





Viruses and Worms

Module 07

Viruses and Worms

A virus is a self-replicating program that produces its own code by attaching copies of it onto other executable codes. Some viruses affect computers as soon as their codes are executed; others lie dormant until a predetermined logical circumstance is met.

ICON KEY

-  Valuable information
-  Test your knowledge
-  Web exercise
-  Workbook review

Lab Scenario

A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels. The biggest danger with a worm is its capability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect. A blended threat is a more sophisticated attack that bundles some of the worst aspects of viruses, worms, Trojan horses and malicious code into one single threat. Blended threats can use server and Internet vulnerabilities to initiate, then transmit and also spread an attack. The attacker would normally serve to transport multiple attacks in one payload. Attacker can launch Dos attack or install a backdoor and maybe even damage a local system or network systems.

Since you are an expert Ethical Hacker and Penetration Tester, the IT director instructs you to test the network for any viruses and worms that damage or steal the organization's information. You need to construct viruses and worms and try to inject them in a dummy network (virtual machine) and check whether they are detected by antivirus programs or able to bypass the network firewall.

Lab Objectives

The objective of this lab is to make students learn how to create viruses and worms.


In this lab, you will learn how to:

- Create viruses using tools
- Create worms using worm generator tool

Lab Environment

To carry this out, you need:

- A computer running **Window Server 2012** as host machine
- **Window Server 2008, Windows 7** and **Windows 8** running on virtual machine as guest machine
- A web browser with Internet access
- Administrative privileges to run tools

 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms**

Lab Duration

Time: 30 Minutes

Overview of Viruses and Worms

A virus is a **self-replicating** program that produces its own code by attaching copies of it onto other **executable codes**. Some viruses affect computers as soon as their codes are **executed**; others lie dormant until a predetermined logical circumstance is met.

Computer worms are **malicious programs** that replicate, execute, and spread across network connections independently **without human interaction**. Most worms are created only to **replicate** and spread across a network consuming available computing resources. However, some worms carry a **payload** to damage the host system.



TASK 1

Overview

Lab Tasks

Recommended labs to assist you in creating Viruses and Worms:

- Creating a virus using the JPS Virus Maker tool
- Virus analysis using IDA Pro
- Virus Analysis using Virus Total
- Scan for Viruses using Kaspersky Antivirus 2013
- Virus Analysis Using OllyDbg
- Creating a Worm Using the Internet Worm Maker Thing

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.





PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS
RELATED TO THIS LAB.



Creating a Virus Using the JPS Virus Maker Tool

JPS Virus Maker is a tool to create viruses. It also has a feature to convert a virus into a worm.

ICON KEY

-  Valuable information
-  Test your knowledge
-  Web exercise
-  Workbook review

Lab Scenario

In recent years there has been a large growth in Internet traffic generated by malware, that is, Internet worms and viruses. This traffic usually only impinges on the user when either their machine gets infected or during the epidemic stage of a new worm, when the Internet becomes unusable due to overloaded routers. What is less well-known is that there is a background level of malware traffic at times of non-epidemic growth and that anyone plugging an unfirewalled machine into the Internet today will see a steady stream of port scans, back-scatter from attempted distributed denial-of-service attacks, and hostscans. We need to build better firewalls, protect the Internet router infrastructure, and provide early-warning mechanisms for new attacks.

Since you are an expert ethical hacker and penetration tester, your IT director instructs you to test the network to determine whether any viruses and worms will damage or steal the organization's information. You need to construct viruses and worms, try to inject them into a dummy network (virtual machine), and check their behavior, whether they are detected by an antivirus and if they bypass the firewall.


Lab Objectives

The objective of this lab is to make students learn and understand how to make viruses and worms.

Lab Environment

To carry out the lab, you need:

- **JPS** tool located at **D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Virus Construction Kits\JPS Virus Maker**

 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms**

- A computer running **Windows Server 2012** as host machine
- **Windows Server 2008** running on virtual machine as guest machine
- Run this tool on **Windows Server 2008**
- Administrative privileges to run tools

Lab Duration

Time: 15 Minutes

Overview of Virus and Worms

A virus is a **self-replicating program** that produces its own code by attaching copies of it onto other **executable codes**. Some viruses affect computers as soon as their codes are **executed**; others lie dormant until a predetermined logical circumstance is met.

Lab Tasks

TASK 1

Make a Virus

1. Launch your **Windows Server 2008** virtual machine.
2. Navigate to **Z:\CEHv8 Module 07 Viruses and Worms\Virus Construction Kits\JPS Virus Maker**.
3. Launch the **JPS Virus Maker** tool. Installation is not required for **JPS Virus maker**. Double-click and launch the **jps.exe** file.
4. The **JPS (Virus Maker 3.0)** window appears.

Note: Take a Snapshot of the virtual machine before launching the JPS Virus Maker tool.

The option, Auto Startup is always checked by default and start the virus whenever the system boots on.



Module 07 – Viruses and Worms

FIGURE 1.1: JPS Virus Maker main window

- JPS lists the **Virus Options**; check the options that you want to embed in a new virus file.

📖 This creation of a virus is only for knowledge purposes; don't misuse this tool.

📖 A list of names for the virus after install is shown in the Name after Install drop-down list.



FIGURE 1.2: JPS Virus Maker main window with options selected

- Select one of the **radio** buttons to specify when the virus should **start attacking** the system after creation.

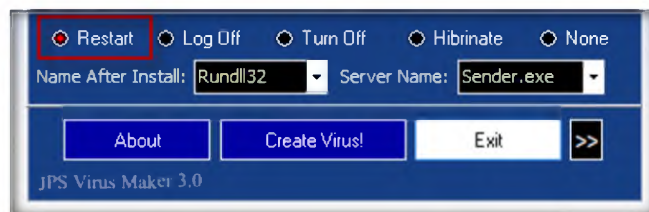


FIGURE 1.3: JPS Virus Maker main window with Restart selected

📖 A list of server names is present in the Server Name drop-down list. Select any server name.

- Select the name of the **service** you want to make virus behave like from the **Name after Install** drop-down list.

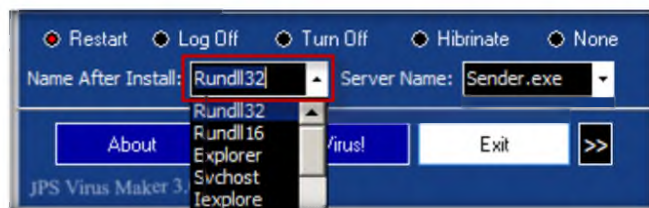


FIGURE 1.4: JPS Virus Maker main window with the Name after Install option

- Select a **server** name for the virus from the **Server Name** drop-down list.

Module 07 – Viruses and Worms

Don't forget to change the settings for every new virus creation. Otherwise, by default, it takes the same name as an earlier virus.

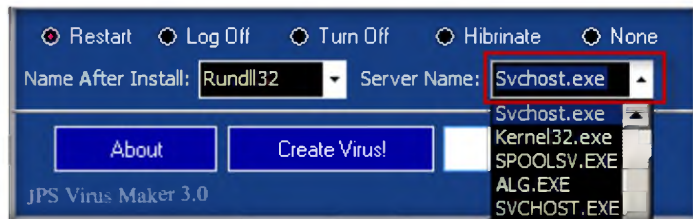


FIGURE 1.5: JPS Virus Maker main window with Server Name option


9. Now, before clicking on **Create Virus!** change setting and virus options by clicking the  icon.



FIGURE 1.6: JPS Virus Maker main window with Settings option

10. Here you see more options for the virus. Check the options and provide related information in the respective text field.

TASK 2

Make a Worm

You can select any icon from the change icon options. A new icon can be added apart from those on the list.

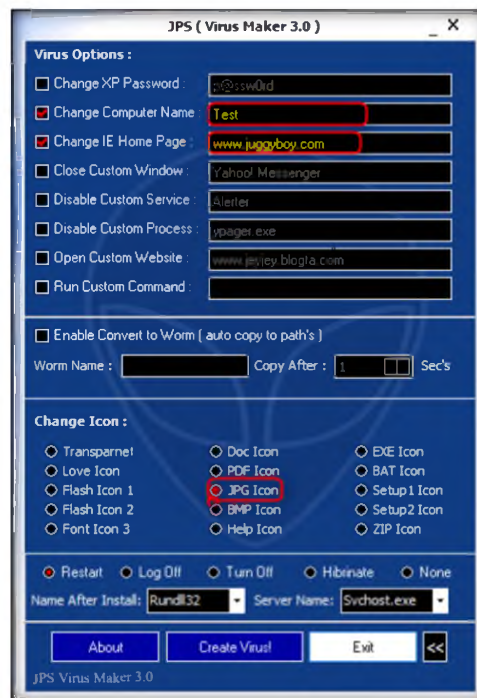



FIGURE 1.7: JPS Virus Maker Settings option

11. You can change **Windows XP password**, **IE home page**, **close custom window**, **disable a particular custom service**, etc.
12. You can even allow the virus to convert to a worm. To do this, check the **Enable Convert to Worm** checkbox and provide a **Worm Name**.

Module 07 – Viruses and Worms

- For the worm to self-replicate after a particular time period, specify the time (in seconds) in the **Copy after** field.
- You can also change the **virus icon**. Select the type of icon you want to view for the created virus by selecting the radio button under the **Change Icon** section.

 Make sure to check all the options and settings before clicking on Create Virus!

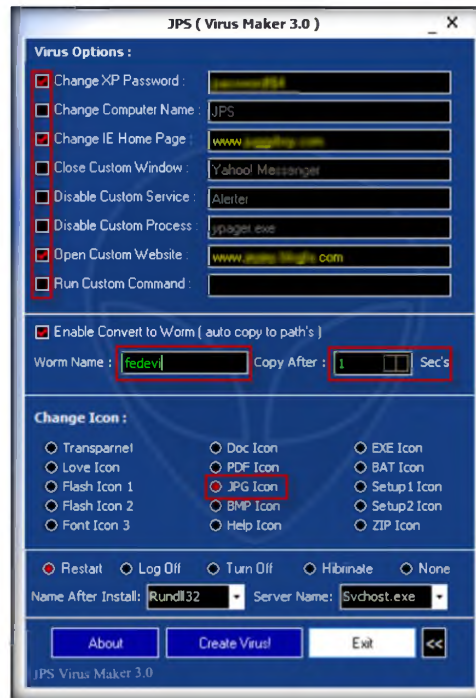


FIGURE 1.8: JPS Virus Maker main window with Options

- After completing your selection of options, click **Create Virus!**



FIGURE 1.9: JPS Virus Maker Main window with Create Virus! Button

- A pop-up window with the message **Server Created Successfully** appears. Click **OK**.

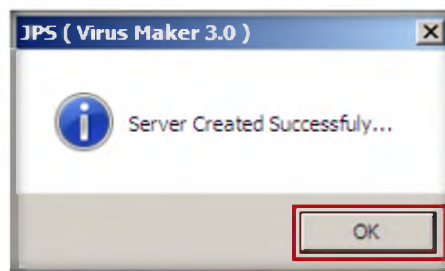



FIGURE 1.10: JPS Virus Maker Server Created successfully message

 Features
Change XP Password
Change Computer Name
Change IE Home Page
Close Custom Windows
Disable Custom Service
Disable Process
Open Custom Website
Run Custom Command
Enable Convert To Worm
- Auto Copy Server To
Active Path With Custom
Name & Time
Change Custom Icon For
your created Virus (15
Icons)

17. The newly created virus (server) is placed automatically in the same folder as **jps.exe** but with name **Svchost.exe**.
18. Now pack this virus with a binder or virus packager and send it to the victim machine. **ENJOY!**

Lab Analysis

Document all the files, created viruses, and worms in a separate location.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS
RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
JPS Virus Maker Tool	To make Virus options are used: <ul style="list-style-type: none">▪ Disable Yahoo▪ Disable Internet Explorer▪ Disable Norton Antivirus▪ Disable McAfee Antivirus▪ Disable Taskbar▪ Disable Security Restore▪ Disable Control Panel▪ Hide Windows Clock▪ Hide All Tasks in Task.mgr▪ Change Explorer Caption▪ Destroy Taskbar▪ Destroy Offlines (Y!Messenger)▪ Destroy Audio Services▪ Terminate Windows▪ Auto Setup

Questions

1. Infect a virtual machine with the created viruses and evaluate the behavior of the virtual machine.
2. Examine whether the created viruses are detected or blocked by any antivirus programs or antispyware.

Module 07 – Viruses and Worms





Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Virus Analysis Using IDA Pro

Computer worms are malicious programs that replicate, execute, and spread themselves across network connections independently, without human interaction.

ICON KEY

-  Valuable information
-  Test your knowledge
-  Web exercise
-  Workbook review

Lab Scenario

Virus, worms, or Trojans can erase your disk, send your credit card numbers and passwords to a stranger, or let others use your computer for illegal purposes like denial of service attacks. Hacker mercenaries view Instant Messaging clients as their personal banks because of the ease by which they can access your computer via the publicly open and interpretable standards. They unleash a Trojan horse, virus, or worm, as well as gather your personal and confidential information. Since you are an expert ethical hacker and penetration tester, the IT director instructs you to test the network for any viruses and worms that can damage or steal the organization's information. You need to construct viruses and worms, try to inject them in a dummy network (virtual machine), and check their behavior, whether they are detected by any antivirus programs or bypass the firewall of an organization.

Lab Objectives

The objective of this lab is to make students learn and understand how to make viruses and worms to test the organization's firewall and antivirus programs.

Lab Environment

To carry out the lab, you need:

- **IDA Pro** located at **D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Malware Analysis Tools\IDA Pro**
- A computer running **Windows Server 2012** as host machine
- **Windows Server 2008** running on virtual machine as guest machine
- Run this tool on **Windows Server 2008**
- You can also download the latest version of **IDA Pro** from the link <http://www.hex-rays.com/products/ida/index.shtml>

 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms**

- Administrative privileges to run tools

Lab Duration

Time: 15 Minutes

Overview of Virus and Worms

Computer worms are **malicious programs** that **replicate, execute**, and spread across network connections independently, without human interaction. Attackers use worm payloads to install backdoors **in infected computers**, which turn them into zombies and **create botnets**; these botnets can be used to carry out further cyber-attacks.

Lab Tasks



TASK 1

IDA Pro

1. Go to **Windows Server 2008** Virtual Machine.
2. Install **IDA Pro**, which is located at **D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Malware Analysis Tools\IDA Pro**.
3. Open **IDA Pro**, and click **Run** in the **Open File-Security Warning** dialog box.



You have to agree the License agreement before proceeding further on this tool



FIGURE 2.1: IDA Pro About.

4. Click **Next** to continue the installation.



 Read the License Agreement carefully before accepting.



FIGURE 2.2: IDA Pro Setup

5. Select the **I accept the agreement** radio button for the IDA Pro license agreement.
6. Click **Next**.

 Reload the input file
This command reloads the same input file into the database. IDA tries to retain as much information as possible in the database. All the names, comments, segmentation information and similar will be retained.

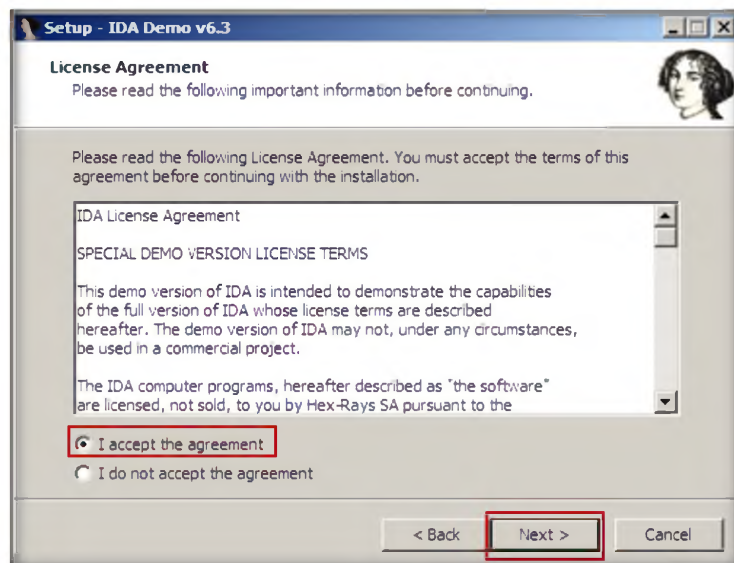


FIGURE 2.3: IDA Pro license.

