Keeper

nmap

```
└─$ nmap -sC -sV -oN nmap/init.nmap 10.10.11.227
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-12 15:16 EDT
Nmap scan report for 10.10.11.227
Host is up (0.089s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 35:39:d4:39:40:4b:1f:61:86:dd:7c:37:bb:4b:98:9e (ECDSA)
|_  256 1a:e9:72:be:8b:b1:05:d5:ef:fe:dd:80:d8:ef:c0:66 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.07 seconds
```

Looks like a simple web challenge involving nginx running on ubuntu

port 80

Navigating to the ip address, there is a link to http://tickets.keeper.htb
-> let's add to our hosts file

gobuster for directories, ffuf for subdirectories doesn't find anything

We need to look into http://tickets.keeper.htb which looks like a request tracker app

There is a login prompt for request tracker. Default creds of root:password let's us in

Emails found on the website
lnorgaard@keeper.htb
webmaster@keeper.htb

Found on request tracker admin page:

DatabaseAdmin	'postgres'
DatabaseExtraDSN	{}
DatabaseHost	'localhost'
DatabaseName	'rtdb'
DatabasePassword	*Password not printed*
DatabasePort	'3306'
DatabaseRTHost	'localhost'
DatabaseType	'mysql'
DatabaseUser	'rtuser'

Found initial password for the user on the user modification page:
lnorgaard:Welcome2023!
-> Allows us to ssh in!

priv esc

In lnorgaard's home directory, we find a dump file and a zip containing a passcodes.kdbx file

CVE-2023-32784 allows us to dump most of the master password
-> POC: https://github.com/vdohney/keepass-password-dumper
using the POC, we extract the master password with some missing characters:
●{,, l, `, -, ',], A, I, :, =, _, c, M}dgr●d med fl●de

recalling from the website that lnorgaard is danish, I use google translate to confirm that “med” is indeed danish.

now searching med flode, I find out that Rødgrød med fløde is a danish red berry pudding
so the master password is:
rødgrød med fløde

Logging into passcodes.kdbx using my windows box,
we find out root's PuTTY SSH password is:
F4><3K0nd!
-> This actually does not help

What actually helps is there is a PuTTY ssh private key in the comments we can use to login as root
- Copy paste the key into Notepad++ (idk why but using regular notepad did not work)
- Transfer to kali using an smb share
- Use `putty` to ssh in as root using the key