WRITE-UP

HACKY' NOV

Pas le pingouin qui glisse le plus loin - Système

Linux

HACKY'NOV

Hacky'Nov est une association créée dans le cadre des YDAYS organisés par l'école YNOV qui organise chaque année un CTF afin d'initier le grand public aux différentes problématiques de cybersécurité.

L'événement est organisé par les étudiants du campus YNOV d'Aix-en-Provence et se décompose en trois parties.

La première partie est l'organisation d'un Capture The Flag (CTF). Chaque étudiant, de bachelor 1 à master 2 propose des challenges de cybersécurité, afin que les participants puissent en résoudre le maximum et gagner la compétition ! Les challenges sont axés de sorte que même les débutants puissent en résoudre un maximum tout en sachant faire plaisir aux plus expérimentés

La deuxième partie est dédiée à l'organisation de conférences autour de problématiques et sujets de cybersécurité. Elles sont proposées soit par des étudiants volontaires, soit par des intervenants externes afin de former et de sensibiliser les participants sur des sujets ciblés.

La troisième et dernière partie permet d'organiser la rencontre des étudiants avec des entreprises travaillant autour de la cybersécurité. Les entreprises partenaires de l'événement qui sont en majorité de grands acteurs du domaine, auront un espace unique et dédié à la mise en relation avec les participants, qui sont pour la plupart, des étudiants en cybersécurité.

https://hackynov.fr/

Table des matières

Partie 1 : Présentation du challenge

Nom du challenge : Pas le pingouin qui glisse le plus loin

Domaine : Système

Difficulté : Facile ★ ★ ★ ★ ★

Auteur : Linux

Description : Beeeeen Maurice là il a un ordi sous linux là, il sait même pas pourquoi mais il veut quand même savoir ce qu'il y a dessus au cas où t'as vu ? Du coup beeeen trouve comment faire quoi. Le contenu du flag est en minuscule

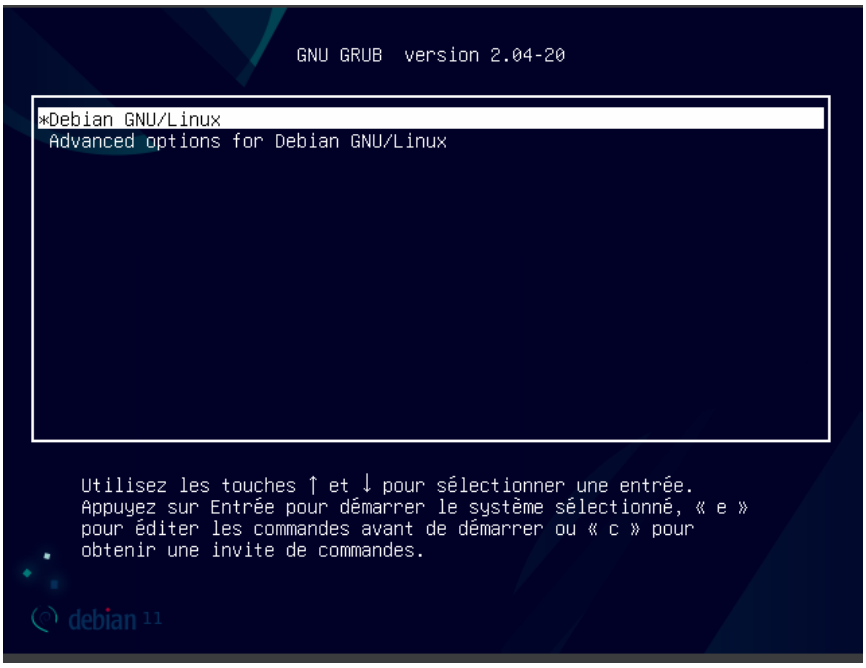
Partie 2 : Sources

Le challenge est à réalisé sur un des deux postes mis à disposition durant l'évènement. Il était donc composé d'une tour, d'un clavier et d'une souris.

