

Building Your Digital Forensics Laboratory

Ce texte constitue une introduction technique à la **création d'un laboratoire de criminalistique numérique**, en insistant sur l'importance cruciale de la **pratique réelle** pour maîtriser la cybersécurité. L'auteur privilégie l'utilisation de la **virtualisation de bureau**, avec des outils comme VMware ou VirtualBox, afin de simuler des environnements d'enquête à moindre coût. Une large portion du document détaille l'**installation sécurisée de Kali Linux**, tout en soulignant la nécessité de vérifier l'intégrité des fichiers pour éviter les logiciels malveillants. Les sources présentent également le **mode forensique** et l'utilisation de systèmes délibérément vulnérables, tels que Metasploitable, pour s'exercer aux tests d'intrusion. Enfin, l'ouvrage rappelle l'importance de l'**isolation réseau** pour protéger les infrastructures de production lors des simulations d'attaques.

Quels sont les avantages du mode forensique de Kali Linux?

Le mode forensique de Kali Linux offre plusieurs avantages déterminants pour les spécialistes en criminalistique numérique :

- **Préservation de l'intégrité des preuves** : C'est l'atout majeur de ce mode. Kali est configuré pour que le système de fichiers de la machine hôte ne soit pas modifié. Contrairement à un démarrage classique, le mode forensique **n'accède pas au disque dur** et ne peut pas altérer les données présentes, ce qui permet aux enquêteurs de préserver l'état exact de la machine.
- **Rapidité et efficacité** : Le système est **opérationnel rapidement**, ce qui permet de débiter une investigation sans délai inutile. De plus, il est facile d'effacer toute trace numérique de l'intervention une fois l'enquête terminée.
- **Portabilité et simplicité** : Lorsqu'il est utilisé sur une clé USB, Kali Linux devient extrêmement portable et peut être lancé sur n'importe quel ordinateur compatible en quelques minutes. Une fois l'enquête

finie, il suffit de retirer la clé et de redémarrer pour que le système hôte retrouve son état initial.

- **Personnalisation** : Ce mode permet aux experts d'ajouter des outils et des programmes spécifiques dont ils pourraient avoir besoin pour une mission particulière, au-delà de l'installation standard.

Il est toutefois important de noter que si le mode forensique protège le disque dur, un redémarrage du système peut tout de même **effacer des preuves volatiles**, telles que les données stockées en mémoire vive. De plus, bien que l'accès au disque dur soit désactivé par défaut, ce comportement peut être modifié manuellement, bien que cette manipulation soit complexe à réaliser par accident.

Comment le mode forensique préserve-t-il les preuves volatiles ?

Contrairement à la préservation du disque dur, le mode forensique de Kali Linux présente une limite importante concernant les **preuves volatiles** (comme les données stockées en mémoire vive ou RAM).

Voici les précisions apportées par les sources à ce sujet :

- **Risque de perte lors du démarrage** : Les sources soulignent qu'un simple redémarrage du système, souvent nécessaire pour lancer Kali en mode Live ou Forensique, peut **effacer des preuves volatiles**, notamment les données présentes en mémoire.
- **Focus sur le stockage non volatil** : L'avantage principal du mode forensique est de ne pas accéder au **disque dur** de la machine hôte par défaut. Il est configuré pour ne pas modifier le système de fichiers, ce qui permet de préserver l'état physique des données non volatiles de la machine.
- **Procédure de préservation** : Bien que le mode forensique soit un outil crucial pour les experts, la méthodologie spécifique pour la collecte et la préservation de l'ensemble des données (incluant potentiellement les preuves volatiles avant l'arrêt du système) est traitée plus en détail dans d'autres sections spécialisées, comme le chapitre 6 mentionné dans les sources.

En résumé, si le mode forensique est excellent pour protéger l'intégrité des disques durs contre toute écriture accidentelle, il ne "fixe" pas

magiquement la mémoire vive ; au contraire, l'acte de redémarrer pour entrer dans ce mode risque de supprimer les informations volatiles qui s'y trouvent.

Comment Kali Linux est-il configuré pour ne pas modifier le disque dur ?

Le mode forensique de Kali Linux est configuré pour ne pas modifier le disque dur grâce à plusieurs mécanismes de sécurité intégrés lors de son démarrage :

- **Absence d'installation** : Le système s'exécute en mode « Live » (depuis un CD/DVD ou une clé USB), ce qui signifie que le système d'exploitation n'est pas installé sur le disque dur de l'ordinateur hôte et n'utilise que la mémoire vive.
- **Désactivation par défaut** : Dans ce mode spécifique, Kali Linux est « désactivé par défaut », ce qui empêche toute interaction automatique avec les supports de stockage détectés.
- **Restriction d'accès au système de fichiers** : Le système est configuré pour ne pas pouvoir modifier le système de fichiers de la machine hôte. Par défaut, il n'accède même pas au disque dur, garantissant ainsi que les preuves numériques restent intactes et dans leur état d'origine.
- **Protection contre les erreurs accidentelles** : Bien qu'il soit techniquement possible de modifier manuellement ce comportement pour accéder au disque dur, les sources précisent que cette manipulation est complexe à réaliser. Il est donc très peu probable qu'un enquêteur modifie le contenu du disque par accident.

En résumé, cette configuration permet aux experts de démarrer sur une machine cible, d'utiliser leurs outils et, une fois l'enquête terminée, de simplement retirer le support Live pour que l'ordinateur retrouve son état initial sans qu'aucune trace n'ait été laissée sur le disque.

Quels outils peut-on ajouter en mode personnalisé ?

