# Documentation Installation

## CYBERHAWK

### DOCUMENTATION INSTALLATION

# SOMMAIRE

# 1. Introduction

## 1.1 Définitions

**ANTIVIRUS** Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants (dont les virus informatique).

**CHIFFREMENT** Le chiffrement (ou cryptage) est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement.

**CYBERHAWK** Solution NÉOSOFT de SAS de décontamination.

**DEBIAN** Debian GNU/Linux est une distribution spécifique du système d'exploitation Linux disposant de nombreux paquets.

**FIREWALL** Un pare-feu (de l'anglais Firewall) est un logiciel et / ou un matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Il mesure la prévention des applications et des paquets.

**LOG** Le terme log désigne un historique d'événements et par extension le fichier contenant cet historique.

**SAS** Le SAS est un dispositif qui permet de passer d'un lieu à un autre, d'un environnement à un autre.

## 1.2 Abréviations

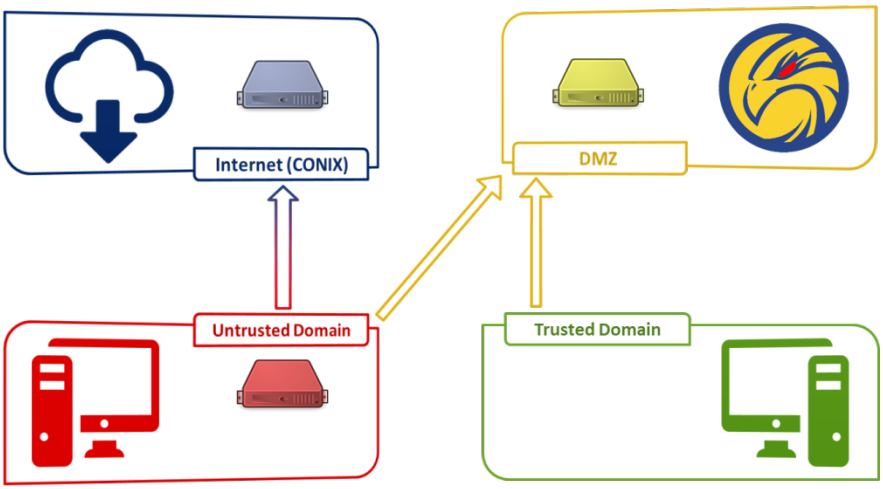
| | |
|---|---|
| **AMD** | Advanced Micro Devices |
| **APT** | Advanced Package Tool |
| **AV** | Antivirus |
| **BDD** | Base De Données |
| **CD** | Compact Disk |
| **CPU** | Central Processing Unit |
| **DHCP** | Dynamic Host Configuration Protocol |
| **DMZ** | DeMilitarized Zone |
| **DVD** | Digital Versatile Disc |
| **EN** | English |
| **FR** | Français |
| **FW** | Firewall |
| **GHZ** | Gigahertz |
| **Go** | Gigaoctet |
| **GRUB** | GRand Unified Bootloader |
| **HDD** | Hard Disk Drive |
| **HTTP** | HyperText Transfer Protocol |
| **HTTPS** | HyperText Transfer Protocol Secure |
| **ID** | IDentifier |
| **IP** | Internet Protocol |
| **ISO** | International Organization for Standardization (ISO 9600) |
| **MAJ** | Mise-A-Jour |
| **MBPS** | MegaBits Per Second |
| **MD5** | Message Digest 5 |
| **MySQL** | My Structured Query Language |
| **NT** | New Technoogy |
| **NTLM** | NT Lan Manager |
| **OS** | Operating System |
| **OVH** | On Vous Héberge |
| **RAM** | Random Access Memory |
| **RO/RW** | Read Only / Read Write |
| **SI** | Système d'Information |

| | |
|---|---|
| **SHA-1** | Secure Hash Algorithm 1 |
| **SSH** | Secure Shell |
| **TCP** | Transmission Control Protocol |
| **TXT** | Texte |
| **URL** | Uniform Resource Locator |
| **USB** | Universal Serial Bus |

# 2. Préambule

## 2.1 Rôle de la documentation

Ce document décrit les procédures d'installation des différents serveurs utilisés pour la plateforme CyberHawk. Chaque installation (logique) de plateforme est détaillée pas à pas dans ce manuel. L'installation physique n'est en revanche pas couverte.




Trois serveurs sont pour l'instant utilisés, dont deux à réinstaller pour chaque nouveau client. Le **Serveur miroir** n'est à réinstaller qu'en cas de panne.

**Serveur Principal CyberHawk**

*Ce serveur est composé d'un système Debian, d'un Firewall local et d'une sécurité renforcée. Il permet l'hébergement des services nécessaires à CyberHawk et propose une interface Web aux utilisateurs du service.*

**Serveur miroir**

*Ce serveur est composé d'un système Debian, d'un Firewall local et d'une sécurité renforcée. Il permet le stockage des mises-à-jour (Antivirus, Signatures Antivirales) après les avoir téléchargées sur les différents sites éditeurs. Les mises-à-jours sont ensuite packagées (conteneur chiffré) pour chaque client.*

**Serveur de mises-à-jour CyberHawk**

*Ce serveur est composé d'un système Debian, d'un Firewall local et d'une sécurité renforcée. Il permet l'obtention des mises à jour CyberHawk (Antivirus, Signatures Antivirales, Code Source) depuis le **Serveur miroir**. Une fois téléchargées, les mises-à-jour sont envoyées vers le **Serveur Principal CyberHawk**.*

En supplément, un système de type « Kiosque » ou « Borne Libre-Service » peut être demandée par le client. Une partie dédiée permet de détailler l'installation logique de cette borne.

### 2.2 Gestion des « Mots de passes »

Tout au long de cette documentation et de son application, des mots de passes vont être demandés.

Qu'ils soient créés de façon automatique ou non, ces mots de passes doivent respecter les bonnes pratiques de sécurité (8 caractères au moins en alternant chiffres, lettres majuscules, lettres minuscules et caractères spéciaux).

- *Exemple de mauvais mot de passe : Toto2016*
- *Exemple de mot de passe robuste : Ai@9Pr66?E9J6n8Xtroo4znS*

Aucun mot de passe ne sera proposé ou suggéré dans la documentation, car chaque mot de passe doit être unique à un système et / ou logiciel. Un mot de passe n'est pas choisi en fonction d'un client. Tout au long de l'application de la procédure, lorsqu'un mot de passe sera à choisir, il se trouvera sous la forme suivante : $PASS$.

La personne en charge de l'installation est garante du respect de ces règles pour les différents mots de passes et doit tenir à jour, tout au long des installations, un document sécurisé (conteneur chiffré de mots de passe par exemple).

### 2.3 Ordre d'installation

Pour que les systèmes fonctionnent correctement, aucun ordre d'installation n'est à respecter. Néanmoins et pour gagner du temps lors de l'installation tout en évitant les « allers-retours » entre systèmes, il est conseillé de suivre l'ordre décrit par cette documentation.

