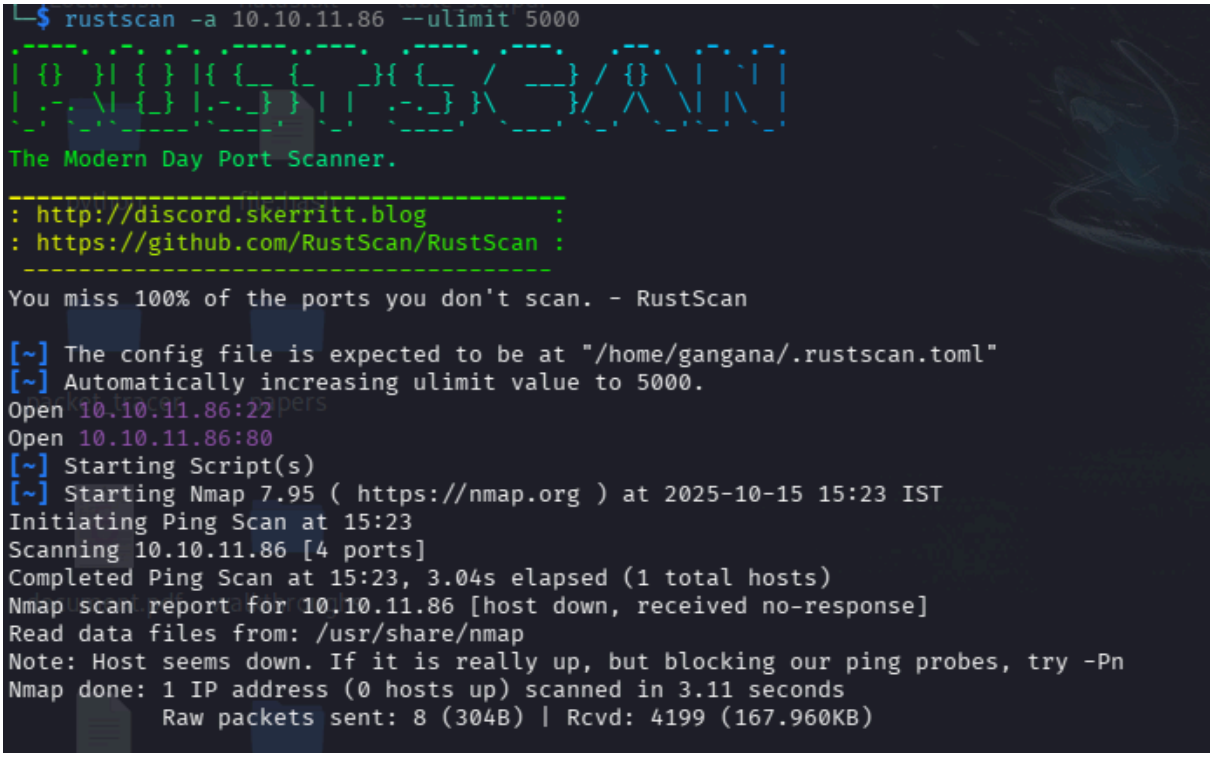
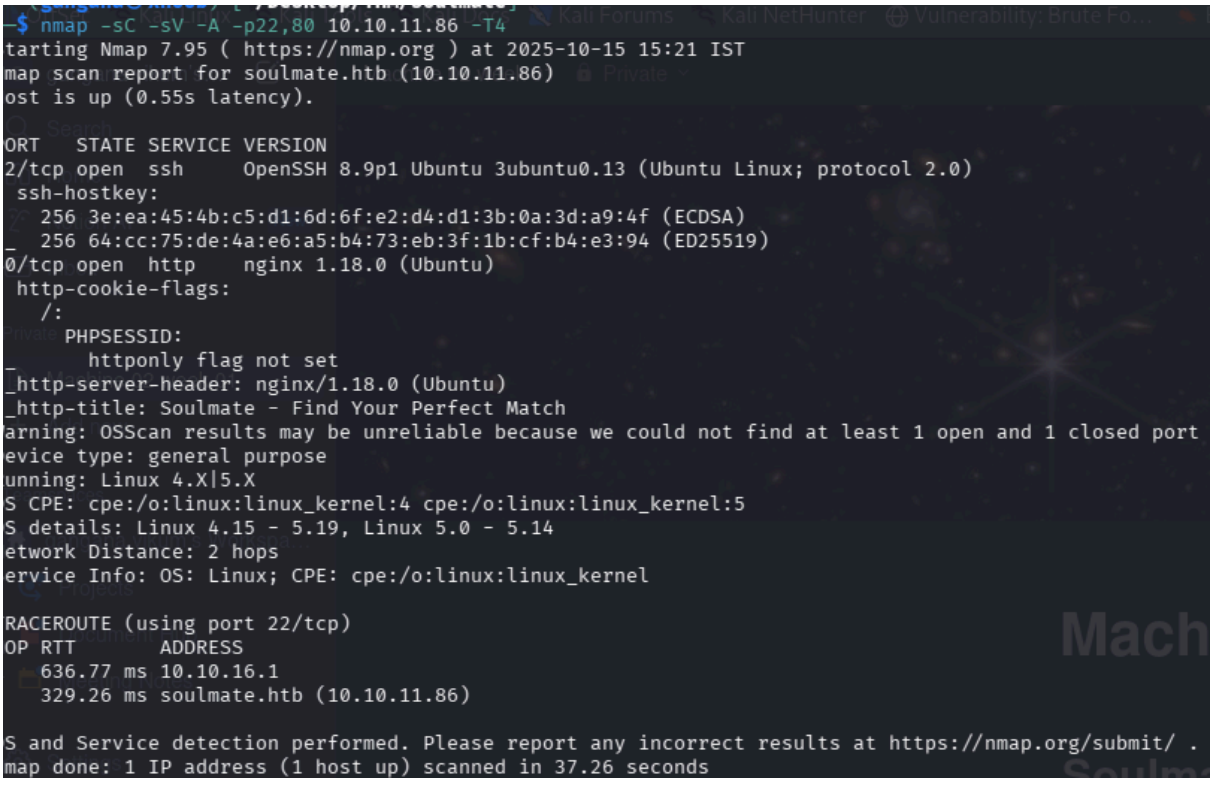
Hackthebox Retired Machines.