Grâce à sa nature **personnalisable**, Kali Linux permet aux experts d'intégrer des outils et programmes spécifiques qui ne sont pas inclus dans

l'installation standard afin de répondre aux besoins précis d'une mission. Les sources décrivent plusieurs outils majeurs pouvant être ajoutés ou configurés dans le cadre d'un laboratoire de criminalistique :

- **Analyse de disques et de systèmes de fichiers** : On peut ajouter **The Sleuth Kit** (et son interface Autopsy), une suite d'outils en ligne de commande pour l'analyse forensique de supports de stockage.
- **Analyse de réseaux** : L'installation de **Cisco Snort** permet de mettre en place un système de détection (IDS) et de prévention d'intrusions (IPS) extrêmement personnalisable pour surveiller le trafic réseau.
- **Analyse de logiciels malveillants** : L'ajout du **sandbox Cuckoo** offre un environnement sécurisé et automatisé pour exécuter et analyser des fichiers suspects, en fournissant des rapports détaillés sur leur comportement.
- **Analyse de firmware** : L'outil **Binwalk** peut être utilisé pour détecter du code embarqué ou exécutable dans les images de firmware, ce qui est utile pour trouver des vulnérabilités ou des portes dérobées dans des objets connectés.
- **Collecte de trafic réseau** : L'installation de **TCPdump** est recommandée, par exemple en complément de Cuckoo, pour inspecter et enregistrer l'activité réseau de manière détaillée.
- **Outils d'attaque et de test** : Des frameworks comme **Metasploit** sont utilisés pour tester les vulnérabilités et simuler des exploitations de failles.

Cette capacité de personnalisation permet aux enquêteurs de disposer d'une plateforme portable et parfaitement adaptée aux exigences techniques de leurs investigations.

Qu'est-ce que le framework Metasploit ?

Le framework **Metasploit** est décrit dans les sources comme l'une des **applications de sécurité majeures** conçues pour faciliter les tests de vulnérabilités. Il s'agit d'un outil polyvalent utilisé par les professionnels de la sécurité, les administrateurs réseau et les étudiants pour s'exercer aux techniques d'attaque et de défense.

Voici les aspects clés de ce framework tels que présentés dans les sources :

- **Recherche et sélection d'exploits** : Metasploit permet de rechercher des failles spécifiques par mots-clés (via la commande `search`). Cela aide les experts à associer des vulnérabilités critiques découvertes lors de l'analyse d'un système cible à des exploits exploitables déjà disponibles dans le framework.
- **Interface de commande (msfconsole)** : On utilise généralement la commande `msfconsole` dans un terminal (comme celui de Kali Linux) pour charger le framework et accéder à son invite de commande dédiée.
- **Configuration d'attaques personnalisées** : Pour mener une attaque, l'utilisateur choisit un module d'exploitation (par exemple `use exploit/unix/misc/distcc_exec`) et configure des paramètres tels que l'hôte distant cible (`set RHOST`). Il est également possible de définir le type de **charge utile** (*payload*) malveillante à exécuter après la réussite de l'exploitation.
- **Exécution et compromission** : Une fois configuré, la commande `exploit` lance l'attaque. En cas de succès, le framework peut fournir un **accès shell** au système victime, permettant à l'enquêteur de vérifier le niveau d'accès obtenu et de naviguer dans le système compromis.

Dans le contexte d'un laboratoire de criminalistique numérique, Metasploit est considéré comme un outil précieux pour tester des preuves et des scénarios d'exploitation découverts lors d'investigations. Il est fréquemment utilisé en tandem avec des systèmes volontairement vulnérables, comme **Metasploitable**, pour tester un large éventail de failles de sécurité.

Comment installer Kali Linux sur une clé USB ?

L'installation de Kali Linux sur une clé USB permet de créer une version **portable** et **forensique** du système, idéale pour les interventions rapides. Voici les étapes détaillées pour réaliser cette installation, selon les sources :

1. Préparation

- **Matériel** : Vous avez besoin d'une clé USB d'une capacité minimale de **8 Go**.
- **Téléchargement** : Téléchargez l'image ISO officielle sur le site kali.org/downloads/. L'utilisation d'un client BitTorrent est recommandée pour plus de rapidité.
- **Vérification** : Il est crucial de vérifier l'intégrité du fichier téléchargé en comparant son hachage **SHA-256** avec celui fourni sur le site officiel pour éviter toute corruption ou logiciel malveillant.

2. Procédure selon votre système d'exploitation

Sous Windows

Utilisez un utilitaire dédié comme **Win32 Disk Imager** pour copier l'image ISO sur la clé USB.

Sous macOS et Linux (ligne de commande)

La méthode privilégiée utilise la commande dd. Voici la procédure pas à pas :

1. **Identifier la clé USB** : Branchez la clé et identifiez son chemin d'accès (par exemple /dev/disk2 sur Mac ou /dev/sdb sur Linux) en utilisant diskutil list (macOS) ou sudo fdisk -l (Linux).
2. **Démonter le lecteur** : Avant d'écrire, vous devez démonter la clé. Sur Mac, utilisez sudo diskutil unmountDisk /dev/diskX (remplacez X par le numéro de votre disque).
3. **Écrire l'image** : Utilisez la commande suivante pour créer la copie exacte de l'ISO sur la clé : `sudo dd if=nom_de_votre_fichier.iso of=/dev/diskX bs=1m`.
 - a. *Note sur la taille des blocs (bs=1m)* : Une taille de 1 Mo est fiable, bien que l'opération puisse durer jusqu'à deux heures.
 - b. *Suivi* : La commande dd ne donne pas de retour visuel immédiat. Sous macOS, vous pouvez appuyer sur **Ctrl+T** pour vérifier la progression du transfert de données.

3. Finalisation

Une fois la copie terminée, démontez ou éjectez proprement la clé USB avant de la retirer.

Vous pourrez ensuite démarrer n'importe quel ordinateur compatible à partir de cette clé. Lors du démarrage, il vous suffira de choisir l'option

"Live (forensic mode)" si vous souhaitez effectuer une analyse sans modifier le disque dur de la machine hôte.

Comment installer Snort pour la détection d'intrusions ?

