





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

Lab Environment

To carry out this, you need:

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

- 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

Lab Tasks

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 web servers. It will teach you how to:


- 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**

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

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

- You can also download the latest version of **httprecon** from the link **<http://www.compute.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

Lab Duration

Time: 10 Minutes

Overview of httprecon


httprecon is a tool for advanced **web server** fingerprinting, similar to **httpprint**. 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

Lab Tasks

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.

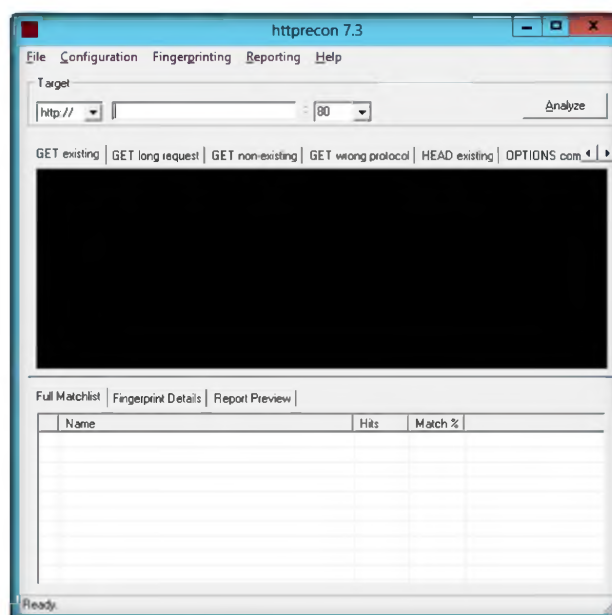


FIGURE 1.1: httprecon main window

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.

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

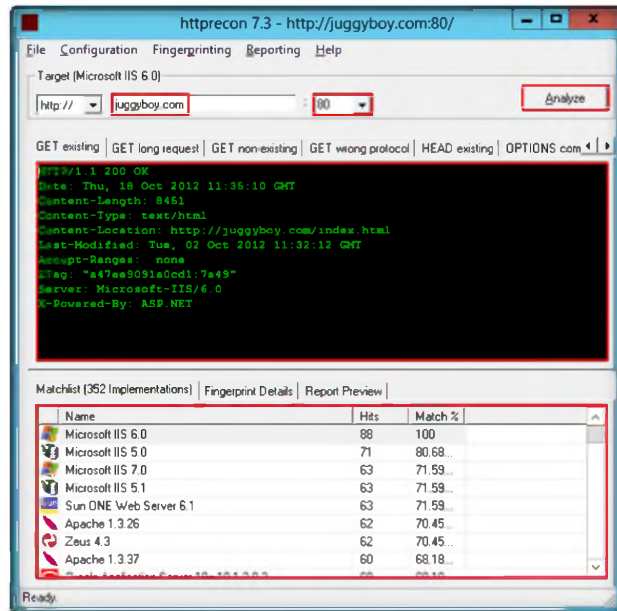


FIGURE 1.2: The footprint result of the entered website

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

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

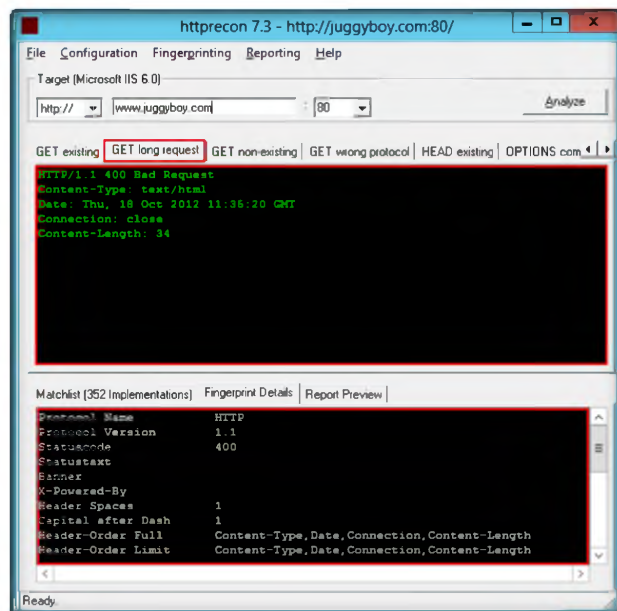


FIGURE 1.3: The fingerprint and GET long request result of the entered website

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

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	Output: Footprint of the juggyboy website <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 httpprint.

