

WRITE-UP

Sensibilisation

SARTORI BOUTY Marie-Laure & LASSEAUX Rémy

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.....	4
Partie 2 : Sources	4
Partie 3 : Résolution	5
Mauvaise pratique 1	5
Mauvaise pratique 2.....	6
Mauvaise pratique 3.....	7
Mauvaise pratique 4.....	8
Mauvaise pratique 5.....	8
Mauvaise pratique 6.....	10
Mauvaise pratique 7.....	11
Mauvaise pratique 8.....	12
Partie 4 : constitution du flag.....	13

Partie 1 : Présentation du challenge



Nom du challenge : Mauvaises pratiques

Domaine : Sensibilisation sur Unity

Difficulté : ★ ★ ★ ★ ★

Auteur : SARTORI BOUTY ML & LASSEAUX
Rémy

Description :

La sécurité des systèmes d'informations est de plus en plus cruciale,

Cependant beaucoup d'entre nous sont encore de mauvais élèves et n'ont pas les petits réflexes simples du quotidien au travail comme dans la vie personnelle.

Et vous ? les avez-vous ?

Découvrez 8 mauvaises pratiques que certains employés possèdent !

A l'issue du challenge vous obtiendrez un mot. Pour valider ce challenge, remplacez "FLAG" par le mot trouvé.
Format attendu : HN0x02{FLAG}

Partie 2 : Sources

Rendu Hacky'Nov : Build unity (code compiler)

Docker file avec Nginx

Mettre à disposition des participants : URL

Partie 3 : Résolution

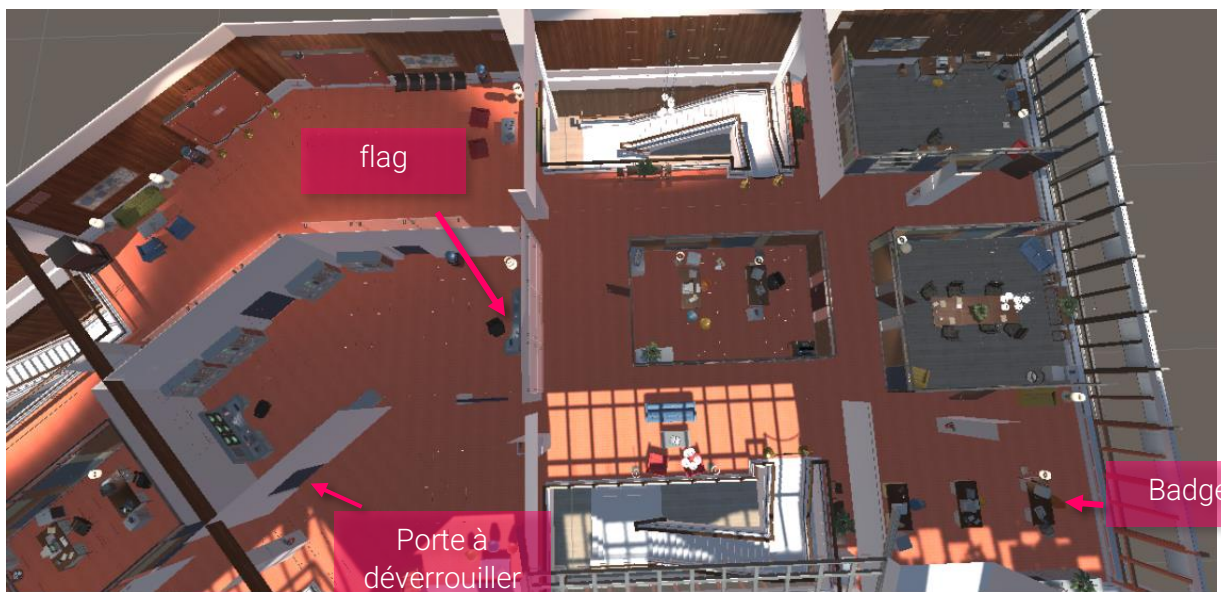
Chaque mauvaise pratique peut être trouvée indépendamment des autres et ne suit en aucun cas un ordre précis.