L'installation de **Cisco Snort**, un système de détection (IDS) et de prévention d'intrusions (IPS) open source, nécessite une configuration rigoureuse pour être efficace. Bien qu'il soit plus simple de l'utiliser via la distribution *Security Onion OS*, les sources détaillent une procédure d'installation manuelle sur **Ubuntu Desktop**, recommandée pour sa facilité de gestion via une interface graphique.

Voici les étapes clés pour installer et configurer Snort :

1. Préparation et installation des composants

- **Dépendances** : Commencez par installer toutes les bibliothèques nécessaires (gcc, zlib1g-dev, libpcap-dev, etc.) via la commande `sudo apt install`.
- **Téléchargement et compilation** :
 - Créez un répertoire de travail : `mkdir ~/snort_src && cd ~/snort_src`.
 - Téléchargez et installez **DAQ** (Data Acquisition library) en le décompressant et en utilisant les commandes `./configure && make && sudo make install`.
 - Téléchargez ensuite les fichiers sources de Snort depuis le site officiel, décompressez-les et procédez à l'installation avec `make install`.

2. Configuration du système

- **Bibliothèques et liens** : Mettez à jour les bibliothèques avec `sudo ldconfig` et créez un lien symbolique : `sudo ln -s /usr/local/bin/snort /usr/sbin/snort`.
- **Sécurité** : Pour des raisons de sécurité, créez un utilisateur et un groupe dédiés nommés « snort » afin de ne pas exécuter l'outil avec les privilèges root.
- **Structure des dossiers** : Créez les répertoires nécessaires pour les règles et les journaux (ex: `/etc/snort/rules`, `/var/log/snort`) et attribuez-en la propriété à l'utilisateur snort.

3. Gestion des règles de détection

- **Fichiers de règles** : Créez les fichiers de règles locales, listes blanches et listes noires avec la commande touch.
- **Règles communautaires** : Téléchargez les règles gratuites de la communauté Snort (nécessite un compte pour obtenir un code « OINK ») et installez-les dans /etc/snort/rules.
- **Ajustement pour Ubuntu** : Il est nécessaire de commenter certaines lignes dans le fichier snort.conf (via la commande sed) pour éviter des erreurs spécifiques à l'exécution sur Ubuntu.

4. Configuration réseau et tests

- **Édition de snort.conf** : Modifiez le fichier de configuration pour définir votre réseau domestique (HOME_NET) avec l'adresse IP de votre serveur, et définissez le réseau externe (EXTERNAL_NET) sur any.
- **Mode Test** : Vérifiez que la configuration est valide avec la commande : `sudo snort -T -c /etc/snort/snort.conf`.
- **Test d'alerte** : Ajoutez une règle simple dans local.rules pour détecter le trafic ICMP (ping) et lancez Snort avec l'option -A console pour voir les alertes s'afficher en temps réel.

5. Automatisation

Pour que Snort démarre automatiquement au lancement du système, vous devez créer un script de service dans /lib/systemd/system/snort.service, puis activer le démon avec `sudo systemctl enable snort`.

Comment installer et utiliser le sandbox Cuckoo ?

Le sandbox **Cuckoo** est un système d'analyse automatisée de logiciels malveillants en code ouvert. Il permet d'exécuter des fichiers suspects dans un environnement sécurisé et isolé afin d'observer leur comportement en temps réel.

L'installation de Cuckoo est décrite comme complexe et chronophage. Voici les étapes de configuration et d'utilisation basées sur les sources :

1. Installation du système et des bibliothèques (sur Ubuntu)

Il est fortement recommandé d'utiliser **Ubuntu** pour l'installation, car la majorité de l'assistance et des guides y sont consacrés.

- **Mise à jour et dépendances** : Commencez par mettre à jour votre système, puis installez les bibliothèques Python et de sécurité nécessaires :
 - `sudo apt-get install python python-pip python-dev libffi-dev libssl-dev -y.`
 - `sudo apt-get install python-virtualenv python-setuptools -y.`
 - `sudo apt-get install libjpeg-dev zlib1g-dev swig -y.`
- **Bases de données** : Cuckoo requiert deux bases de données pour fonctionner :
 - **MongoDB** (pour l'interface web) : `sudo apt-get install mongodb.`
 - **PostgreSQL** (pour le suivi des données) : `sudo apt-get install postgresql libpq-dev.`

2. Configuration de l'environnement virtuel

Cuckoo utilise la virtualisation pour exécuter les logiciels malveillants sur des systèmes d'exploitation « invités ».

- **VirtualBox** : Installez VirtualBox (version 5.1 dans l'exemple) en ajoutant le dépôt officiel et en utilisant `sudo apt-get install virtualbox-5.1.`
- **TCPdump** : Cet outil est essentiel pour que Cuckoo puisse enregistrer l'activité réseau détaillée. Après l'installation (`sudo apt-get install tcpdump`), vous devez désactiver le profil AppArmor associé et configurer les permissions pour qu'il s'exécute avec les privilèges appropriés.
- **Utilisateur dédié** : Créez un utilisateur système nommé « cuckoo » et ajoutez-le au groupe vboxusers.

3. Utilisation de Cuckoo

Une fois le système de base installé, vous devez configurer un système d'exploitation invité (comme Windows 7) à l'intérieur de VirtualBox.

- **Soumission de fichiers** : L'utilisation se fait généralement via une **interface web** accessible depuis un navigateur. Vous y téléchargez le fichier ou l'URL que vous souhaitez analyser.
- **Analyse et rapport** : Cuckoo exécute le fichier dans l'environnement isolé et génère un **compte rendu détaillé**. Ce rapport inclut :
 - Les connexions réseau établies.

- Les modifications apportées au registre du système.
- Les fichiers supplémentaires qui auraient pu être téléchargés par le logiciel malveillant.