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/idserve.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

Lab Tasks

1. In Windows Server 2012, navigate to **D:\CEH-Tools\CEHv8 Module 12 Hacking Webservers\Webserver Footprinting Tools\ID Serve**.
2. Double-click **idservice.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.

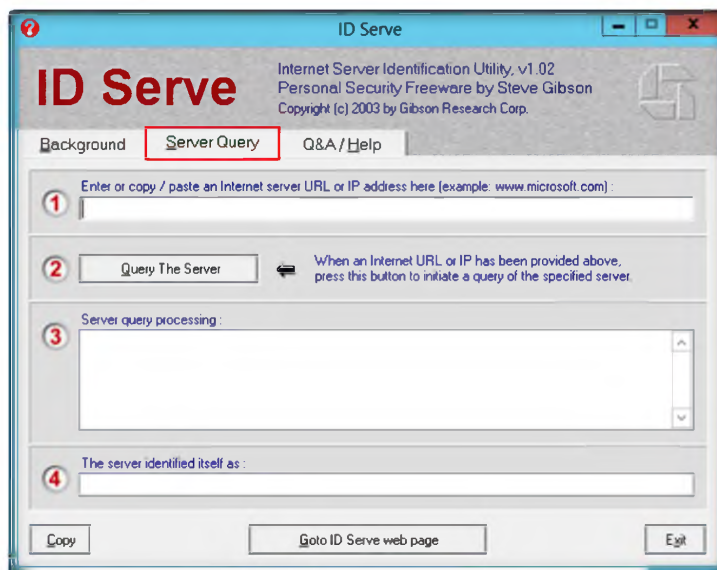


FIGURE 2.1: Welcome screen of ID Serve

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/realhome> (IP address is where the real home site is hosted) in step 1.

Module 12 – Hacking Webservers

- Click **Query the Server** to start querying the entered website.
- 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.

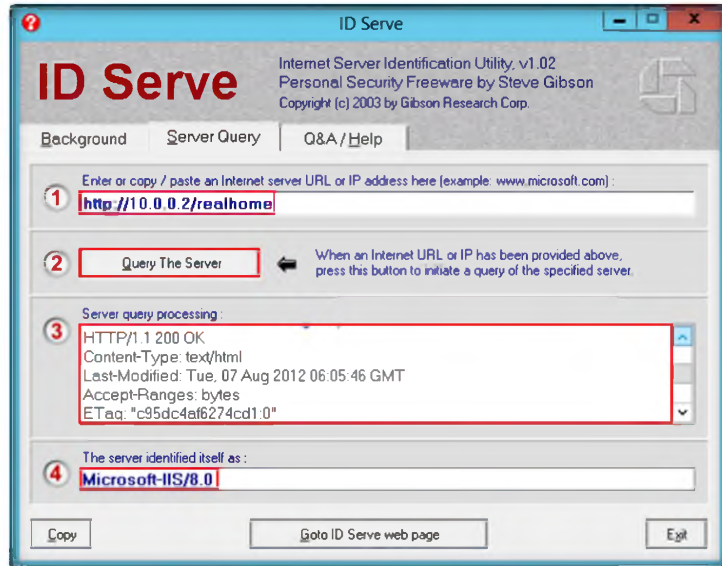


FIGURE 2.2: ID Serve detecting the footprint

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	Server Identified: Microsoft-IIS/8.0
	Server Query Processing: <ul style="list-style-type: none">HTTP/1.1 200 okcontent-Type: text/htmlLast-Modification: Tue, 07 Aug 2012 06:05:46 GMTAccept-Ranges: bytesETag: "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.

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:

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

- **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

TASK 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.