7. Keep the destination location default, and click **Next**.

📖 Add breakpoint

This command adds a breakpoint at the current address. If an instruction exists at this address, an instruction breakpoint is created. Or else, IDA offers to create a hardware breakpoint, and allows the user to edit breakpoint settings.

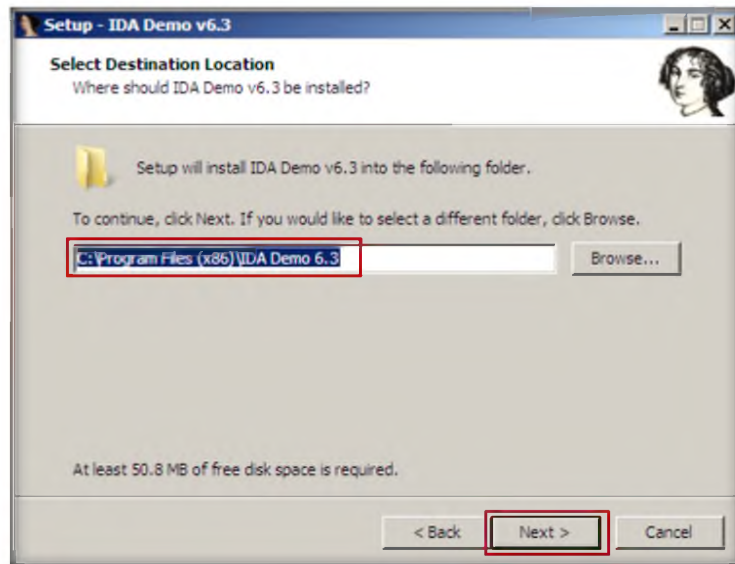


FIGURE 2.4: IDA Pro destination folder

8. Check the **Create a desktop icon** check box, and click **Next**.

📖 Trace window

In this window, you can view some information related to all traced events. The tracing events are the information saved during the execution of a program. Different type of trace events are available: instruction tracing events, function tracing events and write, read/write or execution tracing events.

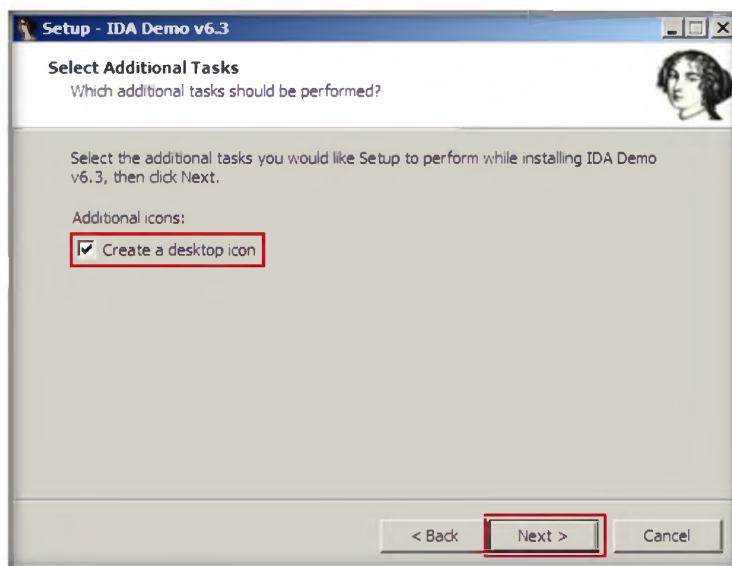


FIGURE 3.5: Creating IDA Pro shortcut

9. The **Ready to Install** window appears; click **Install**.

Module 07 – Viruses and Worms

Add execution trace

This command adds an execution trace to the current address.

Instruction tracing

This command starts instruction tracing. You can then use all the debugger commands as usual: the debugger will save all the modified register values for each instruction. When you click on an instruction trace event in the trace window, IDA displays the corresponding register values preceding the execution of this instruction. In the 'Result' column of the Trace window, you can also see which registers were modified by this instruction.

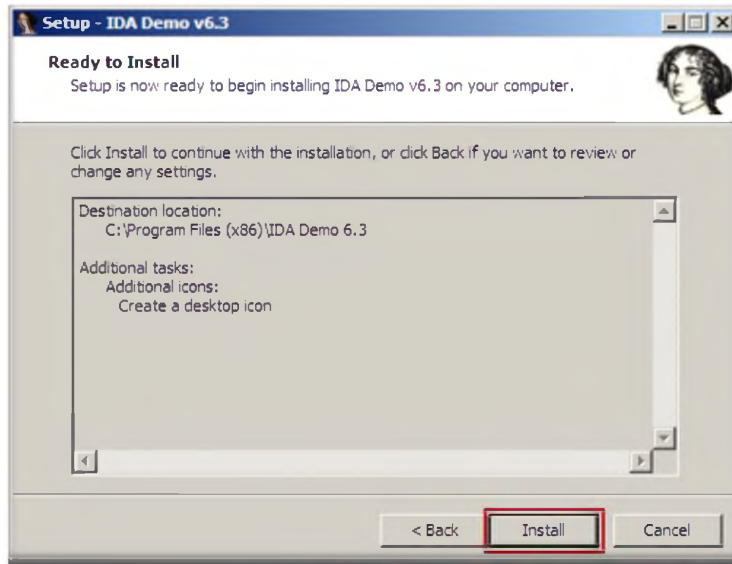


FIGURE 2.6: IDA Pro install

10. Click **Finish**.



FIGURE 2.7: IDA Pro complete installation

11. The **IDA License** window appears. Click **I Agree**.

Module 07 – Viruses and Worms

The configuration files are searched in the IDA.EXE directory. In the configuration files, you can use C, C++ style comments and include files. If no file is found, IDA uses default values.

```
// Compile an IDC script.  
// The input should not  
// contain functions that are  
// currently executing -  
// otherwise the behavior of  
// the replaced  
// functions is undefined.  
// input - if isfile != 0,  
// then this is the name of file  
// to compile  
// otherwise it  
// hold the text to compile  
// returns: 0 - ok,  
// otherwise it returns an  
// error message.
```

```
string CompileEx(string  
input, long isfile);
```

```
// Convenience macro:
```

```
#define Compile(file)  
CompileEx(file, 1)
```

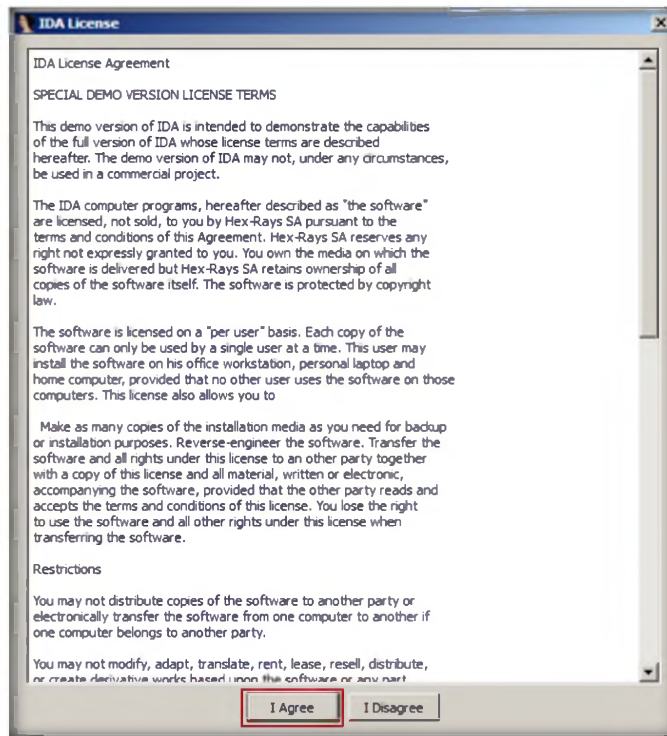


FIGURE 2.8: IDA Pro License accepts.

12. Click the **New** button in the **Welcome** window.



FIGURE 2.9: IDA Pro Welcome window.

13. A file browse window appears; select **Z:\CEHv8 Module 07 Viruses and Worms\Viruses\Klez Virus Live\face.exe** and click **Open**.

Module 07 – Viruses and Worms

Function tracing

This command starts function tracing. You can then use all debugger commands as usual: the debugger will save all addresses where a call to a function or a return from a function occurred.

Add/Edit an enum

Action name: AddEnum

Action name: EditEnum

These commands allow you to define and to edit an enum type. You need to specify:

- name of enum
- its serial number (1,2...)

- representation of enum members

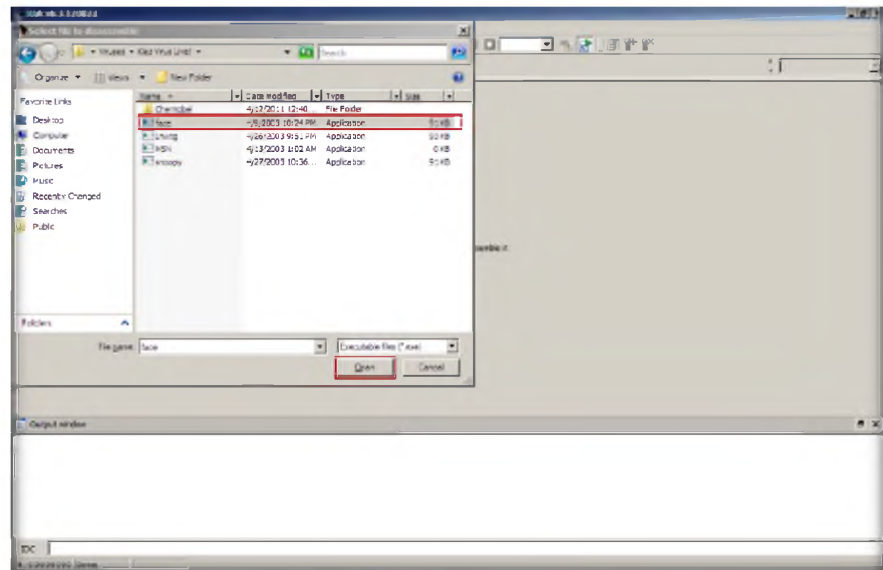


FIGURE 2.10: IDA Pro file browse window.

14. The **Load a new file** window appears. Keep the default settings and click **OK**.

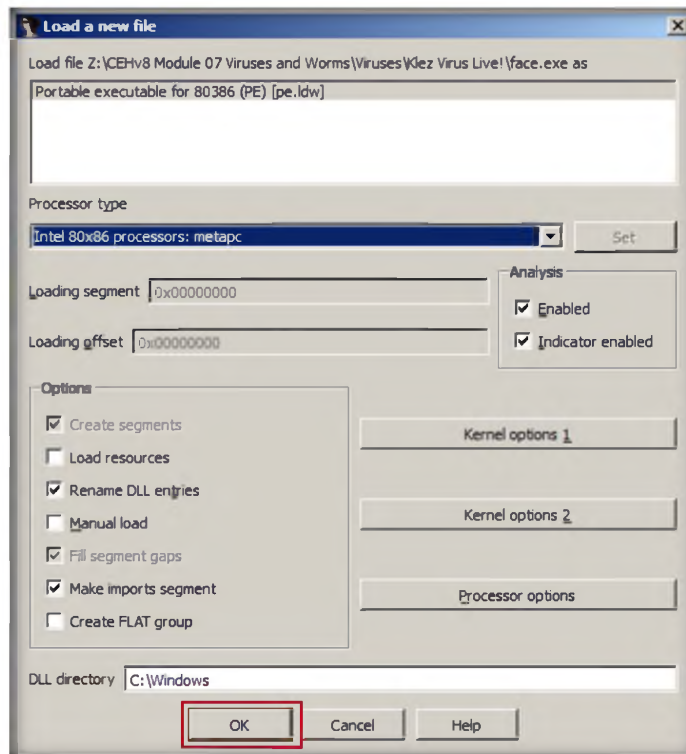



FIGURE 2.11: Load a new file window.

15. If any warning window prompts appear, click **OK**.

Module 07 – Viruses and Worms

16. The **Please confirm** window appears; read the instructions carefully and click **Yes**.

 Select appropriate options as per your requirement

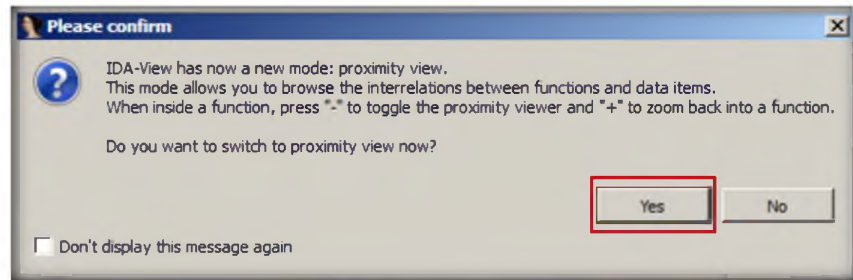



FIGURE 2.12: Confirmation wizard.

17. The final window appears after analysis.

 TMP or TEMP:
Specifies the directory where the temporary files will be created.

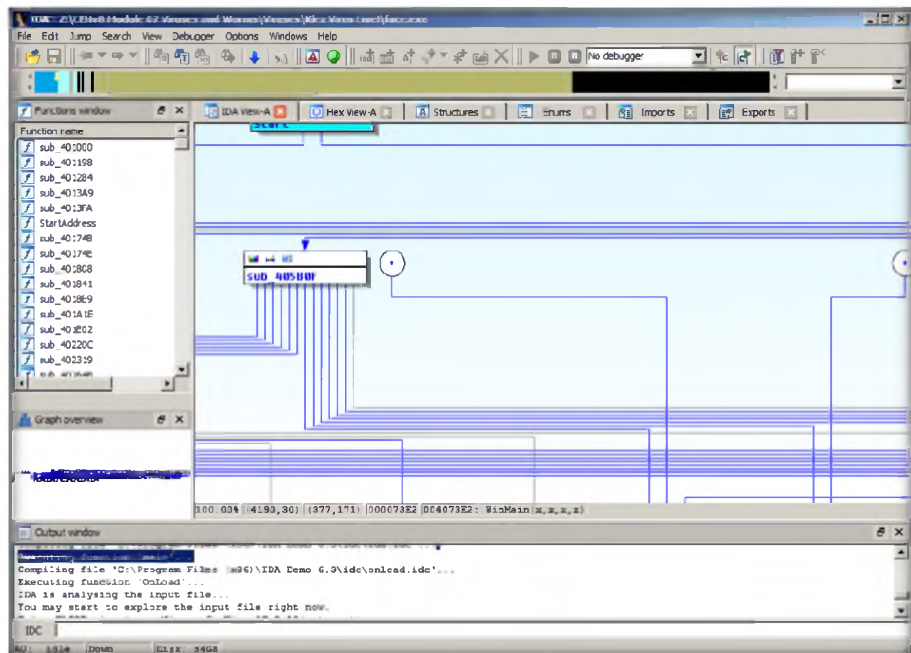


FIGURE 2.13: IDA Pro window after analysis.

18. Click **View → Graphs → Flow Chart** from the menu bar.

 Add read/write trace

This command adds a read/write trace to the current address.

Each time the given address will be accessed in read or write mode, the debugger will add a trace event to the Trace window

Module 07 – Viruses and Worms

Create alignment directive

Action name: Make Alignment

This command allows you to create an alignment directive.

