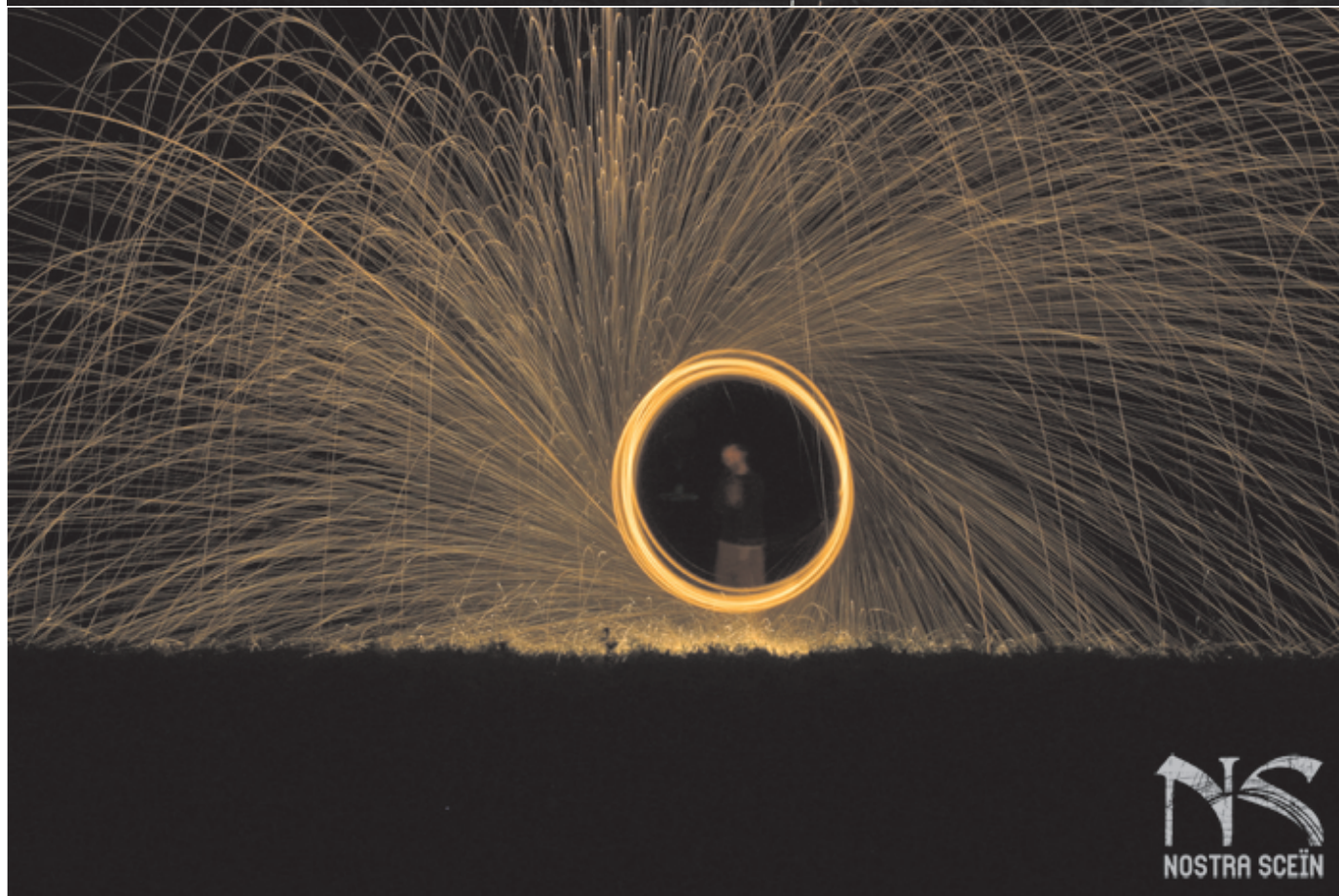




PHOTO



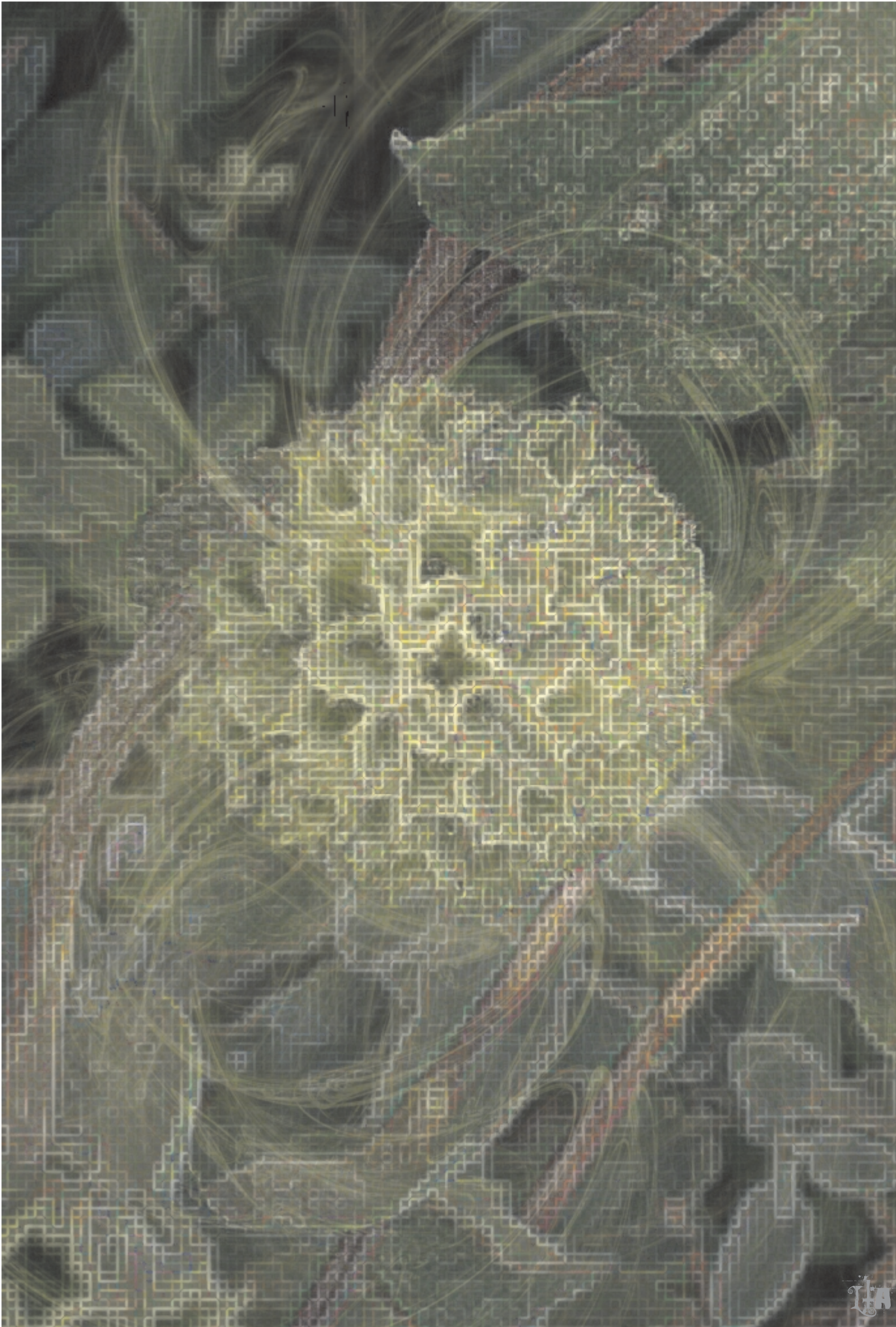
NS
NOSTRA SCEĪN



NS
NOSTRA SCEĪN







Encyclopédie symbolique

FreeTekno

L'encyclopédie symbolique des mouvances freetekno a pour objectif d'explorer certains symboles et mots récurrents dans ces cultures. Nous entamons ici une série de courts articles, dans chacun d'entre eux vous découvrirez certains symboles et l'interprétation que nous en avons. N'hésitez pas à prendre contact si vous souhaitez y participer en explorant certaines symboliques, ou d'autres cultures.

