

---

## TP Ressources HackademINT

HackademINT, Comment ça marche ?

zTeeed



## Table des matières

<b>La communication</b>	<b>3</b>
Facebook/Twitter . . . . .	3
La Mailing List . . . . .	4
CTFTime . . . . .	4
Discord . . . . .	5
<b>Containers / Machines Virtuelles</b>	<b>6</b>
Configuration . . . . .	8
Quelles machines ? . . . . .	10
<b>Se connecter via SSH</b>	<b>11</b>
Authentification par mot de passe . . . . .	11
Authentification par clé RSA . . . . .	11
Utiliser ~/.ssh/config . . . . .	12
<b>Réparer quand c'est cassé</b>	<b>12</b>
<b>vim</b>	<b>13</b>
C'est quoi ? . . . . .	13
Comment installer des plugins ? . . . . .	13
<b>Mettre à jour le site web : faire du php</b>	<b>14</b>
<b>git</b>	<b>15</b>
Commandes utiles (+Google) . . . . .	15

## La communication

### Facebook/Twitter

Objectif : Obtenir un fil d'actualité technique, être le plus actif possible pour augmenter notre visibilité.

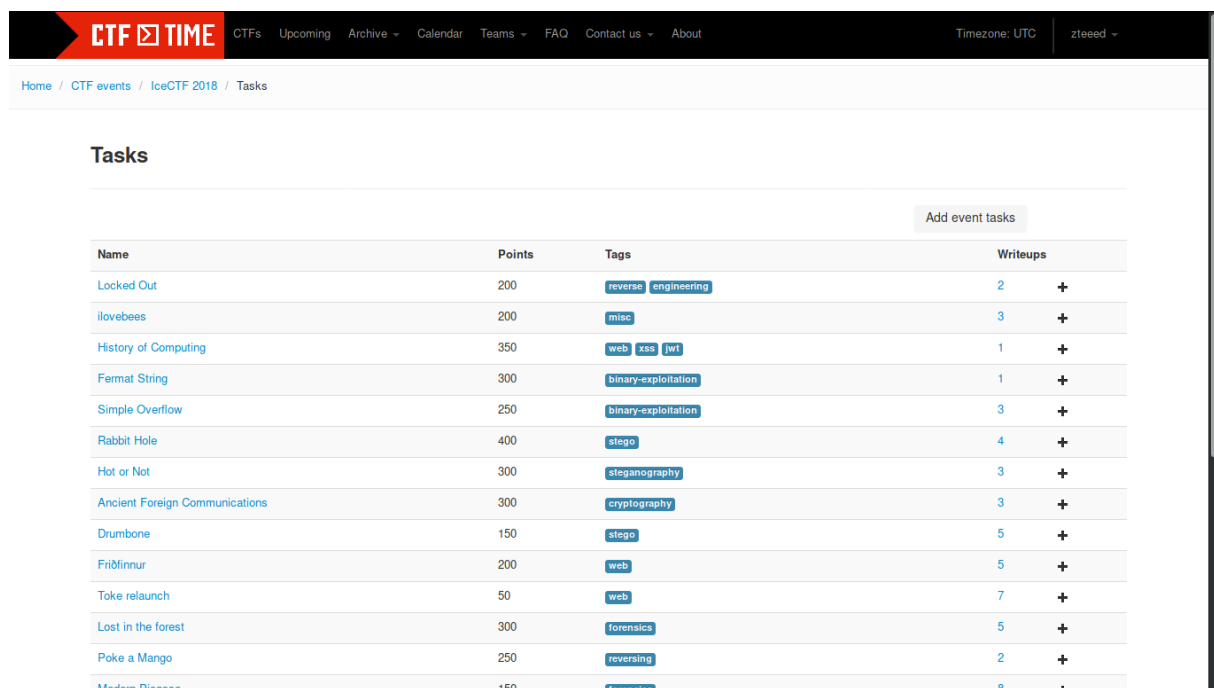
The image displays two social media profiles side-by-side. The top profile is the Facebook page for 'Loïc Hackademint'. It features a cover photo of two penguins on a rocky shore. The profile picture is a circular logo with a blue bird-like character and the text 'HackademINT'. The page shows a 'Journal' tab, an 'Intro' section with the website 'hackademint.minet.net', a 'Photos' section with a screenshot of a 'Google Capture the Flag 2018' report, and a post from September 15, 2016, about a bug in the 'StarHackademint.minet.net' platform. The bottom profile is the Twitter account for 'HackademINT' (@hackademint). It has a blue header with the same circular logo. The bio identifies it as the 'Club de cybersécurité de Telecom SudParis' and mentions the website 'hackademint.minet.net'. The profile shows 52 tweets, 102 followers, and 48 following. A tweet from @LiveOverflow is highlighted, discussing a bug in the 'The Curse of Cross-Origin Stylesheets' project. The tweet includes a video link and a meme image of a character pointing at a sign that says '<styles> web' and 'The Curse of CSS'.