Alternative simplifiée

Si l'installation locale est trop complexe, vous pouvez utiliser **Malwr** (malwr.com). Il s'agit d'un service en ligne gratuit qui utilise le sandbox Cuckoo pour analyser vos fichiers sans nécessiter de configuration de votre part.

Comment configurer Metasploitable sur un réseau virtuel isolé ?

La configuration de **Metasploitable** sur un réseau virtuel isolé est une étape critique pour la sécurité de votre laboratoire, car ce système est volontairement vulnérable et pourrait servir de point d'entrée à un attaquant s'il était exposé.

Voici les étapes et recommandations pour mettre en place cette isolation, selon les sources :

1. Création du réseau virtuel privé

Vous devez créer un réseau virtuel spécifique au sein de votre hyperviseur (VMware ou VirtualBox).

- **Plage d'adresses** : Les sources recommandent d'utiliser un réseau privé, par exemple le sous-réseau **192.168.99.0/24**.
- **Segmentation** : Assurez-vous que ce réseau est totalement **isolé de votre système hôte** et du reste de votre réseau domestique ou de production.

2. Configuration des cartes réseau des machines virtuelles

Pour que vos outils (comme Kali Linux) puissent interagir avec la cible (Metasploitable) sans risque extérieur :

- **Affectation** : Attribuez une carte réseau à votre machine Kali Linux et une autre à votre machine Metasploitable, toutes deux connectées à ce même réseau virtuel isolé.
- **Une seule interface** : Veillez à ce que chaque machine virtuelle ne dispose que d'**une seule carte réseau** active pour empêcher tout transfert de trafic accidentel vers d'autres réseaux.

3. Restrictions de connectivité

Pour garantir une étanchéité totale du laboratoire :

- **Désactivation du NAT** : Assurez-vous qu'aucune traduction d'adresse réseau (NAT) n'est active pour ces machines.
- **Pas d'accès Internet** : Aucun accès à Internet ne doit être autorisé pour le réseau virtuel isolé.

4. Premier accès à Metasploitable

Une fois la machine virtuelle démarrée dans cet environnement sécurisé, vous pouvez vous y connecter avec les identifiants suivants fournis par les sources :

- **Utilisateur standard** : user / mot de passe : user.
- **Privilèges Root** : msfadmin / mot de passe : msfadmin.

Une fois configuré, vous pourrez utiliser des outils comme **Nmap** depuis votre instance Kali pour identifier les nombreux ports ouverts sur Metasploitable et commencer vos tests d'exploitation en toute sécurité.

Comment analyser un disque avec The Sleuth Kit ?

L'analyse d'un disque avec **The Sleuth Kit** (souvent associé à son interface Autopsy) repose sur une suite d'outils en ligne de commande permettant d'examiner en profondeur les systèmes de fichiers et les images disques.

Pour mener à bien cette analyse, le Kit d'enquête propose une méthodologie structurée en trois phases distinctes :

- **Extraction de fichiers** : Cette première phase consiste à analyser les images disques et les fichiers pour en extraire les informations pertinentes. Les données trouvées sont automatiquement enregistrées dans une **base de données centrale** (SQLite par défaut, ou PostgreSQL), ce qui permet de conserver une trace structurée pour les étapes suivantes.
- **Analyse des fichiers** : Une fois les fichiers extraits, ils sont traités par différents modules spécialisés selon les besoins de l'enquête. Par exemple, le module *HashCalcModule* peut être utilisé pour calculer les hachages des fichiers afin d'en vérifier l'intégrité ou de les comparer à des bases de données de fichiers connus. Les résultats

de chaque module sont également stockés dans la base de données centrale.

- **Journalisation et génération de rapports** : La phase finale permet de compiler les résultats issus des différents modules d'analyse. L'outil génère un **rapport unique fusionné**, ce qui facilite grandement la lecture et l'interprétation des preuves par l'enquêteur par rapport à des rapports fragmentés.

Installation et utilisation sur Kali Linux

The Sleuth Kit est généralement déjà intégré aux versions récentes de Kali Linux. Si ce n'est pas le cas, vous pouvez l'installer via le terminal avec la commande : `apt-get install sleuthkit`.

Une fois installé, chaque outil de la suite s'utilise directement depuis le terminal. Bien que des interfaces graphiques existent, la plupart des experts préfèrent utiliser les commandes directement pour plus de flexibilité. Pour chaque commande spécifique, vous pouvez consulter le manuel détaillé en tapant `man [nom_de_la_commande]` dans votre terminal.

Qu'est-ce que l'application web OWASP Mutillidae ?

L'**OWASP Mutillidae** est une application web **volontairement vulnérable**, conçue pour servir d'outil d'entraînement et de test dans un environnement de laboratoire.

Voici ses caractéristiques principales selon les sources :

- **Objectif pédagogique** : Elle permet aux utilisateurs (étudiants, administrateurs réseau ou professionnels de la sécurité) de tester et de comprendre les techniques utilisées par les attaquants pour exploiter des failles de sécurité.
- **Similitude avec DVWA** : Elle est décrite comme étant similaire à la *Damn Vulnerable Web App* (DVWA). Elle permet de tester bon nombre des mêmes vulnérabilités, mais en utilise des approches légèrement différentes, ce qui offre une perspective complémentaire pour l'apprentissage.
- **Utilisation en laboratoire** : Il est recommandé de l'utiliser comme « machine virtuelle d'attaque » au sein d'un laboratoire de

criminalistique numérique, notamment pour s'exercer avec les outils de la distribution Kali Linux.

- **Accessibilité** : Cette application est disponible en téléchargement gratuit, notamment sur le site SourceForge.

Comme pour tout système volontairement vulnérable, les sources insistent sur l'importance de l'installer dans un **environnement réseau isolé** et déconnecté d'Internet pour éviter qu'il ne serve de point d'entrée à de véritables attaquants.

Comment installer Snort sur Ubuntu Desktop ?

