Olympian Selection Trial Report

Name: Chan Zun Mun Terence
Email used for registration: zunmun@gmail.com

Instructions:
Write a report of how you solved the **top 3 highest scoring challenges** in the trial. Your report should include as much details as possible and can include the steps, screenshots and command lines of how you cracked these challenges.

Once completed, please save as PDF file and upload to the google form as follows.
https://forms.gle/QtJ6B1Uek4mDFGqZ7

Please note that submission of this report is required to be considered as having completed the trials.

1. Challenge name: Password Attack

Solution for the challenge:
On opening the file Passwd_Attack file, we can see that it looks like a unix `/etc/passwd` file.

```
daemon:*:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:*:2:2:bin:/bin:/usr/sbin/nologin
sys:*:3:3:sys:/dev:/usr/sbin/nologin
sync:*:4:65534:sync:/bin:/bin/sync
games:*:5:60:games:/usr/games:/usr/sbin/nologin
man:*:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:*:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:*:8:8:mail:/var/mail:/usr/sbin/nologin
news:*:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:*:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:*:13:13:proxy:/bin:/usr/sbin/nologin
www-data:*:33:33:www-data:/var/www:/usr/sbin/nologin
backup:*:34:34:backup:/var/backups:/usr/sbin/nologin
list:*:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:*:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:*:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:*:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:*:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:*:101:102:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:*:102:103:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
```

systemd-resolve:*:103:104:systemd
Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:!:104:109:MySQL Server,,,:/nonexistent:/bin/false
Debian-exim:!:105:110::/var/spool/exim4:/usr/sbin/nologin
uuidd:*:106:112::/run/uuidd:/usr/sbin/nologin
rwhod:*:107:65534::/var/spool/rwho:/usr/sbin/nologin
redsocks:!:108:113::/var/run/redsocks:/usr/sbin/nologin
usbmux:*:109:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
miredo:*:110:65534::/var/run/miredo:/usr/sbin/nologin
ntp:*:111:114::/nonexistent:/usr/sbin/nologin
postgres:*:112:116:PostgreSQL
administrator,,,:/var/lib/postgresql:/bin/bash
dnsmasq:*:113:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
messagebus:*:114:117::/nonexistent:/usr/sbin/nologin
iodine:*:115:65534::/var/run/iodine:/usr/sbin/nologin
arpwatch:!:116:119:ARP Watcher,,,:/var/lib/arpwatch:/bin/sh
stunnel4:!:118:123::/var/run/stunnel4:/usr/sbin/nologin
rtkit:*:119:124:RealtimeKit,,,:/proc:/usr/sbin/nologin
sslh:!:120:126::/nonexistent:/usr/sbin/nologin
inetsim:*:121:128::/var/lib/inetsim:/usr/sbin/nologin
sshd:*:122:65534::/run/sshd:/usr/sbin/nologin
speech-dispatcher:!:123:29:Speech
Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
gluster:*:124:131::/var/lib/glusterd:/usr/sbin/nologin
geoclue:*:125:133::/var/lib/geoclue:/usr/sbin/nologin
colord:*:126:134:colord colour management
daemon,,,:/var/lib/colord:/usr/sbin/nologin
saned:*:127:135::/var/lib/saned:/usr/sbin/nologin
avahi:*:128:136:Avahi mDNS
daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
pulse:*:129:137:PulseAudio
daemon,,,:/var/run/pulse:/usr/sbin/nologin
dradis:*:130:139::/var/lib/dradis:/usr/sbin/nologin
king-phisher:*:131:140::/var/lib/king-phisher:/usr/sbin/nologin
beef-xss:*:132:141::/var/lib/beef-xss:/usr/sbin/nologin
Debian-gdm:*:133:142:Gnome Display
Manager:/var/lib/gdm3:/bin/false
systemd-coredump:!!:998:998:systemd Core Dumper:/:/sbin/nologin
Debian-snmp:!:117:122::/var/lib/snmp:/bin/false
vboxadd:!:999:1::/var/run/vboxadd:/bin/false
debian-tor:*:134:145::/var/lib/tor:/bin/false
_rpc:*:135:65534::/run/rpcbind:/usr/sbin/nologin
statd:*:136:65534::/var/lib/nfs:/usr/sbin/nologin
admin_user:**$6$7LYU9cUOW22Imt83$2thOaEfwnm5vjaxWgIFh2My4F//QdwmUB16BGTXz1S9rTc7x7tesUO0vu/dRkvVukAG5VhiuRS8flkzpEtO0p/**:1003:1003::/home/admin_user:/bin/sh

The most interesting entry is admin_user. It is the only one with a password hash, which is between the 1st and 2nd colon of the line. All other lines have * instead.