## La Mailing List

Les mails servent uniquement à faire passer les informations les plus importantes. La quantité de mails doit rester restreinte au maximum. On ne doit pas avoir plus 3/4 mails dans la semaine. Les périodes de rentrée font évidemment exception.

## CTFTime

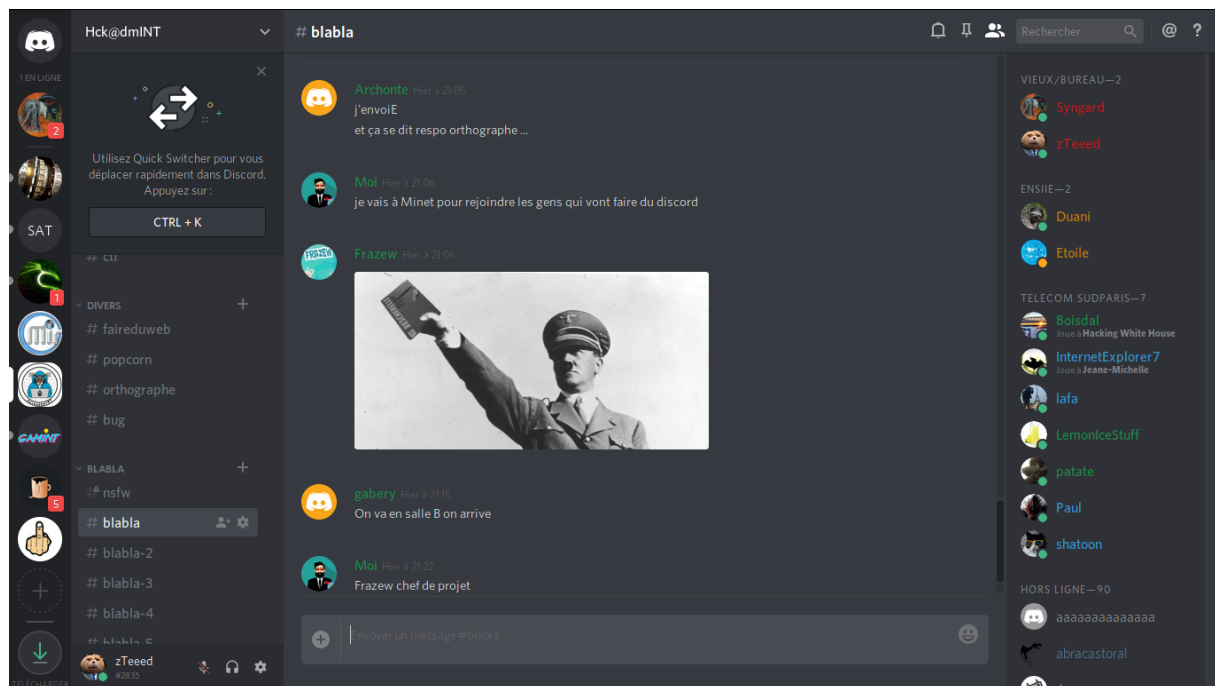
CTFTime est la plateforme qui recense l'activité des équipes de CTF sur le plan international. Son intérêt majeur réside dans la visibilité des CTFs organisés et dans notre visibilité personnelle. En effet, après avoir rédigé des writeups sur le site, il faut ajouter une proposition de solution sur la page qui concerne le CTF afin d'augmenter notre visibilité et le trafic sur notre site web.