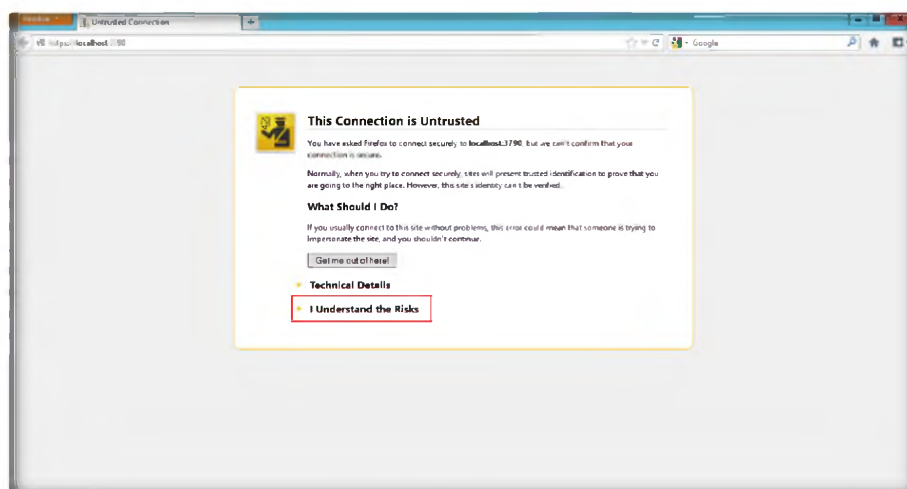


FIGURE 3.1: Metasploit Untrusted connection in web browser

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).

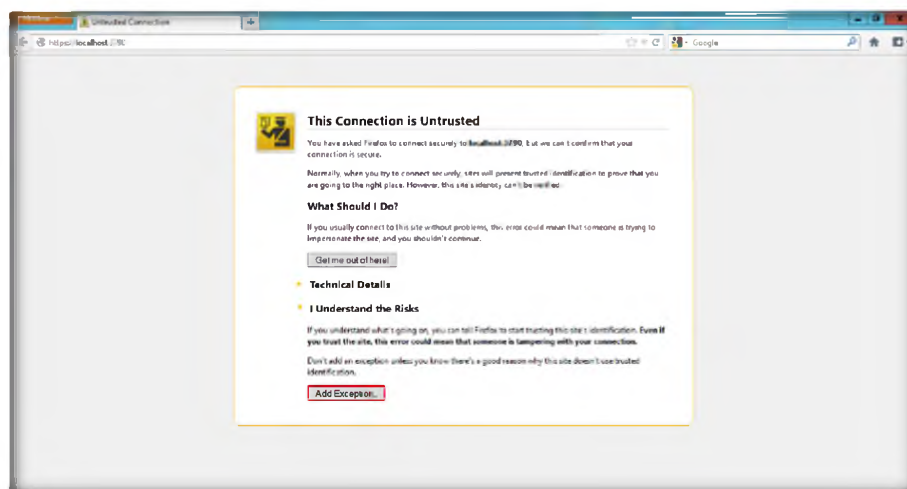


FIGURE 3.2: Metasploit Adding Exceptions

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 `SecurityManager`.

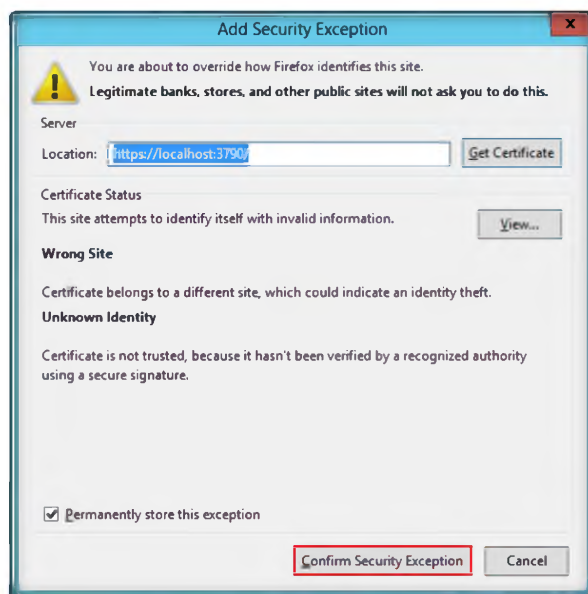


FIGURE 3.3: Metasploit Add Security Exception

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

Once `SecurityManager` 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.