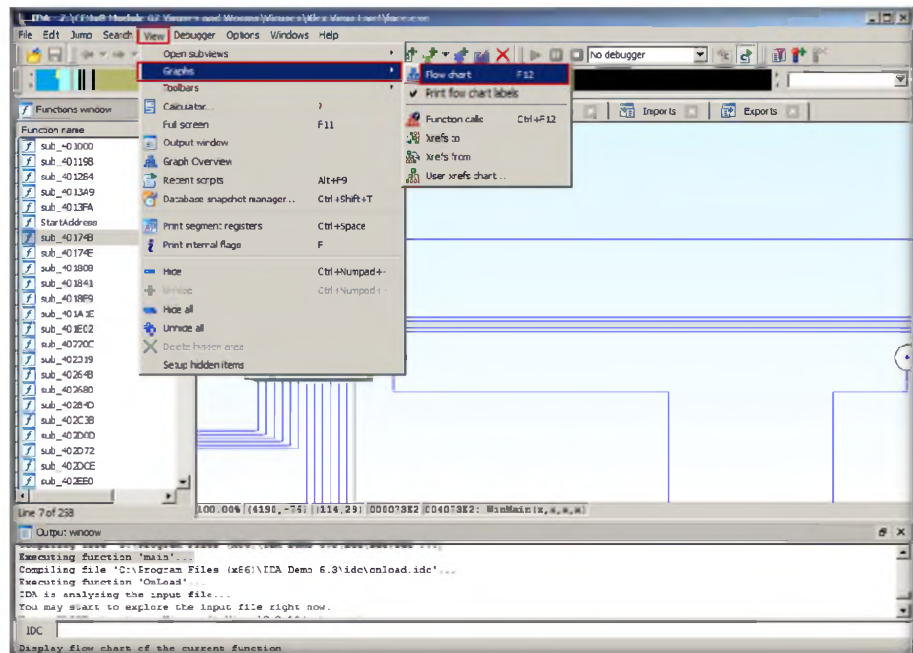


FIGURE 214: IDA Pro flow chart menu.

19. A **Graph** window appears with the flow; zoom to view clearly.

Zoom in to have a better view of the details

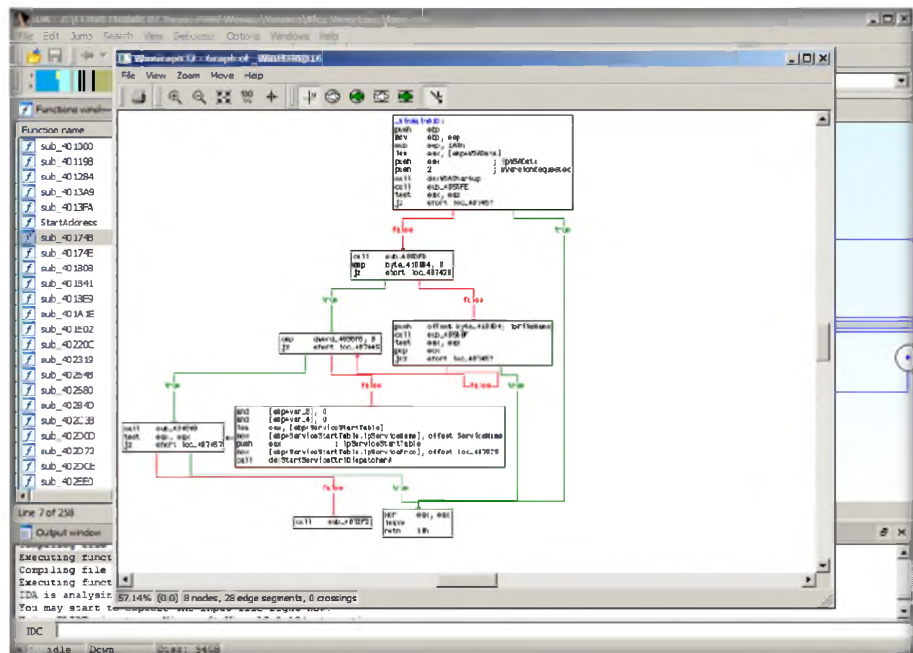


FIGURE 215: IDA Pro flow chart.

Module 07 – Viruses and Worms

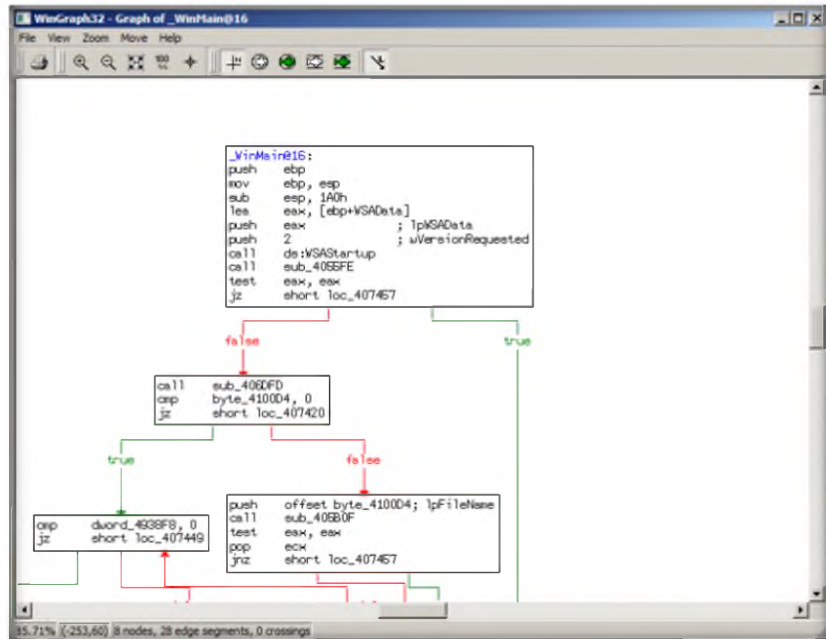


FIGURE 216: IDA Pro zoom flow chart.

Zoom in to have a better view of the details

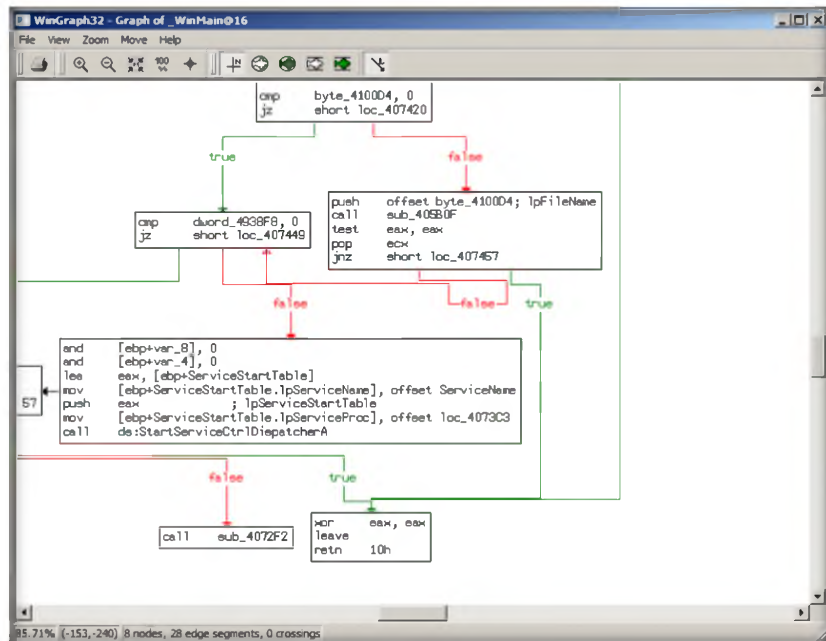


FIGURE 217: IDA Pro zoom flow chart.

20. Click **View → Graphs → Function Calls** from the menu bar.

Module 07 – Viruses and Worms

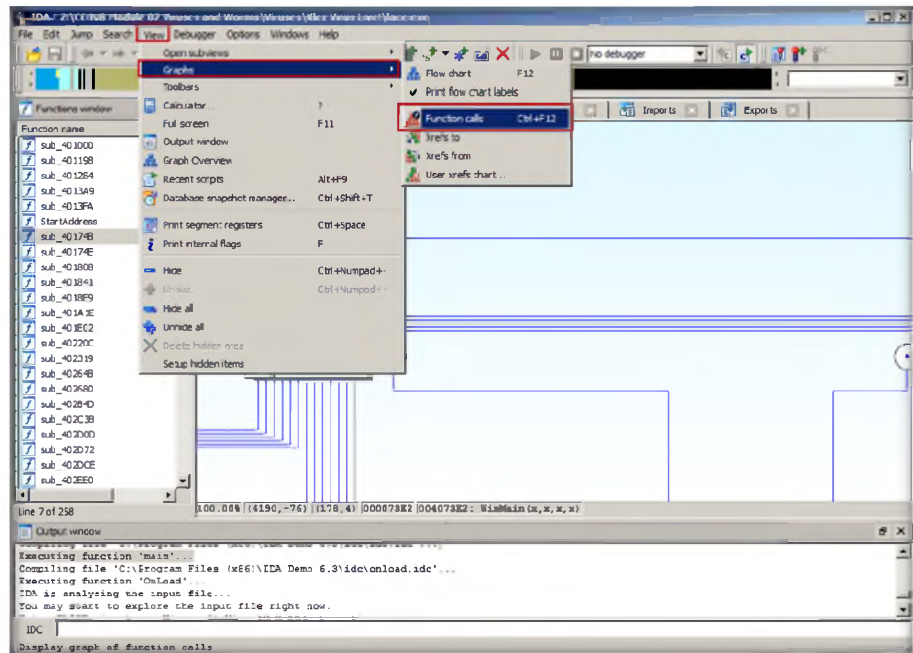


FIGURE 2.18: IDA Pro Function calls menu.

Empty input file

The input file doesn't contain any instructions or data, i.e. there is nothing to disassemble.

Some file formats allow the situation when the file is not empty but it doesn't contain anything to disassemble. For example, COFF/OMF/EXE formats could contain a file header which just declares that there are no executable sections in the file.

21. A window showing **call flow** appears; zoom to have a better view.

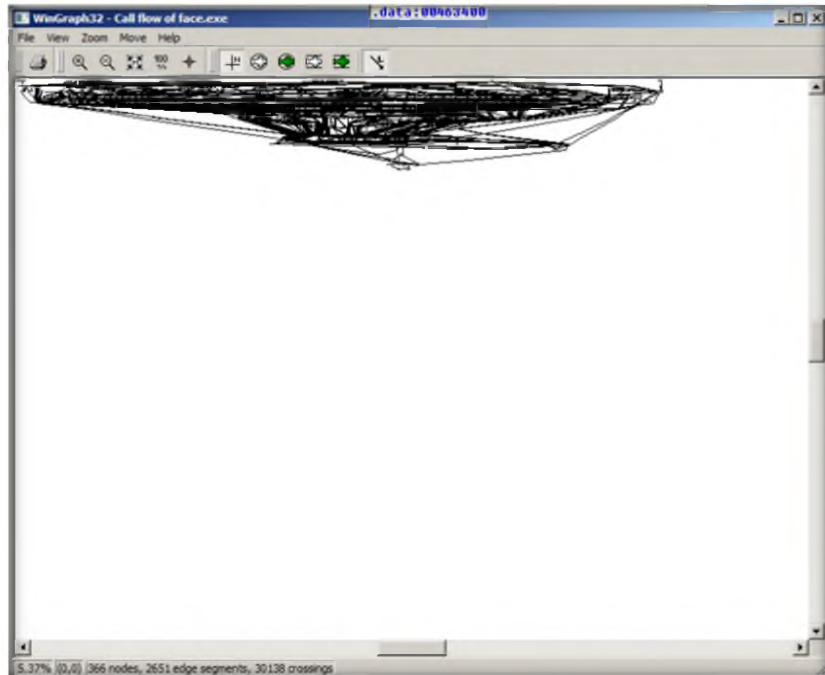


FIGURE 2.19: IDA Pro call flow of face.

Module 07 – Viruses and Worms

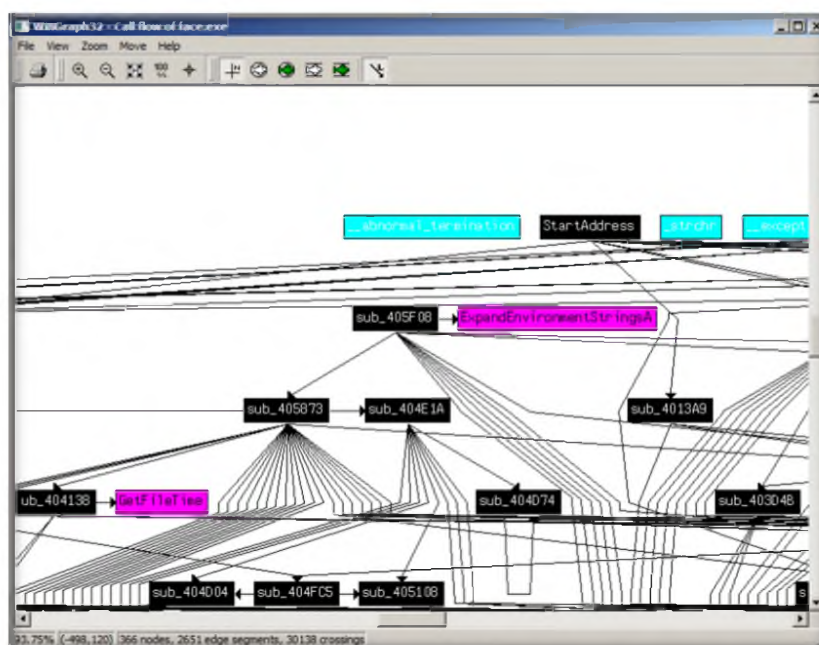


FIGURE 220: IDA Pro call flow of face with zoom.

Empty input file

The input file doesn't contain any instructions or data, i.e. there is nothing to disassemble.

Some file formats allow the situation when the file is not empty but it doesn't contain anything to disassemble. For example, COFF/OMF/EXE formats could contain a file header which just declares that there are no executable sections in the file.

22. Click **Windows** → **Hex View-A**.

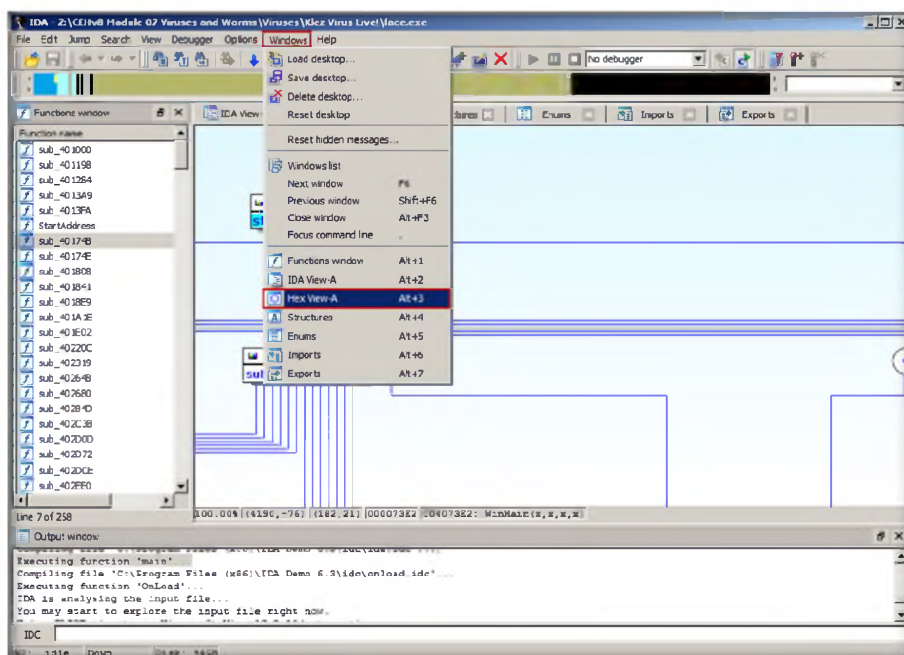


FIGURE 221: IDA Pro Hex View-A menu.