### 2.4 GitHub NÉOSOFT

NÉOSOFT met à disposition un répertoire GitHub dédié à CyberHawk et utilisé pour stocker tous les fichiers nécessaires à l'installation des différents serveurs.

***Important :*** Les scripts de configuration récupérés à l'aide du '**`git clone`**' permettent d'effectuer la configuration finale des serveurs. Ces scripts ayant besoin des informations réseau clients, il convient de les télécharger avant l'installation physique mais de les exécuter après.

## 3. Installation Système (Debian)

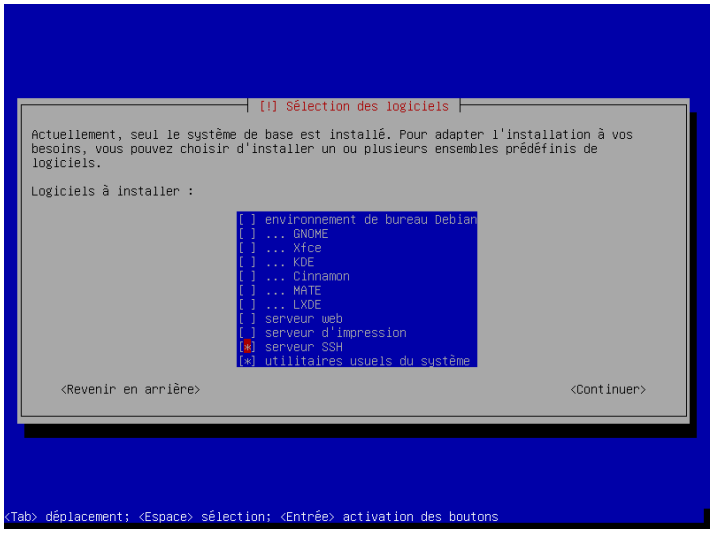
L'installation des systèmes d'exploitation (Debian) est un point redondant de cette documentation puisque qu'elle s'applique à l'ensemble des trois serveurs. Par conséquent, ce

chapitre couvrira uniquement l'installation / configuration minimale à respecter lors de l'installation. Des références seront créées dans les autres parties de ce manuel.

## 3.1 Système de base

Après avoir provisionné le matériel, il est possible d'installer le système Debian en utilisant les ***derniers*** fichiers ISO fournis sur le site de l'éditeur. L'installation du système par le réseau est préférable afin d'installer des paquets à jour en toute simplicité.


Lors de l'installation, il est nécessaire de désactiver tout ce qui n'est pas utile pour le système (Bureau, BDD, WEB, etc.). Les paquets seront installés manuellement, si nécessaires. Ne laisser que le « *serveur SSH* » et les « *utilitaires usuels du système* ».




Enfin, terminez l'installation en activant « GRUB » sur le secteur d'amorçage du disque. Vous pouvez maintenant redémarrer votre système.

## 3.2 Configuration réseau

La configuration réseau dépend des spécificités de chaque client et doit être mise en place une fois les serveurs installés physiquement.

Pour chaque serveur, les questions suivantes doivent trouver réponse avant l'installation de la plateforme :

- *Serveur Principal CyberHawk*
  - *Mode d'attribution IP [Statique / Dynamique DHCP]*
  - *IP réservée [@IP / Masque Réseau / Passerelle]*
- *Serveur de mises-à-jour CyberHawk*
  - *Mode d'attribution IP [Statique / Dynamique DHCP]*
  - *IP réservée [@IP / Masque Réseau / Passerelle]*
  - *Mode d'accès à Internet [Direct / Proxy Interne / NTLM / Autre]*
- *Poste de travail « Libre-Service / Kiosque »*
  - *Mode d'attribution IP [Statique / Dynamique DHCP]*
  - *IP réservée [@IP / Masque Réseau / Passerelle]*

***Note :*** L'installation sur place est impossible tant que l'un des points au moins reste en suspens.

# 4. Serveur miroir

## 4.1 Utilité & Fonctionnement

Ce serveur permet de fournir à nos clients les mises à jour antivirales dont ils ont besoin quotidiennement. Il peut aussi être utilisé pour les mises à jour de code source et de moteurs antiviraux à distance, avec l'accord du client.

Ce serveur possède deux fonctions principales :

- Télécharger quotidiennement les mises à jour des solutions antivirales. Pour simplifier la tâche, les moteurs antiviraux sont directement installés sur ce système, avec une mise à jour automatique activée.
- Envoyer les mises à jour aux clients lorsque ceux-ci en feront la demande (via leur serveur de mises à jour ou manuellement)

Chaque package de mises à jour est envoyé chiffré pour chaque client. Le serveur comprend donc un script permettant la génération d'identifiants uniques clients (XXXXX-XXXXX-XXXXX-XXXXX-XXXXX) ainsi que la génération d'une clé de chiffrement unique. Cette clé doit être créée avant l'installation du Serveur Principal CyberHawk puisqu'elle vous sera demandée lors du processus d'installation de l'application WEB.

Les clients peuvent ensuite venir récupérer leurs mises-à-jour dans un conteneur chiffré à l'URL suivante :

- http://www.IP or DNS/download.php?ID=XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

## 4.2 Prérequis & Installation Système

Avant toute installation de la plateforme, il convient de respecter, à minima, les spécificités suivantes pour le système d'exploitation ainsi que pour le matériel à provisionner :

| CPU | RAM | HDD | NETWORK | OS | ARCHITECTURE |
|---|---|---|---|---|---|
| 1Core 2,4Ghz | 6Go | 25Go | 100 Mbps | Debian 9 | AMD 64 |

L'installation de la plateforme doit être ensuite réalisée telle que décrit précédemment en §3. Lorsque les informations vous seront demandées, veuillez renseigner les champs suivants :

- *Langue :* « Français »
- *Nom de Machine :* « CYBERHAWKMIROR »
- *Mot de passe « root » :* $PASS$
- *Nouvel utilisateur (nom / identifiant) :* « USER1 »
- *Mot de passe « Néosoft » :* $PASS$
- *Installation dans la même partition*
- *Choix des paquets par défaut* sans mandataire http

## 4.3 Installation packages de base

Plusieurs packages de base sont nécessaires sur le système et doivent être installés à cette étape :

- **cd /root/**
- **apt-get update && apt-get upgrade**
- **apt-get install linux-headers-$(uname -r)**
- **apt-get install apache2 php7.0 git php7.0-mysql php7.0-xml clamav make ssmtp**
- **apt-get install libice6 libsm6 x11-common**

En raison de la réutilisation de ce serveur pour les démonstrations de CyberHawk, il convient également d'installer une base de données MySQL et de lui appliquer la bonne configuration (choisir un mot de passe $PASS$ différent de ceux déjà générés) :

- **apt-get install mysql-server**
- **mysql –uroot –p**
  - **CREATE USER 'cyberhawk'@'localhost' IDENTIFIED BY '$PASS$';**
  - **CREATE DATABASE cyberhawk;**
  - **GRANT ALL ON cyberhawk.* TO 'cyberhawk'@'127.0.0.1';**

D'autres packages doivent être téléchargés au préalable depuis le site de l'éditeur et installés sur le système :

- **wget libssl0.9.8_0.9.8o-7_amd64.deb**
- **wget cav-linux_x64.deb**
- **wget sav-linux-free-9.tgz**
- **dpkg -i libssl0.9.8_0.9.8o-7_amd64.deb**
- **dpkg -i cav-linux_x64.deb**
- **/opt/COMODO/post_setup.sh**
- **tar -xzvf sav-linux-free-9.tgz**
- **./sophos-av/install.sh**

Lors de l'installation de Sophos sur le miroir, plusieurs choix vous seront demandés. Par défaut, veuillez ne pas activer les scans « On Access » et choisir une installation gratuite « Free » avec une mise à jour directe depuis les serveurs Sophos.