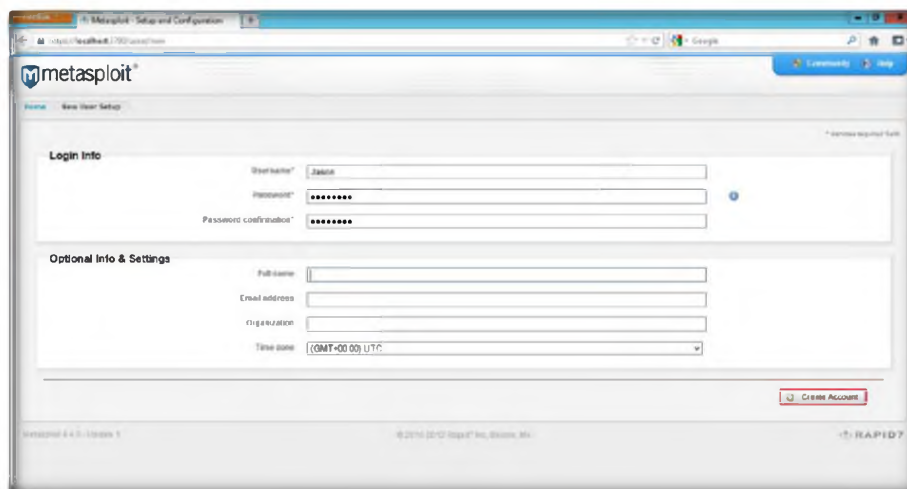


FIGURE 3.4: Metasploit Creating an Account

TASK 2

Product Key Activation

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

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.

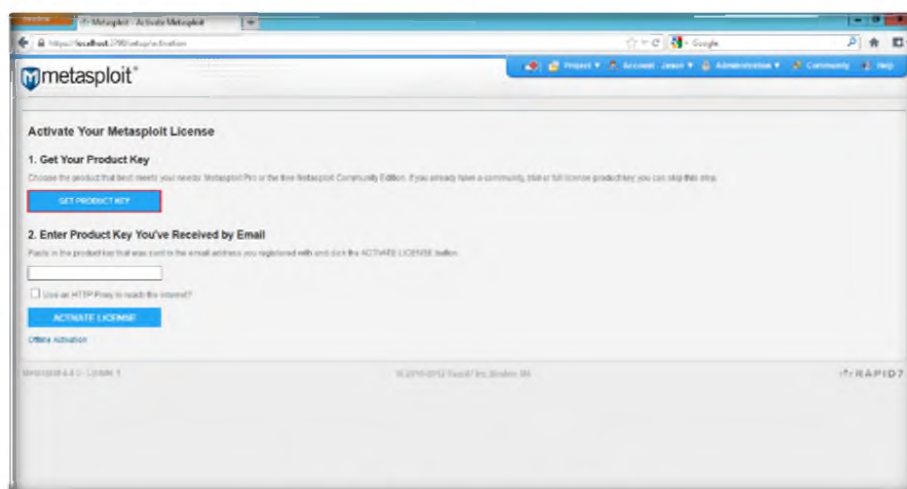


FIGURE 3.5: Metasploit Activating License Key

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

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

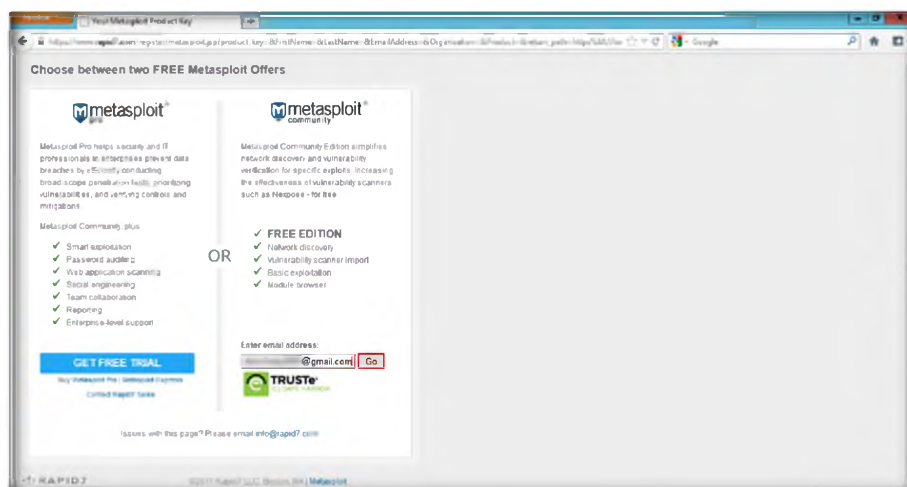


FIGURE 3.6: Metasploit Community version for License Key

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.