23. The following is a window showing **Hex View-A**.

Module 07 – Viruses and Worms

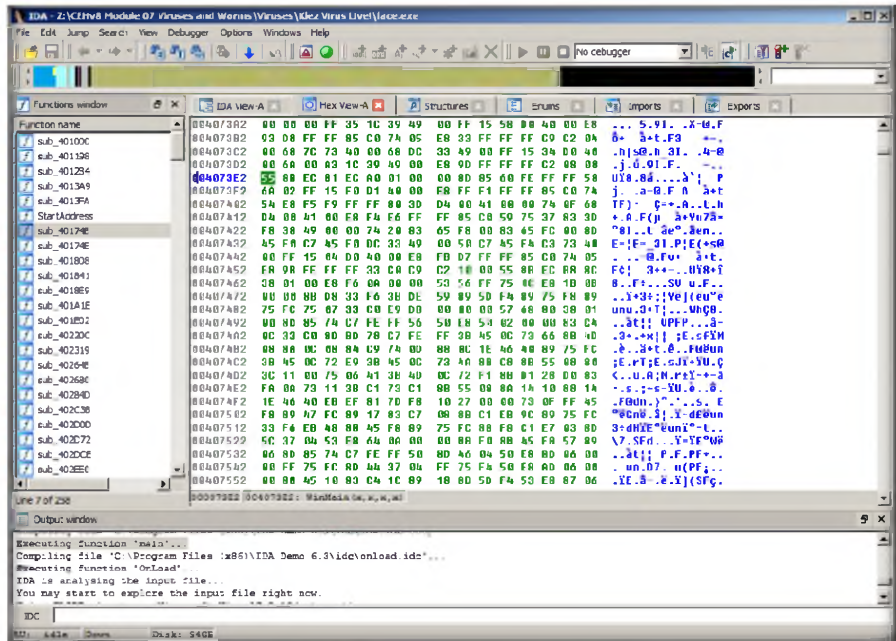


FIGURE 2.22: IDA Pro Hex View-A result.

24. Click **Windows** → **Structures**.

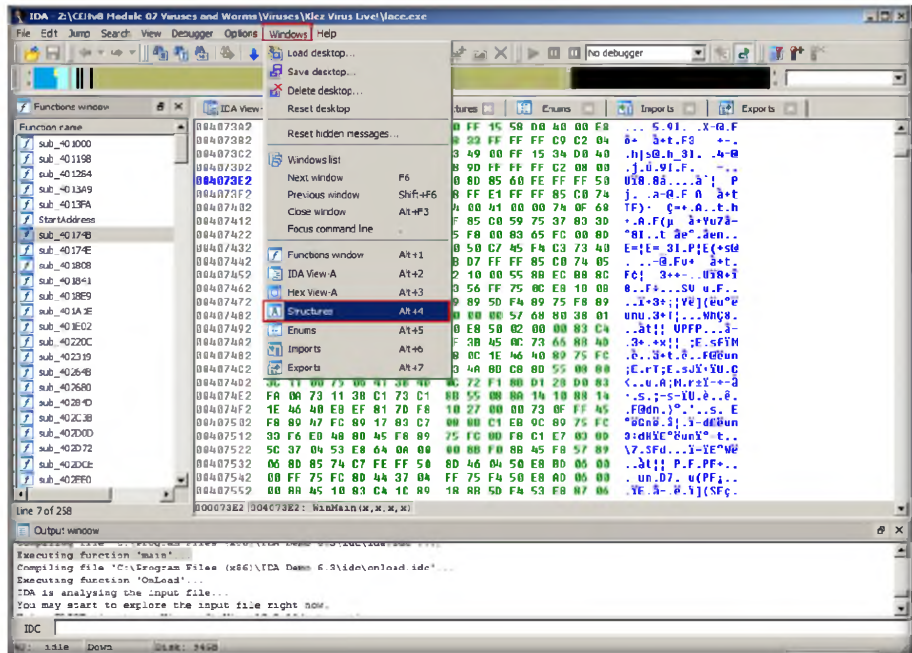


FIGURE 2.23: IDA Pro Hex Structure menu

25. The following is a window showing **Structures** (to expend structures click **Ctrl and +**).

Module 07 – Viruses and Worms

Tools demonstrated in this lab are available in **D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms**

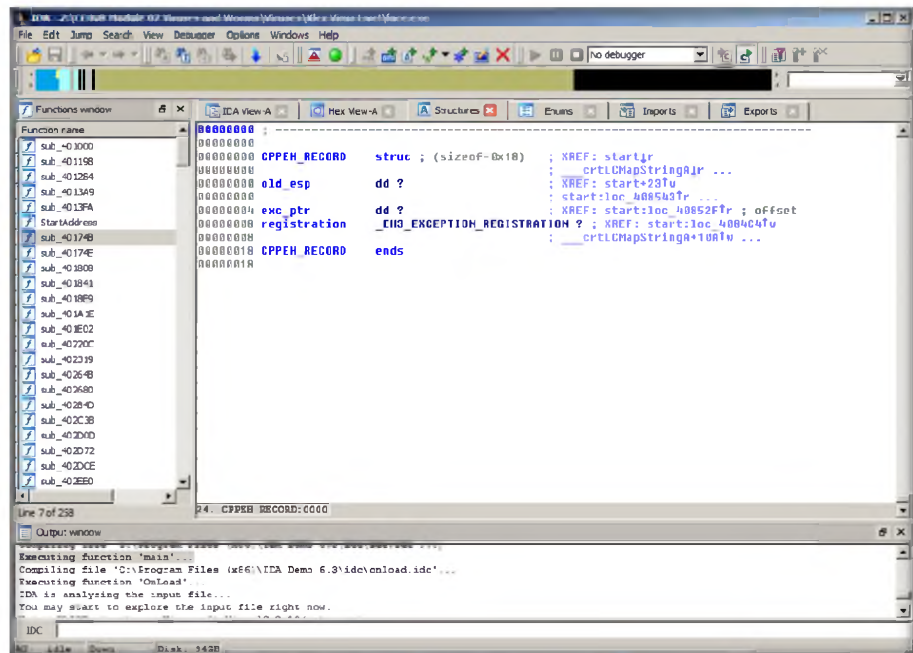


FIGURE 2.24: IDA Pro Hex Structure result

26. Click **Windows** → **Enums**.

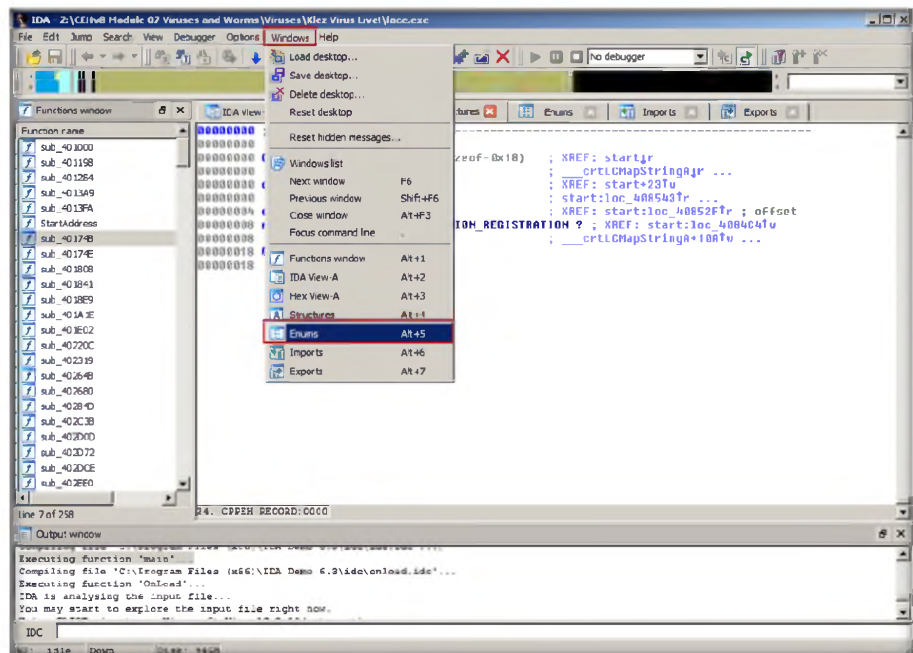


FIGURE 2.25: IDA Pro Enums menu.

27. A window appears, showing the **Enum** result.

Module 07 – Viruses and Worms

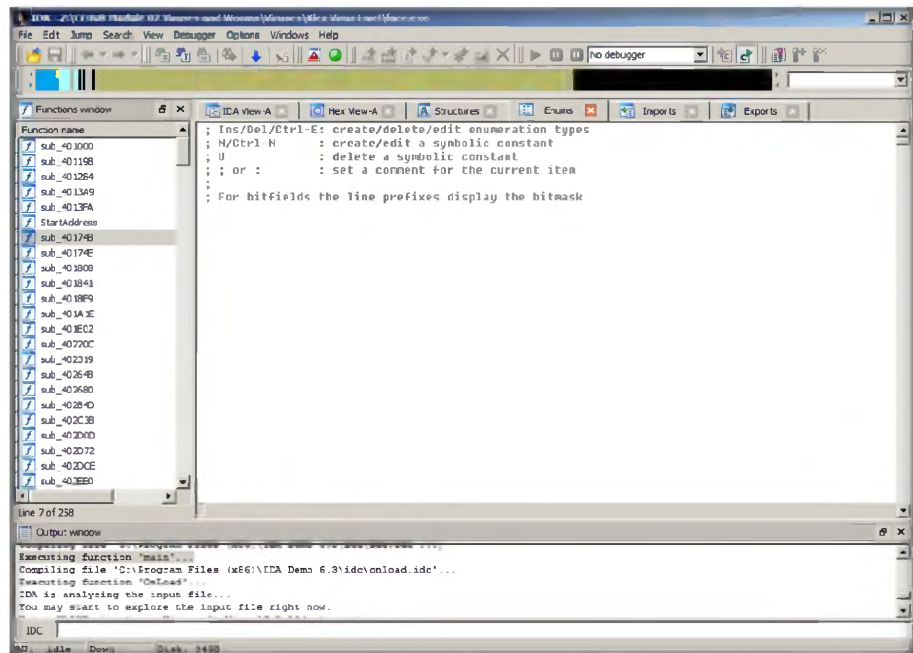


FIGURE 2.26: IDA Pro Enums result.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS
RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
IDA Pro	File name: face.exe
	Output: <ul style="list-style-type: none">▪ View functional calls▪ Hex view-A▪ View structures▪ View enums

Questions

1. Analyze the chart generated with the flow chart and function calls; try to find the possible defect that can be caused by the virus file.
2. Try to analyze more virus files from the location **D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Viruses\Klez Virus Live!**.





Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Virus Analysis Using Virus Total

Computer worms are malicious programs that replicate, execute, and spread themselves across network connections independently, without human interaction.

ICON KEY

-  Valuable information
-  Test your knowledge
-  Web exercise
-  Workbook review

Lab Scenario

In today's online environment it's important to know what risks lie ahead at each click. Every day millions of people go online to find information, to do business, to have a good time. There have been many warnings issues, about theft of data: identity theft, phishing scams and pharming; most people have at least heard of denial-of-service attacks and "zombie" computers, and now one more type of online attack has emerged: holding data for ransom. Since you are an expert ethical hacker and penetration tester, the IT director instructs you to test the network for any viruses and worms that can damage or steal the organization's information. In this lab we explain how to analyze a virus using online virus analysis services.

Lab Objectives

The objective of this lab is to make students learn and understand how to make viruses and worms to test the organization's firewall and antivirus programs.

- Analyze **virus files** over the Internet


Lab Environment

To carry out the lab, you need:

- A computer running **Windows Server 2012** as host machine
- A web browser with Internet connection

Lab Duration

Time: 15 Minutes

 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms**

Overview of Virus and Worms

Computer worms are **malicious programs** that **replicate, execute**, and spread across network connections independently, without human interaction. Attackers use worm payloads to install backdoors **in infected computers**, which turn them into zombies and **create botnets**; these botnets can be used to carry out further cyber-attacks.

Lab Tasks



TASK 1

VirusTotal Scanning service

1. Open a web browser in the **Windows Server 2012** host machine,
2. Access the website <http://www.virustotal.com>.

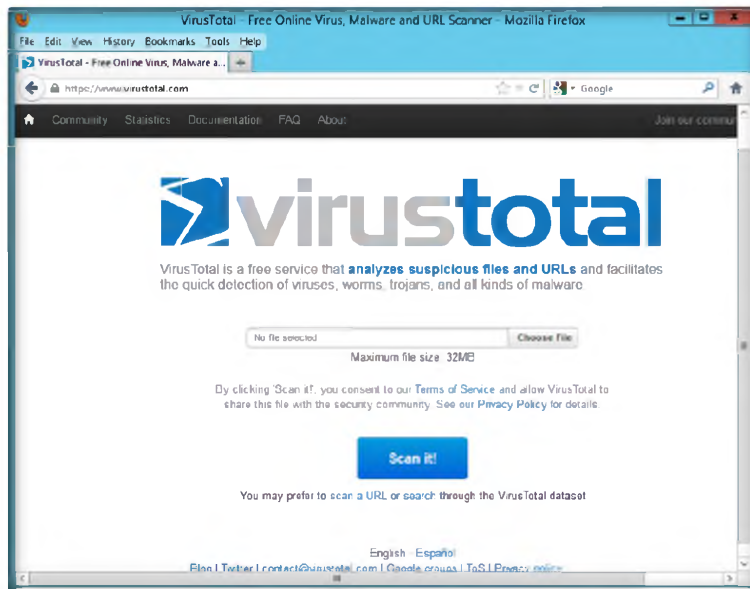


FIGURE 3.1: Virus Total Home Page

3. The Virus Total website is used to analyze online viruses.
4. Click the **Choose file** button, and select a virus file located in **D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Viruses\tini.exe**.
5. Click **Open**.