## 4.4 Configuration système

Après l'installation des packages, le reste de la configuration est fait de façon totalement automatique. Il suffit seulement de récupérer les packages nécessaires, stockés sur le GitHub :

- *Commande :* **git clone** https://github.com/NeosoftCybersecurite/CyberHawk.git
- *Commande :* **sh ./cyberhawk/CYBERHAWK_MIRROR/config.sh**

Une fois la configuration terminée, le système redémarre et devient opérationnel. Pensez à impérativement passer aux tests de fonctionnement afin de s'assurer de la bonne mise en place de toutes les règles.

***Note :*** Toute erreur remontée lors du lancement de l'une des commandes précédentes doit donner lieu à une investigation.

## 4.5 Test de fonctionnement

Il convient de tester le bon fonctionnement des moteurs antiviraux et de leurs mises à jour manuellement avant de laisser le travail se réaliser de façon automatique :

- **`python /root/scripts/av_updates_clients.py`**
- **`clamscan /root/scripts/crontab.file`**
- **`savscan /root/scripts/crontab.file`**
- **`/opt/COMODO/cmdscan -s /root/scripts/crontab.file`**

```
root@vps336332:~# python scripts/av_updates_client.py
ClamAV update process started at [redacted]
main.cvd is up to date (version: 57, sigs: 4218790, f-level: 60, builder: amishhammer)
daily.cld is up to date (version: 22593, sigs: 915322, f-level: 63, builder: neo)
bytecode.cld is up to date (version: 285, sigs: 57, f-level: 63, builder: bbaker)
Successfully updated Sophos Anti-Virus from sdds:SOPHOS
--[redacted]--  http://download.comodo.com/av/updates58/sigs/bases/bases.cav
Resolving download.comodo.com (download.comodo.com)... 178.255.82.5, 2a02:1788:4fd::b2ff:5205
Connecting to download.comodo.com (download.comodo.com)|178.255.82.5|:80... connected.
HTTP request sent, awaiting response... 302 Moved Temporarily
Location: http://download-cn.comodo.com/av/updates58/sigs/bases/bases.cav [following]
--[redacted]--  http://download-cn.comodo.com/av/updates58/sigs/bases/bases.cav
Resolving download-cn.comodo.com (download-cn.comodo.com)... 178.255.82.1, 2a02:1788:4fd::b2ff:5201
Connecting to download-cn.comodo.com (download-cn.comodo.com)|178.255.82.1|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 308329845 (294M) [application/octet-stream]
Saving to: `bases.cav'

100%[======================================================================================================>] 308,329,845 12.0M/s   in 25s

[redacted] (11.8 MB/s) - `bases.cav' saved [308329845/308329845]
```

Enfin, il ne reste plus qu'à tester l'ajout de nouveaux clients sur le serveur et le téléchargement manuel du package de mises à jour.

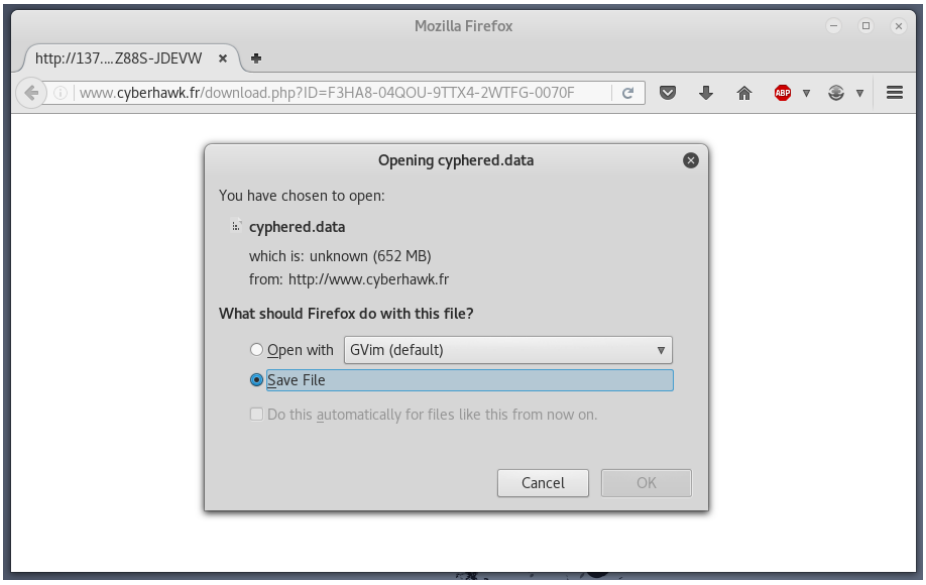
L'ajout d'un nouveau client permet de générer un identifiant unique client ainsi qu'une clé de chiffrement pour ses fichiers de mises à jour. Les informations crées doivent être envoyées systématiquement à « vous@vous.fr » afin d'en garder une copie :

- **`python /root/scripts/add_new_client.py`**
-

```
root@vps336332:~# python scripts/add_new_client.py
Nom du client à ajouter : CONIX


--Récapitulatif--
        Nom du client : CONIX
        IDentifiant client (à ajouter dans le Serveur de MAJ) : F3HA8-04QOU-9TTX4-2WTFG-0070F
        Clé du client (à ajouter dans l'installation CyberHawk) : JXU9JC4SPPCI0ZK
```

- **Téléchargement depuis un navigateur avec ID client (en majuscule) :**




***Note :*** Toute erreur remontée lors du lancement de l'une des commandes précédentes doit donner lieu à une investigation.

Modifier le fichier mail.txt en rajoutant vos coordonnées pour l'émission et la réception des courriels.

Modifier le fichier ssmtp.conf en rajoutant les authentifiants permettant la connexion au serveur d'émission des courriels.

## 4.6 Mises-à-jour du Système

Ce serveur est exposé directement sur Internet. L'application de mises-à-jour régulières est donc importante. Ces mises-à-jour sont faite manuellement comme suit :

- Chaque mois pour l'ensemble du système
- Directement en cas de découverte d'une vulnérabilité critique exposée

La mise à jour doit s'effectuer grâce aux commandes suivantes :

- **`apt-get update && apt-get upgrade`**
- **`reboot`**

# 5. Serveur Principal CyberHawk

## 5.1 Utilité & Fonctionnement

Ce serveur, hébergé dans les locaux du client, représente le cœur de la solution et permet la décontamination des fichiers utilisateurs.