Farfadet :

Le farfadet tient une place de choix dans l'imaginaire et la culture des free party. C'est un petit être farceur et joyeux souvent représenté tout habillé de vert avec un chapeau pointu. Dans la littérature et les légendes françaises, c'est une sorte de génie domestique toujours souriant jamais malfaisant ; au service des hommes. Il se place au même titre que les korriganes ; les lutins, les elfes et les fées dans un imaginaire et un folklore millénaire tout comme dans la culture celte, fortement représentée par les bretons particulièrement actifs dans le milieu des free party. Sans doute est-il le préféré des teufeurs car il fait référence à la nature, plus particulièrement à la forêt dans lesquelles se déroulent bon nombre de fêtes clandestines. Le farfadet s'est fait sacralisé dans un livre désormais bien connu dont l'origine est source de doute, nombre de légendes urbaines existent à ce sujet mais on peut néanmoins croire que l'auteur est Tetrips, avec l'histoire du farfadet, tirée du film Le créateur d'Albert Dupontel.

Si ce personnage touche le public techno c'est car il fait appel à de nombreuses références communes à cette culture, comme le côté caché, underground du farfadet débrouillard et rigolard. C'est un thème récurant autour duquel sont construits de nombreux décors devant le son. Le farfadet inspire également un style vestimentaire avec la création de robes et de pulls aux capuches longues et pointues. Une chose est sûre même perdu dans la lande le farfadet tout comme le teufeur ne s'arrête pas de danser.

[hdh hln](#)

Le Magicien aveugle :

C'est un symbole qu'on peut trouver parfois dans certaines visualisations, décorations ou simplement dessins personnels. Le magicien évoque l'artiste, sous différentes formes : musicien, mais aussi jongleur, ..., ainsi que ... le danseur. (cf. Magie). L'absence d'yeux quant à elle évoque la recherche du regard de l'artiste pour celui qui profite de son art. L'image a une dimension particulière ds le rapport qui unit le musicien, qui regarde ses machines ou ses platines, au danseur, qui voyage seul dans l'univers offert par le musicien. La danse dans la freetekno est une expérience introspective et solitaire qui veut

briser la règle selon laquelle on existe dans le regard d'autrui. Malgré tout il arrive parfois (souvent ?) que l'on recherche l'existence dans le regard du musicien, ce qui est rarement possible, ainsi le magicien n'a pas d'yeux (visibles) et le danseur doit chercher son existence en lui-même.

D'autre part, le magicien existe pour lui-même et joue pour lui-même.[...]

[hdh Ita](#)

Magie :

Ce symbole n'a rien de très spécifique à la freetekno mais il me semble nécessaire de l'explicitier à des fins de complétude. La magie dans la littérature est une allégorie de la création artistique. Elle trouve sa justification dans la fosse qui parfois sépare l'artiste de l'amateur. Ainsi pour ce dernier les étapes qui mènent de la volonté à la réalisation sont obscures voire inconnues, et apparaissent donc comme une seule étape : une matérialisation dans le monde sensible de la pensée de l'artiste, de la magie en somme.

[hdh Ita](#)

Noize is Silence :

Le réveil sonne, et on se lève. Le gaz, la cafetière ou le four à micro-onde nous préparent un petit déjeuner. On sort dehors, les voitures crachent et toussent, des gens parlent. Il y a, ou pas, des travaux pas très loin. Au travail, ou au bahut, ce sont les autres qui vivent : ça gratte, toque, parle ou crie, ça ronronne en dessous, rit au dessus. On met la radio pas très loin. Le midi ce sont les couverts qui tintinabulent, puis encore les transports ? L'après-midi n'est pas plus calme, car c'est un bébé qui pleure, un chien qui aboie, la sirène des pompiers qui déchire le réel. Que ce soit l'ordinateurs, les outils ou les stylos et papiers, il n'est pas plus de silence que le soir avec la télé. Le silence n'existe plus, ce n'est plus qu'un concept. Où donc le retrouver ? En soirée ! Devant les enceintes, au milieu d'un son que l'on a choisi, on retrouve la sérénité du silence, la paix intérieure. C'est faire le choix du support de notre introspection. Faire un putain de bruit, c'est rejoindre le plus doux silence. Alors pour prêcher par la redondance, je vous le dit : "Noize is silence".