Module 07 – Viruses and Worms

You can upload any infected file to analyze

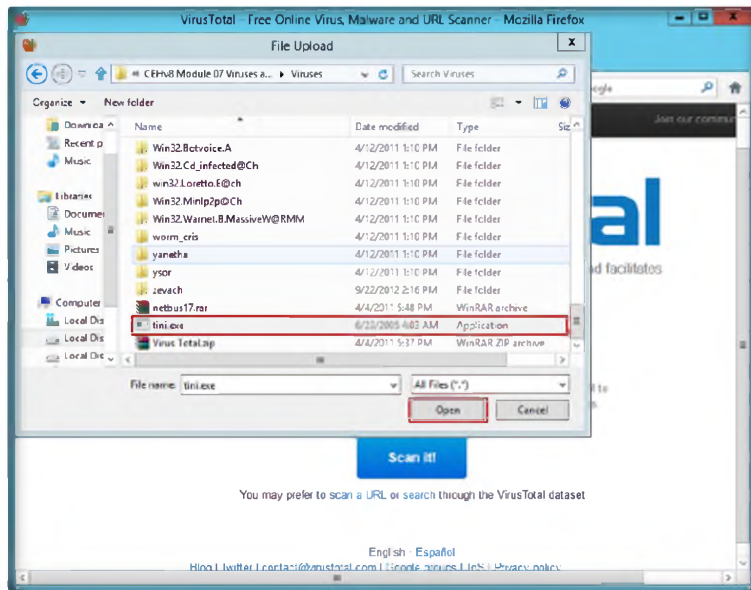


FIGURE 3.2: Select a file for Virus analysis

6. Click **Scan it!**.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms

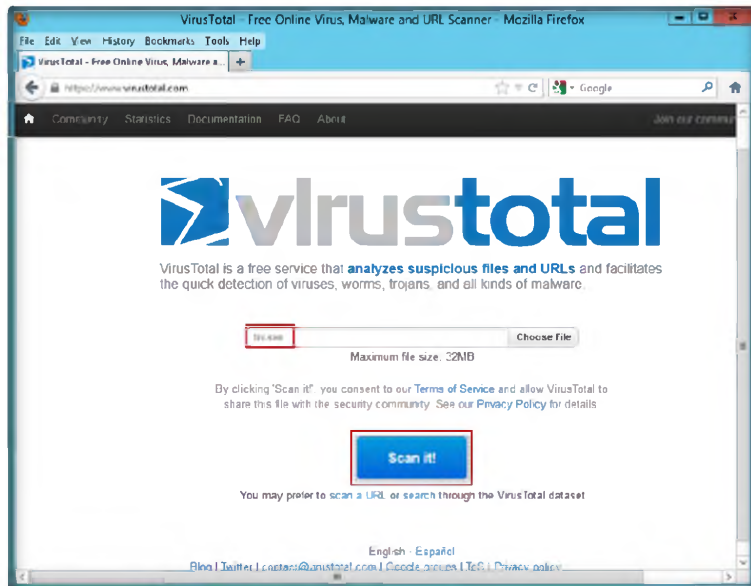


FIGURE 3.3: Click Send button to send the files for analysis

7. The selected file will be sent to the server for analysis.
8. Click **Reanalyze**.

Module 07 – Viruses and Worms

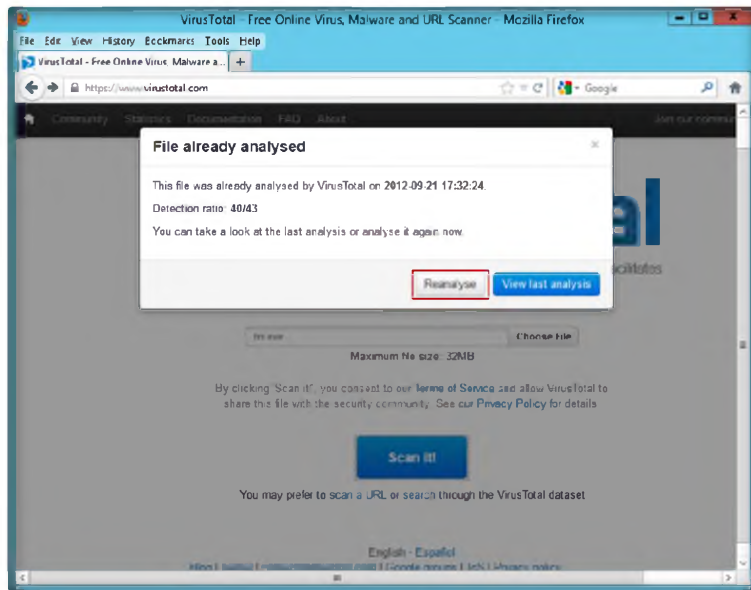


FIGURE 3.4: Sending File

9. The selected file analysis queues are scanned, as shown in the following figure.

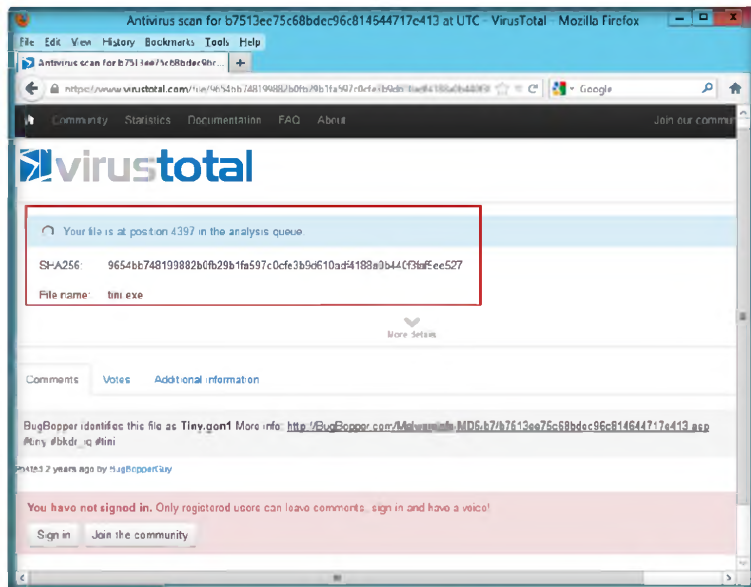


FIGURE 3.5: Scanned File

10. A detailed report will be displayed after analysis.

Module 07 – Viruses and Worms

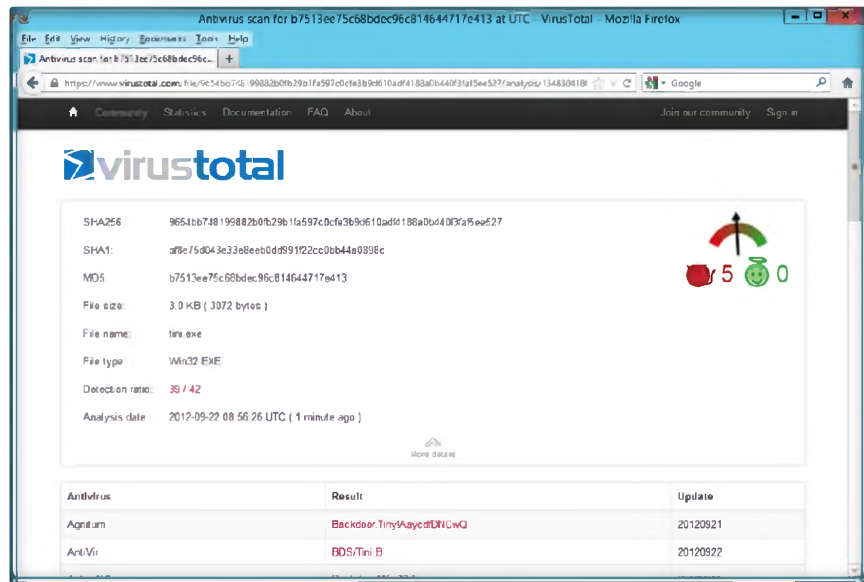


FIGURE 3.6: File Queued for analysis

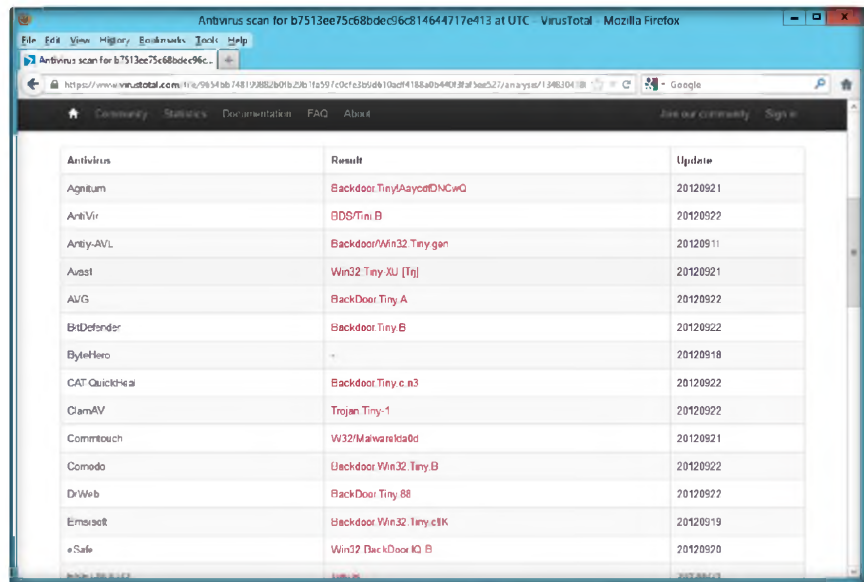


FIGURE 3.7: Analyzing the file

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

Module 07 – Viruses and Worms

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS
RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Virus Total	Scan Report shows: <ul style="list-style-type: none">▪ SHA256▪ SHA1▪ MD5▪ File size▪ File name▪ File type▪ Detection ration▪ Analysis date

Questions

1. Analyze more virus files from **D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Viruses** with the demonstrated process.





Internet Connection Required	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input type="checkbox"/> iLabs



Scan for Viruses Using Kaspersky Antivirus 2013

Computer worms are malicious programs that replicate, execute, and spread themselves across network connections independently, without human interaction.


ICON KEY

-  Valuable information
-  Test your knowledge
-  Web exercise
-  Workbook review

Lab Scenario

Today, many people rely on computers to do work and create or store useful information. Therefore, it is important for the information on the computer to be stored and kept properly. It is also extremely important for people on computers to protect their computer from data loss, misuse, and abuse. For example, it is crucial for businesses to keep information they have secure so that hackers can't access the information. Home users also need to take means to make sure that their credit card numbers are secure when they are participating in online transactions. A computer security risk is any action that could cause loss of information, software, data, processing incompatibilities, or cause damage to computer hardware.

Once you start suspecting that there is spyware on your computer system, you must act at once. The best thing to do is to use spyware remover software. The spyware remover software is a kind of program that scans the computer files and settings and eliminates those malicious programs that you actually do not want to keep on your operating system. In this lab Kaspersky Antivirus 2013 program detect the malicious programs and vulnerabilities in the system.

 **Tools**
demonstrated in
this lab are
available in
**D:\CEH-
Tools\CEHv8
Module 07 Viruses
and Worms**

Lab Objectives

The objective of this lab is to make students learn and understand how to make viruses and worms to test the organization's firewall and antivirus programs.

Lab Environment

To carry out the lab, you need:

- **Kaspersky Antivirus 2013** is located at **D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Anti-Virus Tools\Kaspersky Anti-Virus**

Download the Kaspersky Antivirus 2013 from the link <http://www.kaspersky.com/anti-virus>

- You can also download the latest version of **Kaspersky Antivirus 2013** from the link <http://www.kaspersky.com/anti-virus>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Run this tool in **Windows 7** virtual machine
- Active Internet connection

Lab Duration

Time: 15 Minutes

Overview of Virus and Worms

Computer worms are **malicious programs** that **replicate, execute**, and spread across network connections independently, without human interaction. Attackers use worm payloads to install backdoors in **infected computers**, which turn them into zombies and **create botnets**; these botnets can be used to carry out further cyber-attacks.

Lab Tasks

Note: Before running this lab, take a snapshot of your virtual machine.

1. Start the **Windows 7** Virtual Machine.
2. Before scanning the disk, infect the disk with viruses.
3. Open the **CEH-Tools** folder and browse to the location **Z:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Viruses**.
4. Double-click the **tini.exe** file.



FIGURE 4.1: Tini Virus file

5. Open the **CEH-Tools** folder and browse to the location **Z:\CEHv8 Module 07 Viruses and Worms\Viruses\netbus17**.
6. Double-click the **Patch.exe** file.

Advanced anti-phishing technologies proactively detect fraudulent URLs and use real-time information from the cloud, to help ensure you're not tricked into disclosing your valuable data to phishing websites.

Module 07 – Viruses and Worms

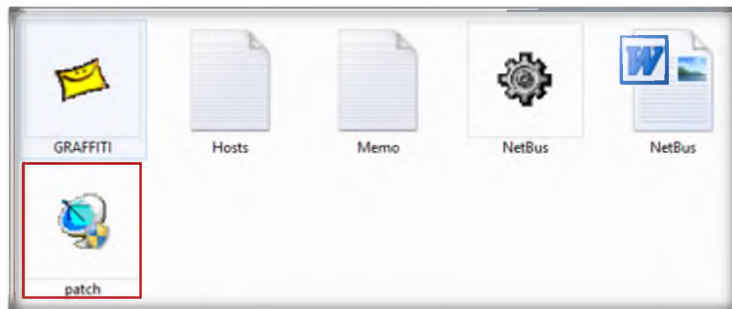


FIGURE 4.2: Patch Virus file in Netbus 17

7. Open the **CEH-Tools** folder and browse to the location **Z:\CEHv8 Module 07 Viruses and Worms\Viruses\Klez Virus Live!**.
8. Double-click the **face.exe** file.

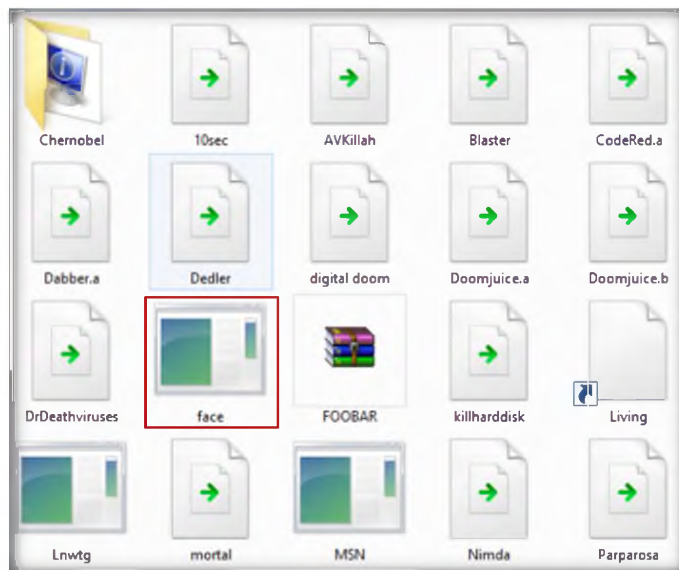



FIGURE 4.3: Face Virus file

9. Note that these tools will not reflect any changes.
10. Go to the location **D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Anti-Virus Tools\Kaspersky Anti-Virus**.
11. Install **Kaspersky Antivirus 2013** software in **Windows 7**.
12. While installing it will ask for activation; click **Activate Trial Version** and then click **Next**.
13. The main window of Kaspersky Antivirus 2013 as show in below figure.

 **Kaspersky**
Protects against
all viruses by
combining cloud-
based
functionality and
powerful security
technologies that
runs on your PC

 **Kaspersky Anti-Virus**
2013 works behind-the-
scenes – defending you and
your PC against viruses,
spyware, Trojans, rootkits and
other threats

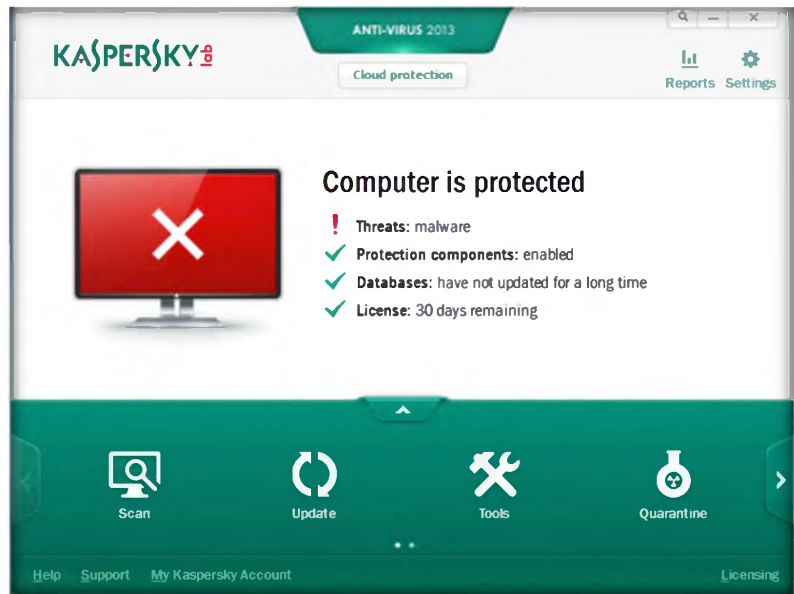


FIGURE 4.4: Kaspersky main window

14. Select **Scan Icon**.

Kaspersky Antivirus 2013 is fully compatible with Microsoft's latest operating system

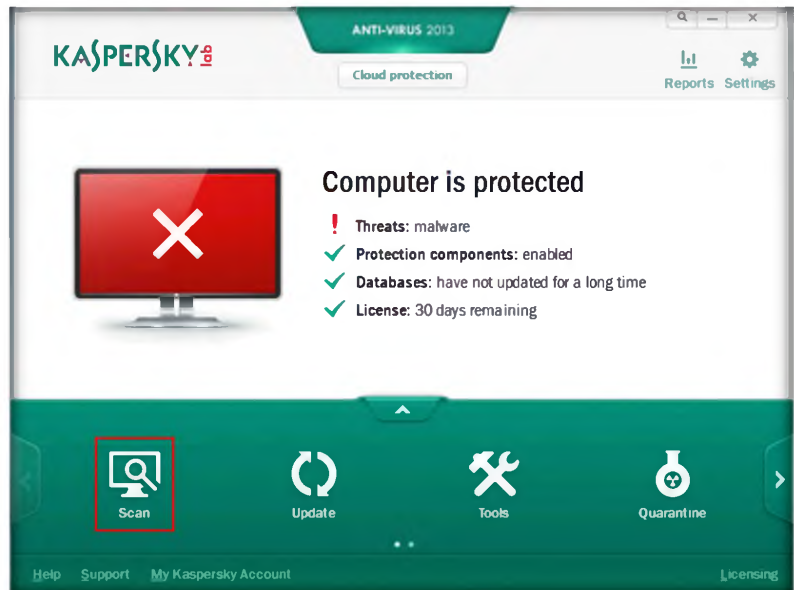


FIGURE 4.5: Kaspersky Scan window

15. Select **Full Scan** to scan the computer (Windows 7 Virtual Machine).

Module 07 – Viruses and Worms

 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms**

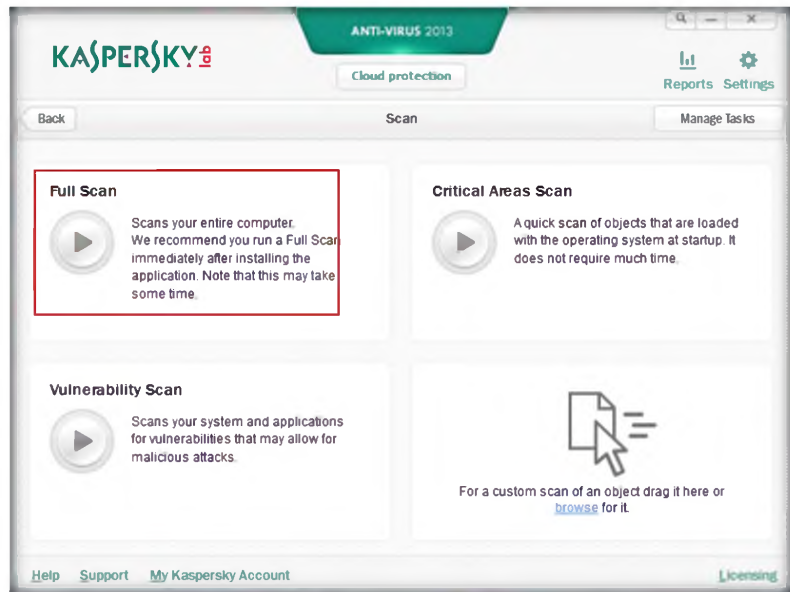



FIGURE 4.6: Kaspersky Starting full scan

16. It will display the **Full scan** window. Click **Scan now**.

 Kaspersky Anti-Virus 2013 is optimised so that it does not have a significant impact on network activity, the installation of programs, the launch of web browsers or the launch of programs.

