2025.06.02 Bloc 3 - TP5 Yolocft

**

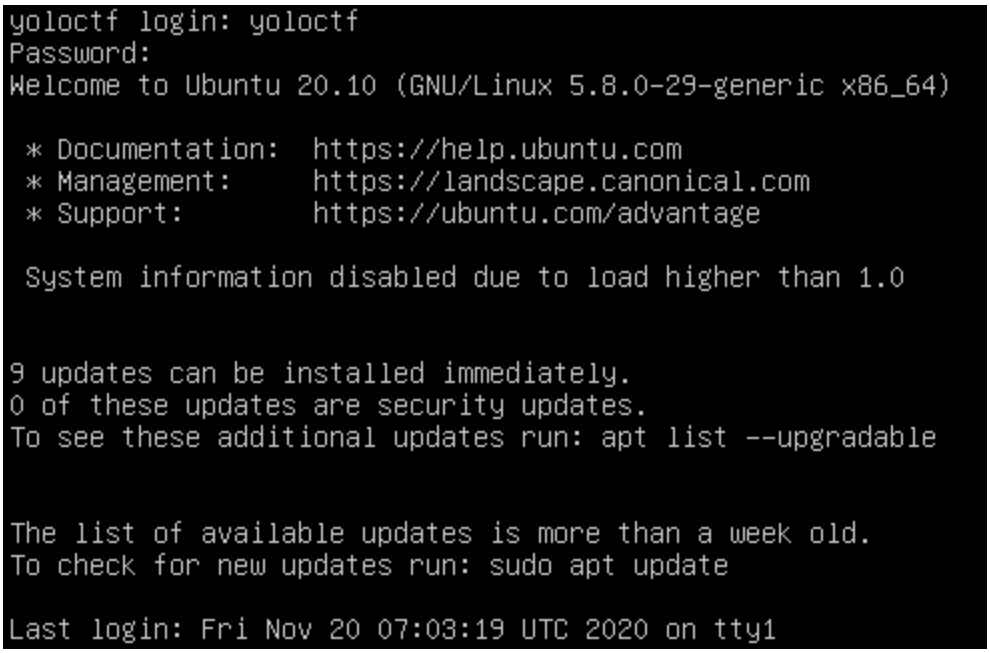
Pour installer l'image disque sur notre VMware il faut déjà la télécharger sur : https://drive.google.com/uc?id=1LvcRQ8aUUXzW4xIUsc8UmsR_kseuti4i&export=download

Une fois téléchargé, il faut extraire le dossier via 7zip (uniquement 7zip) et ainsi récupérer le VMDK (et non simplement l'image OVA) et Mettez vous en BRIDGE

Une fois sur le terminal, il demande de choisir un login.

Login : yoloctf

password : yoloctf



Si nous ne sommes pas seul sur le réseau, il faut changer le mot de passe.

Identifiez l'adresse IP du serveur

```
yoloctf@yoloctf:~$ ifconfig | grep enp -A 1
yoloctf@yoloctf:~$ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 984  bytes 70352 (70.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 984  bytes 70352 (70.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```


Allons maintenant dans le répertoire des fichier et ainsi personnaliser un peu la configuration

```
yoloctf@yoloctf:~$ cd ~/mon_premier_ctf
yoloctf@yoloctf:~/mon_premier_ctf$ cd ~/mon_premier_ctf/web_server
yoloctf@yoloctf:~/mon_premier_ctf/web_server$ nano .env
```

```
  GNU nano 5.2                                    .env
#
# docker-compose environement file
#


MYSQL_ROOT_PASSWORD=amkixiuaxvyzbohb
MYSQL_USER_PASSWORD=ivahohyoyznkhgys

#
# web server admin account
# change the password
#
CTF_ADMIN_ACCOUNT=admin
CTF_ADMIN_UID=rgibfmttpwufwvcm
CTF_ADMIN_PASSWORD=adminyolo


# CTF_SCOREBOARD_AFF
# all       : all users
# user_only : only logged user, or joined CTF
CTF_SCOREBOARD_AFF=all


# CTF_LOCALE_ENABLED
# true : let user change langage (english)
# false : french only
CTF_LOCALE_ENABLED=false


# CTF_REQUIRE_EMAIL_VALIDATION
#
# true  : User account enabled after mail validation. CTF_MAIL_ENABLED must be true, CTF_MAIL_XXXX >
# false : User account enabled withour mail validation
                                [ Read 57 lines ]
^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line M-E Redo
```

Definissons un code d’invitation pour filtrer les participants dans werb_server/.env

Retirez le # dans cette ligne :

CTF_REGISTER_CODE=YOLO

et mettez y le filtre “MonCode”

```
# CTF_REGISTER_CODE
#
# Not set or empty : no code needed to register
CTF_REGISTER_CODE=MonCode_
```


On peux également donner un titre perso à notre CTF en enlevant le # en début de ligne dans cette ligne :

#CTF_SUBTITLE=Mon 2nd CTF

```
# CTF_TITLE=YOLO CTF
CTF_SUBTITLE=Montargis CTF
# CTF_LOGOFILE_1=img/logo-iut-blagnac.png
```

Mot de passe admin statique

cd web_server

./go_rebuild_db

Lancez le serveur

cd ~/mon_premier_ctf

./go_first_install_webserver_run