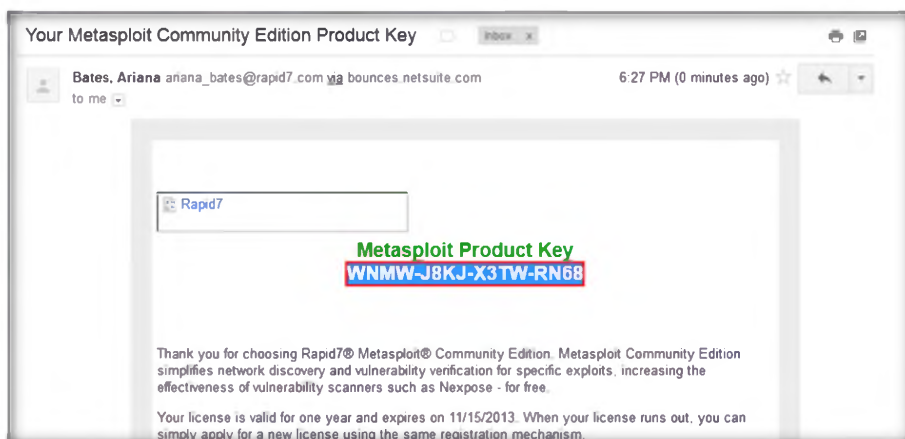


FIGURE 3.7: Metasploit License Key in your email ID provided

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.

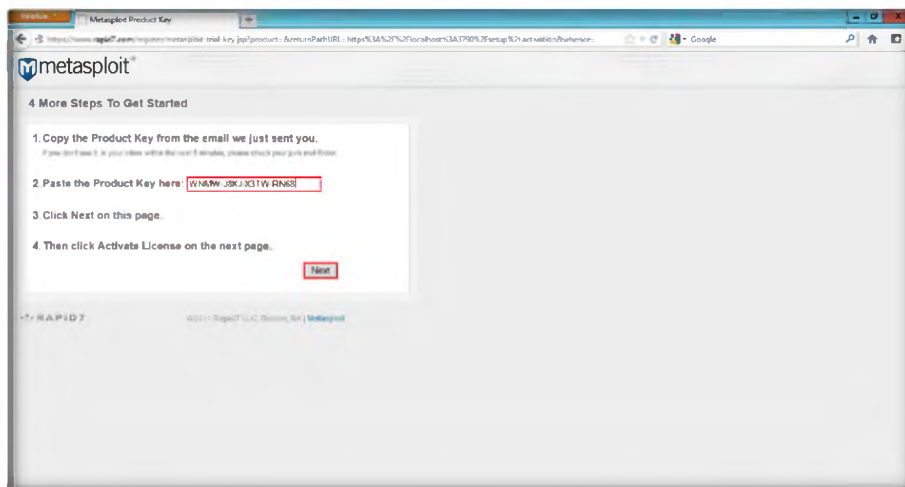


FIGURE 3.8: Metasploit Activating using License Key

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.

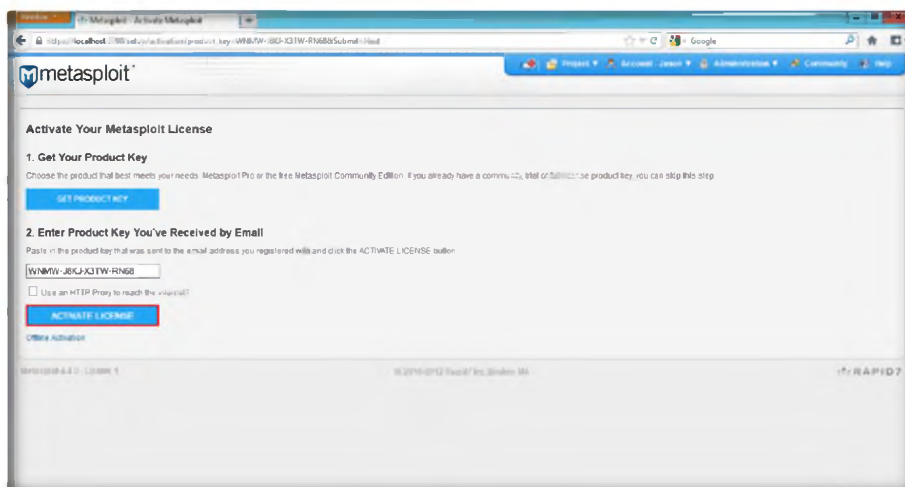


FIGURE 3.9: Metasploit Activation

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.