[hdh Ita](#)

Cette protection est très puissante, car elle empêche toute exécution de code 'injecté' dans un processus. Ainsi on s'assure qu'il n'y a vraiment que les sections '.text' des programmes chargées par le système qui seront exécutées par le processeur.

2.2/ L'Address Space Layout Randomisation

Cela rend aléatoire toutes les adresses virtuelles des sections à l'exécution. Ce qui est sensé empêcher les exploitations de types 'return to libc' qui font exécuter du code déjà chargé dans une zone exécutable. Il n'est ainsi plus possible de prédire l'endroit où seront chargées les données.

Démonstration :

```
-----8<-----8<-----8<-----8<-----
int main(int argc, char *argv[]) {
    printf("Affichage des adresses de différentes zones
           mémoire\n");
    printf("stack: %p\nheap: %p\ntext: %p\n", &argc,
           malloc(1024), main);
}
```

Si vous exécutez plusieurs fois ce programme sur Netbsd par exemple, les adresses seront fixes, donc prédictibles.

Note: sur linux ia32, depuis la version 2.6.12 les adresses virtuelles sont aussi rendues aléatoires par default. On peut désactiver cette protection en exécutant dans un shell administrateur 'echo 0 >

/proc/sys/kernel/randomize_va_space'. La randomization fournie par PaX est bien plus complète, et randomize au minimum 6 bit de plus (au total 16 bit au minimum, 23 pour la stack). Sur une adresse de la pille, 23 bits sont ainsi rendus aléatoires à chaque exécution (8.4 millions de possibilités).

2.3/ 'Memory Sanitize'

D'après la documentation, le kernel détruit les pages au moment de leur suppression. Ce qui est une avancée en terme de sécurité, en effet dans la mémoire, volatile ou persistante, la suppression d'un élément n'entraîne en général que la déréférencement (pas de destruction physique des données).

L'activation de cette option permet donc en théorie la destruction des données sensibles (les mots de passes décryptés, les mails, les numéros de cartes bancaires, ... tout ce qui est manipulé par le système) au moment de leur suppression (i.e. lorsqu'elles ne sont plus utilisées).

'The tradeoff is performance impact, on a single CPU system kernel compilation sees a 3% slowdown' ...

Note: la destruction des pages utilisées dans une interruption (in_interrupt()), est effectuée par un appel à la fonction fast_clear_page.

2.4/ 'Prevent invalid userland pointer dereference'

Cette option ajoute des protections contre certains types de fautes kernel, de la famille des null pointer dereference.

#file: 0x01/docs/unusual_bugs.pdf#

2.5/ Impact sur les performances négligable

La sécurité apportée face à une perte de performance quasiment nulle (de 1 à 10%) l'emporte largement.

Personnellement je l'utilise avec toutes les fonctionnalités et il n'y a pas de réelle différence.

#link: <http://www.pjvenda.org/linux/doc/pax-performance/#>

3/ Installation

Il s'agit dans cette partie de recompiler un kernel linux 2.6 patché avec PaX.

3.1/ System linux

Grosso modo, au chargement d'un programme ELF, le loader du kernel va chercher dans le fichier comment appliquer PAX. Pour cela il y a deux possibilités, soit via une section spéciale dans le 'program header', soit via un 'legacy ELF header marking'.

L'idéal est d'avoir un système dit 'hardened'. C'est à dire compilé avec un toolchain spécial (gcc patché PIE-SSP), qui permet à tous les programmes de profiter pleinement de PaX. Les distributions majeures sont gentoo-hardened et adamantix basée sur debian. Dans un tel système, tous les programmes marcheront sans problème avec toutes les restrictions pax, et bénéficieront d'une section PT_PAX_FLAGS.