Soulmate - HTB Machine

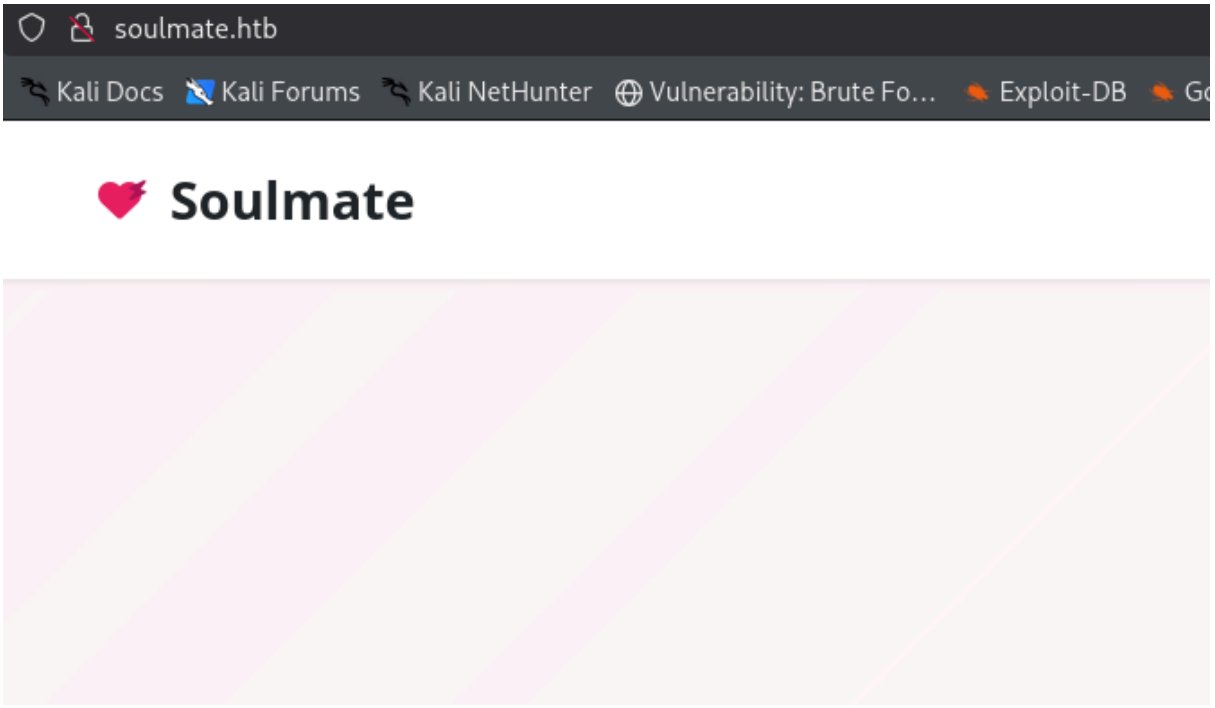
Rustscan and nmap results:

Here I prefer to run rustscan first because we can find out what ports are open the run the nmap to scan relevant ports for further dive deeper.