L'installation manuelle de **Cisco Snort** sur **Ubuntu Desktop** est recommandée par les sources pour faciliter la gestion des composants via une interface graphique et l'utilisation d'éditeurs de texte comme Gedit,. Voici la procédure détaillée étape par étape :

1. Préparation du système et dépendances

- **Mises à jour** : Commencez par installer Ubuntu et effectuez toutes les mises à jour système nécessaires.
- **Installation des dépendances** : Exécutez la commande suivante pour installer les bibliothèques requises (gcc, libpcap, zlib, openssl, etc.) : `sudo apt install -y gcc libpcap-dev zlib1g-dev libpcap-dev openssl libssl-dev libnghttp2-dev libdumbnet-dev bison flex libdnet`.
- **Répertoire de travail** : Créez un dossier pour les sources : `mkdir ~/snort_src && cd ~/snort_src`.

2. Compilation et installation

L'installation se fait en deux temps : d'abord la bibliothèque d'acquisition de données (**DAQ**), puis **Snort** lui-même.

- **Installation de DAQ** :
 - Téléchargez l'archive : `wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz`.
 - Décompressez et entrez dans le dossier : `tar -xvzf daq-2.0.6.tar.gz && cd daq-2.0.6`.
 - Compilez et installez : `./configure && make && sudo make install`.

- **Installation de Snort :**

- Revenez dans le répertoire source, téléchargez Snort (ici version 2.9.9.0) et décompressez-le.
- Lancez la configuration et l'installation : `./configure && make && sudo make install`.

3. Configuration du système

- **Liens et bibliothèques :** Mettez à jour les bibliothèques avec `sudo ldconfig` et créez un lien symbolique crucial : `sudo ln -s /usr/local/bin/snort /usr/sbin/snort`.
- **Utilisateur dédié :** Pour la sécurité, créez un utilisateur et un groupe « snort » sans privilèges root,.
- **Structure des dossiers :** Créez les répertoires pour les règles, les journaux et les règles dynamiques, puis attribuez les permissions appropriées à l'utilisateur snort,.
- **Fichiers de base :** Créez les fichiers vides pour les listes blanches, noires et les règles locales, puis copiez les fichiers de configuration (`.conf` et `.map`) du répertoire source vers `/etc/snort`,.

4. Gestion des règles et ajustement pour Ubuntu

- **Règles communautaires :** Téléchargez les règles gratuites (manuellement ou via un code OINK) et installez-les dans `/etc/snort/rules`,.
- **Correctif spécifique Ubuntu :** L'installation par défaut sur Ubuntu cherche des fichiers non inclus dans les règles communautaires. Vous devez commenter ces lignes dans `snort.conf` pour éviter des erreurs au démarrage : `sudo sed -i 's/include \${RULE}_PATH/#include \${RULE}_PATH/' /etc/snort/snort.conf`.

5. Configuration réseau et tests

- **Édition de `snort.conf` :** Modifiez le fichier de configuration pour définir votre réseau domestique (`ipvar HOME_NET`) avec l'adresse IP de votre serveur, et réglez le réseau externe sur `ANY`,.
- **Chemins d'accès :** Vérifiez que les variables de chemin (`RULE_PATH`, etc.) pointent vers les bons répertoires,.
- **Mode Test :** Validez votre configuration avant de lancer le service : `sudo snort -T -c /etc/snort/snort.conf`.

- **Test d'alerte** : Ajoutez une règle de test pour le trafic ICMP dans local.rules et lancez Snort avec l'option -A console pour visualiser les alertes en direct lors d'un ping,,.

6. Automatisation

Pour que Snort se lance au démarrage, créez un script de service dans /lib/systemd/system/snort.service, rechargez le démon système (daemon-reload), puis activez le service avec systemctl enable snort,,.

Comment puis-je configurer un miroir réseau dans Kali?

La configuration du **miroir réseau** est une étape cruciale qui intervient lors du processus d'installation de Kali Linux (Étape 3).

Voici les détails et recommandations fournis par les sources concernant cette configuration :

- **Moment de la configuration** : Cette option vous est proposée parmi une série de questions standard lors de l'**installation graphique** du système.
- **Recommandation** : Il est **vivement recommandé** de configurer un miroir réseau.
- **Utilité** : Le miroir réseau indique à votre système d'utiliser les **dépôts centraux de Kali**. Cela est indispensable pour :
 - Télécharger de nouveaux paquets logiciels.
 - Mettre à jour les logiciels déjà existants.
- **Risque en cas d'omission** : Si vous choisissez de ne pas le configurer, vous risquez de ne pas pouvoir installer de nouveaux outils ni effectuer les mises à jour de sécurité nécessaires.
- **Validation après installation** : Une fois l'installation terminée, vous devez vous assurer que votre machine dispose d'une connexion Internet. Vous pouvez alors finaliser l'opération en ouvrant un terminal et en exécutant la commande suivante pour synchroniser votre système avec les miroirs : apt-get -y update && apt-get -y upgrade.

Les sources insistent sur le fait que de nombreux problèmes techniques rencontrés avec les outils de Kali sont résolus par une simple mise à jour,

rendant cette configuration initiale du miroir réseau d'autant plus importante.

Comment vérifier le hachage SHA-256 de l'image ISO ?

La vérification du hachage **SHA-256** est une étape cruciale pour s'assurer que le fichier ISO téléchargé n'a été ni corrompu lors du transfert, ni altéré par un logiciel malveillant.

Voici comment procéder selon votre système d'exploitation :

- **Sur macOS ou Linux** : La procédure est simple et s'effectue directement dans le terminal avec la commande suivante : `shasum -a 256 emplacement_du_fichier`.
- **Sur Windows** : Il est généralement nécessaire de télécharger un utilitaire spécifique. Les sources recommandent l'outil **MD5 and SHA Checksum Utility** (développé par Raymond), qui permet de calculer et d'afficher facilement l'empreinte numérique du fichier.