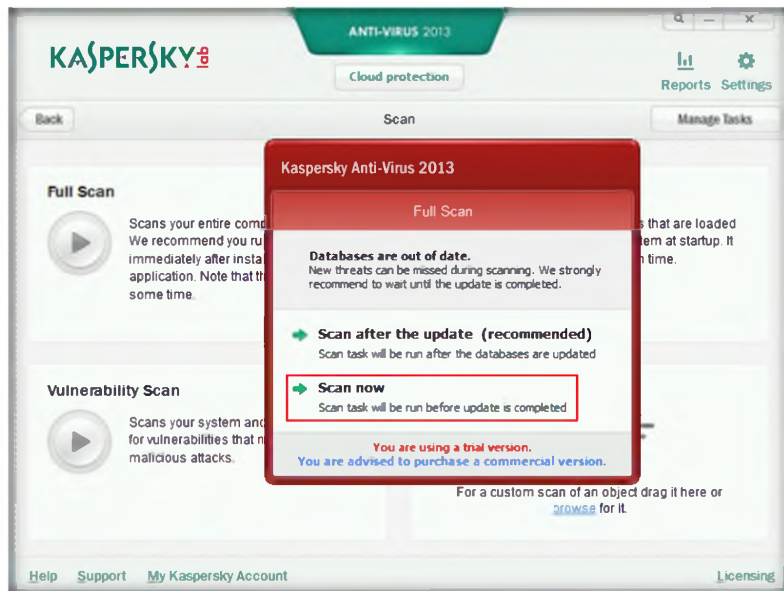


FIGURE 4.7: Scanning process

17. Kaspersky Antivirus 2013 scans the computer. (It will take some time so be patient.)

Even if your PC and the applications running on it haven't been updated with the latest fixes, Kaspersky Anti-Virus 2013 can prevent exploitation of vulnerabilities by:

- controlling the launch of executable files from applications with vulnerabilities
- analysing the behaviour of executable files for any similarities with malicious programs
- restricting the actions allowed by applications with vulnerabilities

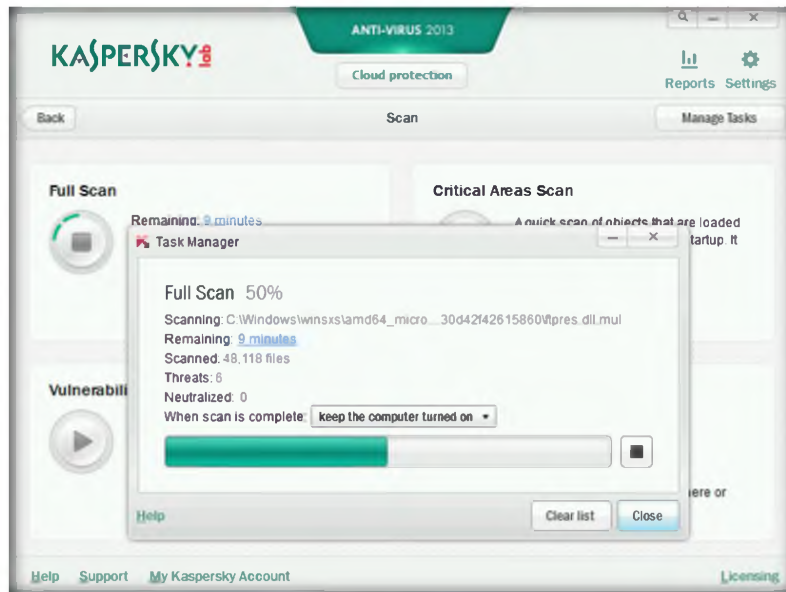


FIGURE 4.8: Scanning process

- The **Virus Scan** window appears; it will ask for to perform a special disinfection procedure.
- Click **Yes, disinfect with reboot (recommended)**.

The main interface window is optimised to help boost performance and ease of use for many popular user scenarios – including launching scans and fixing problems

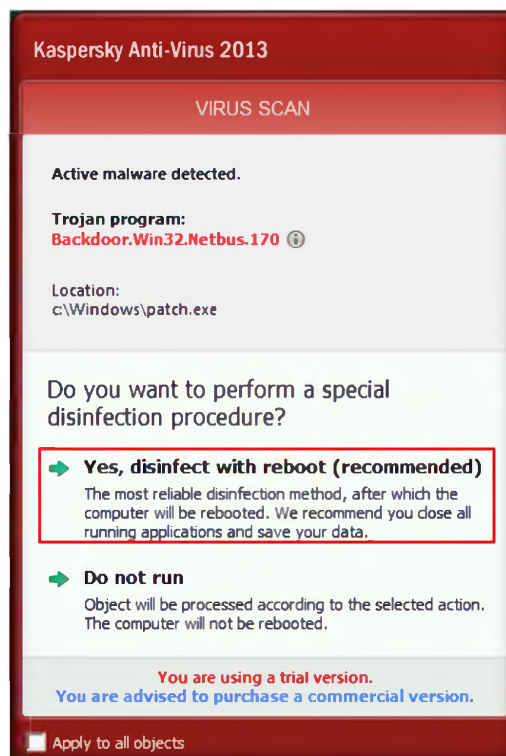


FIGURE 4.9: Detecting the malware

Module 07 – Viruses and Worms

20. The **Advanced Disinfection scan** will start; it will scan the complete system (this may take some time).

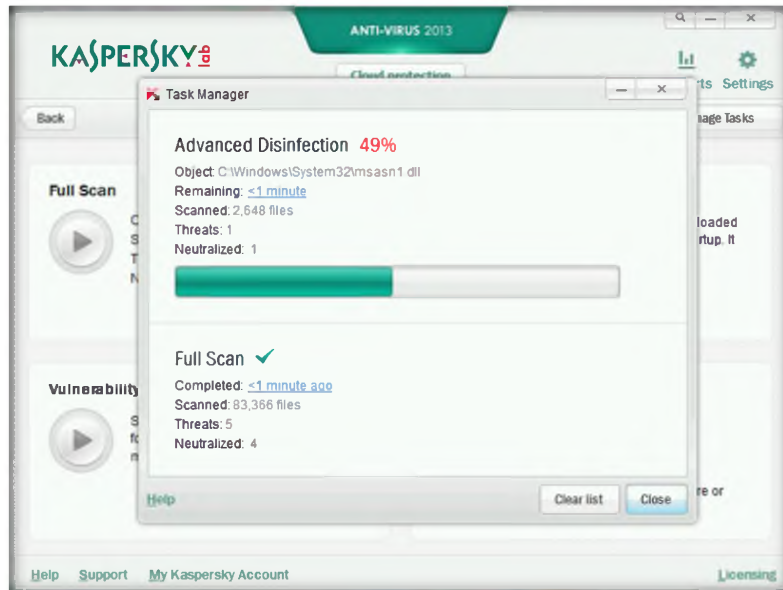


FIGURE 4.10: Advanced Disinfection scanning

21. The cleaned viruses will appear, as shown in the following figure.

Tools
demonstrated in
this lab are
available in
D:\CEH-
Tools\CEHv8
Module 07 Viruses
and Worms

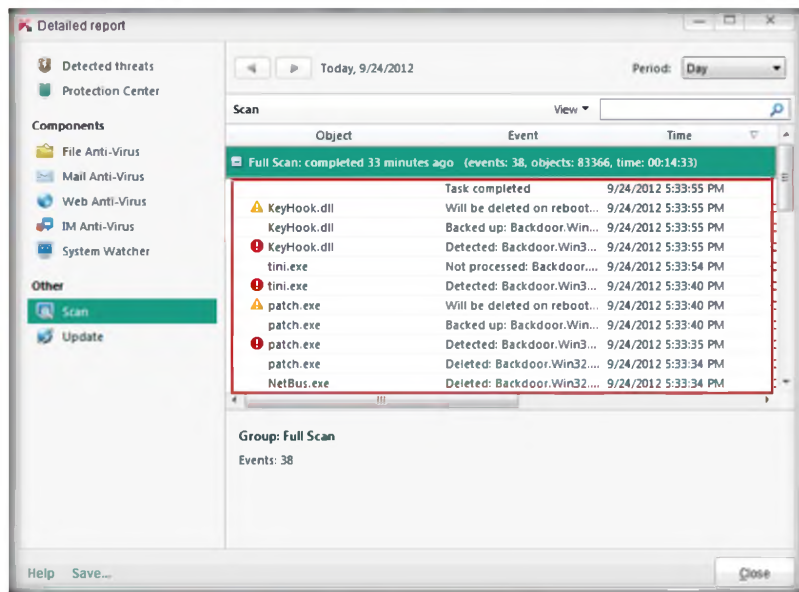


FIGURE 4.11: Cleaned infected files

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS
RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Kaspersky Antivirus 2013	Result: List of detected vulnerabilities in the system

Questions

1. Using the final report, analyze the processes affected by the virus files.





Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Virus Analysis Using OllyDbg

OllyDbg is a debugger that emphasizes binary code analysis, which is useful when source code is not available. It traces registers, recognizes procedures, API calls, switches, tables, constants and strings, as well as locates routines from object files and libraries.

ICON KEY


-  Valuable information
-  Test your knowledge
-  Web exercise
-  Workbook review

Lab Scenario

There are literally thousands of malicious logic programs and new ones come out all the time, so that's why it's important to keep up-to-date with the new ones that come out. Many websites keep track of this. There is no known method for providing 100% protection for any computer or computer network from computer viruses, worms, and Trojan horses, but people can take several precautions to significantly reduce their chances of being infected by one of those malicious programs. Since you are an expert ethical hacker and penetration tester, your IT director instructs you to test the network to determine whether any viruses and worms will damage or steal the organization's information. In this lab ollyDbg is used to analyze viruses registers, procedures, API calls, tables, libraries, constants, and strings.

Lab Objectives

The objective of this lab is to make students learn and understand analysis of the viruses.

 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms**

Lab Environment

To carry out the lab, you need:

- **OllyDbg** tool located at **D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Debugging Tool\OllyDbg**
- A computer running **Windows Server 2012** as host machine
- You can also download the latest version of **OllyDbg** from the link <http://www.ollydbg.de/>
- Run this tool on **Windows Server 2012**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of OllyDbg

The debugging engine is now more stable, especially if one steps into the exception handlers. There is a new debugging option, "Set permanent breakpoints on system calls." When active, it requests OllyDbg to set breakpoints on `KERNEL32.UnhandledExceptionFilter()`, `NTDLL.KiUserExceptionDispatcher()`, `NTDLL.ZwContinue()`, and `NTDLL.NtQueryInformationProcess()`.

Lab Tasks

TASK 1

Debug a Virus

1. Launch the **OllyDbg** tool. Installation is not required for **OllyDbg**. Double-click and launch the **ollydbg.exe** file.
2. The **OllyDbg** window appears.

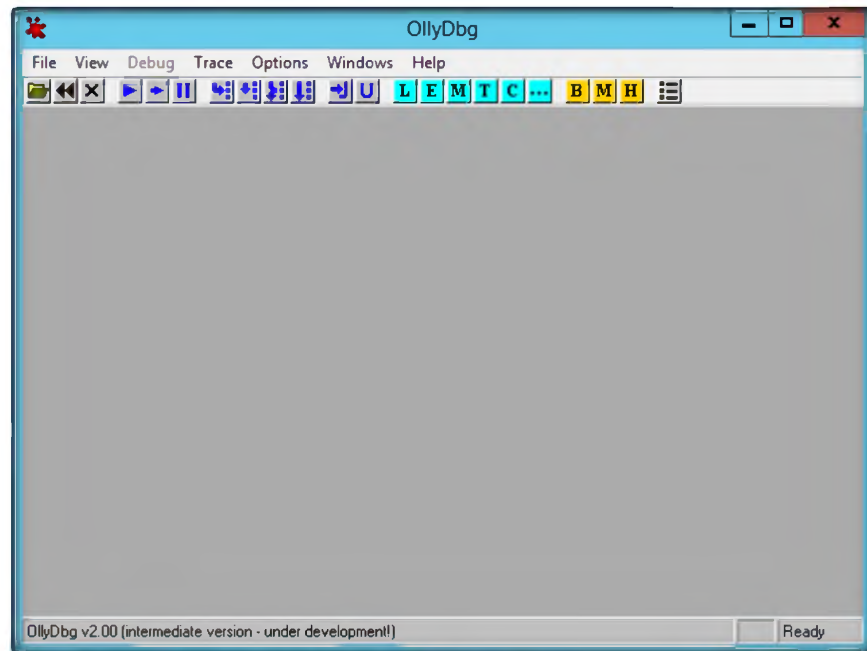



FIGURE 5.1: OllyDbg main window

3. Go to **File** from menu bar and click **Open...**
4. Browse to **D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Viruses\Virus Total\tini.exe**.
5. Click **Open**.

You can also download the latest version of OllyDbg from the link <http://www.ollydbg.de>

Module 07 – Viruses and Worms

 Data formats. Dump windows display data in all common formats: hexadecimal, ASCII, UNICODE, 16-and 32-bit signed/unsigned/hexadecimal integers, 32/64/80-bit floats, addresses, disassembly (MASM, IDEAL, HLA or AT&T).

