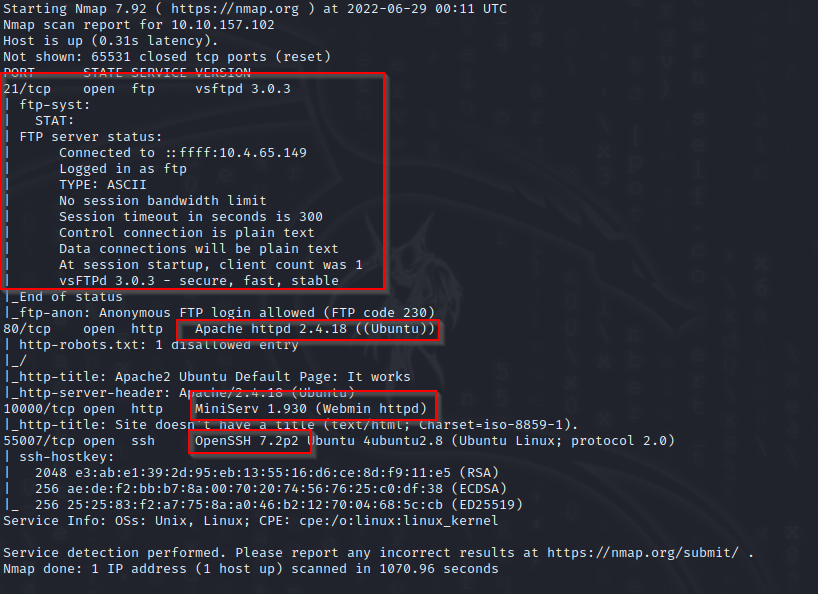
<https://tryhackme.com/room/boilerctf2>

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 11251 users are in here and this room is 1042 days old.

Created by  [MrSeth6797](https://tryhackme.com/p/MrSeth6797)

rustscan -a $ip

(Initially I only found two ports open, when I came back from break a rescanned and found 4 ports open, so I did a full Nmap scan again.



We found 4 ports open

**Port 21**

FTP port running vsftp 3.0.3

Anonymous log on allowed

**Port 80**

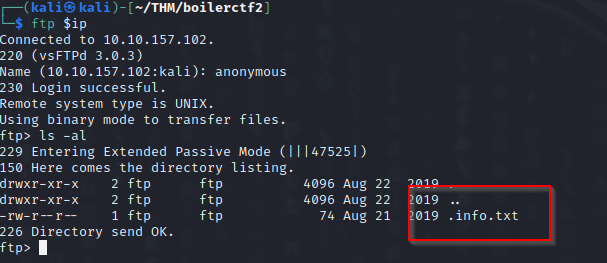
HTTP server Apache 2.4.18 most likely on Ubuntu