After finding port 80 is open past the ip in browser and http://solmate.htb domain has reached.



after trying ,

- source code hint
- web directory fuzzing
- sql injection
- bruteforuce attack(some commom credentials to findout error responses leak any info.)

finally done a subdomain fuzzing using gobuster

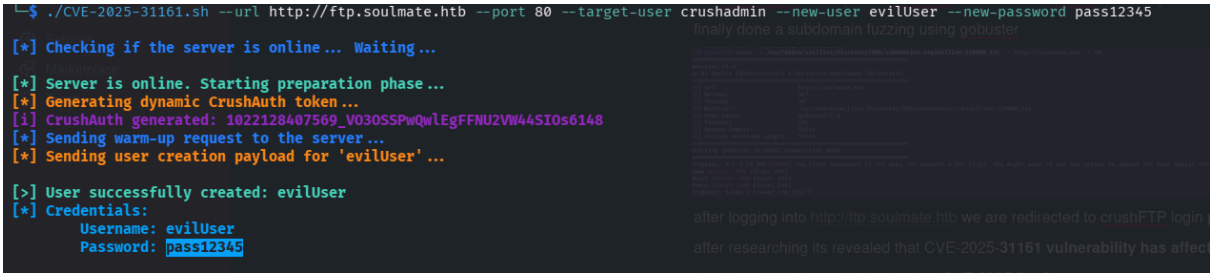
after logging into http://ftp.soulmate.htb we are redirected to crushFTP login page

after researching its revealed that CVE-2025-**31161 vulnerability has affected.**

▼ https://www.huntress.com/blog/crushftp-cve-2025-31161-auth-bypass-and-post-exploitationhttps://github.com/f4dee-backup/CVE-2025-

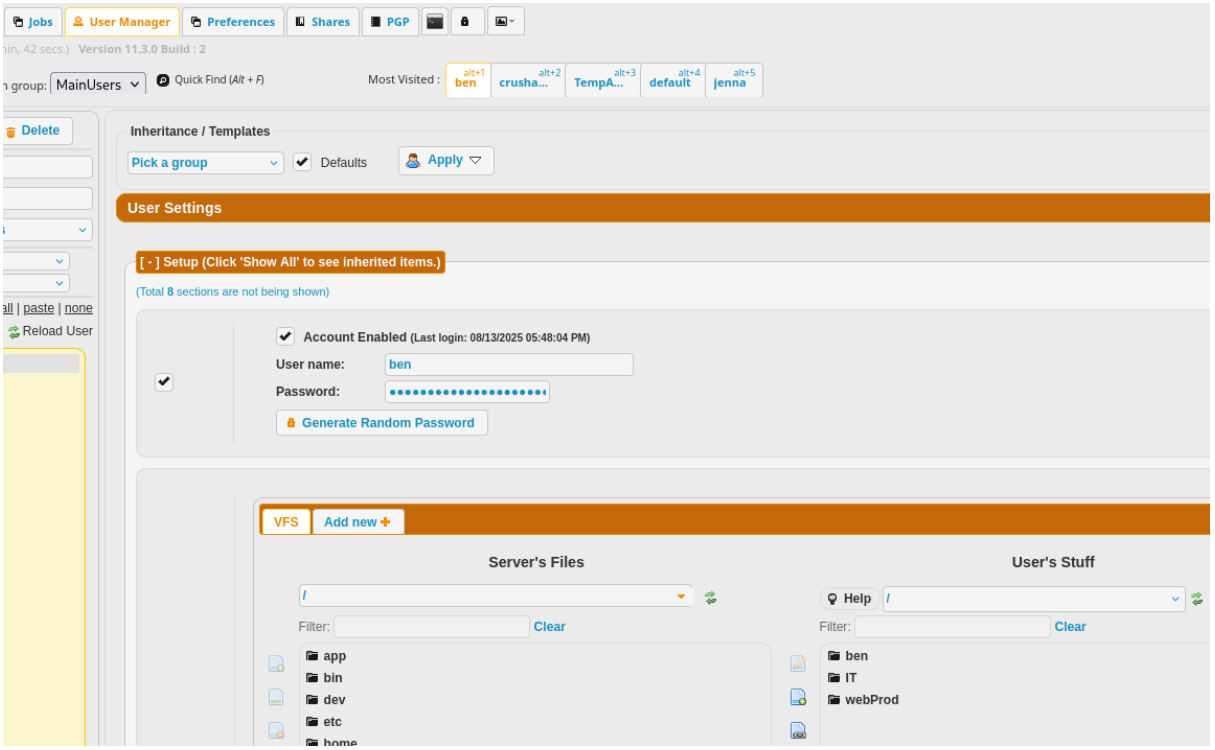
31161https://github.com/f4dee-backup/CVE-2025-31161