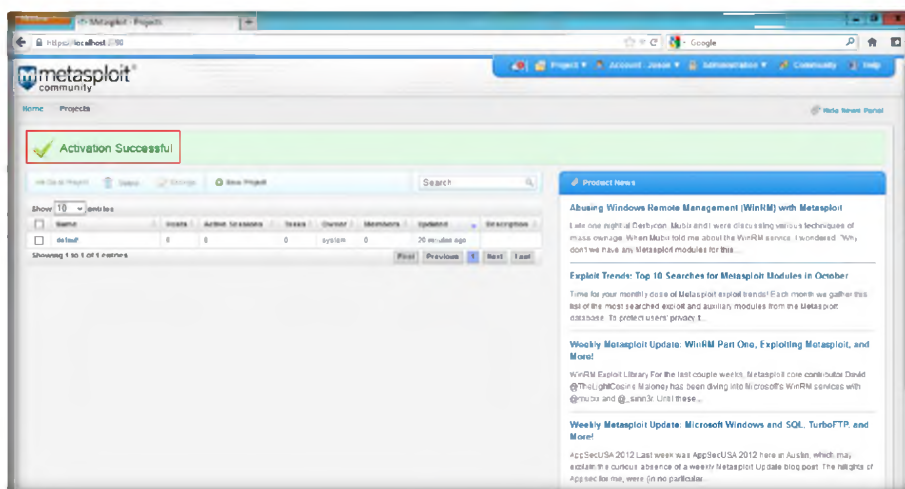


FIGURE 3.10: Metasploit Activation Successful

TASK 3

Updating Metasploit

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

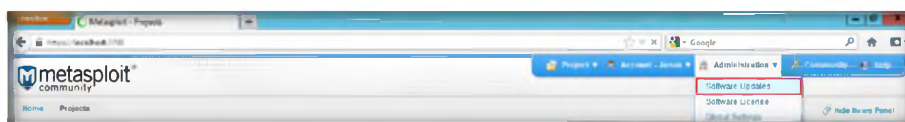


FIGURE 3.11: Metasploit Updating Software

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.)