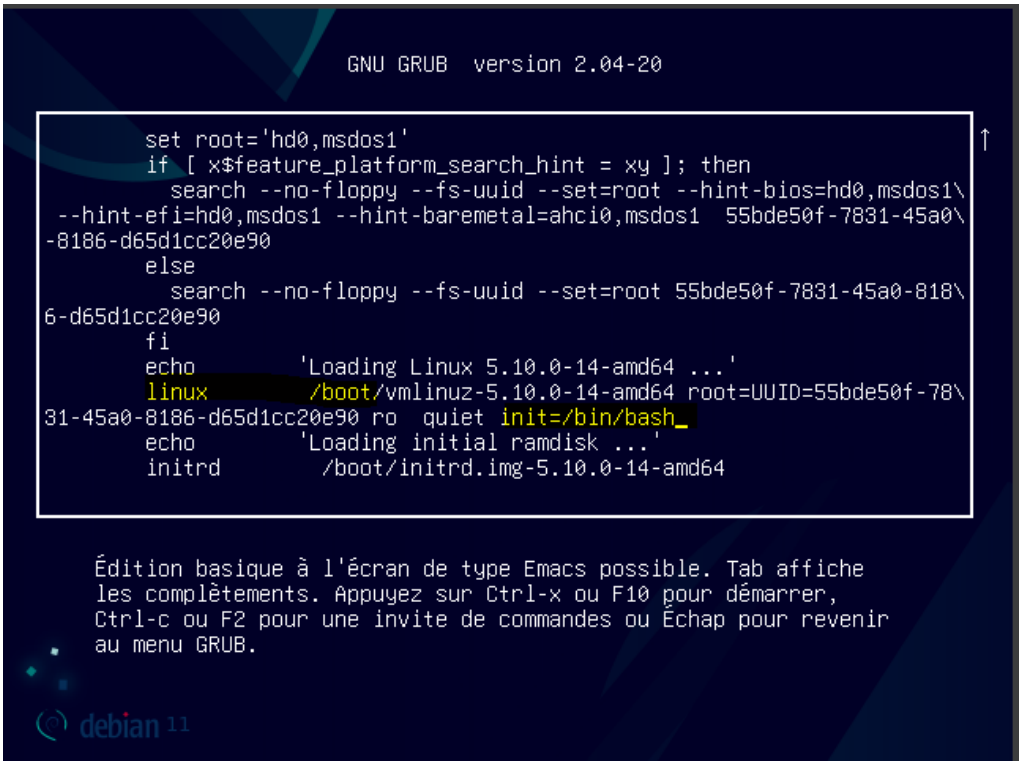
Le challenge se réalise sans rien brancher sur le poste (pas de clé USB), les modifications sont autorisées du moment que celles-ci ne sont pas destructives (pas d'altération/destruction des fichiers systèmes).

Partie 3 : Résolution

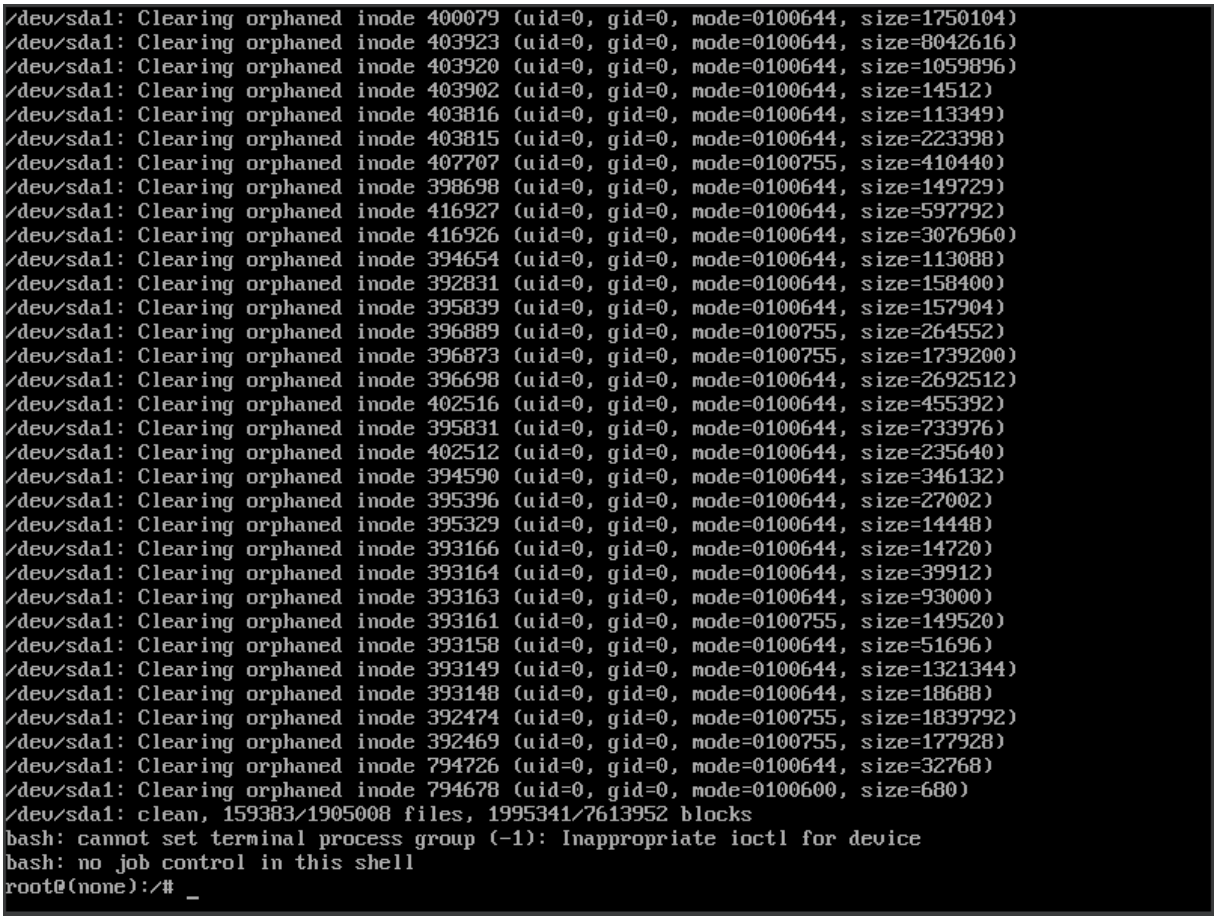
Lorsque nous arrivons sur le poste celui-ci est verrouillé et aucun mot de passe basique ne fonctionne. Il faut donc faire une manipulation bien connue qui est le reset de mot de passe via le grub. Lorsque l'on arrive sur ce menu, il faut appuyer sur E :