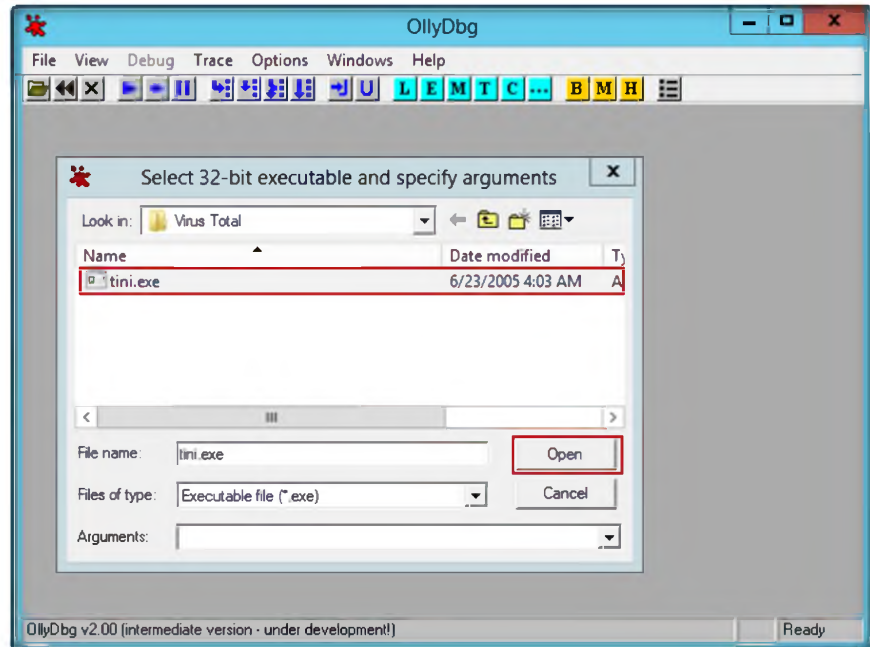



FIGURE 5.2: Select tini.exe Virus total

- The output of **CPU-main thread, module tini** is shown in the following figure.

 OllyDbg can debug multithread applications. You can switch from one thread to another, suspend, resume and kill threads or change their priorities.

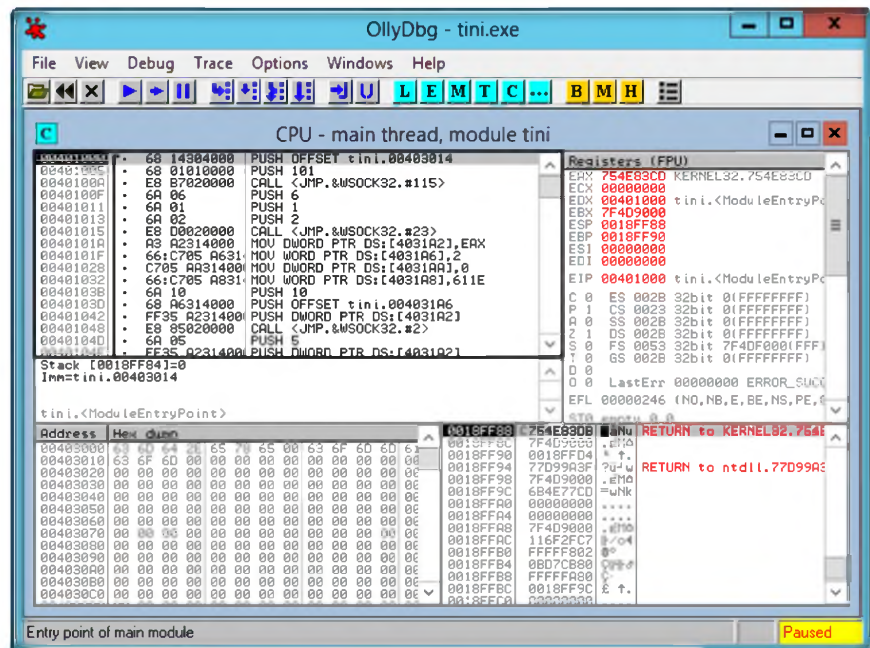



FIGURE 5.3: CPU utilization of tini.exe

- Click **View** from the menu bar, and then click **Log (Alt+L)**.

Module 07 – Viruses and Worms

 Full UNICODE support. All operations available for ASCII strings are also available for UNICODE, and vice versa. OllyDbg is able to recognize UTF-8 strings.

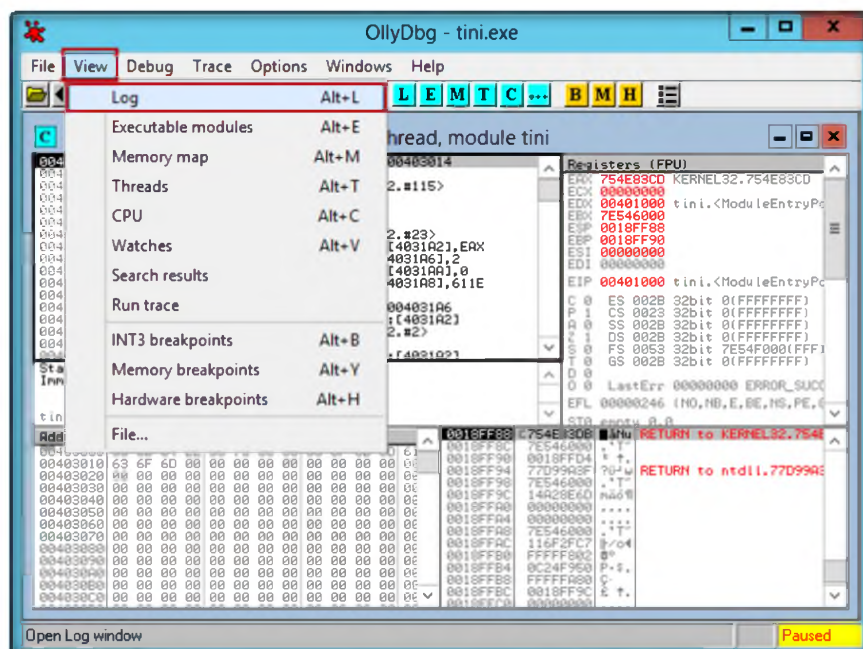



FIGURE 5.4: Select log information

8. The output of log data `tini.exe` is shown in the following figure.

 **Breakpoints:** OllyDbg supports all common kinds of breakpoints: INT3, memory and hardware. You may specify number of passes and set conditions for pause

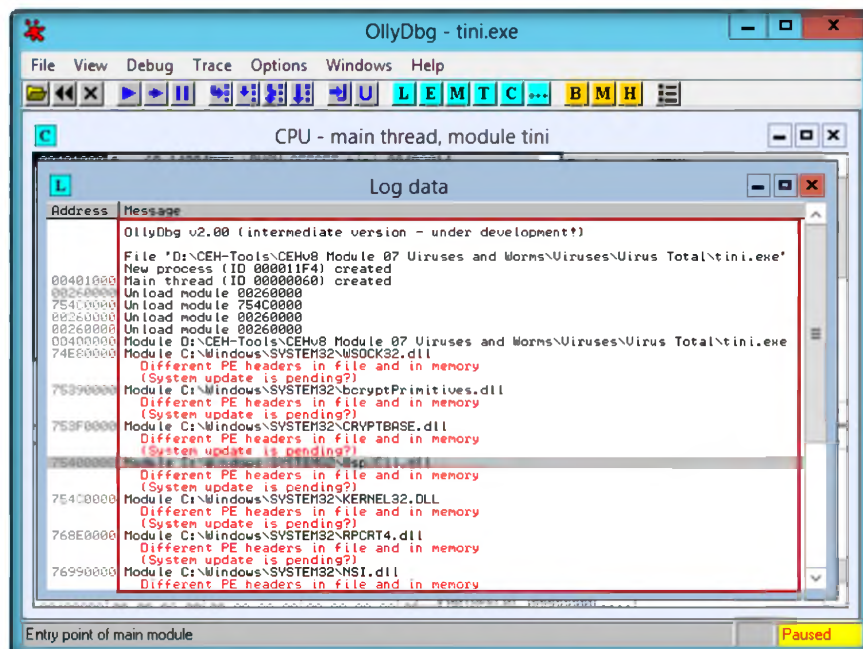



FIGURE 5.5: Output of Log data information of `tini.exe`

9. Click **View** from the menu bar, and click **Executable module (Alt+E)**.
10. The output of **Executable modules** is shown in the following figure.

Module 07 – Viruses and Worms

 **Watches:** Watch is an expression evaluated each time the program pauses. You can use registers, constants, address expressions, Boolean and algebraical operations of any complexity

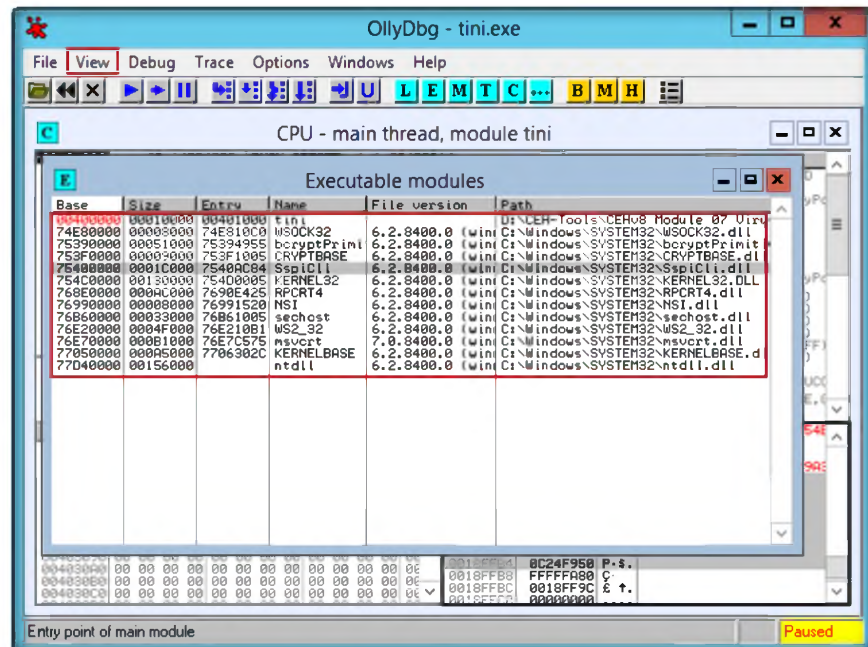


FIGURE 5.6: Output of executable modules of tini.exe

- Click **View** from the menu bar, and then click **Memory Map (Alt+M)**.
- The output of **Memory Map** is shown in the following figure.

 **OllyDbg** supports four different decoding modes: MASM, Ideal, HLA and AT&T

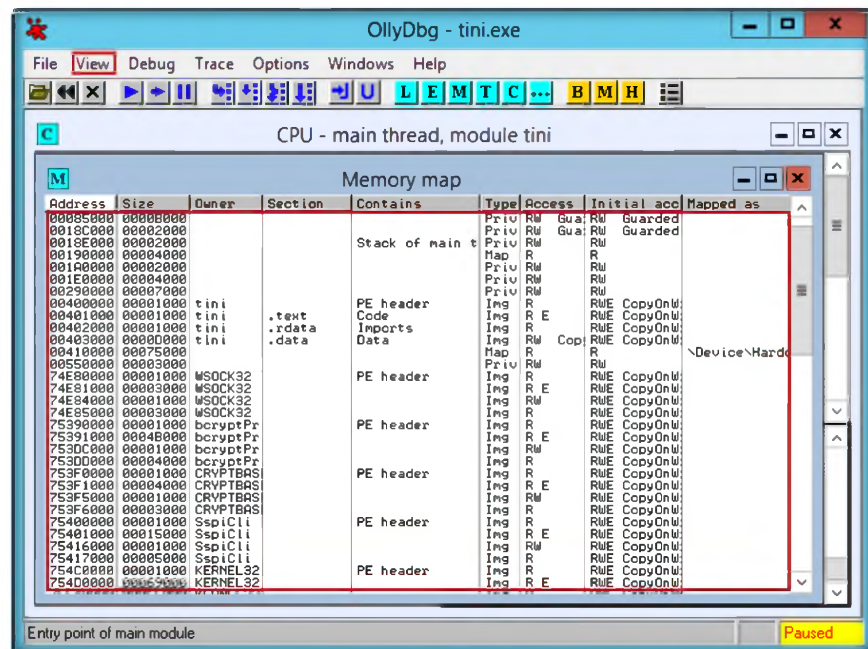


FIGURE 5.7: Output of Memory map of tini.exe

- Click **View** from the menu bar, and then click **Threads (Alt+T)**.
- The output of **Threads** is shown in the following figure.

Module 07 – Viruses and Worms

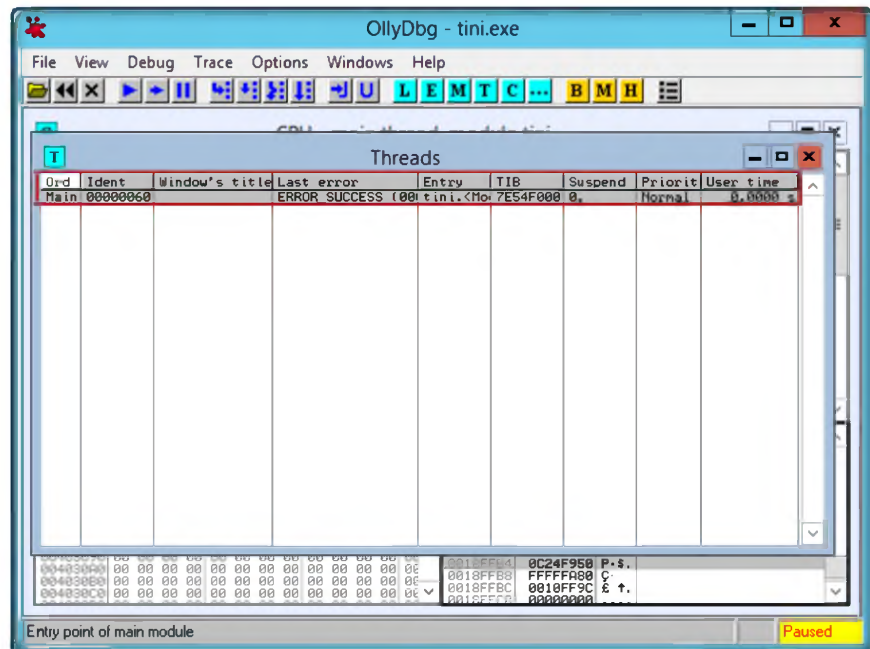


FIGURE 5.8: Output of threads

Lab Analysis

Document all the files, created viruses, and worms in a separate location.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS
RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
OllyDbg	Result: <ul style="list-style-type: none"> ▪ CPU-main thread ▪ Log data ▪ Executable modules ▪ Memory map ▪ Threads

Questions

1. Using the final report, analyze the processes affected by the virus files.





Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Creating a Worm Using Internet Worm Maker Thing

Internet Worm Maker Thing is a tool to create worms. It also has a feature to convert a virus into a worm.

ICON KEY

-  Valuable information
-  Test your knowledge
-  Web exercise
-  Workbook review

Lab Scenario

In recent years there has been a large growth in Internet traffic generated by malware, that is, internet worms and viruses. This traffic usually only impinges on the user when either their machine gets infected or during the epidemic stage of a new worm, when the Internet becomes unusable due to overloaded routers. What is less well-known is that there is a background level of malware traffic at times of non-epidemic growth and that anyone plugging an unfirewalled machine into the Internet today will see a steady stream of port scans, back-scatter from attempted distributed denial-of-service attacks, and hostscans. We must better firewalls, protect the Internet router infrastructure, and provide early-warning mechanisms for new attacks.

Since you are an expert ethical hacker and penetration tester, your IT director instructs you to test the network to determine whether any viruses and worms will damage or steal the organization's information. You need to construct viruses and worms, try to inject them into a dummy network (virtual machine), and check their behavior, whether they are detected by an antivirus and if they bypass the firewall.


Lab Objectives

The objective of this lab is to make students learn and understand how to make viruses and worms.

Lab Environment

To carry out the lab, you need:

- **Internet Worm Maker Thing** located at **D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Makers\Internet Worm Maker Thing\Generator.exe**

 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms**

- A computer running **Windows Server 2012** as host machine
- Run this tool on **Windows Server 2012**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of Virus and Worms

A virus is a **self-replicating program** that produces its own code by attaching copies of it onto other **executable codes**. Some viruses affect computers as soon as their codes are **executed**; others lie dormant until a predetermined logical circumstance is met.

Lab Tasks

TASK 1

Make a Worm

1. Launch the **Internet Worm Maker Thing** tool. Installation is not required for **Internet Worm Maker Thing**. Double-click and launch the **Generator.exe** file.
2. The **Internet Worm Maker Thing** window appears.