CTF TIME					CTFs	Upcoming	Archive	Calendar	Teams	FAQ	Contact us	About	Timezone: UTC	zTeeed
Home / CTF events / IceCTF 2018 / Tasks														
Tasks														
Add event tasks														
Name	Points	Tags		Writeups										
<a href="#">Locked Out</a>	200	<a href="#">reverse</a>	<a href="#">engineering</a>	<a href="#">2</a>	+									
<a href="#">ilovebees</a>	200	<a href="#">misc</a>		<a href="#">3</a>	+									
<a href="#">History of Computing</a>	350	<a href="#">web</a>	<a href="#">xss</a> <a href="#">jwt</a>	<a href="#">1</a>	+									
<a href="#">Fermat String</a>	300	<a href="#">binary-exploitation</a>		<a href="#">1</a>	+									
<a href="#">Simple Overflow</a>	250	<a href="#">binary-exploitation</a>		<a href="#">3</a>	+									
<a href="#">Rabbit Hole</a>	400	<a href="#">stego</a>		<a href="#">4</a>	+									
<a href="#">Hot or Not</a>	300	<a href="#">steganography</a>		<a href="#">3</a>	+									
<a href="#">Ancient Foreign Communications</a>	300	<a href="#">cryptography</a>		<a href="#">3</a>	+									
<a href="#">Drumbone</a>	150	<a href="#">stego</a>		<a href="#">5</a>	+									
<a href="#">Friðfinnur</a>	200	<a href="#">web</a>		<a href="#">5</a>	+									
<a href="#">Toke relaunch</a>	50	<a href="#">web</a>		<a href="#">7</a>	+									
<a href="#">Lost in the forest</a>	300	<a href="#">forensics</a>		<a href="#">5</a>	+									
<a href="#">Poke a Mango</a>	250	<a href="#">reversing</a>		<a href="#">2</a>	+									
<a href="#">Modern Picasso</a>	150	<a href="#">forensics</a>		<a href="#">8</a>	+									

## Discord

Discord est notre outil de communication en interne, on y établit toutes les discussions en ce qui concerne notre travail sur les challenges de CTFs ou ceux des autres plateformes dédiées à l'apprentissage de la sécurité informatique. C'est notre meilleur outil pour s'entraider et c'est comme ça que l'on progresse. Il ne faut donc pas hésiter à être actif afin d'augmenter votre interaction avec les autres membres. Cela vous profitera à tous.



## Containers / Machines Virtuelles

- C'est quoi un hyperviseur ?

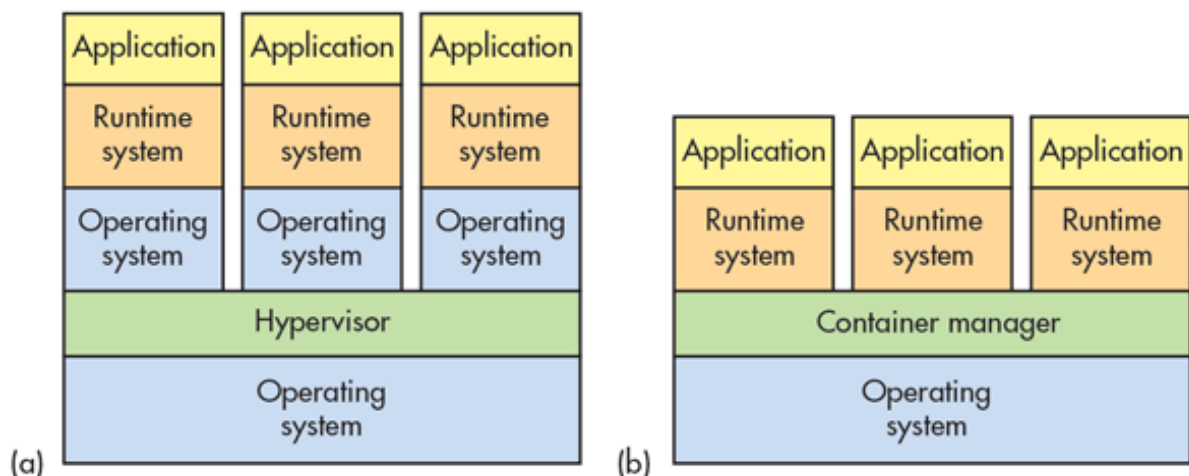
En informatique, un hyperviseur est une plate-forme de virtualisation qui permet à plusieurs systèmes d'exploitation de travailler sur une même machine physique en même temps.

