

Proposer un contenu

Identifiant

Identifiant

Mot de passe

Mot de passe

☐ Connexion automatique

Se connecter

Pas de compte ? S'inscrire...

# Journal : Écrire des writeups CTF en français : documenter une méthode plutôt qu'une solution

Posté par NoelNac (site web personnel) le 10 octobre 2026 à 16:44. Licence CC By-SA.

Étiquettes : ctf, rien\_compris



## Sommaire

- - [Une solution ne suffit pas](#)
  - [Documenter le raisonnement](#)
  - [Écrire pour transmettre](#)
  - [Pourquoi en français ?](#)
  - [Et vous, comment documentez-vous vos résolutions ?](#)

Résoudre une machine Hack The Box, obtenir un premier accès, récupérer `user.txt`, puis parvenir aux privilèges nécessaires pour obtenir `root.txt` : voilà un objectif bien connu des amateurs de challenges CTF.

Mais une fois la machine résolue, que reste-t-il de cette expérience ?

On peut conserver quelques commandes, noter la vulnérabilité exploitée et passer à la machine suivante. On peut aussi prendre le temps de revenir sur les différentes étapes de la résolution, d'analyser les informations recueillies et d'expliquer le raisonnement qui a permis de progresser.

C'est cette seconde approche qui me tient à cœur et qui guide la rédaction de mes writeups.

Je rédige en français des writeups de machines Hack The Box. Mon objectif n'est pas simplement de montrer comment obtenir les deux flags, mais de documenter la démarche qui y conduit : l'énumération, la prise de pied et l'escalade de privilèges.

Cela m'amène à une question plus générale : **qu'est-ce qui rend un writeup véritablement utile pour apprendre, plutôt que simplement pratique pour reproduire une solution ?**

## Une solution ne suffit pas

Un writeup peut se limiter à une succession de commandes accompagnées de leurs résultats. Cela peut suffire pour reproduire une résolution, mais pas toujours pour comprendre ce qui a permis de progresser d'une étape à la suivante.

Lorsqu'on débute dans les CTF, il est tentant de suivre ces commandes les unes après les autres. On parvient parfois à obtenir les deux flags sans réellement comprendre les mécanismes mis en œuvre.

À mon sens, l'intérêt pédagogique d'un writeup réside surtout dans les explications qui accompagnent les différentes étapes : ce que révèlent les résultats de l'énumération, comment ces informations peuvent être exploitées pour obtenir un premier accès, puis comment l'analyse méthodique de l'environnement permet de rechercher une voie vers des privilèges plus élevés.

L'objectif n'est donc pas seulement de permettre au lecteur de reproduire la solution, mais de lui donner des éléments de compréhension qu'il pourra réutiliser face à une autre machine.

## Documenter le raisonnement

Pour rendre cette progression compréhensible, j'organise mes writeups autour de trois grandes étapes : **l'énumération, la prise de pied et l'escalade de privilèges**.

L'énumération constitue le point de départ. Elle consiste à recueillir des informations sur la machine cible à l'aide de différents outils. Pour faciliter et automatiser certaines de ces tâches, j'ai développé plusieurs scripts Bash que j'utilise régulièrement lors de mes résolutions. Dans mes writeups, je conserve les résultats obtenus sans chercher à les interpréter immédiatement. Cela permet de disposer d'une base d'observations sur laquelle s'appuyer pour la suite.

La prise de pied commence par l'analyse de ces résultats. L'objectif est de comprendre ce qu'ils révèlent, d'identifier les possibilités d'exploitation et de progresser jusqu'à obtenir un premier accès à la machine, puis à récupérer le fichier `user.txt`.

Enfin, l'escalade de privilèges repose sur une nouvelle phase d'observation et d'analyse méthodique de l'environnement, cette fois depuis l'accès obtenu. Pour cette étape, je m'appuie notamment sur une recette personnelle qui rassemble les vérifications et les commandes utiles pour rechercher une voie vers les privilèges `root` et récupérer `root.txt`.