Procédure de comparaison

Une fois que vous avez obtenu le hachage de votre fichier local, vous devez le **comparer à celui affiché sur le site officiel de l'éditeur** (kali.org).

Astuce pratique : Pour simplifier la vérification manuelle, il n'est généralement pas nécessaire de comparer chaque caractère. Vérifier que les **quatre ou cinq derniers caractères** correspondent suffit à confirmer, avec une très forte probabilité, que le hachage complet est correct et que votre fichier est intègre.

Qu'est-ce que le mode persistant pour une clé USB Kali ?

Le **mode persistant** (ou *persistence*) pour une clé USB Kali Linux est une option de démarrage qui permet de transformer une simple clé "Live" en une véritable **installation portable**.

D'après les sources, ce mode se distingue par les caractéristiques suivantes :

- **Sauvegarde des modifications** : Contrairement au mode "Live" classique qui démarre systématiquement sur un "système d'exploitation vierge" (où toutes les modifications sont perdues au

redémarrage), le mode persistant permet de conserver les changements effectués.

- **Personnalisation** : Il permet à l'utilisateur d'**ajouter des outils et des programmes spécifiques** qui ne font pas partie de l'installation standard de Kali Linux, adaptant ainsi le système aux besoins précis d'une mission.
- **Variantes disponibles** : Le menu de démarrage de Kali propose deux types de persistance : "**Live USB Persistence**" et "**Live USB Encrypted Persistence**" (le second ajoutant un chiffrement pour sécuriser les données stockées sur la clé).
- **Praticité** : Cette méthode est considérée comme l'une des plus rapides pour disposer d'un système opérationnel et personnalisé en quelques minutes sur n'importe quel ordinateur prenant en charge le démarrage USB.

En somme, si le **mode forensique** (également présent dans le menu de démarrage) est conçu pour ne pas modifier le disque dur de la machine hôte afin de préserver l'intégrité des preuves, le **mode persistant** vise à permettre à l'enquêteur de sauvegarder son propre travail et ses outils personnalisés directement sur sa clé USB.

Quels sont les identifiants par défaut de Metasploitable ?

Pour vous connecter à la machine virtuelle **Metasploitable**, vous pouvez utiliser les deux combinaisons d'identifiants par défaut suivantes :

- **Utilisateur standard** : Le nom d'utilisateur est **user** et le mot de passe est également **user**.
- **Privilèges Root** : Pour obtenir un accès avec les privilèges d'administrateur (root), vous devez utiliser l'identifiant **msfadmin** avec le mot de passe **msfadmin**.

Les sources rappellent qu'il est impératif d'isoler cette machine de votre réseau de production et d'Internet, car sa nature volontairement vulnérable et ses identifiants connus en font une cible facile pour de véritables attaquants.

Comment chiffrer ma clé USB Kali ?

Pour chiffrer votre clé USB Kali Linux, les sources décrivent deux méthodes principales selon que vous utilisez Kali en mode portable (Live) ou que vous l'installez de manière permanente sur la clé :

- **Mode Live avec persistance chiffrée** : Si vous utilisez une clé USB "Live" pour sa portabilité, vous pouvez choisir l'option « **Live USB Encrypted Persistence** » directement dans le menu de démarrage (*boot menu*). Ce mode est conçu pour ajouter une couche de **chiffrement** afin de sécuriser les données, les outils et les programmes spécifiques que vous sauvegardez sur la clé dans votre espace de persistance.
- **Chiffrement lors d'une installation complète** : Si vous effectuez une installation complète de Kali sur la clé USB (comme sur un disque dur), les sources recommandent vivement d'utiliser **l'intégralité du disque chiffré avec LVM** (*Logical Volume Management*) lors de l'étape de partitionnement. LVM est un logiciel qui facilite le redimensionnement dynamique des partitions tout en permettant un chiffrement robuste de l'ensemble du support.

Précautions de sécurité supplémentaires : En complément du chiffrement, il est crucial de ne pas conserver les identifiants par défaut. Les sources précisent qu'il est indispensable de **modifier le mot de passe** « **toor** » (mot de passe historique de l'utilisateur root), car il s'agit d'une faille courante que les attaquants exploitent fréquemment pour compromettre des systèmes.

Quelles sont les différences entre DVWA et Mutillidae ?

D'après les sources, les applications **DVWA** (*Damn Vulnerable Web App*) et **OWASP Mutillidae** sont toutes deux des outils d'entraînement essentiels au sein d'un laboratoire de criminalistique numérique, mais elles présentent des approches complémentaires :

- **Similitudes de fond** : Ce sont deux applications web **volontairement vulnérables** conçues pour permettre aux étudiants et aux professionnels de tester des scénarios d'attaque et de défense dans un environnement contrôlé. Elles permettent de s'exercer sur un large éventail de failles de sécurité courantes.

- **Différence d'approche** : Bien que Mutillidae soit décrite comme étant **similaire à DVWA**, elle se distingue en testant bon nombre des mêmes vulnérabilités mais **d'une manière légèrement différente**.
- **Valeur pédagogique** : Cette différence de méthode est cruciale car elle permet aux utilisateurs de ne pas se limiter à un seul modèle de faille. L'utilisation de Mutillidae en complément de DVWA offre une perspective plus large, permettant de **mieux comprendre la diversité des techniques** réellement utilisées par les attaquants pour exploiter une même catégorie de vulnérabilité.

En résumé, si DVWA est souvent citée comme une référence de base extrêmement vulnérable, Mutillidae constitue un outil supplémentaire précieux pour approfondir sa compréhension technique grâce à ses variantes dans l'implémentation des failles.

Comment changer le mot de passe root par défaut ?

Selon les sources, le changement du mot de passe root par défaut est une étape critique de la sécurisation de votre système, généralement effectuée lors du processus d'installation.