**Port 10000**

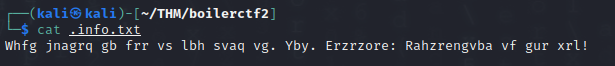
Webmin 1.930

**Port 55007**

Ssh

**Anonymous FTP**

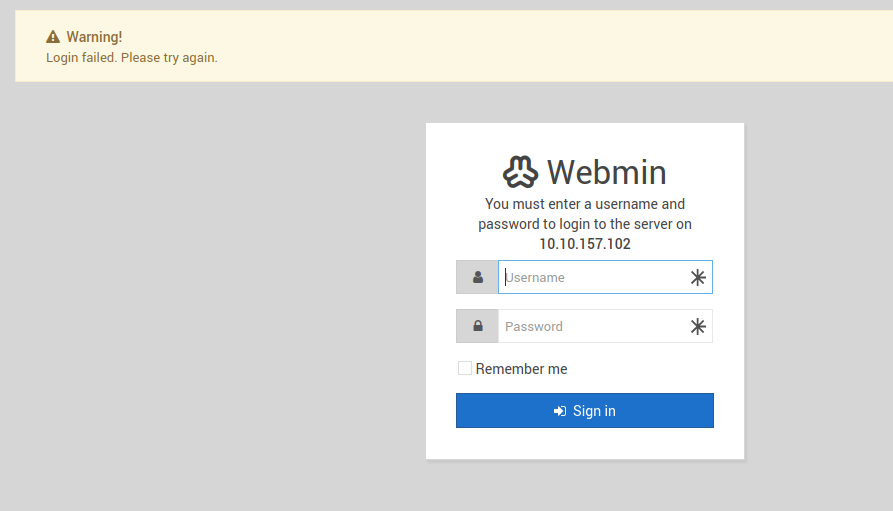
There is a hidden file .info.txt



Some sort of coded message

**Port 10000 webmin**

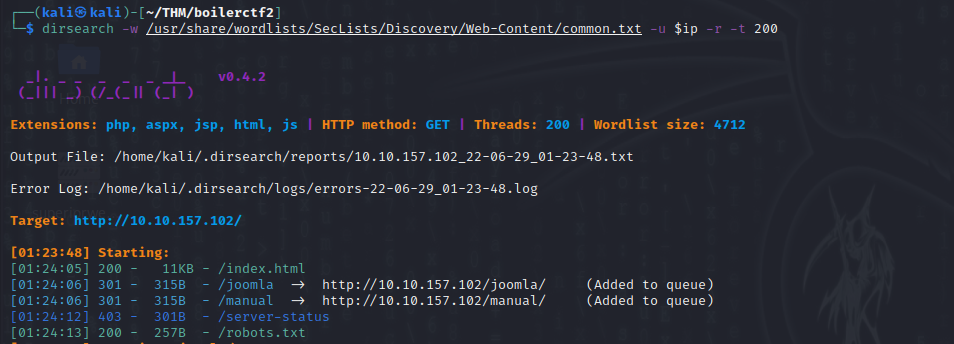
Webmin provides:



The server does not have the vulnerability of displaying users with failed logon attempts

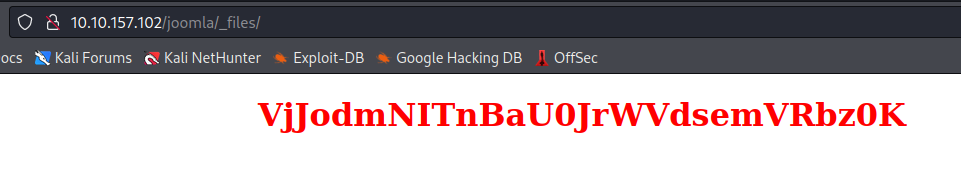
**Port 80**

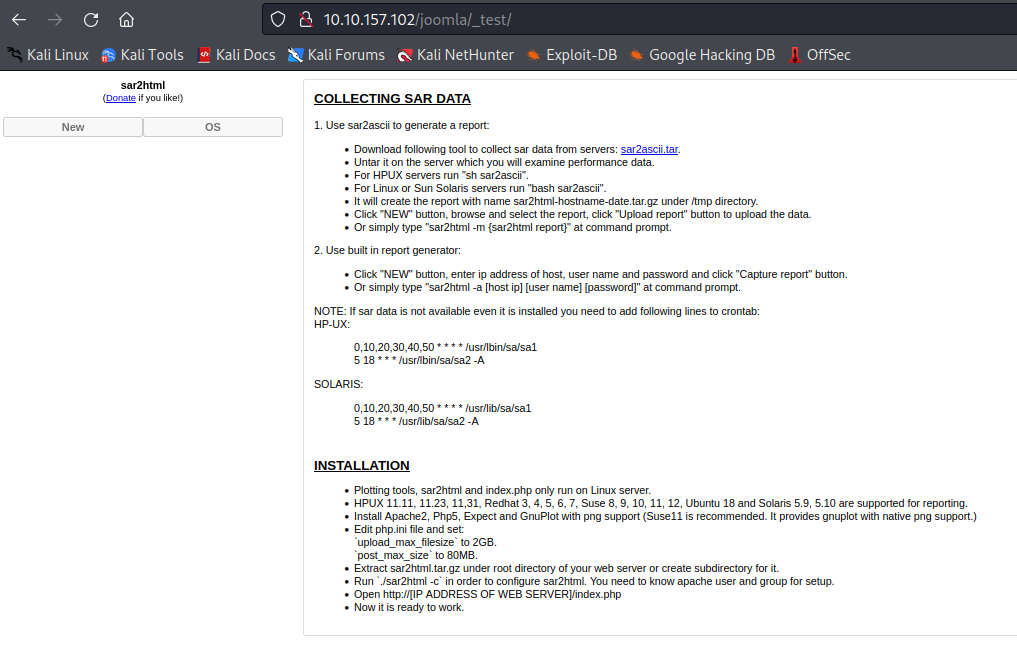
We run a dir search



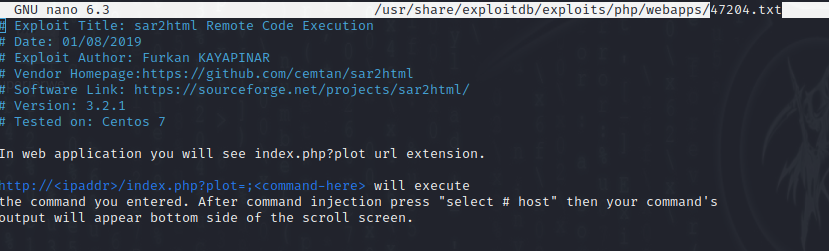
The robots.txt files shows something interesting 

Dirsearch found \_files and \_test

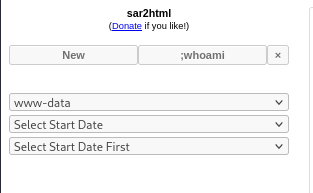




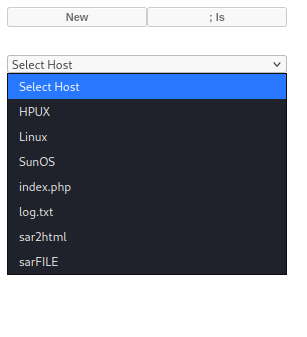
After searching for a exploit if found this :



I used it and tested with whoami



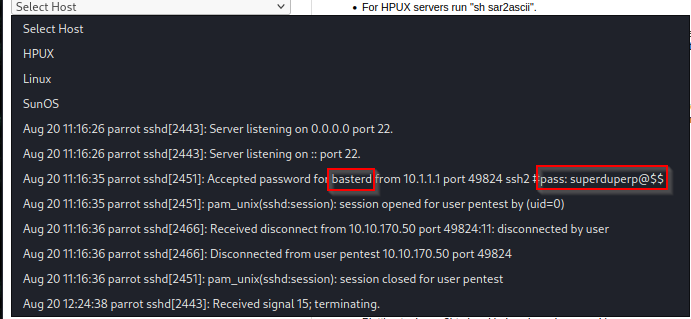
And ls



/etc/passwd



Catting the log file shows a username and password

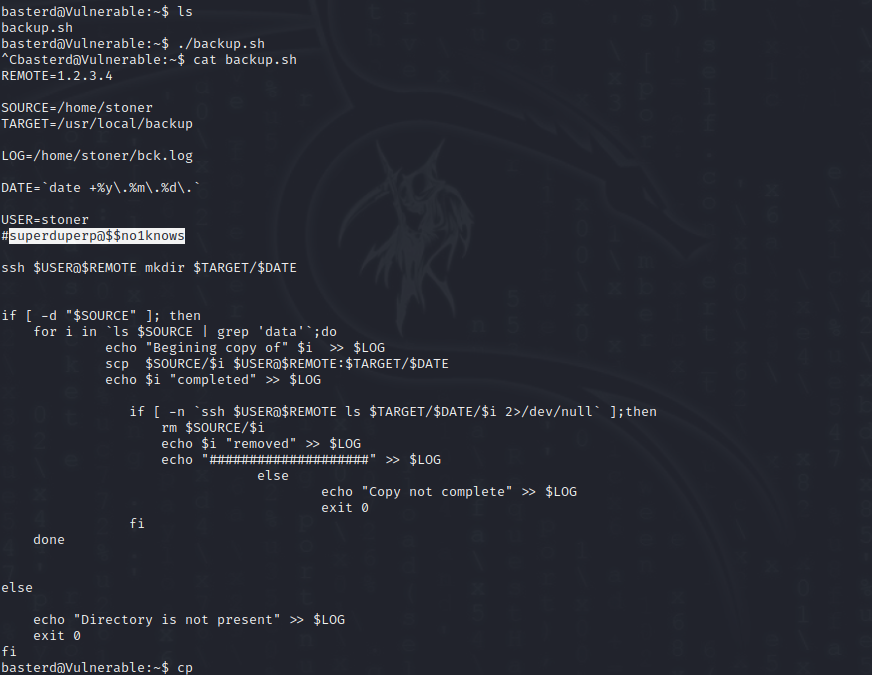


We confirmed the username basterd and the password of superduperp@$$

Inside bastards home folder there is a backup scrip

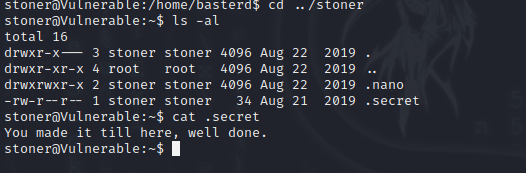
Inside the scrip there seem to be more user credentials

User stoner password superduperp@$$no1knows



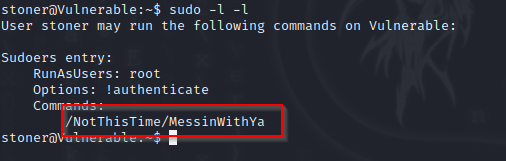
Changing users, su, givers us access to the stoner users

Inside his home folder, there is another .secret file



See what the sudo –l givers us ☺

The creator is very creative



To dig further we use linpeas

Wget is not available so we used scp instead





As usual linpeas comes to the save

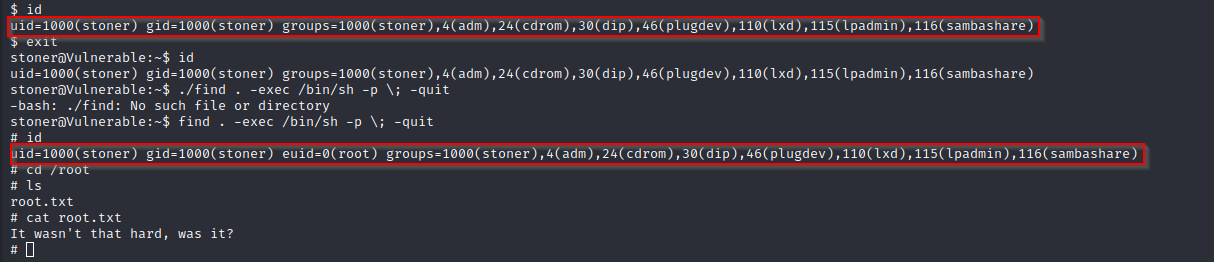
It finds “find” being vulnerable to SUID



Running

* ./find . -exec /bin/sh -p \; -quit

Gives us root group access and access to the root folder



**Summary**

The system contains a lot of “rabbit holes” and false leads to follow.

Lot of what seems like encodes messages or text

Eventually a vulnerability was found inside the sar2html app.

This in itself was hard to find

Inside the folder were a clear saved credential that we were able to use to ssh to the account bastard

In the home folder of bastard, we located the credentials of stoner

We changed users to stoner and found that the “find” command provided us with SUID access

**Recommendation**

Update all software/web apps to the latest version

Restrict access to some URL / services

A firewall can black a url to the sar2html location

Clear and delete all clear saved password files: log.txt and backup.sh

Use private/public keys

Change the suid for the find command