Mauvaise pratique 1

Le badge

Il est nécessaire de mettre la main sur le badge d'un des employés qu'il aurait égaré ou oublié. Ce badge ouvre les portes de la pièce centrale de l'entreprise. Le flag se trouve sur un des paquets disposés dans la pièce.

Flag à trouver : A6



Mauvaise pratique 2

La poubelle

Certains employés ne mesurent pas l'importance de la destruction des documents pouvant porter des informations plus ou moins sensibles. Il faut fouiller chacun des poubelles de l'entreprise. L'une d'entre elle contient un document confidentiel qui n'a pas été détruit par une broyeuse.

Flag à trouver : C3

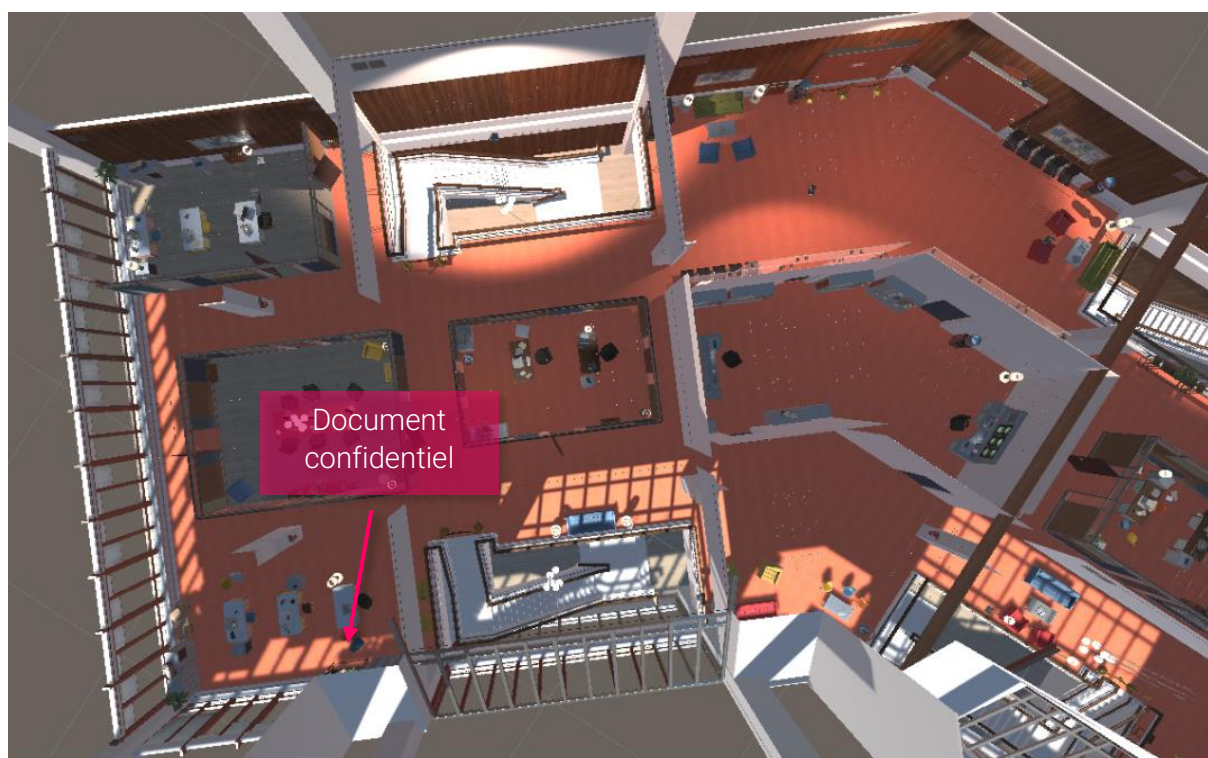


Mauvaise pratique 3

Document confidentiel en libre accès

En fonction de la sensibilité du contenu du document, il est important de limiter son accès en le gardant dans une armoire sous clef. Mais ce n'est parfois pas le cas. Il faut trouver un casier comportant le document et l'ouvrir.