Le mot de passe par défaut

Historiquement, Kali Linux (ainsi que les images de machines virtuelles préconfigurées) était fourni avec les identifiants suivants :

- **Nom d'utilisateur** : root
- **Mot de passe** : toor (soit « root » à l'envers).

Comment effectuer le changement

Le changement s'opère à deux moments principaux selon votre mode d'utilisation :

1. **Lors de l'installation (Étape 3)** : Si vous effectuez une **installation graphique** sur un disque dur ou une machine virtuelle, le système vous posera une série de questions standard. Parmi celles-ci, il vous sera explicitement demandé de **choisir un nouveau mot de passe** pour remplacer l'identifiant par défaut.
2. **Après l'installation** : Bien que les sources ne détaillent pas la commande spécifique pour un changement post-installation (contrairement aux procédures pour Snort ou Cuckoo), il est d'usage

dans les systèmes Linux d'utiliser la commande `passwd` dans un terminal pour modifier le mot de passe de l'utilisateur actuel. *Cette information spécifique à la commande terminal ne provient pas des sources fournies et devrait être vérifiée indépendamment.*

Pourquoi est-ce indispensable ?

Le maintien du mot de passe par défaut constitue une faille de sécurité majeure pour plusieurs raisons :

- **Vulnérabilité aux attaques** : « Toor » est un mot de passe extrêmement courant que les attaquants et les testeurs d'intrusion recherchent systématiquement.
- **Risque de compromission totale** : Les auteurs notent avoir déjà pu compromettre des réseaux entiers simplement en exploitant ce mot de passe par défaut sur un système exposé.
- **Crédibilité professionnelle** : Pour un spécialiste en cybersécurité, il serait particulièrement embarrassant de voir ses propres outils de sécurité compromis à cause d'une négligence aussi élémentaire.

Dans le cadre d'un laboratoire de criminalistique, la **rigueur et la pratique** (comme le soulignent les conseils de l'entraîneur mentionnés en début d'ouvrage) commencent par la mise en place de ces mesures de sécurité fondamentales.

Comment installer l'application OWASP Mutillidae ?

D'après les sources, il n'existe pas de procédure d'installation pas à pas détaillée pour **OWASP Mutillidae** (contrairement à Snort ou Cuckoo), mais le document fournit les informations essentielles pour sa mise en place dans votre laboratoire :

- **Téléchargement** : Vous pouvez télécharger l'application gratuitement à l'adresse suivante :
<https://sourceforge.net/projects/mutillidae/>.
- **Environnement préconisé** : Comme pour les autres systèmes volontairement vulnérables, Mutillidae est généralement utilisé sous forme de **machine virtuelle d'attaque**. Les sources recommandent de l'installer au sein d'un **réseau virtuel privé et isolé** (par exemple,

un sous-réseau de type 192.168.99.0/24 dans VMware ou VirtualBox).

- **Configuration réseau** : Il est conseillé d'attribuer une carte réseau à cette machine virtuelle et de la connecter au même réseau isolé que votre instance Kali Linux.
- **Sécurité impérative** : Il est crucial de **déconnecter cette machine d'Internet**. Étant conçue pour être vulnérable, elle pourrait être découverte par de véritables attaquants et servir de point d'entrée pour compromettre le reste de votre réseau personnel.

En résumé, l'installation consiste à télécharger les fichiers depuis SourceForge et à les déployer sur un système d'exploitation invité (comme Ubuntu ou Windows) configuré dans un environnement virtuel strictement isolé de tout réseau de production.

Comment isoler complètement un réseau virtuel dans VMware ?

Pour isoler complètement un réseau virtuel dans VMware afin de tester des scénarios d'attaque et de défense en toute sécurité, les sources recommandent de suivre une configuration rigoureuse :

- **Logiciel requis** : Pour créer et modifier des réseaux virtuels personnalisés, vous devez utiliser la version **Professionnelle de VMware Fusion** (sur Mac) ou **VMware Workstation** (sur Windows/Linux), car la version de base ne permet pas ces manipulations avancées.
- **Création d'un réseau privé** : Créez un réseau virtuel privé (par exemple, en utilisant le sous-réseau **192.168.99.0/24**) au sein de votre hyperviseur.
- **Configuration des cartes réseau** :
 - Attribuez une carte réseau à chaque machine virtuelle (par exemple, une pour votre instance Kali Linux et une pour votre cible vulnérable comme Metasploitable) et connectez-les à ce **réseau virtuel isolé**.
 - **Important** : Veillez à ce que chaque machine virtuelle ne dispose que d'**une seule carte réseau active** afin d'empêcher tout transfert accidentel de trafic d'une interface à une autre.

- **Restrictions de connectivité :**
 - Assurez-vous qu'**aucune traduction NAT** (*Network Address Translation*) n'est activée pour ce réseau.
 - Vérifiez qu'**aucun accès Internet** n'est autorisé pour cet environnement.

Cette isolation est impérative pour éviter que des attaquants externes ne découvrent vos machines vulnérables et ne s'en servent comme point d'entrée pour compromettre le reste de votre réseau de production. Une illustration de cette configuration d'isolation est présentée dans la **Figure 3-11** des sources.

Comment utiliser l'outil Binwalk pour analyser un firmware ?

Binwalk est un outil spécialisé dans l'**analyse de firmware** qui permet de détecter la présence de code embarqué ou exécutable à l'intérieur d'images binaires. Il est fréquemment utilisé pour identifier des vulnérabilités, des logiciels malveillants ou des portes dérobées dans des routeurs, des caméras ou d'autres objets connectés.