Ce serveur possède trois fonctions principales :

- Proposer aux utilisateurs un espace de partage de fichiers (interface WEB disponible en HTTP / HTTPS).
- Décontaminer les fichiers envoyés à la volée tout en supprimant les fichiers suspicieux.
- Recevoir les mises à jour périodiques depuis le Serveur de mises-à-jour CyberHawk et les appliquer sur son propre système après les avoir déchiffrées.

## 5.2 Prérequis & Installation Système

Avant toute installation de la plateforme, il convient de respecter, à minima, les spécificités suivantes pour le système d'exploitation ainsi que pour le matériel à provisionner :

| CPU | RAM | HDD | NETWORK | OS | ARCHITECTURE |
|---|---|---|---|---|---|
| 4Core 2,1Ghz | 8Go | 20Go + (A x B)<br>A : Nombre d'utilisateurs<br>B : Go par utilisateur | 100 Mbps | Debian 9 | AMD 64 |

L'installation de la plateforme doit être ensuite réalisée telle que décrit précédemment en §3. Lorsque les informations vous seront demandées, veuillez renseigner les champs suivants :

- *Langue :* « Français »
- *Nom de Machine :* « CYBERHAWKSRV »
- *Mot de passe « root » :* $PASS$
- *Nouvel utilisateur (nom / identifiant) :* « cyberhawkmaj »
- *Mot de passe « cyberhawkmaj » :* $PASS$
- *Installation dans la même partition*
- *Choix des paquets par défaut* sans mandataire http

## 5.3 Installation packages de base

Plusieurs packages de base sont nécessaires sur le système et doivent être installés à cette étape :

- `cd /root/`
- `apt-get update && apt-get upgrade`
- `apt-get install apache2 php7.0 apt-offline git php7.0-mysql php7.0-xml clamav`
- `apt-get install libice6 libsm6 x11-common make`
- `apt-get install linux-headers-$(uname -r)`
- `apt-get install clamav-daemon clamdscan poppler-utils tesseract-ocr`

Le Serveur Principal CyberHawk nécessite une base de données de type MySQL pour fonctionner, avec l'application d'une configuration correcte (choisir un mot de passe $PASS$ différent de ceux déjà générés) :

- **apt-get install mysql-server**
- **mysql –uroot –p**
  - **CREATE USER 'cyberhawk'@'127.0.0.1' IDENTIFIED BY '$PASS$';**
  - **CREATE DATABASE cyberhawk;**
  - **GRANT ALL ON cyberhawk.* TO 'cyberhawk'@'127.0.0.1';**

D'autres packages doivent être téléchargés au préalable depuis le site de l'éditeur et installés sur le système, ils sont à disposition sur son miroir (dernière version à jour) pour plus de simplicité :

- **wget http://www.IP ou DNS du serveur miroir/libssl0.9.8_0.9.8o-7_amd64.deb**
- **wget http://www.IP ou DNS du serveur miroir/cav-linux_x64.deb**
- **wget http://www.IP ou DNS du serveur miroir/sav-linux-free-9.tgz**
- **wget http://www.IP ou DNS du serveur miroir/savdi-linux-64bit.tar**
- **wget http://www.IP ou DNS du serveur miroir/scan-sophos-sssp.sh**
- **wget http://www.IP ou DNS du serveur miroir/oletools.tar.gz**

- **dpkg -i libssl0.9.8_0.9.8o-7_amd64.deb**
- **dpkg -i cav-linux_x64.deb**
- **/opt/COMODO/post_setup.sh**
- **tar -xzvf sav-linux-free-9.tgz**
- **./sophos-av/install.sh**

Lors de l'installation de Sophos sur le miroir, plusieurs choix vous seront demandés. Par défaut, veuillez ne pas activer les scans « On Access » et choisir une installation gratuite « Free » avec une mise à jour depuis '**/home/cyberhawkmaj/SOPHOS/Primary/**' (own server 'o').

## 5.4 Configuration système

Après l'installation des packages, le reste de la configuration est fait de façon totalement automatique. Il suffit seulement de récupérer les packages nécessaires, stockés sur le GitHub :

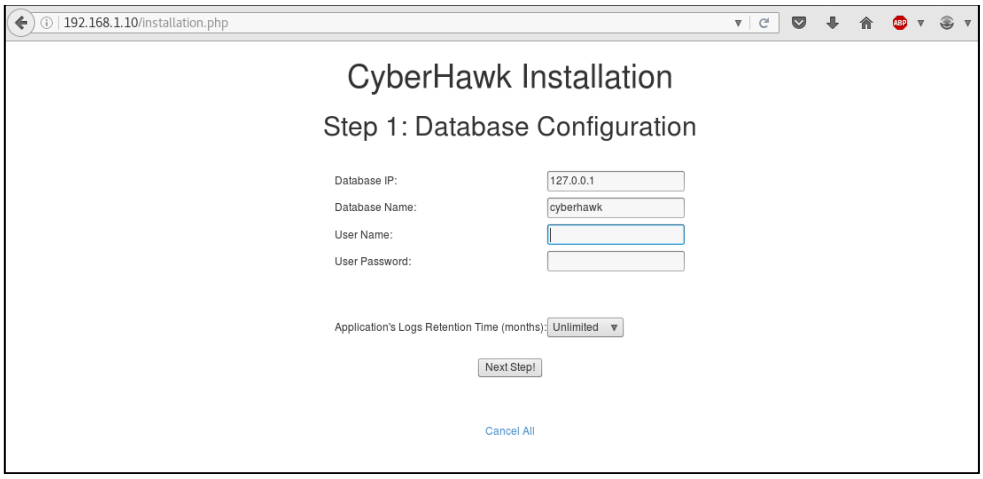
- *Commande :* **git clone https://github.com/NeosoftCybersecurite/CyberHawk.git**
- *Commande :* **sh ./cyberhawk/CYBERHAWK_SERVER/scripts/config.sh**

Une fois la configuration terminée, le système redémarre et devient opérationnel. Pensez à impérativement passer aux tests de fonctionnement afin de s'assurer de la bonne mise en place de toutes les règles.

***Note :*** Toute erreur remontée lors du lancement de l'une des commandes précédentes doit donner lieu à une investigation.

## 5.5 Test de fonctionnement

Le fonctionnement de ce serveur se teste en deux parties. Premièrement, il est utile de tester l'accès à l'interface WEB CyberHawk depuis un autre poste afin de constater si l'installation s'est bien déroulée. L'accès à la racine WEB du serveur doit être possible et vous rediriger vers la page d'installation CyberHawk. Rendez-vous au chapitre suivant pour l'installation web (*avant de terminer ce chapitre*) !

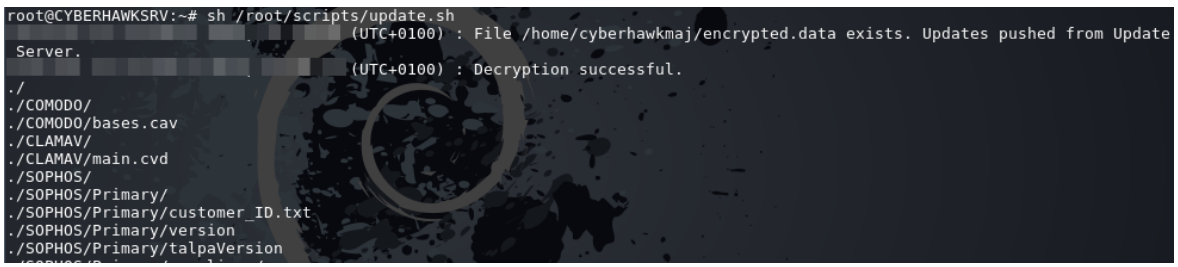



Enfin, il ne restera plus que le test final, l'épreuve ultime, consistant à tester que le serveur CyberHawk se met bien à jour correctement, grâce au serveur de mises-à-jour !

Malheureusement, ce test n'est pas réalisable à cette étape. Il est d'abord nécessaire d'installer le Serveur de mises-à-jour CyberHawk afin que celui-ci envoie le conteneur chiffré vers le serveur actuel.

Une fois cet envoi réalisé seulement, il sera possible d'effectuer le test manuel suivant :

- **`sh /root/scripts/update.sh`**
- **`/opt/Sophos-av/bin/savupdate`**



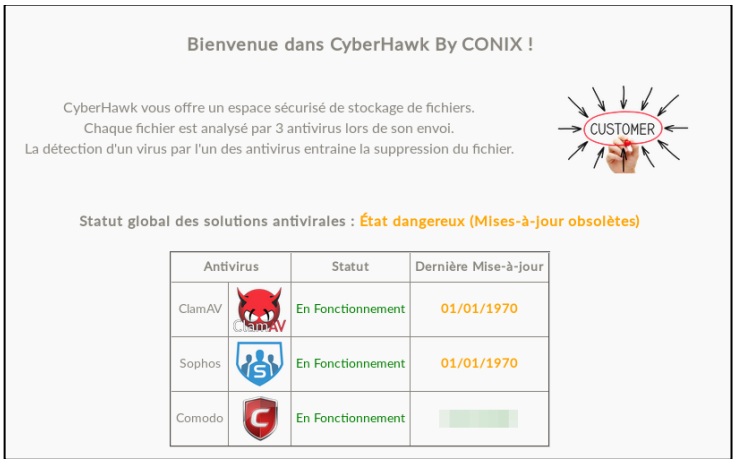
***Note :*** Toute erreur remontée lors du lancement de l'une des commandes précédentes doit donner lieu à une investigation.

## 5.6 Installation WEB

L'installation web ne sera pas décrite ici en détail, car très simple à réaliser. En effet, l'interface intuitive permet de tout configurer de façon graphique sans modifications à réaliser sur le système.

Beaucoup d'options sont à choisir lors de cette installation (logos, délais de rétentions, paramétrages des comptes, etc.). A part les options de bases de données et relatives au système Debian / CyberHawk, aucun choix ne doit être fait par NÉOSOFT. Les choix doivent être dictés par le document « *[CyberHawk] Questionnaire Client* » qui doit être rempli par le client avant installation.

La fin de l'installation aboutit sur une redirection vers l'accueil de CyberHawk (tout en supprimant les fichiers nécessaires à l'installation).




Le dernier test à réaliser est celui de se connecter réellement à l'application avec le compte 'Administrator' qui vient d'être créé, puis de vérifier le bon fonctionnement de l'envoi de fichiers, puis de leur suppression.

Pour l'instant, deux des antivirus n'ont encore jamais reçu leurs bases antivirales, comme le montre la capture précédente. Il ne sera donc pas possible d'envoyer un fichier tant que la mise à jour (manuelle ou automatique) n'aura pas été effectuée une première fois. Il faut donc terminer l'étape décrite en §5.5, puis se rendre de nouveau sur la plateforme pour le dernier test !



## 5.7 Mises-à-jour du Système

Ce serveur est n'est pas exposé directement sur Internet. L'application de mises-à-jour régulières est recommandée, mais peuvent être réalisées de façon espacée (tous les 4/6 mois). Ces mises-à-jour sont réalisées à distance, mais nécessitent une intervention du client sur son espace administrateur.

***Etape 1*** : Génération d'un fichier de signatures système sur le Serveur Principal CyberHawk (offline). **Opérations à effectuer sur le Serveur miroir** (création de l'archive, chiffrement de l'archive avec la clé client, puis stockage de l'archive dans l'espace administrateur) :

- `cd /var/clients/CLIENT/`
- `nano ./instructions.sh`
  - `# Ajouter les lignes suivantes`
  - `apt-offline set /tmp/apt-offline-cyberhawksrv.sig`
  - `tar -cvf '/var/files/Administrator/UPDATE_JUNE_NÉOSOFT.tar' '/tmp/apt-offline-cyberhawksrv.sig'`

- `openssl enc -aes-256-cbc -salt -in '/var/files/Administrator/UPDATE_JUNE_NÉOSOFT.tar' -out '/var/files/Administrator/UPDATE_JUNE_NÉOSOFT.encrypted' -pass file:'/root/scripts/key.cfg'`
- `rm -f '/var/files/Administrator/UPDATE_JUNE_NÉOSOFT.tar'`
- `rm –f '/tmp/apt-offline-cyberhawksrv.sig'`

***Etape 2*** : La récupération des fichiers est impossible à distance pour des raisons de sécurité. Le fichier chiffré créé devra donc être téléchargé par le client dans son espace 'Administrator' puis envoyé par mail.

***Etape 3*** : Sur un poste en ligne, téléchargez ensuite les mises à jours correspondantes au fichier de signature client :

- `mkdir /tmp/apt/`
- `apt-offline get apt-offline-cyberhawksrc.sig -d /tmp/apt/ --threads 5`
- `tar –cvf maj.tar /tmp/apt/`

***Etape 4*** : Envoi des nouvelles instructions au client via le **Serveur miroir** afin de réaliser les mises à jour. **Opérations à effectuer sur le Serveur miroir** (envoi de l'archive dans le répertoire client, puis envoi des commandes pour appliquer la mise à jour) :

- `cd /var/clients/CLIENT/`
- `mv maj.tar ./packages/`
- `nano ./instructions.sh`
  - `# Ajouter les lignes suivantes`
  - `tar –xvf /home/cyberhawkmaj/packages/maj.tar`
  - `apt-offline install /home/cyberhawkmaj/apt/`
  - `apt list –upgradable`
  - `apt upgrade`
  - `rm –Rf /home/cyberhawkmaj/apt/`

# 6. Serveur de mises-à-jour CyberHawk

## 6.1 Utilité & Fonctionnement

Ce serveur, hébergé dans les locaux du client, sert de passerelle entre le Serveur miroir et le Serveur Principal CyberHawk.

Ce serveur possède deux fonctions principales :

- Télécharger quotidiennement les mises à jour des solutions antivirales (conteneur chiffré) depuis le Serveur miroir (http:// **IP ou DNS du serveur miroir** /download.php?id=XXXXX-XXXXX-XXXXX-XXXXX-XXXXX).

- Envoyer le conteneur de mises-à-jour (sans déchiffrement ni altération) vers le Serveur Principal CyberHawk.

## 6.2 Prérequis & Installation Système

Avant toute installation de la plateforme, il convient de respecter, à minima, les spécificités suivantes pour le système d'exploitation ainsi que pour le matériel à provisionner :

| CPU | RAM | HDD | NETWORK | OS | ARCHITECTURE |
|---|---|---|---|---|---|
| 1Core 2,4Ghz | 1Go | 20Go | 100 Mbps | Debian 9 | AMD 64 |

***Note :*** En raison des faibles capacités CPU et espace disque nécessaires sur cette machine, la virtualisation est envisageable.

L'installation de la plateforme doit être ensuite réalisée telle que décrit précédemment en §3. Lorsque les informations vous seront demandées, veuillez renseigner les champs suivants :

- *Langue :* « Français »
- *Nom de Machine :* « CYBERHAWKUPDATE »
- *Mot de passe « root » :* $PASS$
- *Nouvel utilisateur (nom / identifiant) :* « Néosoft »
- *Mot de passe « Néosoft » :* $PASS$
- *Installation dans la même partition*
- *Choix des paquets par défaut* sans mandataire http

## 6.3 Installation packages de base

Plusieurs packages de base sont nécessaires sur le système et doivent être installés à cette étape :

- **`cd /root/`**
- **`apt-get update && apt-get upgrade`**

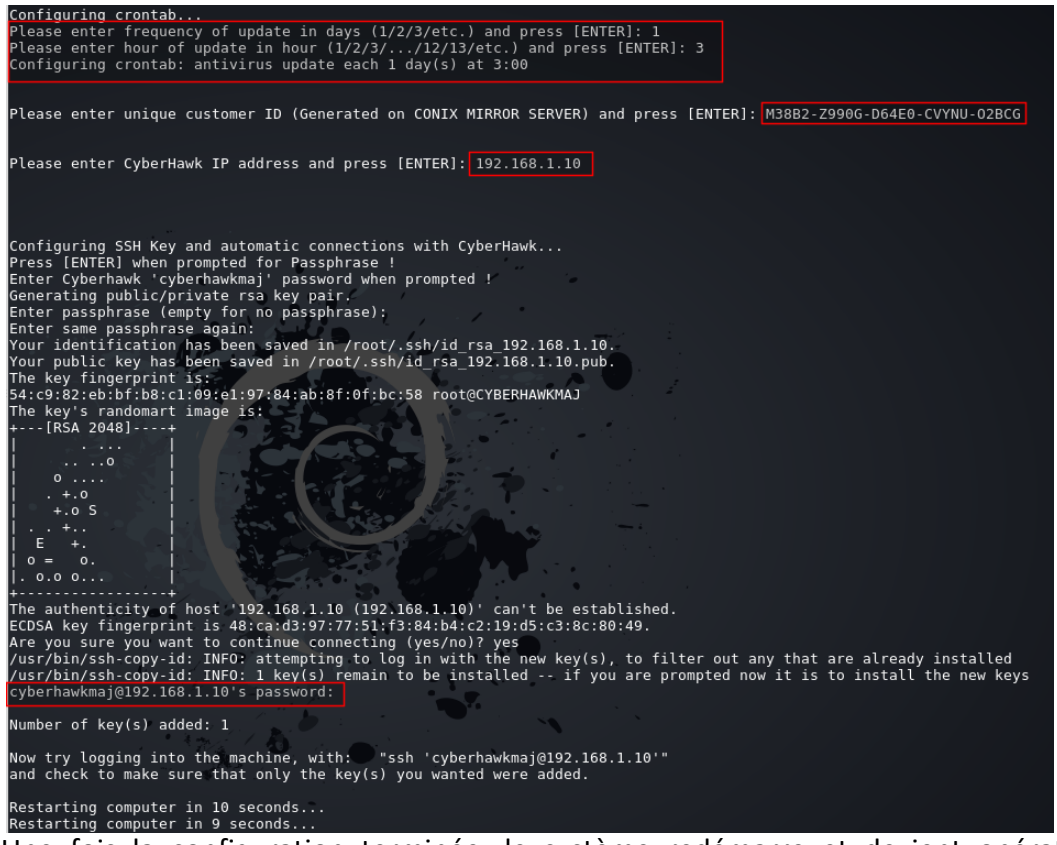
- **apt-get install git apt-offline cntlm**

## 6.4 Configuration système

Après l'installation des packages, le reste de la configuration est fait de façon totalement automatique. Il suffit seulement de récupérer les packages nécessaires, stockés sur le GitHub :

- *Commande :* **git clone** https://github.com/NeosoftCybersecurite/CyberHawk.git
  Modifier le fichier config.cfg afin de rajouter l'ip du serveur mirroir ou son DNS
- *Commande :* **sh ./cyberhawk/CYBERHAWK_UPDATE/config.sh**

Quelques informations essentielles vous seront demandées pendant cette étape afin de configurer au mieux le serveur (Fréquence de mise à jour, ID unique client, IP Serveur Principal CyberHawk, etc.).




Une fois la configuration terminée, le système redémarre et devient opérationnel. Pensez à impérativement passer aux tests de fonctionnement afin de s'assurer de la bonne mise en place de toutes les règles.

***Note :*** Toute erreur remontée lors du lancement de l'une des commandes précédentes doit donner lieu à une investigation.

## 6.5 Configuration PROXY (si nécessaire)

Dans le cas où le client utiliserait un proxy (authentifiant ou non) afin de sortir sur Internet, il convient de paramétrer le serveur en fonction des adresses et identifiants fournis.

Par exemple, dans le cas d'un proxy simple, il est nécessaire d'éditer le fichier « /etc/wgetrc » afin de permettre à la commande wget de récupérer les mises-à-jour :

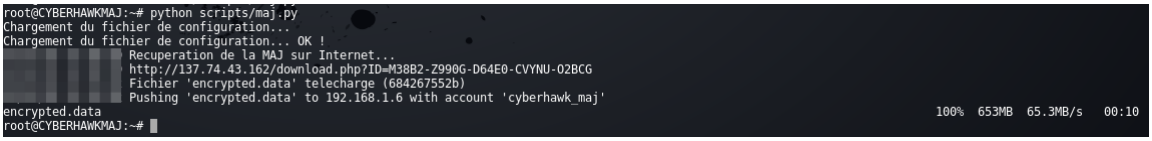
- **http_proxy = http://user:password@server:port**

Dans le cas de l'utilisation d'un proxy avec authentification NTLM, il est nécéssaire d'utiliser la librairie « cntlm » préinstallée et de configurer le fichier « /etc/cntlm.conf » avec les informations appropriées.

## 6.6 Test de fonctionnement

Il convient de tester le bon fonctionnement des moteurs antiviraux et de leurs mises à jour manuellement avant de laisser le travail se réaliser de façon automatique :

- **python /root/scripts/maj.py**




***Note :*** Toute erreur remontée lors du lancement de l'une des commandes précédentes doit donner lieu à une investigation.

## 6.7 Ajout d'un Serveur Principal CyberHawk

Le Serveur de mises-à-jour CyberHawk peut être utilisé pour alimenter plusieurs Serveurs Principaux CyberHawk. Pour cela, il suffit d'ajouter l'IP du nouveau serveur CyberHawk (ex. 192.168.1.6) à la liste de configuration du script de mises à jour, et de pousser notre clé SSH sur ce serveur :

- **vi /root/scripts/config.cfg**
  - ips = 192.168.1.10,**192.168.1.6**
- **ssh-copy-id –i /root/.ssh/id_rsa cyberhawkmaj@192.168.1.6**

## 6.8 Mises-à-jour du Système

Ce serveur est n'est pas exposé directement sur Internet. L'application de mises-à-jour régulières est recommandée, mais peuvent être réalisées de façon espacée (tous les 4/6 mois). Ces mises-à-jour sont faite manuellement, soit en se déplaçant dans les locaux du client, soit en lui donnant les commandes à taper et les fichiers à retourner.

***Etape 1*** : Génération d'un fichier de signatures système sur le Serveur de mises-à-jour CyberHawk (offline) avec un support USB branché (/media/) :

- **`apt-offline set /media/apt-offline-cyberhawkmaj.sig`**

***Etape 2*** : Sur un poste en ligne, téléchargez ensuite les mises à jours correspondantes au fichier de signature :

- **`mkdir /media/apt/`**
- **`apt-offline get /media/apt-offline-cyberhawkmaj.sig -d /media/apt/ --threads 5`**

***Etape 3*** : Reconnecter le support USB sur le Serveur de mises-à-jour CyberHawk (offline) afin de réaliser les mises à jour :

- **`apt-offline install /media/apt/`**
- **`apt list –upgradable`**
- **`apt upgrade`**

# 7. Poste « Libre-Service » / Kiosque Interactif

## 7.1 Utilité & Fonctionnement

Le Poste « Libre-Service », ou « Kiosque Interactif » est un poste de travail utilisé seulement dans le but d'accéder à la plateforme WEB CyberHawk.

L'environnement est un poste de travail Linux (Porteus) avec un système de fichiers simple, robuste et léger. Au démarrage, la plateforme ne propose donc rien d'autre que la page d'accueil de CyberHawk, en plein écran. Il est impossible d'en sortir pour naviguer dans le système à part pour sélectionner les fichiers contenus sur le support amovible branché.

## 7.2 Prérequis & Installation Système

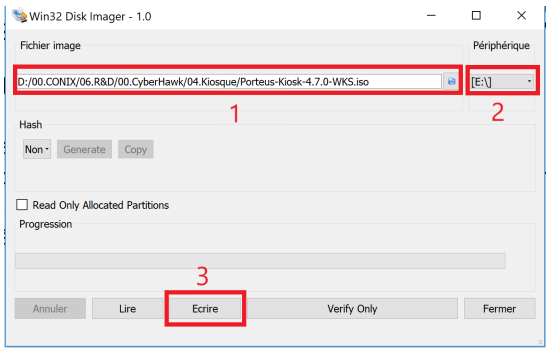
Avant toute installation de la plateforme, il convient de respecter, à minima, les spécificités suivantes pour le système d'exploitation ainsi que pour le matériel à provisionner :

| CPU | RAM | HDD | NETWORK | OS | ARCHITECTURE |
|---|---|---|---|---|---|
| 1Core 2,4Ghz | 1Go | 4Go | 100 Mbps | Porteus Kiosk 4.6.0 | AMD 64 |

Afin de réaliser l'installation du Kiosque CyberHawk, un fichier ISO doit être téléchargé et gravé sur CD/DVD ou média amovible. Ce fichier contient le système d'exploitation et peut être téléchargée sur les liens suivants :

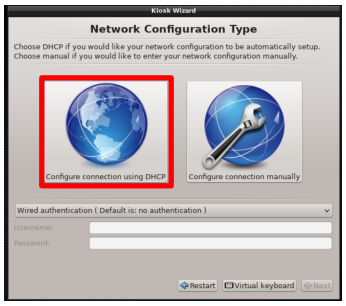
- Version Workstation : http:// IP ou DNS du serveur miroir /Porteus-Kiosk-4.7.0-WKS.iso
- Version Kiosk : http:// IP ou DNS du serveur miroir //Porteus-Kiosk-4.7.0-KSK.iso

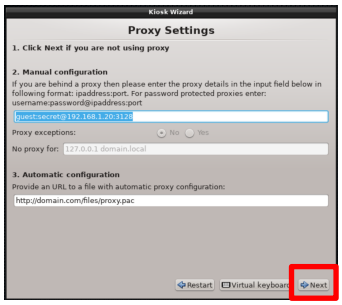
Le fichier téléchargé doit ensuite être gravé sur CD/DVD ou écrit sur clé USB. Sur Linux, la commande « dd » peut être utilisé pour l'écriture du fichier sur une clé USB. Sur Windows, la gravure sur CD/DVD peut être réalisée de façon classique, et l'écriture sur clé du fichier ISO doit se faire avec l'utilitaire « Win32DiskImager ». Le fichier doit être sélectionné (1), puis le lecteur USB de destination (2) avant d'écrire sur la clé (3).



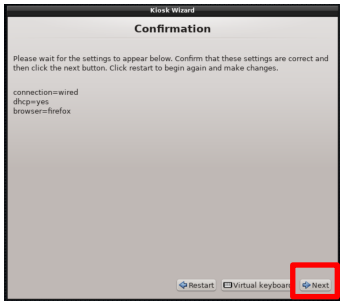

Il suffit ensuite d'insérer le CD/DVD ou clé USB au démarrage de l'ordinateur et de démarrer sur celui-ci / celle-ci (touche F9).

La première partie de l'installation est relativement simple et permet de configurer le réseau ainsi que le navigateur utilisé. Les choix entourés en rouge sont à utiliser.



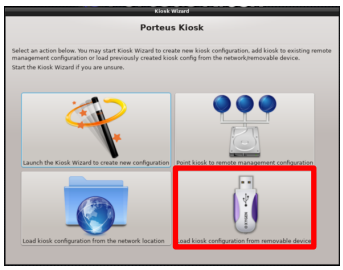


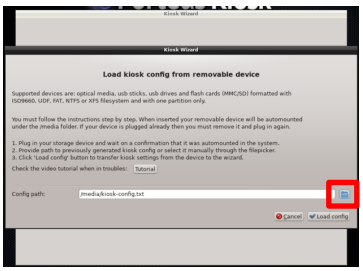

La deuxième partie également simple, puisque la configuration est réalisée en entière partie depuis un fichier de configuration. Ce fichier permet d'éviter d'avoir à tout reconfigurer manuellement depuis le menu.

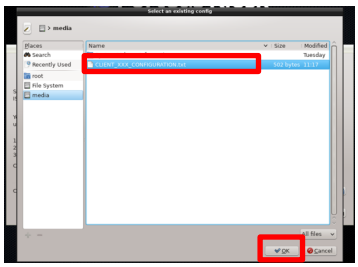
Le fichier de configuration (généré pour chaque client) doit également être téléchargé depuis le miroir, puis copié sur une seconde clé USB :

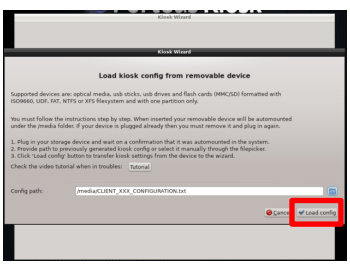
- http:// IP ou DNS du serveur miroir //CLIENT_XXX_CONFIGURATION.txt

Choisissez un chargement de la configuration depuis un média amovible, puis sélectionnez le fichier téléchargé (des modifications sont ensuite possibles) :



Modifiez les paramètres nécessaires (IP du serveur CyberHawk, IP locale, etc.) au besoin, puis terminez l'installation avec les options par défaut (« Next » en prenant soin de choisir le bon disque dur de l'ordinateur pour installation) avant de redémarrer le système et d'en tester les fonctionnalités (envoi et téléchargement depuis média amovible) :


## 7.3 Modifications apportées (ISO)

***Note :*** Ce paragraphe n'est pas utile à l'installation du serveur et tant que la version du fichier ISO installée chez le client reste la même (disponible sur le site CyberHawk). En revanche, si une montée de version éditeur est réalisée, il sera utile de réintégrer dans le fichier ISO les modifications NÉOSOFT. Ce paragraphe apporte donc des précisions sur les modifications à réaliser ainsi que les commandes correspondantes.

Afin d'adapter le système Porteus Kiosk aux besoins NÉOSOFT, certaines modifications ont été apportées directement au fichier ISO et compilées. Ces modifications concernent les points suivants qui n'étaient pas paramétrables nativement à l'installation :

- Changement de langue du clavier par défaut (EN -> FR)
- Changement des droits de montages USB (ro -> rw)
- Sauvegarde des téléchargements Firefox dans '/media/' par défaut
- Ajout d'un clavier Virtuel et d'un Grab&Drag pour l'utilisation sur kiosque (sans souris ou clavier)
- Module permettant l'installation sans accès à Internet
- Bouton permettant de démonter les clés USB avant de les retirer

La procédure de customisation manuelle du Kiosque Porteus est disponible sur le site éditeur en cas de doute : http://porteus-kiosk.org/kiosk-customization.html. Certains packages (Firefox), ont également été intégrés pour éviter leur téléchargement à chaque fois (http://porteus-kiosk.org/public/).

***Etape 1*** : Monter le fichier ISO téléchargé sur le site éditeur dans un dossier au choix (/tmp/KIOSK_ISO) :

- **`mkdir /tmp/KIOSK_ISO/`**
- **`mount -o loop Downloads/Porteus-Kiosk-4.1.0-x86_64.iso /mnt/cdrom/`**
- **`cp -a /mnt/cdrom/* /tmp/KIOSK_ISO/`**
- **`umount /mnt/cdrom`**

***Etape 2*** : Récupération des packages nécessaires, stockés sur le GitHub :

- *Commande :* **`git clone https://github.com/NeosoftCybersecurite/CyberHawk.git`**
- *Commande :* **`cp ./cyberhawk/CYBERHAWK_KIOSK/* /tmp/KIOSK_ISO/xzm/`**

***Etape 3*** : Téléchargement de Firefox et construction du fichier ISO :

- **`cd /tmp/KIOSK_ISO/`**
- **`./make_iso.sh`**
- **`isohybrid ../Porteus-Kiosk.iso`**
- **`dd if=../Porteus-Kiosk.iso of=/dev/sdb`**

*Le fichier ISO généré est ensuite prêt à être installé sur le système cible.*

## 7.4 Mises-à-jour du Système

Cette machine est n'est pas exposée sur Internet mais seulement sur le réseau Interne. L'application de mises-à-jour n'est pas forcément utile sur ce système qui est en lecture seule. De plus, ce système n'est pas critique et ne représente aucun risque pour la solution CyberHawk et / ou pour le réseau.

En cas de dysfonctionnement et / ou de besoin réel de mise à jour, la plateforme peut être réinstallée directement depuis la version du GitHub NÉOSOFT la plus récente. L'installation ne prenant que quelques minutes.

# 8. Exemples concrets de Mises-à-Jours chez les clients

## 8.1 Récupération de la configuration du client « A »

***Etape 1*** : Ajout des instructions au client « CLIENT » afin de packager les instructions à distance. **Opérations à effectuer sur le Serveur miroir** (création de l'archive, chiffrement de l'archive avec la clé client, puis stockage de l'archive dans l'espace administrateur) :

- `cd /var/clients/CLIENT/`
- `nano ./instructions.sh`
  - `# Ajouter les lignes suivantes`
  - `tar -cvf '/var/files/Administrator/UPDATE_JUNE_NÉOSOFT.tar' '/var/www/config.php'`
  - `openssl enc -aes-256-cbc -salt -in '/var/files/Administrator/UPDATE_JUNE_NÉOSOFT.tar' -out '/var/files/Administrator/UPDATE_JUNE_NÉOSOFT.encrypted' -pass file:'/root/scripts/key.cfg'`
  - `rm -f '/var/files/Administrator/UPDATE_JUNE_NÉOSOFT.tar'`

***Etape 2*** : La récupération des fichiers est impossible à distance pour des raisons de sécurité. Le fichier chiffré créé devra donc être téléchargé par le client dans son espace 'Administrator' puis envoyé par mail.

## 8.2 Modification des sources web du client « A »

***Etape 1*** : Ajout des sources PHP au client « CLIENT ». **Opérations à effectuer sur le Serveur miroir** (copie des fichiers à envoyer dans le répertoire « www » du client) :

- `cp new_index.php /var/clients/CLIENT/www/index.php`

***Etape 2*** : Le fichier placé dans « www » écrasera celui présent chez le client lors de la prochaine mise à jour (minuit).

## 8.3 Installation d'un nouveau package sur le serveur du « A »

***Etape 1*** : Ajout du package au client « CLIENT ». **Opérations à effectuer sur le Serveur miroir** (copie du package à envoyer dans le répertoire du client) :

- `cp package.deb /var/clients/CLIENT/packages/package.deb`
- `cd /var/clients/CLIENT/`
- `nano ./instructions.sh`
  - `# Ajouter les lignes suivantes`
  - `/usr/bin/dpkg –i /home/cyberhawkmaj/packages/package.deb`

***Etape 2*** : Le sera installé chez le client lors de la prochaine mise à jour (minuit).