```
Building webserver_php
Step 1/3 : FROM php:7-fpm
 ---> 876051031ecc
Step 2/3 : RUN docker-php-ext-install mysqli
 ---> Using cache
 ---> bd84ea48b821
Step 3/3 : COPY www.conf /usr/local/etc/php-fpm.d/www.conf
 ---> Using cache
 ---> 31d836e0d053
Successfully built 31d836e0d053
Successfully tagged web_server_webserver_php:latest
traefik is up-to-date
webserver_mysql is up-to-date
webserver_nginx_frontdoor is up-to-date
webserver_php is up-to-date
webserver_nginx is up-to-date
Starting challenge-box-provider ... done
Running ctf-passwd/challenge_start.sh
Starting ctf-passwd-php ... done
Starting ctf-passwd-web ... done
Running ctf-sqli/challenge_start.sh
Starting ctf-sqli_mysql ... done
Starting ctf-sqli_php   ... done
Starting ctf-sqli       ... done
**********

S'il n'y a pas eu de message d'erreur, vous pouvez à présent vous connecter à l'interface web:
http://localhost/yoloctf/


compte admin   : admin
password admin : adminyolo
```

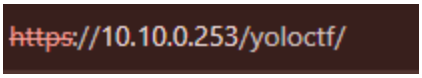
Récupérons les identifiants du compte de l'administrateur du CTF :

admin

adminyolo

```
yoloctf@yoloctf:~/mon_premier_ctf$ ip -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
ens33            UP             10.10.0.253/16 fe80::20c:29ff:fe8f:63f5/64
br-1e91b185bf40  UP             172.22.0.1/16 fe80::42:56ff:fe1b:1c6e/64
br-22b56b97b7e6  UP             172.19.0.1/16 fe80::42:17ff:feb3:e7a2/64
docker0          DOWN           172.17.0.1/16
br-7c038606d012  DOWN           16.2.0.1/16
br-875b67c16dec  UP             172.21.0.1/16 fe80::42:8eff:fe0d:44d9/64
br-cc4a82cd2309  UP             172.18.0.1/16 fe80::42:82ff:fe7e:79f2/64
br-e6ed092819ef  UP             172.20.0.1/16 fe80::42:b6ff:fe87:ed6/64
vetha1eabe3@if10 UP             fe80::bc63:d5ff:fe17:da08/64
vethb0c2cc4@if12 UP             fe80::1ca9:94ff:fe9d:e0ea/64
vethe45baec@if14 UP             fe80::dc65:a3ff:fee2:1b6e/64
vethce32a75@if16 UP             fe80::74a5:fbff:fe15:ae7b/64
veth4cb6cb2@if18 UP             fe80::4497:a9ff:fe07:c568/64
veth522e059@if20 UP             fe80::acd5:75ff:fee6:d1fa/64
veth48cb34e@if22 UP             fe80::e812:c9ff:fe4c:ad81/64
veth5de0c8b@if24 UP             fe80::3c55:c5ff:fed5:c967/64
veth187f3c2@if26 UP             fe80::74f7:7aff:fe49:cf9c/64
veth81911aa@if28 UP             fe80::6450:68ff:fe68:b345/64
veth5c0051a@if30 UP             fe80::601e:16ff:fe29:340b/64
veth80c348b@if32 UP             fe80::9cb0:acff:feb3:1bf0/64
vethaaf7f8c@if34 UP             fe80::18d5:2fff:fe1e:1684/64
veth9652231@if36 UP             fe80::dccf:eff:fedb:eab8/64
veth79b5905@if38 UP             fe80::8c64:59ff:fe40:2eda/64
```

En tapant notre adresse IP dans le navigateur de notre machine physique : 10.10.0.253



YOLO CTF

Montargis CTF

anonymous

Login

C'est quoi un CTF ?

Un CTF est une compétition, basée sur des failles de sécurité réelles. C'est l'idéal pour apprendre, dans une ambiance fun, avec les mains sur le clavier.

Pour qui ?

Les CTF s'adressent aux pro, mais aussi et surtout aux amateurs, étudiants, passionnés, curieux... Cette plateforme est destinée à toute personne ayant un vernis de Linux (cd, ls,...).

Des challenges ?

Vous avez à résoudre des challenges de difficulté croissantes en temps limité. Chaque challenge rapporte des points en fonction de sa difficulté, et le classement est en temps réel.

Jeopardy vs Attack-Defense ?

Il existe deux types de CTF, le 'Jeopardy', où tout le monde résout des challenges, et l' 'Attack-Défense' qui demande un niveau certain. Dans ce dernier mode, vous devez patcher/défendre votre serveur tout en allant prendre les flags chez vos concurrents. Ce CTF est un Jeopardy.

Des thématiques variées

Tout ce qui peut être mal configuré ou présenter une vulnérabilité exploitable est candidat pour un challenge.

- Chiffrement de données avec des algorithmes 'faibles'
- Reverse sur des fichier executables
- Analyse de code source
- Web dans le navigateur
- Web sur le serveur
- Protocole réseau
- IoT: caméras, tv, voiture,...

**