- Ça sert à quoi ?

Théoriquement, c'est une couche logicielle très légère (en comparaison à un OS classique) qui permet d'allouer un maximum de ressources physiques aux containers / machines virtuelles.

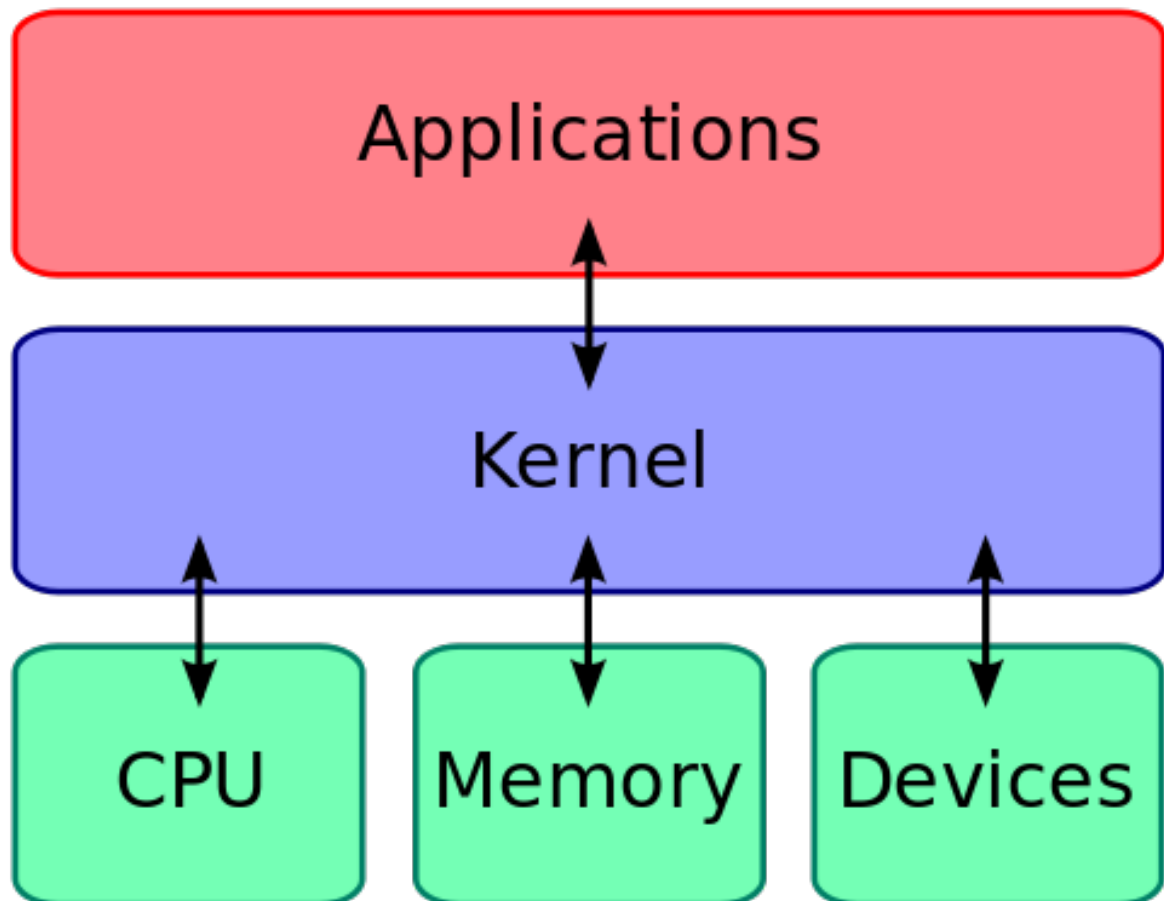
- Quelle est la différence entre un container et une machine virtuelle ?
- Quelles sont leurs caractéristiques ?

À la différence de la machine virtuelle, le container partage le noyau de l'hôte. Du fait que les conteneurs nécessitent beaucoup moins de ressources, leur démarrage est rapide et leur déploiement est simple. La faible utilisation de ressources permet une densité plus élevée. Vous pouvez exécuter davantage de services sur la même unité matérielle et ainsi réduire vos coûts. L'exécution sur le même noyau entraîne une moins bonne isolation comparativement aux machines virtuelles.



- Un noyau ?

Un noyau de système d'exploitation, ou simplement noyau, ou kernel (de l'anglais), est une des parties fondamentales de certains systèmes d'exploitation. Il gère les ressources de l'ordinateur et permet aux différents composants — matériels et logiciels — de communiquer entre eux.



## Configuration

Les différents CTs/VMs sont sur un serveur au sein de l'infra MiNET. À l'origine ils ne disposent pas d'**interface réseau publique** (à MiNET ça concerne les IPs commençant par 157.159), seulement des **interfaces réseau privées** (par convention les IPs commencent par 192.168) donc ces machines sont seulement accessibles derrière le VPN MiNET. En vous connectant via **OpenVPN** au VPN MiNET, vous êtes routés vers le sous-réseau ayant accès à ces machines. L'ensemble des membres d'HackademINT n'étant pas forcément à MiNET, il a été configuré sur ces machines des interfaces publiques.

Plutôt que d'administrer les CTs/VMs en vous connectant via **SSH** sur le noeud de calcul et de tout faire en lignes de commandes, il existe **Proxmox**, une jolie interface graphique pour la gestion « clic clic ».

Type	Description	Disk usage...	Memory us...	CPU usage	Uptime
lxc	115 (hackdemintcounter)	10.1 %	3.5 %	0.1% of 1C...	1 day 06:32:57
lxc	117 (patrick)	18.8 %	17.3 %	0.0% of 1C...	8 days 03:26...
lxc	118 (nburritos)	8.4 %	3.2 %	0.0% of 1C...	8 days 02:07...
lxc	119 (adh7)				-
lxc	123 (soiree.minet.net)	9.0 %	4.1 %	0.0% of 1C...	112 days 23:...
lxc	124 (soiree-dev)	16.2 %	14.4 %	0.0% of 1C...	4 days 02:05...
lxc	125 (HackademINTWebsite...)	41.4 %	4.8 %	0.0% of 2C...	3 days 01:22...
lxc	130 (tacos)	4.7 %	2.8 %	0.0% of 1C...	112 days 23:...
lxc	156 (wiki-cassiope)				-
lxc	190 (mumble)	10.3 %	3.7 %	0.2% of 1C...	112 days 23:...
lxc	192 (faqdf)				-
lxc	199 (Moog-Wow)	64.2 %	67.6 %	8.6% of 2C...	7 days 01:35...
lxc	203 (ceph-admin)				-
lxc	116 (vmlinux.minet.net)	32.8 %	2.7 %	0.0% of 1C...	8 days 09:45...