Cette organisation permet de distinguer les informations recueillies de leur interprétation et de montrer comment chaque étape contribue à la progression vers l'objectif final.

## Écrire pour transmettre

La rédaction d'un writeup ne se résume pas à mettre en forme les notes prises pendant une résolution. C'est aussi l'occasion de revenir sur les différentes étapes, de vérifier certaines explications et de prendre le temps de comprendre les mécanismes rencontrés.

Cet exercice est également formateur pour celui qui écrit. Expliquer une technique de manière claire oblige parfois à approfondir un point que l'on pensait avoir compris lors de la résolution.

Une fois publié, le writeup devient une ressource que d'autres peuvent consulter pour découvrir une tech-

nique, comprendre une démarche ou retrouver une commande et son contexte d'utilisation.

## Pourquoi en français ?

La cybersécurité est un domaine dans lequel l'anglais occupe une place prépondérante. Une grande partie de la documentation des outils et des ressources consacrées aux CTF est rédigée dans cette langue.

Pour autant, je pense qu'il reste intéressant de produire et de partager des contenus techniques en français.

Découvrir une technique ou comprendre un mécanisme dans sa langue peut faciliter l'apprentissage, particulièrement lorsqu'on aborde un sujet nouveau.

Il ne s'agit évidemment pas de traduire systématiquement le vocabulaire technique. Des termes comme *reverse shell*, *payload* ou *privilege escalation* font partie du langage courant en cybersécurité et peuvent parfaitement être conservés lorsqu'ils sont accompagnés d'explications adaptées.

Publier des writeups en français, c'est simplement une manière de partager mon expérience et de rendre mes résolutions accessibles à ceux qui préfèrent lire des explications techniques dans leur langue.

## Et vous, comment documentez-vous vos résolutions ?

Au fil de mes résolutions Hack The Box, la rédaction d'un writeup est devenue une partie intégrante de l'exercice. Elle me permet de prolonger l'apprentissage au-delà de l'obtention des deux flags.

C'est dans cet esprit que je partage mes résolutions, ainsi que mes scripts et mes recettes techniques, sur [writeups.hackethical.be](https://writeups.hackethical.be).

Je serais curieux de connaître votre approche. Lorsque vous résolvez un challenge CTF, prenez-vous le temps de documenter votre démarche ? Et lorsque vous consultez un writeup, qu'attendez-vous principalement de son contenu : une solution reproductible, des explications détaillées ou un peu des deux ?

(0 commentaire).

Markdown

EPUB

Envoyer un commentaire

Suivre le flux des commentaires

**Note** : les commentaires appartiennent à celles et ceux qui les ont postés. Nous n'en sommes pas responsables.

Revenir en haut de page

### Derniers commentaires

- Re: dns
- Ca m'intéresse, tu p...
- Re: je me disais bien...
- Re: La partie qui n'a ...
- Mauvaise question
- La partie qui n'a "rie...
- J'ai pas regardé
- Re: Slovénie
- Re: Jugera tout ?
- Re: Mauvais choix
- Re: Information à la ...
- Re: dns

### Étiquettes (tags) populaires

- intelligence\_artificielle
- slop
- merdification
- grands\_modèles\_de...
- états-unis
- chine
- jihad\_butlérien
- capitalisme
- bigtech
- meta
- politique
- administration\_fran...

### Sites amis

- Agenda du Libre
- April
- Éditions D-BookeR
- Éditions Diamond
- Éditions Eyrolles
- Éditions ENI
- En Vente Libre
- Framasoft
- La Quadrature du Net
- Lea-Linux
- Open Source Initiative
- Imprimerie Grafik Plus

### À propos de LinuxFr.org

- Mentions légales
- Faire un don
- L'équipe de LinuxFr....
- Informations sur le s...
- Aide / Foire aux que...
- Suivi des suggestion...
- Wiki du site
- Règles de modération
- Statistiques
- API pour le développ...
- Code source du site
- Plan du site