Flag à trouver : D6

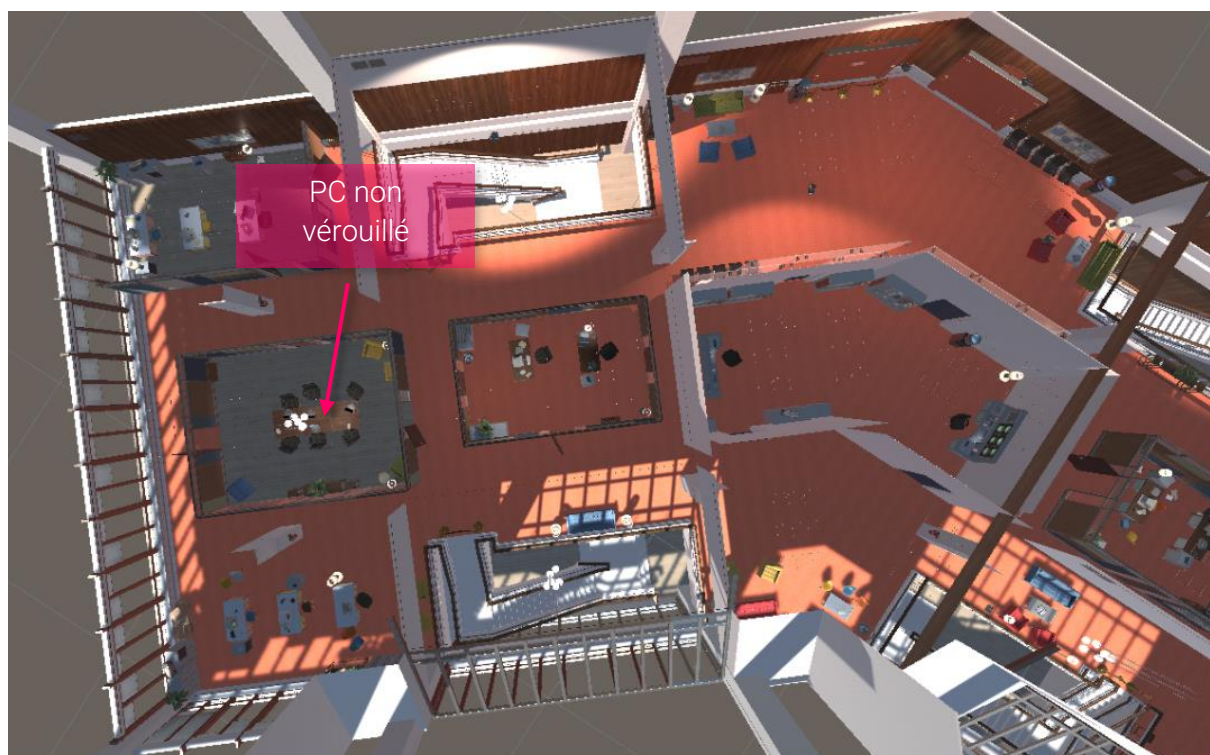


Mauvaise pratique 4

Session non verrouillée

Ne pas verrouiller son ordinateur pendant notre absence, laisse la porte ouverte à toutes personnes, malveillante ou non, à notre système. Un pc non verrouillé est laissé dans une salle de réunion. Il suffit d'y mettre la clef au contenu douteux pour obtenir le flag.

Flag à trouver : E1



Mauvaise pratique 5

Social engineering

Certains hackers usent de l'observation pour récolter des informations personnelles pouvant être utilisé en tant que mot de passe de session. Dans l'un des bureaux de l'entreprise, un cadre est posé à côté d'un ordinateur verrouillé. Cependant, ce cadre comporte le mot de passe de la session...

Flag à trouver : A3



Mauvaise pratique 6

Dossier égaré en salle de réunion

Mal conservé, oublié ou tout simplement penser que 5 minutes d'absences n'auront aucune conséquence peut être cruciale. Un document confidentiel a été laissé dans une salle de réunion.