For context, password hashes in unix are usually stored in /etc/shadow, which is only readable by root. There is a similar file /etc/passwd with the list of users, but world readable and without the password hashes.

I firstly converted the password hash into a format john can parse. This is done by creating a dummy passwd file, and using unshadow to convert the dummy file and Passwd_Attack into the appropriate format. I then cracked the hash with john the ripper. The rockyou.txt password list is used.

```
┌──(kali㉿kali)-[~]
└─$ echo
"admin_user:$6$7LYU9cUOW22Imt83$2thOaEfwnm5vjaxWgIFh2My4F//QdwmUB1
6BGTXz1S9rTc7x7tesUO0vu/dRkvVukAG5VhiuRS8flkzpEtO0p/:1003:1003::/h
ome/admin_user:/bin/sh" > passwd

┌──(kali㉿kali)-[~]
└─$ unshadow passwd Passwd_Attack > hash

┌──(kali㉿kali)-[~]
└─$ john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256
AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
cookie1          (admin_user)
1g 0:00:00:00 DONE (2022-10-29 07:45) 2.857g/s 2925p/s 2925c/s
2925C/s football1..bethany
Use the "--show" option to display all of the cracked passwords
reliably
Session completed

┌──(kali㉿kali)-[~]
└─$
```

The password found is `cookie1`, which is the flag

2. Challenge name: Port Up!

Solution for the challenge:
On running the binary in linux (most executable binaries which do not have the `.exe` extension are likely x86/x64 linux binaries), it said that a socket is created, bind to and is listening.

```
(base) [hacker@hackerbook blockcyber]$ file portup3.bin
portup3.bin: ELF 64-bit LSB executable, x86-64, version 1 (SYSV),
dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2,
BuildID[sha1]=3f71fafa6e2e915b9bed491dd97e1bab785158de, for GNU/Linux
2.6.32, stripped
(base) [hacker@hackerbook blockcyber]$ chmod +x portup* # Make binary
executable
(base) [hacker@hackerbook blockcyber]$ ./portup3.bin
Socket created
Socket bind complete
Socket now listening
```

On my local linux machine, I scanned the ports which are opened, in an effort to find the port the program is bound to and listening on. It revealed that port 65000 is open.

```
(base) [hacker@hackerbook ~]$ nmap -sT 127.0.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-29 16:59 +08
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000094s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
65000/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
(base) [hacker@hackerbook ~]$
```

Connecting to that local port reveals the flag

```
(base) [hacker@hackerbook ~]$ nc 127.0.0.1 65000
flag{b30363fab42cf3a08fdfc45b3472c5ee}
```

3. Challenge name: Hardcrack

Solution for the challenge:

I extracted the password hash of the zip file using a tool zip2john. I then used john the ripper to crack the hash to get the password.

```
┌──(kali㉿kali)-[/tmp]
└─$ zip2john Dict_Crack.zip > hash
ver 2.0 efh 9901 Dict_Crack.zip/flag1.txt PKZIP Encr: cmplen=45,
decmplen=15, crc=0

┌──(kali㉿kali)-[/tmp]
└─$ john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
likeavirgin      (Dict_Crack.zip/flag1.txt)
1g 0:00:00:02 DONE (2022-10-29 05:01) 0.3759g/s 47735p/s 47735c/s
47735C/s money89..327327
Use the "--show" option to display all of the cracked passwords
reliably
Session completed

┌──(kali㉿kali)-[/tmp]
└─$
```

I extracted flag1.txt using a regular zip extractor program to get the flag, `P@ssw0rdCracker`