Start Time	End Time	Node	User name	Description	Status
Sep 28 12:58:51	Sep 28 12:59:57	challenger	varens@ldap-maste...	CT 211 - Destroy	OK
Sep 28 12:58:21	Sep 28 12:58:21	challenger	varens@ldap-maste...	CT 126 - Create	Error: kbd option must be e...
Sep 28 12:57:02	Sep 28 12:57:11	challenger	varens@ldap-maste...	CT 211 - Destroy	Error: error with cfs lock 'stor...
Sep 28 12:56:54	Sep 28 12:57:55	challenger	varens@ldap-maste...	CT 227 - Destroy	OK
Sep 28 12:54:37	Sep 28 12:56:16	challenger	varens@ldap-maste...	VM/CT 100 - Console	OK

**FIG. 1 :** Illustration de l'interface Proxmox accessible à <https://192.168.103.206:8006>



Pour illustrer la suite de cette présentation, on prendra pour exemple le container sur lequel est hébergé le site web `hackademint.minet.net` dont la configuration est présentée plus bas. Une fois l'interface publique ajoutée, il faut modifier le fichier de conf suivant :

```
1 [root@HackademINTWebsiteOfficial zteeed]# cat /etc/network/interfaces
2 auto lo
3 iface lo inet loopback
4
5 auto eth0
6 iface eth0 inet static
7     address 192.168.103.177
8     netmask 255.255.255.0
9
10 auto eth1
11 iface eth1 inet static
12     address 157.159.40.177
13     netmask 255.255.255.192
14     gateway 157.159.40.129
15
16
17 [root@HackademINTWebsiteOfficial zteeed]# ip a
18 1 : lo : <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    group default qlen 1000
19     link/loopback 00 :00 :00 :00 :00 :00 brd 00 :00 :00 :00 :00 :00
20     inet 127.0.0.1/8 scope host lo
21         valid_lft forever preferred_lft forever
22 241 : eth0@if242 : <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
    noqueue state UP group default qlen 1000
23     link/ether e6 :0b :eb :ba :f2 :f6 brd ff :ff :ff :ff :ff :ff link-netnsid 0
24     inet 192.168.103.177/24 brd 192.168.103.255 scope global
25     eth0
26         valid_lft forever preferred_lft forever
27 243 : eth1@if244 : <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
    noqueue state UP group default qlen 1000
28     link/ether 06 :02 :b0 :a5 :13 :df brd ff :ff :ff :ff :ff :ff link-netnsid 0
29     inet 157.159.40.177/26 brd 157.159.40.191 scope global eth1
30         valid_lft forever preferred_lft forever
```

## Quelles machines ?

Site web hackademint.minet.net - hackademint.minet.net - **IP : 157.159.40.177**

Site web secu.minet.net - secu.minet.net - **IP : 157.159.40.173**

Plateforme de CTF starhackademint.minet.net dans /root - starhackademint.minet.net - **IP : 157.159.40. ???**

Site web webstarhackademint.minet.net / Une partie des challenges web et bases de données mysql - webstarhackademint - **IP : 157.159.40.163**

Une partie des challenges web de starhackademint.minet.net / Chacun des challenge se trouve dans un lxc qui lui est dédié. - webstarhackademint2 - **IP : 157.159.40.170**

## Se connecter via SSH

Description du protocole réseau :

Secure Shell (SSH) est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite, tous les segments TCP sont authentifiés et chiffrés. Il devient donc impossible d'utiliser un sniffer pour voir ce que fait l'utilisateur.

Le protocole SSH a été conçu avec l'objectif de remplacer les différents protocoles non chiffrés comme rlogin, telnet, rcp et rsh.

### Authentification par mot de passe

```
1 ssh root@157.159.40.171
```

### Authentification par clé RSA

- Une clé RSA ?

Quand vous travaillez avec des clés asymétriques, par principe, vous avez deux clés (on parle de paire de clés) : une clé publique, que vous pouvez diffuser librement, voire mettre à disposition sur un serveur de clés ; et une clé privée qui constitue véritablement votre « identité » et ne doit jamais être diffusée : elle reste simplement présente dans votre dépôt de clés personnelles.

- Comment créer une paire de clé ?

[www.aidoweb.com/tutoriaux/securiser-acces-ssh-paire-cles-rsa-generation-cles-application-serveur-646](http://www.aidoweb.com/tutoriaux/securiser-acces-ssh-paire-cles-rsa-generation-cles-application-serveur-646)

```
1 ssh -i id_rsa zteeed@157.159.40.177 -p 2222
```

## Utiliser ~/.ssh/config

Le fichier ~/.ssh/config vous permet de créer des **alias** pour vous connecter en SSH sans avoir à ressaisir toutes les options. Voici un exemple :

```
1 [zteeed@spider ~]$ cat ~/.ssh/config
2
3 Host hackademint.minet.net
4     Hostname 157.159.40.177
5     User zteeed
6     IdentityFile /mnt/Data/Useful/SSH/id_rsa
7
8
9 [zteeed@spider ~]$ ssh hackademint.minet.net
```

## Réparer quand c'est cassé

Quand un challenge sur starhackademint.minet.net ne fonctionne plus c'est souvent dû à plusieurs éléments :

- Le serveur web a été coupé

```
1 systemctl status apache2
```

- La connexion avec certaines bases de données a été rompue (mysql / postgresql)

```
1 systemctl status mysql
```

- Certains containers (oui oui, un container dans un container) sont éteints (lxc)

```
1 systemctl status lxc
2 lxc-ls
3 lxc-info -n ping2
```

## vim

```
1 sudo apt install vim
```

### C'est quoi ?

Vim est un éditeur de texte mais avec quelques plugins ça devient un vrai **IDE**. La gestion des plugins de la configuration sont dans le fichier `~/.vimrc`, vous pouvez piquer le mien sur mon **FTP** :

```
1 wget ftp://zteeed.fr/vimrc
2 mv vimrc ~/.vimrc`
```

Pour apprendre tous les bindings relatifs à vim, tapez `vimtutor` sur votre terminal ou cherchez des tutos en ligne : vous allez rapidement devenir très efficaces pour coder / éditer des fichiers rapidement.

### Comment installer des plugins ?

```
1 sudo apt install git curl
2 git clone https://github.com/junegunn/vim-plug.git
3 curl -fLo ~/.vim/autoload/plug.vim --create-dirs \
4   https://raw.githubusercontent.com/junegunn/vim-plug/master/plug.vim
5 vim ~/.vimrc
6 :PlugInstall
```

## Mettre à jour le site web : faire du php

Le site fonctionne sans **framework**, l'idée est que vous puissiez comprendre facilement et rapidement comment ça fonctionne sans que vous ayez à apprendre tout le fonctionnement d'une structure web complexe.

Toutes les modifications sont locales. Un cron job ajoute vos modifications sur le site tous les jours à 4h00. Voir la partie **git** pour envoyer vos modifications

Exemple pour cloner le site en local :

```
1 sudo apt install apache2
2 cd /var/www
3 rm -r html/
4 git clone https://github.com/zteeed/Cybersecurity-HackademINT.git
5 mv Cybersecurity-HackademINT html
6 firefox localhost
```

On passe à la modification du code php vim /var/www/html/writeups.php

```
1 <li>
2   <a onclick="activate('AngstromCTF')">AngstromCTF</a>
3   <div class="id" id="AngstromCTF">
4     <?php include('/writeups/2017-2018/AngstromCTF/angstromctf.php') ?>
5   </div>
6 </li>
```

/var/www/html/writeups/2017-2018/AngstromCTF/angstromctf.php

```
1 <li><a onclick="activate('AngstromCTFintrotorsa')">introtorsa</a></li>
2 <div class="id" id="AngstromCTFintrotorsa">
3   <?php include('introtorsa/introtorsa.php') ?>
4 </div>
```

/var/www/html/writeups/2017-2018/AngstromCTF/introtorsa

```
1 // contenu du writeup
```

## git

### C'est quoi ça encore ?

git est un outil de versionning de code. Il faut vous créer un compte sur <https://github.com> et que vous me donniez votre pseudo pour que je puisse vous ajouter comme collaborateur sur le **répo** HackademINT.

### Commandes utiles (+Google)

Vérifier que vous maniez git avec votre user

```
1 git config --list
2 git config --global user.name "mon_user"
3 git config --global user.email "mon_user@mail.fr"
4 git status
5 git add fichier.php
6 git commit -m "super update"
7 git push
```