Above Github poc can be used to create the crushadmin account with CrushAuth token



then successfully login into the newly created account.

after logging in click on admin tab and click on the ‘manage users’ tab

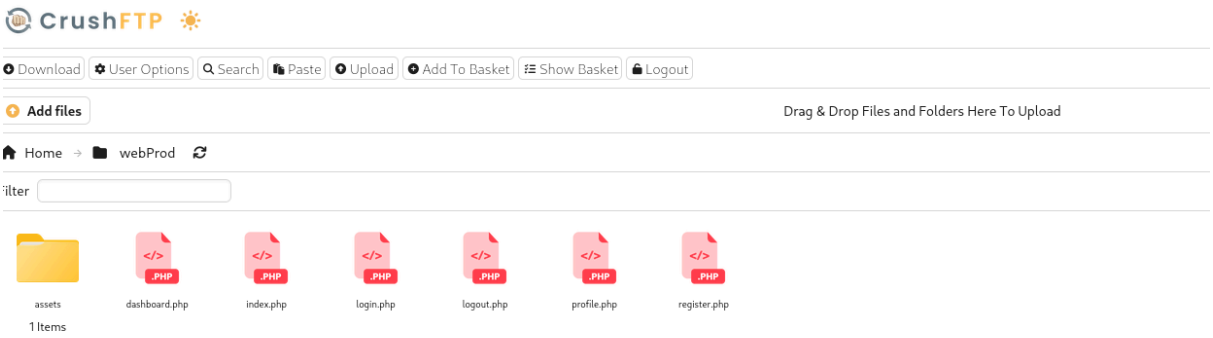


Then i see user ben has uploaded some web stuff like files essential for soulmate.htb site.and i could reset the password of the user ben and logging with ben’s account to do something weird.

make sure to save the changes you have done.before login again.

{Note that most visited account is also ben.}

in jenna’s account she only related with department called directory that contains some scripts like stuff.

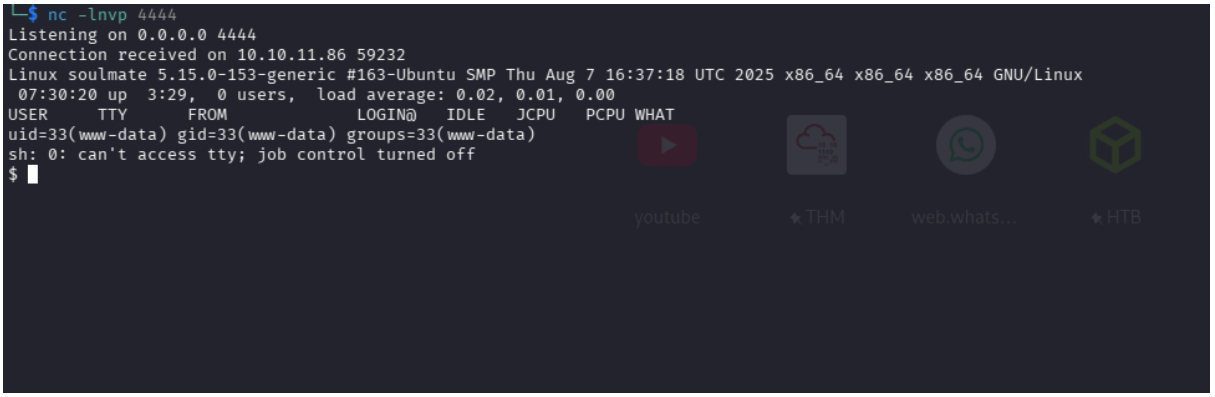


After logging into this account as a beginner i thought how to execute a file if i uploaded a file here.then my mind told register.php files are loadede inthe soulmate.htb/register.php . then i can upload the file and execute from there as above

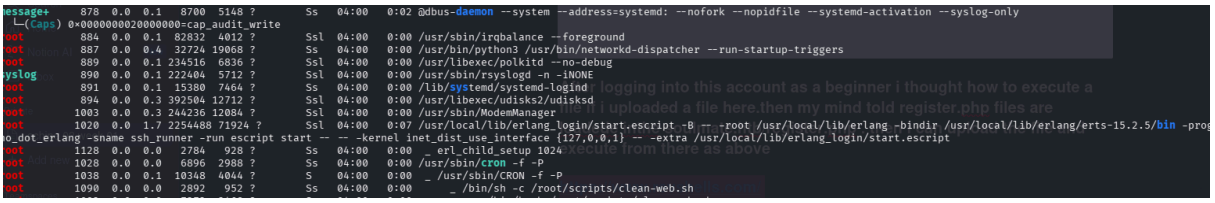
https://www.revshells.com/

from here copied a PHP pentestmonkey reverse shell script and save to a file and uploaded.

then created a listening port from my machine and load the script from soulmate.htb there we got our reverse shell as www-data user (low priviledge account).



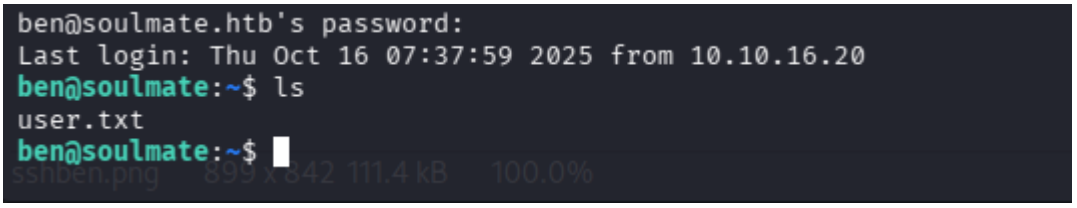
As usual go to /tmp folder and download the linpeas.sh (**https://github.com/peass-ng/PEASS-ng/tree/master/linPEAS**) script to victims machine.



There was an interesting file called start.escript (full path —>> `/usr/local/lib/erlang_login/start.escript`)

There was credentials for uesr ben and i logged as ben through ssh with that password.

then there we can get the user flag.



lets have some enumeration with,

- `sudo -l` (no sudoers running with user ben)
- `find / -perm -4000 -type f 2>/dev/null`
- `cat /etc/crontab` (no any interesting things)

again run linpeas.sh when nothing to do lol

```
        {parallel_login, true}
    ]) of
        {ok, _Pid} →
            io:format("SSH daemon running on port 2222. Press Ctrl+C to exit.~n");
        {error, Reason} →
            io:format("Failed to start SSH daemon: ~p~n", [Reason])
    end,

    receive
        stop → ok
    end.
```

in start.escript telling that SSH daemon is running on port 2222.therefore connect to port 2222 through ssh with previous password.

use `netstat -tulpn` or `ss -tulpn` to check locally what connections are made through.

```
ben@soulmate:/tmp$ ss -tulnp
Netid               State                Recv-Q               Send-Q                             Local Address:Port                             Peer Address:Port
udp                 UNCONN               0                    0                                  127.0.0.53%lo:53                                0.0.0.0:*
tcp                 LISTEN               0                    128                                      0.0.0.0:22                                0.0.0.0:*
tcp                 LISTEN               0                    511                                      0.0.0.0:80                                0.0.0.0:*
tcp                 LISTEN               0                    4096                                 127.0.0.1:46721                               0.0.0.0:*
tcp                 LISTEN               0                    4096                                     0.0.0.0:4369                              0.0.0.0:*
tcp                 LISTEN               0                    4096                                 127.0.0.1:8080                                0.0.0.0:*
tcp                 LISTEN               0                    5                                    127.0.0.1:2222                                0.0.0.0:*
tcp                 LISTEN               0                    4096                                 127.0.0.1:8443                                0.0.0.0:*
tcp                 LISTEN               0                    128                                  127.0.0.1:45327                               0.0.0.0:*
tcp                 LISTEN               0                    4096                           127.0.0.53%lo:53                                    0.0.0.0:*
tcp                 LISTEN               0                    4096                                 127.0.0.1:9090                                0.0.0.0:*
tcp                 LISTEN               0                    128                                     [::]:22                                   [::]:*
tcp                 LISTEN               0                    511                                     [::]:80                                   [::]:*
tcp                 LISTEN               0                    4096                                    [::]:4369                                 [::]:*
```

after connecting to port 2222 there is a EShell .it menas Embeded shell which is a cisco device

you've connected to a **Cisco networking device** running **Cisco IOS version 15.2(5)** and are inside its **Embedded Shell**.

navigate to the /root directory and view the root.txt from Eshell findout commands by help(). command.

there you have the root flag.

Hope you enjoy the machine !