Sinon vous pouvez utiliser une distribution 'normal' de type gentoo, debian edge, ubuntu edgy/feisty. Dans ce cas vous utiliserez le 'legacy ELF header marking' qui est marqué comme 'deprecated'. Si les packages sont suffisamment récents, il ne devrait pas y avoir trop de problèmes.

3.2/ Compilation d'un kernel 'vanilla'

-il vous faut: apt-get install make gcc libncurses5-dev bzip2 lftp links2

-ensuite il faut télécharger 'The latest stable version of the Linux' sur kernel.org (2.6.20.4 à la rédaction de l'article)

```
$ lftp kernel.org #et 'd' sur le lien F
```

```
$ tar xjpf linux-2.6.20.4.tar.bz2
```

```
$ cd linux-2.6.20.4
```

-il faut charger une config de noyau, plusieurs choix s'offrent à vous:

- * vous ne mettez que le strict minimum et pour chaque option cherchez dans l'help 'If unsure chose x'

- * vous avez un fichier /proc/config* qui correspond à la config de votre kernel

```
zcat /proc/config.gz > MYCONFIG
```

(...)

* vous utilisez le kernel fournit par votre distribution, vous trouverez sa config dans le répertoire /boot

* enfin vous pouvez compiler un kernel de test pour qemu, dans ce cas utilisez la config suivante

#file: 0x01/configs/qemu-2.6.20.4.config#

-quand vous avez le fichier de config copiez le dans le repertoire des sources linux et chargez le avec

```
$ make menuconfig
```

-quand la configuration est bien sauvegardée, vous pouvez lancer la compilation du kernel :

```
$ make bzImage
```

-puis les modules

```
$ make modules
```

```
$ make modules_install
```

-ensuite il faut copier le kernel dans le bootloader et créer un nouvelle entrée pour ce kernel (copier coller l'ancienne et changer juste le nom du kernel par le votre

```
$ cp arch/i386/boot/bzImage /boot/mykernel
```

```
# sur ia32
```

```
$ cp arch/x86_64/boot/bzImage /boot/mykernel
```

```
# sur amd64
```

-redémarrer et vérifier que cela marche

3.3/ Patch pax

Maintenant on va patcher les sources de votre kernel avec PaX

-links2 grsecurity.com/test.php

dans la liste des liens prenez le patch correspondant a la version de votre kernel (pax-linux-2.6.20.4-test11.patch)

-appliquez le patch

```
$ cd linux-2.6.20.4
```

```
$ cat /path-to-patch/pax-linux-2.6.20.4-test11.patch | patch -p1 -s
```

```
$ # rien ne devrait apparaitre
```

-activez les fonctionnalités pax (vous pouvez utiliser: #file: 0x01/configs/qemu-2.6.20.4-pax11.config#

```
$ make menuconfig
```

```
---8<-----8<-----8<-----8<-----
```