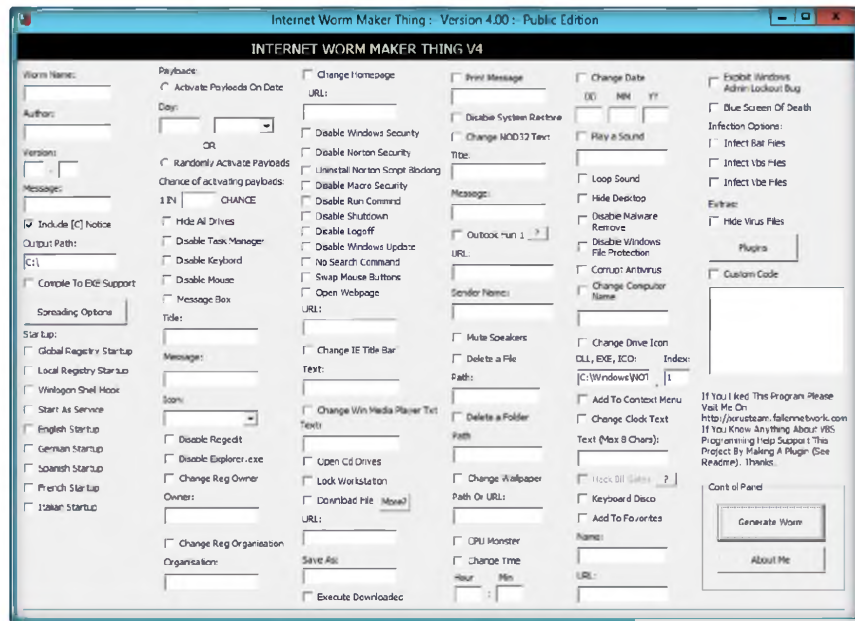




FIGURE 6.1: Internet Worm maker thing main window

3. Enter a **Worm Name**, **Author**, **Version**, **Message**, and **Output Path** for the created worm.
4. Check the **Compile to EXE support** check box.
5. In startup: select **English Startup**.



 The option, Auto Startup is always checked by default and start the virus whenever the system boots on.

Module 07 – Viruses and Worms

 A list of names for the virus after install is shown in the Name after Install drop-down list.

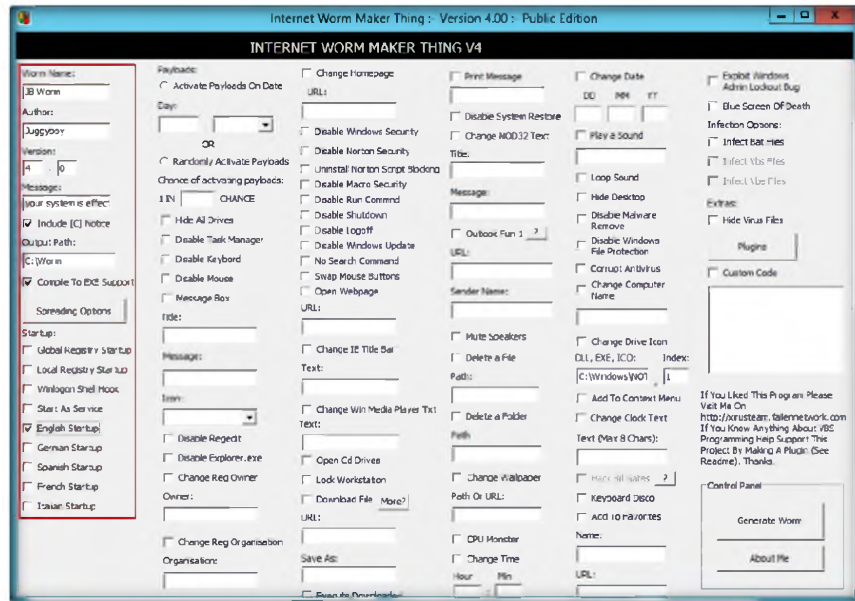


FIGURE 6.2: Select the options for creating Worm

6. Select the **Activate Payloads on Data** radio button, and for **Chance of activating payloads**, enter **5**.
7. Check the **Hide All Drives**, **Disable Task Manager**, **Disable keyboard**, **Disable Mouse** and **Message Box** check boxes.
8. Enter **Tile**, **Message**, and **Select Icon as Information** from the drop-down list.
9. Check the **Disable Regedit**, **Disable Explorer.exe** and **change Reg owner** check boxes.

Module 07 – Viruses and Worms

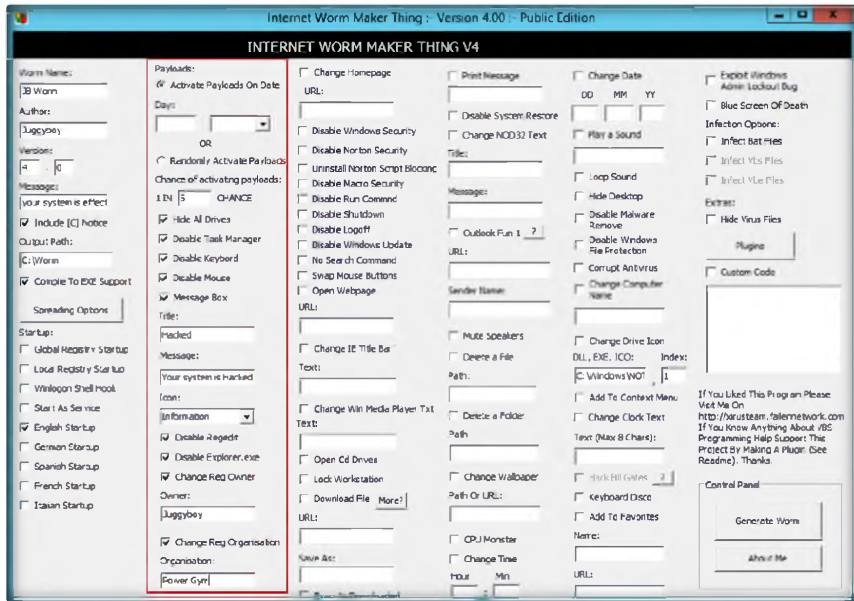
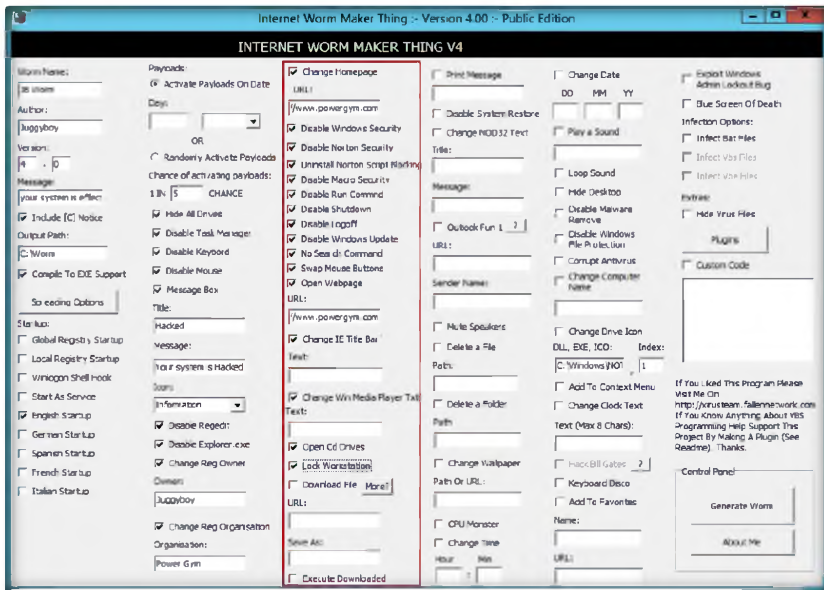


FIGURE 6.3: Select the option for creating worm

10. Check the **Change Homepage** check box. In the **URL** field, enter <http://www.powrgym.com>.
11. Check the **Disable Windows Security, Disable Norton Security, Uninstall Norton Script Blocking, Disable Micro Security, Disable Run Command, Disable Shutdown, Disable Logoff, Disable Windows Updates, No Search Command, Swap Mouse button, and Open Webpage** check boxes.
12. Check the **Change IE Title bar, change win Media Player Txt, Open Cd drive, and Lock workstation** check boxes.



☛ Don't forget to change the settings for every new virus creation. Otherwise, by default, it takes the same name as an earlier virus.

Module 07 – Viruses and Worms

FIGURE 6.4: Select the option for creating worm

13. Check the **Print Message**, **Disable system Restore**, and **Change NOD32 Text** check boxes.
14. Enter a **Title** and **Message** in the respective fields.
15. Enter the **URL** as <http://www.powrgym.com> and the **Sender Name** as **juggyboy**.
16. Check the **Mute speakers**, **Delete a Folder**, **Change Wallpaper**, and **CPU Monster** check boxes.
17. Select the **Change Time** check box enter hour and min the respective fields.

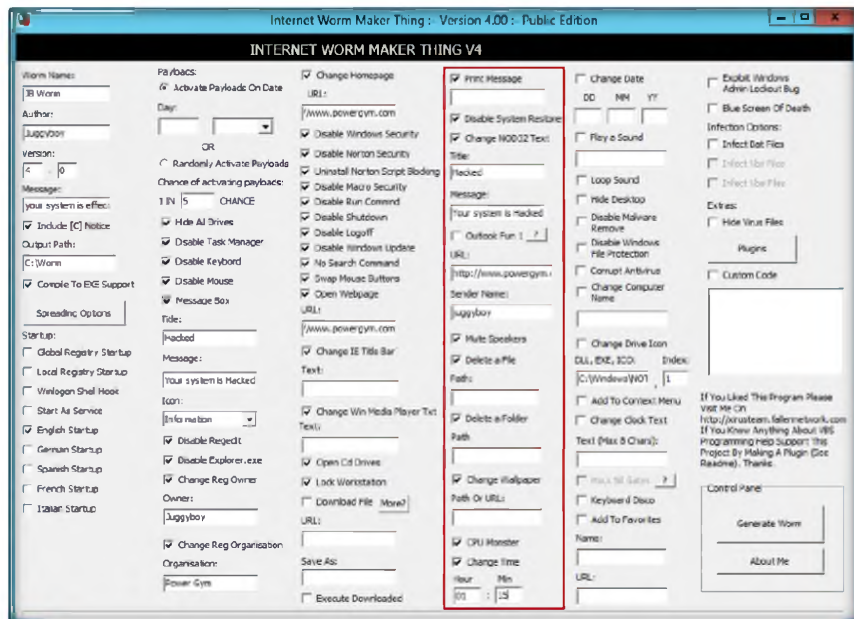



FIGURE 6.5: Select the option for creating worm

18. Check the **Change Date** check box, and enter the DD, MM, YY in the respective fields.
19. Check the **Loop Sound**, **Hide Desktop**, **Disable Malware Remove**, **Disable Windows File Protection**, **Computer Antivirus**, and **Change Computer Name** check boxes.
20. Check the **Change the Drive Icon**, **Add To Context Menu**, **Change Clock Text**, **Keyboard Disco**, and **Add To Favorites** check boxes.

Module 07 – Viruses and Worms

 **Tools**
demonstrated in
this lab are
available in
**D:\CEH-
Tools\CEHv8
Module 07 Viruses
and Worms**

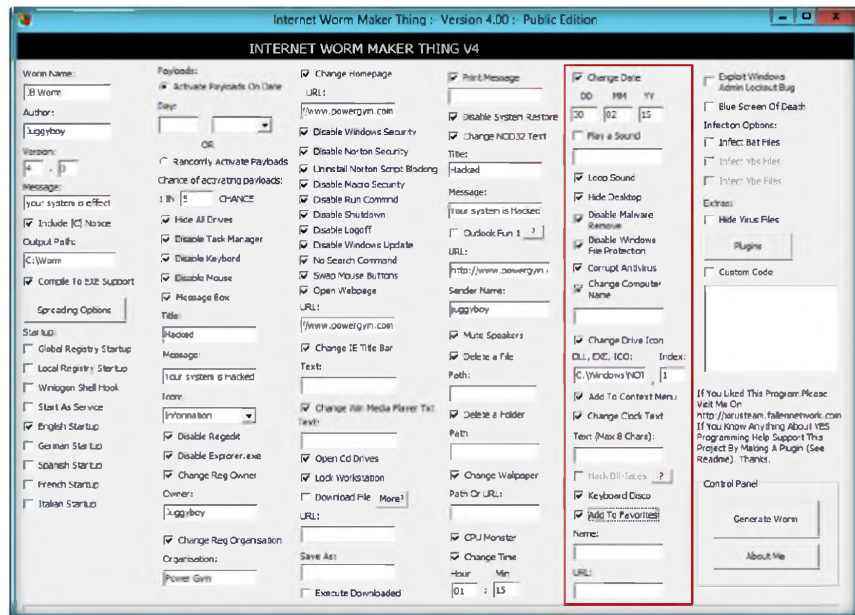


FIGURE 6.6: Select the option for creating worm

21. Check the **Exploit Windows Admin Lockout Bug** and **Blue Screen of Death** check boxes.
22. Check the **Infect Bat Files** check box from **Infection Options**.
23. Check the **Hide Virus Files** check box from **Extras**.
24. Click **Generate Worm** in **Control Panel**.

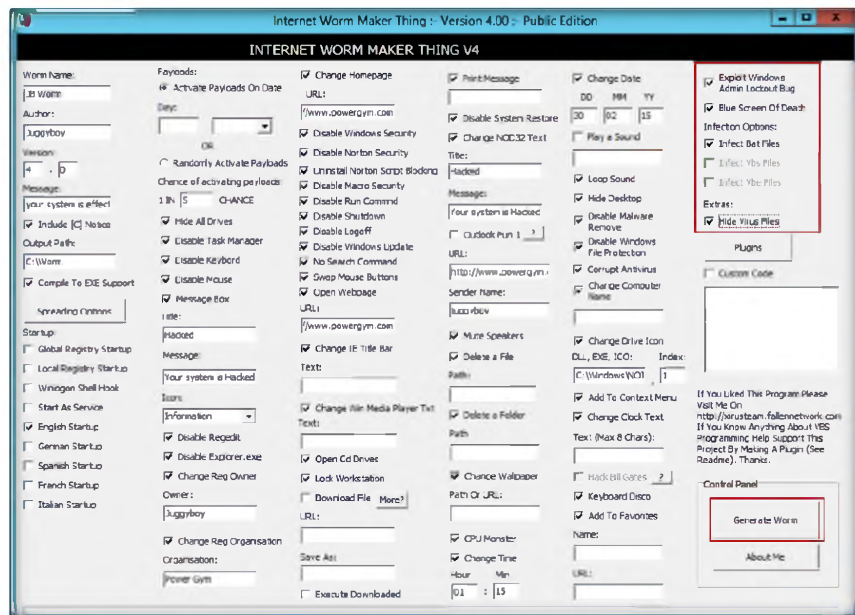
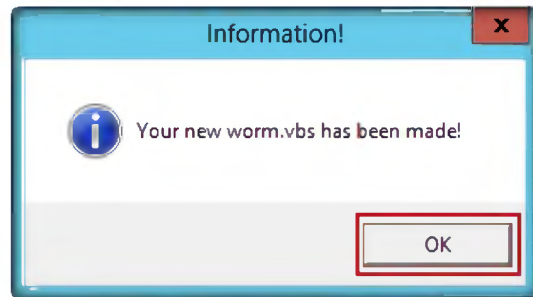


FIGURE 6.7: Select the option for creating worm

Module 07 – Viruses and Worms

25. The worm is successfully created. The following window appears. Click **OK**.



26. The created **worm.vbs** file is located at the **C:** drive.



Lab Analysis

Document all the files, created viruses, and worms in a separate location.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS
RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Internet Worm Maker Thing	To make Worms options are used: <ul style="list-style-type: none">▪ Hide all drives▪ Disable Task Manager▪ Disable keyboard▪ Disable mouse▪ Message box▪ Disable Regedit▪ Disable Explorer.exe▪ Change Reg Owner▪ Change HomePage▪ Disable Windows security▪ Disable Norton security▪ Disable Run command▪ Disable shutdown

Questions

1. Examine whether the created worms are detected or blocked by any antivirus or antispymware programs.

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs