■ Valentine - HackTheBox Writeup

Machine	Valentine
IP Address	10.129.232.136
OS	Linux (Ubuntu 12.04)
Difficulty	Easy
CVE	CVE-2014-0160 (Heartbleed)

Executive Summary

Valentine is a Linux machine that demonstrates the exploitation of **Heartbleed (CVE-2014-0160)**, one of the most critical vulnerabilities in cybersecurity history. This bug in OpenSSL allowed attackers to read server memory, potentially exposing sensitive data like passwords and private keys. The privilege escalation involves hijacking an active tmux session running as root.

1. Reconnaissance

1.1 Port Scanning

Initial enumeration with Nmap revealed three open ports: SSH (22), HTTP (80), and HTTPS (443). The SSL certificate disclosed the hostname **valentine.htb**.

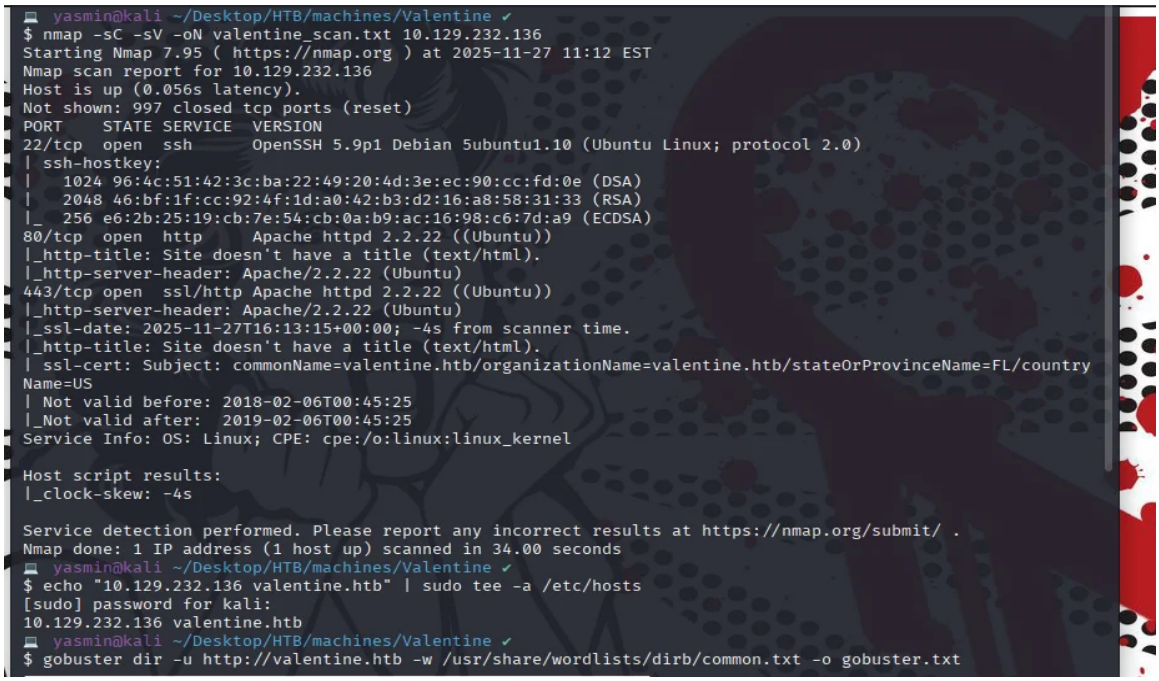

Figure 1: Nmap scan revealing SSH, HTTP, and HTTPS services

1.2 Web Enumeration & Vulnerability Scanning

Gobuster discovered several interesting directories including **/dev/**, **/encode**, and **/decode**. Nmap's ssl-heartbleed script confirmed the server was **VULNERABLE** to Heartbleed.

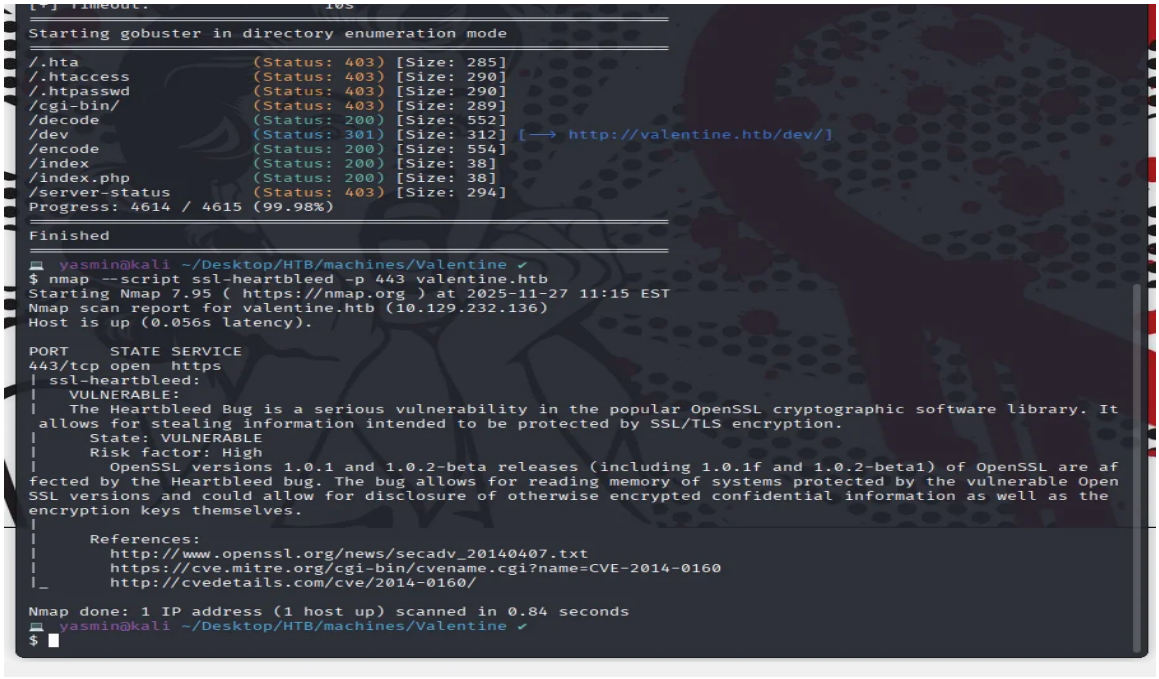

Figure 2: Gobuster enumeration and Heartbleed vulnerability confirmation

2. Enumeration

2.1 Directory /dev/ Contents

The /dev/ directory contained two files: **hype_key** and **notes.txt**. The notes.txt file revealed that the encoder/decoder was not ready for production use.

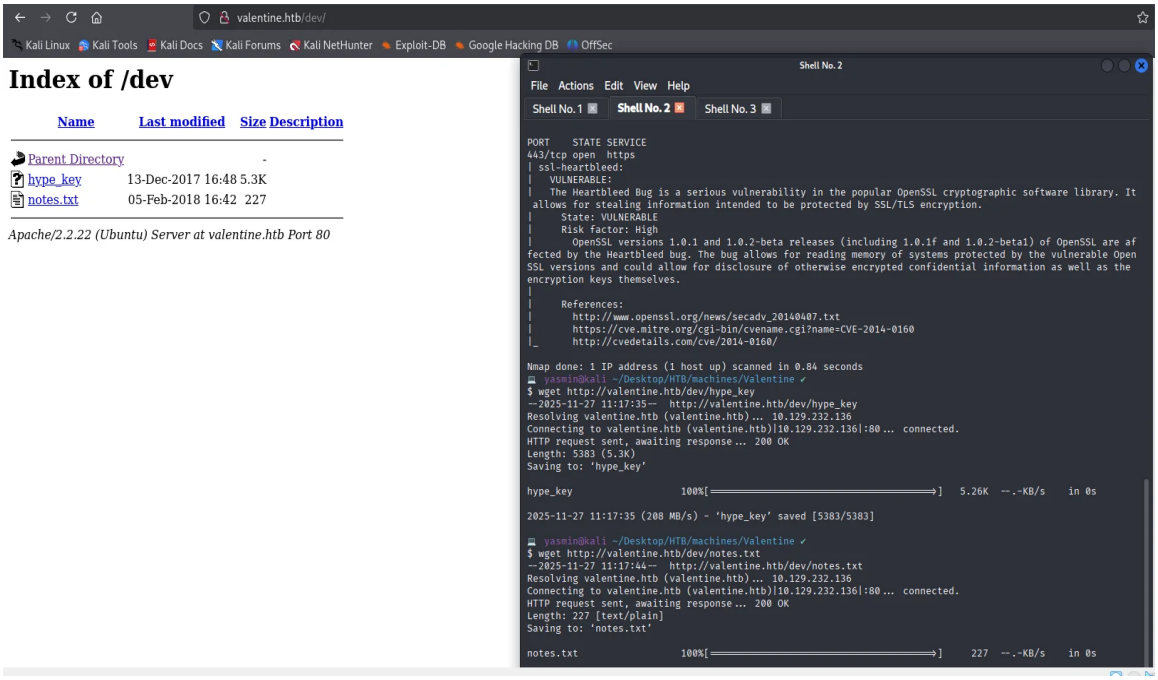

Figure 3: Directory /dev/ containing hype_key and notes.txt

2.2 RSA Key Analysis

The hype_key file contained a hex-encoded RSA private key. After decoding with **xxd -r -p**, the key was revealed to be **encrypted** (AES-128-CBC), requiring a passphrase.

```
$ cat notes.txt
To do:

1) Coffee.
2) Research.
3) Fix decoder/encoder before going live.
4) Make sure encoding/decoding is only done client-side.
5) Don't use the decoder/encoder until any of this is done.
6) Find a better way to take notes.
yasmin@kali ~/Desktop/HTB/machines/Valentine ✔
$ cat hype_key
2d 2d 2d 2d 2d 42 45 47 49 4e 20 52 53 41 20 50 52 49 56 41 54 45 20 4b 45 59 2d 2d 2d 2d 2d 0d 0a 50 72 6f
 63 2d 54 79 70 65 3a 20 34 2c 45 4e 43 52 59 50 54 45 44 0d 0a 44 45 4b 2d 49 6e 66 6f 3a 20 41 45 53 2d 3
1 32 38 2d 43 42 43 2c 41 45 42 38 38 43 31 34 30 46 36 39 42 46 32 30 37 34 37 38 38 44 45 32 34 41 45 34
38 44 34 36 0d 0a 0d 0a 44 62 50 72 4f 37 38 6b 65 67 4e 75 6b 31 44 41 71 6c 41 4e 35 6a 62 6a 58 76 30 50
 50 73 6f 67 33 6a 64 62 4d 46 53 38 69 45 39 70 33 55 4f 4c 30 6c 46 30 78 66 37 50 7a 6d 72 6b 44 61 38 5
2 0d 0a 35 79 2f 62 34 36 2b 39 6e 45 70 43 4d 66 54 50 68 4e 75 4a 52 63 57 32 55 32 67 4a 63 4f 46 48 2b
39 52 4a 44 42 43 35 55 4a 4d 55 53 31 2f 67 6a 42 2f 37 2f 4d 79 30 30 4d 77 78 2b 61 49 36 0d 0a 30 45 49
 30 53 62 4f 59 55 41 56 31 57 34 45 56 37 6d 39 36 51 73 5a 6a 72 77 4a 76 6e 6a 56 61 66 6d 36 56 73 4b 6
1 54 50 42 48 70 75 67 63 41 53 76 4d 71 7a 37 36 57 36 61 62 52 5a 65 58 69 0d 0a 45 62 77 36 36 68 6a 46
6d 41 75 34 41 7a 71 63 4d 2f 6b 69 67 4e 52 46 50 59 75 4e 69 58 72 58 73 31 77 2f 64 65 4c 43 71 43 4a 2b
 45 61 31 54 38 7a 6c 61 73 36 66 63 6d 68 4d 38 41 2b 38 50 0d 0a 4f 58 42 4b 4e 65 36 6c 31 37 68 4b 61 5
4 36 77 46 6e 70 35 65 58 4f 61 55 49 48 76 48 6e 76 4f 36 53 63 48 56 57 52 72 5a 37 30 66 63 70 63 70 69
6d 4c 31 77 31 33 54 67 64 64 32 41 69 47 64 0d 0a 70 48 4c 4a 70 59 55 49 49 35 50 75 4f 36 78 2b 4c 53 38
 6e 31 72 2f 47 57 4d 71 53 4f 45 69 6d 4e 52 44 31 6a 2f 35 39 2f 34 75 33 52 4f 72 54 43 4b 65 6f 39 44 7
3 54 52 71 73 32 6b 31 53 48 0d 0a 51 64 57 77 46 77 61 58 62 59 79 54 31 75 78 41 4d 53 6c 35 48 71 39 4f
44 35 48 4a 38 47 30 52 36 4a 49 35 52 76 43 4e 55 51 6a 77 78 30 46 49 54 6a 6a 4d 6a 6e 4c 49 70 78 6a 76
 66 71 2b 45 0d 0a 70 30 67 44 30 55 63 79 6c 4b 6d 36 72 43 5a 71 61 63 77 6e 53 64 64 48 57 38 57 33 4c 7
8 4a 6d 43 78 64 78 57 35 6c 74 35 64 50 6a 41 6b 42 59 52 55 6e 6c 39 31 45 53 43 69 44 34 5a 2b 75 43 0d
0a 4f 6c 36 6a 4c 46 44 32 6b 61 4f 4c 66 75 79 65 65 30 66 59 43 62 37 47 54 71 4f 65 37 45 6d 4d 42 33 66
 47 49 77 53 64 57 38 4f 43 38 4e 57 54 6b 77 70 6a 63 30 45 4c 62 6c 55 61 36 75 6c 4f 0d 0a 74 39 67 72 5
3 6f 73 52 54 43 73 5a 64 31 34 4f 50 74 73 34 62 4c 73 70 4b 78 4d 4d 4f 73 67 6e 4b 6c 6f 58 76 6e 6c 50
4f 53 77 53 70 57 79 39 57 70 36 79 38 58 58 38 2b 46 34 30 72 78 6c 35 0d 0a 58 71 68 44 55 42 68 79 6b 31
 43 33 59 50 4f 69 44 75 50 4f 6e 4d 58 61 49 70 65 31 64 67 62 30 4e 64 44 31 4d 39 5a 51 53 4e 55 4c 77 3
1 44 48 43 47 50 50 34 4a 53 53 78 58 37 42 57 64 44 4b 0d 0a 61 41 6e 57 4a 76 46 67 6c 41 34 6f 46 42 42
56 41 38 75 41 50 4d 66 56 32 58 46 51 6e 6a 77 55 54 35 62 50 4c 43 36 35 74 46 73 74 6f 52 74 54 5a 31 75
 53 72 75 61 69 32 37 6b 78 54 6e 4c 51 0d 0a 2b 77 51 38 37 6c 4d 61 64 64 73 31 47 51 4e 65 47 73 4b 53 6
6 38 52 2f 72 73 52 4b 65 65 4b 63 69 6c 44 65 50 43 6a 65 61 4c 71 74 71 78 6e 68 4e 6f 46 74 67 30 4d 78
74 36 72 32 67 62 31 45 0d 0a 41 6c 6f 51 36 6a 67 35 54 62 6a 35 4a 37 71 75 59 58 5a 50 79 6c 42 6c 6a 4e
 70 39 47 56 70 69 6e 50 63 33 4b 70 48 74 74 76 67 62 70 74 66 69 57 45 45 73 5a 59 6e 35 79 5a 50 68 55 7
2 39 51 0d 0a 72 30 38 70 6b 4f 78 41 72 58 45 32 64 6a 37 65 58 2b 62 71 36 35 36 33 35 4f 4a 36 54 71 48
62 41 6c 54 51 31 52 73 39 50 75 6c 72 53 37 4b 34 53 4c 58 37 6e 59 38 39 2f 52 5a 35 6f 53 51 65 0d 0a 32
 56 57 52 79 54 5a 31 46 66 6e 67 4a 53 73 76 39 2b 4d 66 76 7a 33 34 31 6c 62 7a 4f 49 57 6d 6b 37 57 66 4
```

Figure 4: Contents of notes.txt and hex-encoded RSA key

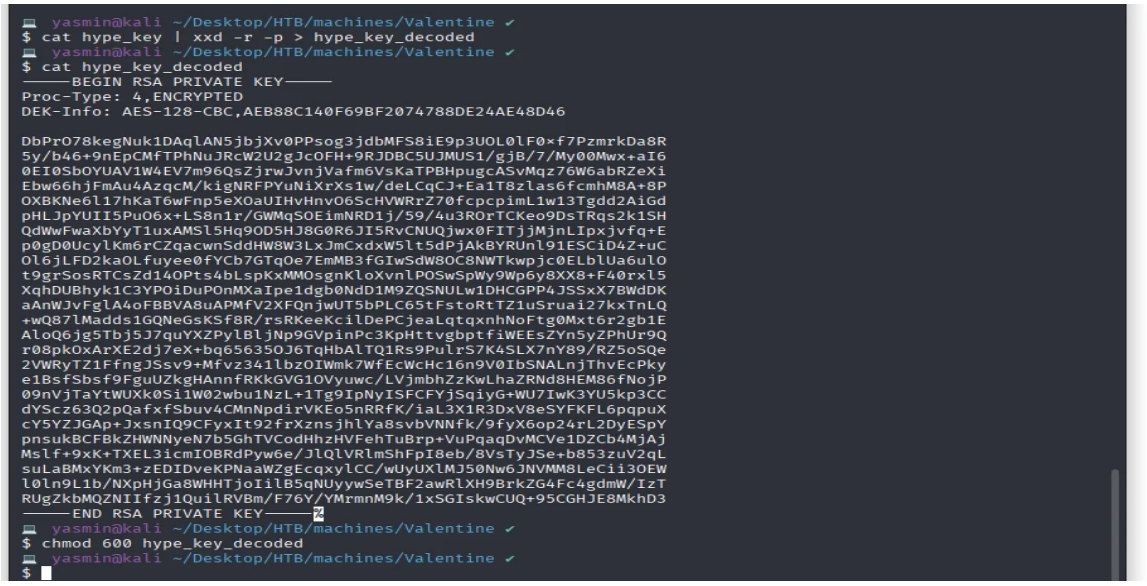

Figure 5: Decoded RSA private key (encrypted)

3. Exploitation

3.1 Heartbleed Attack

The Heartbleed exploit was used to read memory from the server. Multiple executions leaked data including a Base64-encoded string: **aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==**

Decoding this string revealed the passphrase: **heartbleedbelievethehype**

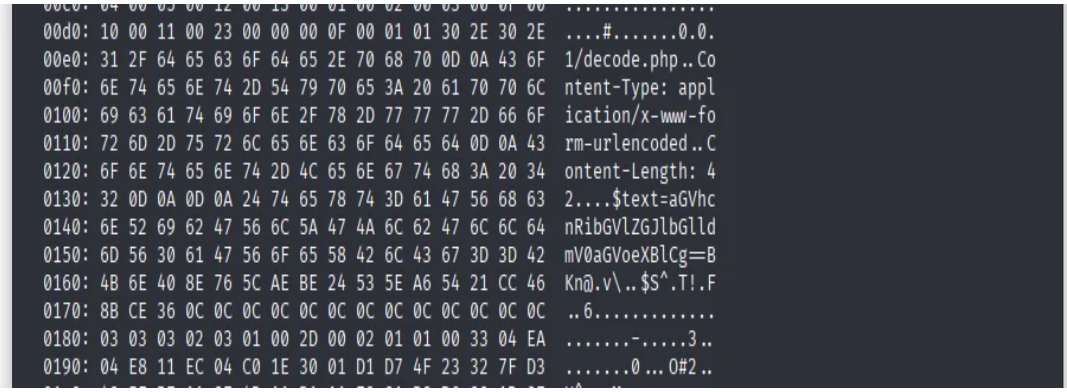

Figure 6: Heartbleed exploit leaking Base64 passphrase

3.2 SSH Access

Using the decoded RSA key and the leaked passphrase, SSH access was obtained as user **hype**. The user flag was retrieved from /home/hype/user.txt.

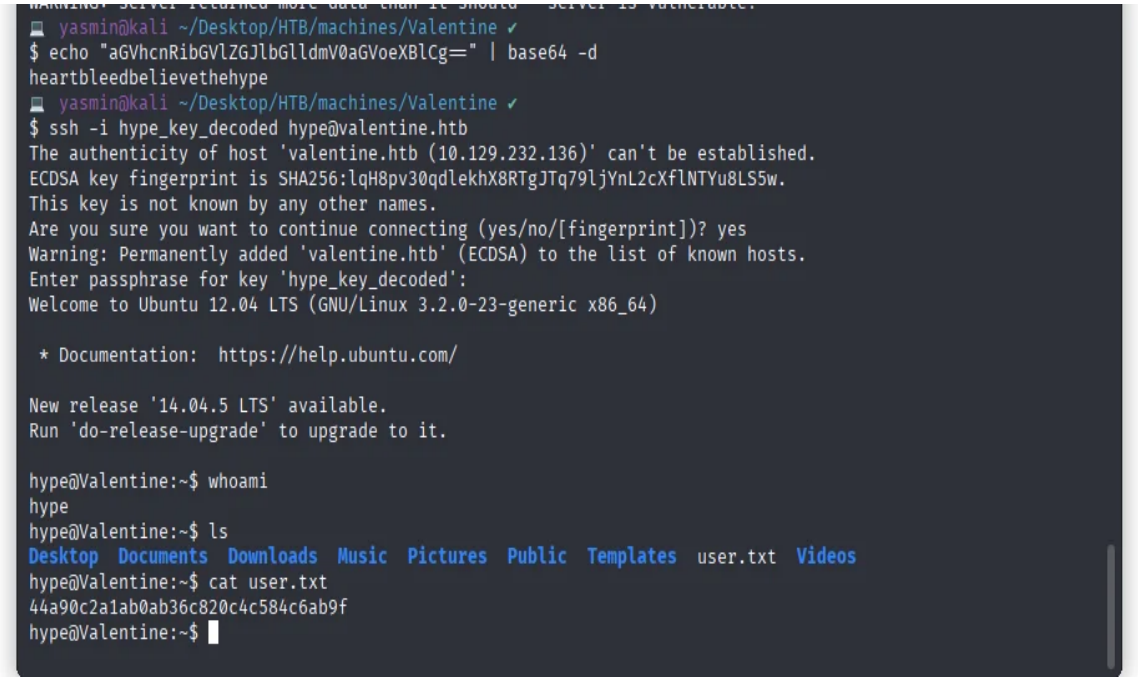

Figure 7: SSH access as user hype and user flag

4. Privilege Escalation

4.1 Tmux Session Hijacking

Enumeration revealed a tmux session running as root with a socket at **/.devs/dev_sess**. The socket's directory was owned by the hype group, allowing connection to the root session.

Command used: `tmux -S /.devs/dev_sess`

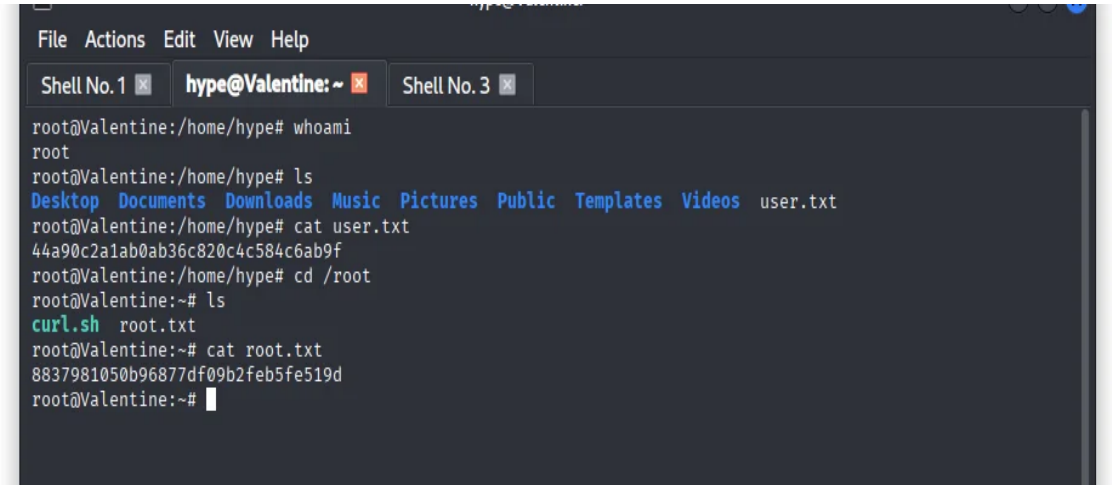

Figure 8: Root access via tmux session hijacking

5. Flags

Flag	Value
User	`44a90c2a1ab0ab36c820c4c584c6ab9f`
Root	`8837981050b96877df09b2feb5fe519d`

6. Lessons Learned

- **Heartbleed Impact:** A simple memory disclosure bug can expose credentials in plaintext.
- **Bash History:** Always check user history files for privilege escalation hints.
- **Socket Permissions:** Misconfigured tmux/screen sockets can lead to session hijacking.
- **Defense in Depth:** Encrypted keys without proper passphrase management are ineffective.

7. Tools Used

Nmap, Gobuster, OpenSSL Heartbleed Exploit (32764.py), xxd, base64, SSH, tmux