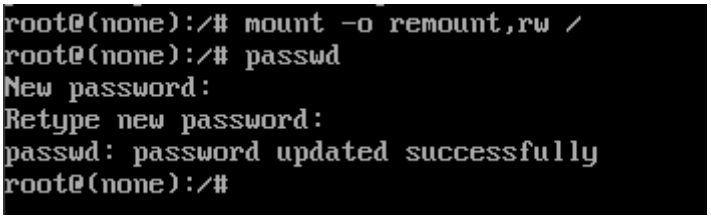
Une fois fait, nous arrivons sur ce fichier, afin de lancer un terminal en root il faut modifier la ligne commençant par « linux /boot » en ajoutant à la fin : init=/bin/bash



Puis appuyer sur F10, pour arriver sur un shell root :

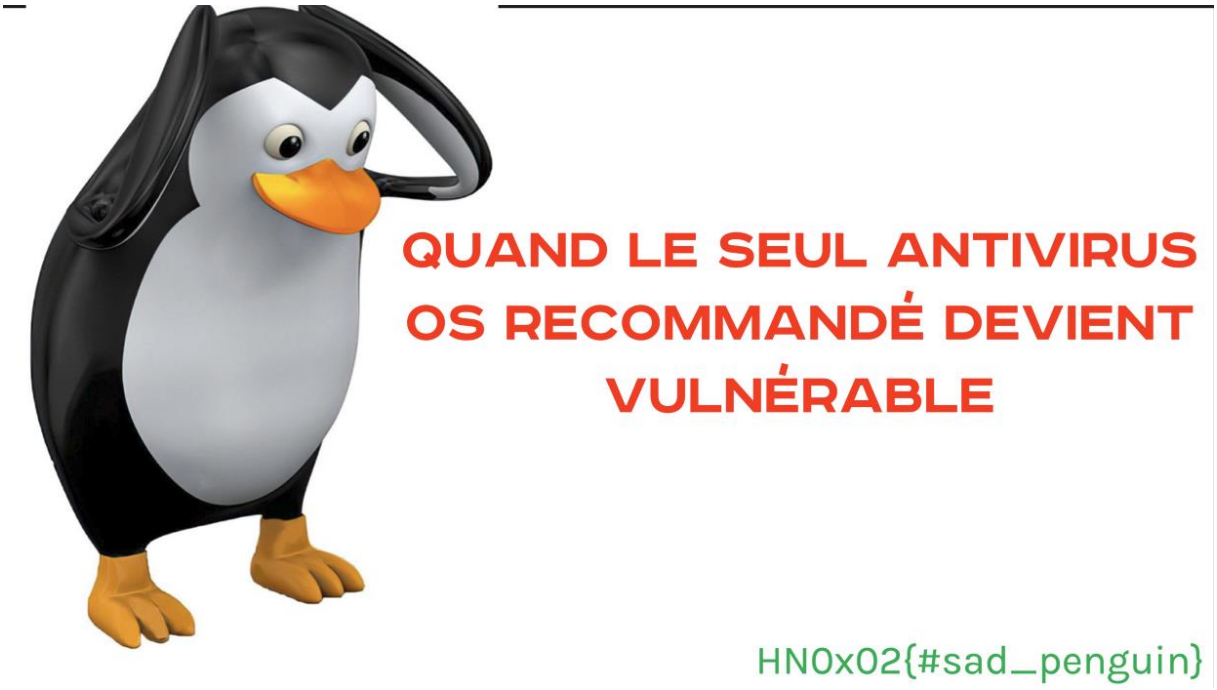


Enfin, il fallait permettre la modification du mot de passe avec la commande « mount -o remount,rw / » pour autoriser l'écriture et ensuite il suffisait de modifier le mot de passe root avec la commande passwd :



Maintenant, redémarrer le poste avec la commande reboot -f (reboot seul ne fonctionne pas dans ce mode)

Nous arrivions enfin sur ce fond d'écran :



Flag : HN0x02{#sad_penguin}