Security options -->

PaX -->

[*] Enable various PaX features

Pax Control -->

[] Support soft mode // a cocher si ca ne boot pas

[*] Use legacy ELF header marking // a cocher sur un system non hardened

[] Use ELF program header marking // a cocher sur un system hardened

MAC system integration (none) // a cocher si pax est controlé par un system

mandataire tel que RSBAC

Non-executable pages: -->

[*] Enforce non-executable pages // NX bit

[] Page based non-executable pages // a cocher sur amd64

[*] Segmentation based non-executable pages // a cocher sur ia32

[] Emulate trampolines // utilisé par certain soft

[*] Restrict mprotect() // restriction supplémentaire

[*] Disallow ELF text relocations // restriction supplémentaire

[] Enforce non-executable kernel pages // cf ci-dessous

Address Space Layout Randomization -->

[*] // il faut tous les cocher

Miscellaneous hardening features: -->

[*] Sanitize all freed memory

[*] Prevent invalid userland pointer dereference

```
//Pour pouvoir activer le NX bit kernelland c'est un peu plus compliqué, voici les pré-requis:
//sur 2.6, d'après l'aide : 'Depends on: PAX && PAX_NOEXEC && X86_32 &&
!HOTPLUG_PCI_COMPAQ_NVRAM && !PCI_BIOS && !EFI && !COMPAT_VDSO && X86_WP_WORKS'
//sur 2.4, d'après le fichier arch/i386/config.in:
//      "$CONFIG_MODULES" != "y" -a \      # pas de modules
//      "$CONFIG_HOTPLUG_PCI_COMPAQ_NVRAM" != "y" -a \ # pas de nvram
//      "$CONFIG_PCI_BIOS" != "y" -a \      # PCI access mode (Direct)
//      "$CONFIG_X86_WP_WORKS_OK" = "y" ]; then '      # i386
//Cette option ne marche pas avec qemu, et est très restrictives, libre à vous d'essayer de la
faire marcher
---8<-----8<-----8<-----8<-----
```

-recompiler le kernel et les modules

```
$ make clean bzImage
$ make modules
# make modules_install
```

-Pour tester dans une vm qemu avec un système minimaliste fait maison (mikro) #file: 0x01/binaries/mikro32.gz#

```
--8<-----8<-----8<-----8<-----
mkdir test-pax; cd test-pax
qemu-img create hda 400M
qemu -kernel-kqemu -M pc -kernel /path-to-kernel/bzImage -hda root -net nic -net -append
"root=/dev/ram0 ro initrd=mikro32.gz pci=nobios" -initrd /path-to-mikro/mikro32.gz
    fdisk /dev/hda
    mkfs.ext3 /dev/hda1
    mount /dev/hda1 /mnt
---8<-----8<-----8<-----8<-----
```

3.4/ Personnaliser le système

3.4.1/ Obtenir des informations sur les binaires de votre distribution

```
$ apt-get install chpax pax-utils
#link: gentoo.org/proj/en/hardened/pax-utils.xml#
```

Chaque programme peut avoir 6 flags:

P protection au niveau des pages
S protection au niveau des segments
E emulation des trampolines (rarement utilisé)
M enforcement de mprotect (une fois une zone protégée, ses attributs ne sont plus modifiables)
R \ randomization

```
---8<-----8<-----8<-----8<-----
```

```
/dev/shm$ ./test_NX
```

```
Killed
```

```
/dev/shm$ dmesg | tail -n 4 | nl
```

```
1 PAX: execution attempt in: <anonymous mapping>, 2157e000-2157f000 00000000
2 PAX: terminating task: /dev/shm/test_NX(test_NX):14366, uid/euid: 1000/1000, PC: 2157e000,
SP: 587c010c
3 PAX: bytes at PC: cc ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
4 PAX: bytes at SP-4: 587c0168 0b3f17e0 00000000 00001000 00000003 00000022 ffffffff 00000000
216b2dac 0b3f18ea 0b3f2fcc 00000000 587c0148 21597760 00000001 587c01b4 0b3f2ee0 2157e000
8ec4b69c 216b2dac 0b3f1880
```

```
---8<-----8<-----8<-----8<-----
```

X / des adresses virtuelles

Si la lettre est en majuscule alors la protection est appliquée. L'idéal est que tout les programmes aient peMRSX

3.4.2/ Comment PaX agit ?

PaX protège de plusieurs façons.

La plus courante est qu'il envoie un signal SIGKILL au processus et log à l'aide de printk() le motifs.

Par exemple avec le programme fourni dans la section 3.1 voici ce qui se passe :

(...)

La ligne 1 signale ce qui se passe, ici un 'execution attempt' dans une map anonyme (mmap(0, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS,-1,0)) de l'adresse 2157e000 à 2157f000 (qui correspond bien à 4096 octets)

La ligne 2 indique l'action effectuée, le programme concerné, et affiche le registre d'exécution eip (PC) ainsi que celui de la stack frame eip (SP)

La ligne 3 dump les instructions sur lesquelles le programme a été tué, (ici le 'int \$3' (xcc)) et le reste de la map. Grosso modo, grace à PaX le shellcode d'une tentative d'intrusion serait affiché ici ('cd80' pour 'int \$0x80', '31c0' pour 'xor %eax,%eax', '2f7368' pour '/sh')

La ligne 4 affiche le contenu de la stack frame avec l'eip (ebp - 4).

PaX peut aussi être détecté par le loader C, qui va interrompre l'exécution proprement.

3.4.3/ Modifier le fonctionnement de pax pour chaque programme

#link: <http://www.gentoo.org/proj/en/hardened/pax-utils.xml>

Si vous utilisez le 'legacy ELF header marking' (ubuntu), pour modifier les flags il faut se servir de chpax, sinon utilisez paxctl.

- Pour obtenir les flags PaX de vos programmes vous pouvez utiliser cette commande :

```
$ scanelf -pmx
```

Comme pour la configuration d'un firewall, il est préférable d'enforcer l'utilisation de PaX au maximum, et de gérer après au cas par cas ce qui ne marche plus.

- Pour activer les bons flags de vos programmes vous pouvez utiliser cette commande :

```
# for i in `echo $PATH | sed 's:/\/* /g`;  
do chpax -peRMSX $i; done
```

3.4.4/ Programmes connues pour ne pas fonctionner avec peRMSX

* les drivers GLX Xorg, utilisez de préférence vesa

* mplayer

* libcrypt.so.0.9.7 qu'il faut recompiler avec --noexecutestack

* qemu

En fonction des versions, de l'environnement de compilation les erreurs sont différentes. Il faut essayer différentes combinaisons de protection PaX.

4/ PaX: une solution ultime ?

Pour la petite histoire, initialement il y avait une équipe qui s'occupait de la maintenance du patch. Fournir un patch kernel linux représente en effet un gros travail : de nouvelles versions sortent presque tous les quinze jours... Mais un jour quelqu'un a trouvé une faille critique dans l'implémentation kernel qui a provoqué la scission du groupe. Depuis seul une personne, rattachée à Grsecurity, s'occupe de publier les mises à jours.

Au final PaX fournit une bonne protection contre un grand nombre de failles logicielles. Mais ne protège pas notamment contre les failles logiques, i.e. celles qui ne proviennent pas d'un bug de l'application, mais d'une erreur de conception (comme les remote include en php).

Ceci dit, en sécurité informatique, il n'y pas de remède miracle. Ce qui est recommandé c'est de cumuler des barrières de protections afin de ralentir l'éventuelle progression d'un attaquant sur un système, PaX en est une bonne.

Sans tomber dans la paranoïa il est théoriquement possible de contourner PaX, voici quelques pistes de réflexion:

* Si le programme est mal conçu, et qu'il ne protège pas ces zones mémoire correctement, alors PaX ne pourrait pas empêcher l'exécution de code arbitraire.

* Si l'attaquant a un accès local, il peut tenter de charger son propre code en le mettant dans une librairie utilisateur qui serait chargé par l'application attaquée comme étant du code valide.

* Si le programme peut être manipulé via une faille logique afin de lui faire exécuter légitimement:

- un appel à mmap() sur une zone arbitraire,

- une copie d'un shellcode dans la zone,

- un call de cette zone.

* L'ASLR peut être contournée avec des attaques relatives aux offset des registres (retour indirect dans le shellcode).

#file: 0x01/docs/smackthetack.txt

cheers

\sc - sortez-couvert@no-log.org

Outro : Merci d'avoir partage avec nous ce HDHQ, faise dans des conditions relativement extremes afin de concretiser ce projet vieux de 3 ans. Nous vous invitons a nous rejoindre sur #hdh sur le serveur irc.freetekno.org pour vos commentaires ou si vous voulez contribuer.

Nous vous donnons rendez-vous pour les prochains numeros, bientot, restez connecte.



Remerciements : A kms pour l'impulsion), hi et se pour leur travail et leur motivation, stalker pour avoir accepte que l'on publie ses textes, a pendabadmotherfucker, falcom6tk, bobardkor pour leurs artworks. Et a plonk pour sa reponse a l'appel de derniere derniere minute (woupwoupwoupwoupwoupwoupwoupwoupwoup...) et tout les autres qui se reconnaissent.