Flag à trouver : D6



Mauvaise pratique 7

Divulgarion du mot de passe

L'une des bonnes pratiques est de garder son mot de passe confidentiel et de ne pas le divulguer. Une lettre au sol indiquera où trouver le papier contenant le mdp. Il se trouve dans un casier noir dans un bureau. La première citation parle d'une « baie » pour B et la deuxième de « 5 »

Flag à trouver : B5



Mauvaise pratique 8

Photocopieuse

Dans une entreprise, il est commun que les différents services qui la composent, partagent la même imprimante. De ce fait, il n'est pas rare que certaines personnes oublient les documents qu'ils auraient imprimés.

Flag à trouver : B4

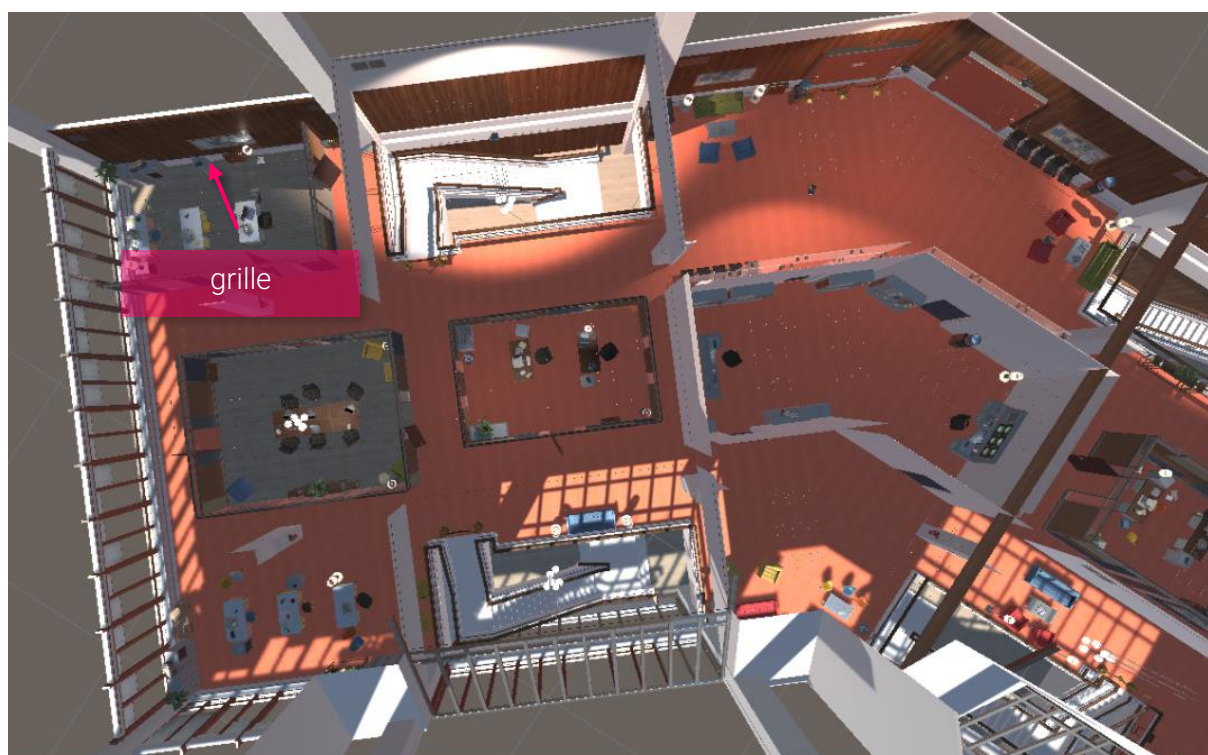


Partie 4 : constitution du flag

Une grille semblable à celle de la bataille navale a été affichée sur un des tableaux de l'entreprise.

Chacune des mauvaises pratiques trouvées désigne l'emplacement d'une lettre de cette grille.

A6 : M
C3 : A
D6 : I
E1 : T
A3 : R
D6 : I
B5 : S
B4 : E



Flag : HN0x02{MAITRISE}