Voici comment utiliser cet outil selon les sources :

- **Format de fichier :** Pour commencer, vous devez disposer du firmware de l'appareil, généralement téléchargé au format **.bin**. L'outil est également capable de traiter d'autres types de fichiers image ou compressés.
- **Exécution de l'analyse :** Dans un terminal (par exemple sous Kali Linux), utilisez l'option **-B** suivie du nom de votre fichier pour lancer l'examen : `binwalk -B nom_du_fichier.bin`.
- **Identification des composants :** Binwalk utilise des signatures (chaînes de caractères spécifiques) pour identifier les différents types de fichiers imbriqués dans l'image. L'analyse permet de voir si le fichier binaire est en réalité un assemblage de plusieurs éléments.
- **Interprétation des résultats :** Le rapport d'analyse détaille les sections trouvées. Par exemple, il peut révéler des zones de **données compressées (gzip)**, des **systèmes de fichiers (squashfs)** ou des architectures spécifiques comme des en-têtes de firmware TRX.

- **Reconnaissance de logiciels connus** : L'outil peut identifier si une partie du firmware utilise des solutions open-source connues, comme **DD-WRT**, ou s'il contient des éléments graphiques spécifiques au fabricant.

En résumé, Binwalk sert de scanner pour "voir" à l'intérieur d'un fichier binaire opaque et comprendre sa structure, ce qui constitue une étape essentielle avant d'utiliser d'autres outils pour extraire ou décompresser ces données.

Qu'est-ce que l'utilitaire Win32 Disk Imager pour Windows ?

L'utilitaire **Win32 Disk Imager** est un outil spécifique aux systèmes d'exploitation **Windows** utilisé pour la création de supports amovibles amorçables.

Selon les sources, ses caractéristiques et fonctions principales sont les suivantes :

- **Création de clés USB bootables** : Il permet de créer une clé USB amorçable à partir d'une image ISO, comme celle de Kali Linux.
- **Équivalent de la commande dd** : Dans le cadre de la mise en place d'un laboratoire de criminalistique, il remplit sous Windows la même fonction que la commande dd utilisée sur les systèmes macOS et Linux pour écrire une copie exacte d'une image disque sur un périphérique de sortie.
- **Exigence matérielle** : Pour réaliser cette opération avec Kali Linux, l'utilisation de cet outil nécessite une clé USB d'une capacité minimale de **8 Go**.
- **Disponibilité** : L'utilitaire est disponible au téléchargement à l'adresse suivante : <https://launchpad.net/win32-image-writer>.

Cet outil est essentiel pour les experts qui souhaitent disposer d'une **installation portable et forensique** de Kali Linux, leur permettant de démarrer un ordinateur cible sans en modifier le disque dur.

Qu'est-ce que l'outil de virtualisation Samurai WTF ?

Le **Samurai WTF** (*Samurai Web Testing Framework*) est un framework de test web utilisé comme système d'exploitation volontairement vulnérable dans un environnement de laboratoire.

Voici les points clés le concernant selon les sources :

- **Objectif** : Il est conçu pour permettre aux utilisateurs d'apprendre à réaliser des démonstrations et à **analyser les vulnérabilités** web dans un cadre contrôlé.
- **Atouts pédagogiques** : Bien qu'il soit moins répandu que d'autres outils comme Metasploitable ou DVWA, son principal avantage réside dans la qualité de ses **tutoriels et cours d'accompagnement**.
- **Disponibilité** : Ce framework est disponible en téléchargement gratuit sur le site **SourceForge**.

Comme pour les autres machines virtuelles d'attaque, il est fortement recommandé de l'utiliser au sein d'un réseau virtuel strictement isolé pour éviter tout risque de sécurité.

Comment installer Snort via le système Security Onion ?

L'installation de **Snort** via la distribution **Security Onion OS** est la méthode vivement recommandée par les sources en raison de sa simplicité.

Voici les points clés concernant cette méthode d'installation :

- **Facilité d'utilisation** : Snort est considéré comme facile à configurer et à exécuter sur Security Onion par rapport à une installation manuelle.
- **Automatisation** : Ce système d'exploitation intègre un **assistant** et des **scripts** dédiés qui simplifient grandement l'ensemble du processus de configuration de Snort.
- **Recommandation pédagogique** : Bien que Security Onion facilite la tâche, les sources conseillent tout de même d'effectuer une installation manuelle (sur Ubuntu par exemple) au moins une fois. Cela permet de mieux comprendre les mécanismes internes de l'outil et de savoir où modifier les configurations spécifiques en cas de besoin.

En résumé, l'installation sur Security Onion se fait de manière guidée grâce aux outils intégrés, ce qui évite la complexité de la compilation et de la configuration manuelle des nombreux fichiers et dépendances du système.

Quels sont les outils d'analyse de firmware recommandés ?

L'outil d'analyse de firmware principalement recommandé et détaillé dans les sources est **Binwalk**.

Voici les informations clés concernant cet outil et son utilisation :

- **Fonction principale** : Binwalk permet de déterminer la présence de **code embarqué ou exécutable** à l'intérieur des images de firmware.
- **Applications concrètes** : Il est particulièrement efficace pour détecter des vulnérabilités, des logiciels malveillants ou des portes dérobées dans des appareils tels que des **routeurs**, des **caméras** et divers **objets connectés** (IoT).
- **Mécanisme de détection** : L'outil utilise des chaînes de caractères spécifiques (signatures) pour identifier de manière unique les différents types de fichiers qui composent l'image binaire.
- **Formats pris en charge** : Il est couramment utilisé avec des fichiers au format **.bin**, mais il est également capable d'analyser d'autres types de fichiers, notamment des fichiers image ou des fichiers compressés.
- **Capacités d'analyse** : Lors d'un examen, Binwalk peut révéler qu'un firmware est en réalité un assemblage de plusieurs éléments, tels que :
 - Des données compressées (ex: **gzip** ou **LZMA**).
 - Des systèmes de fichiers (ex: **squashfs**).
 - Des images de firmware open-source connues, comme **DD-WRT**.
- **Complémentarité** : Une fois que Binwalk a identifié les différentes parties d'un firmware, les sources indiquent que d'autres outils peuvent être utilisés pour séparer et décompresser ces fichiers spécifiques afin de poursuivre l'investigation