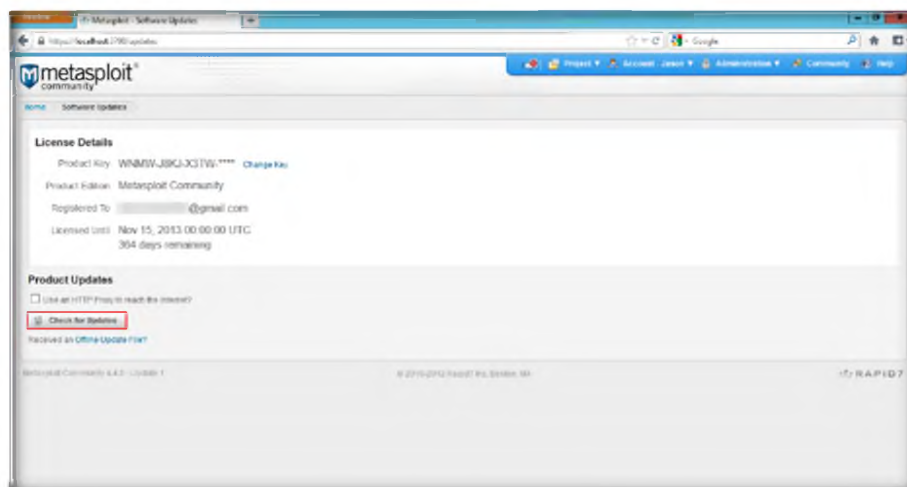


FIGURE 3.12: Metasploit Checking for Updates

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

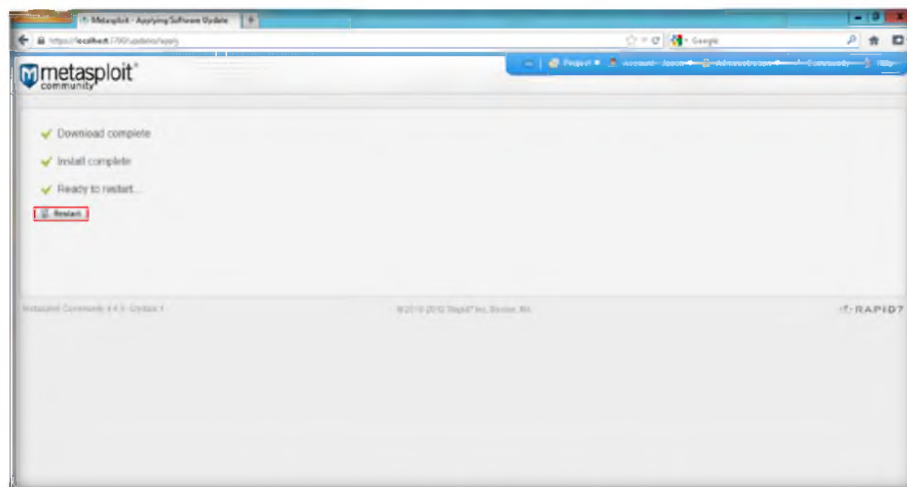


FIGURE 3.13: Metasploit Restarting after installation of updates

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

TCP ports 512, 513, and 514 are known as "r" services, and have been misconfigured to allow remote access from any host (a standard ".rhosts + " 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.

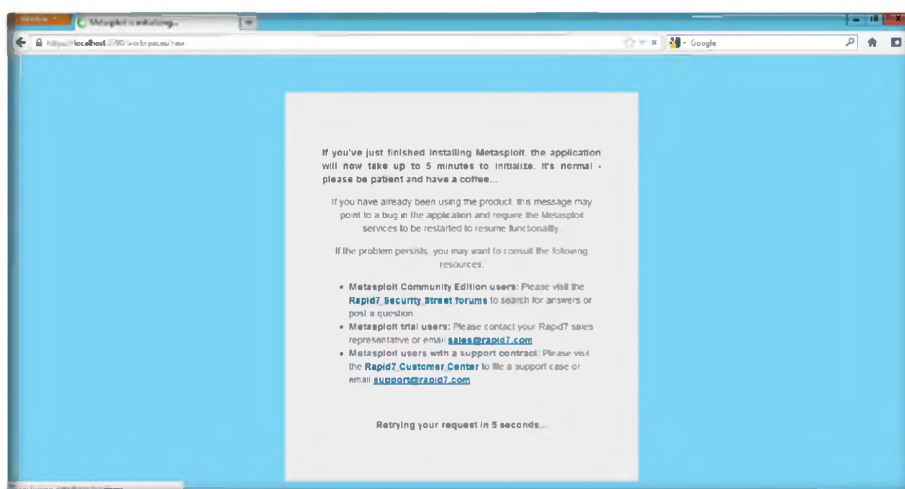


FIGURE 3.14: Metasploit Restarts

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.

17. After completion of restart it will redirect to **Metasploit – Home**. Now click **Create New Project** from the **Project** drop-down list.

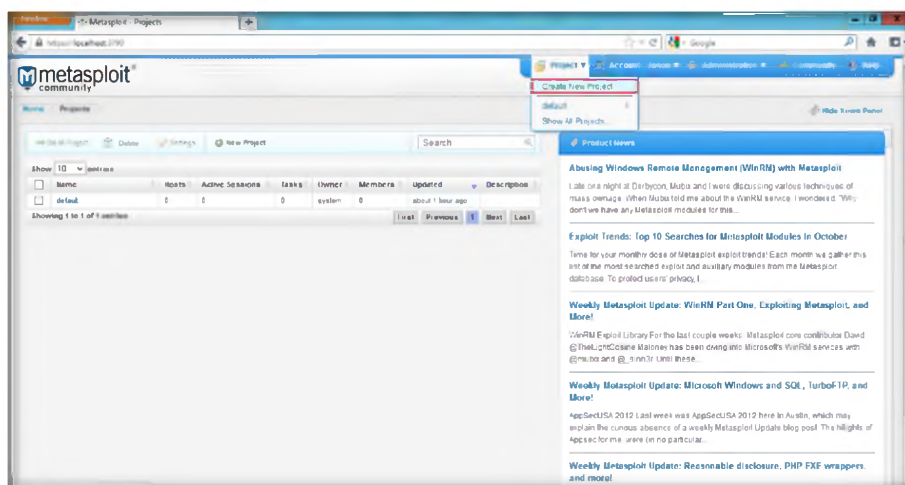


FIGURE 3.15: Metasploit Creating a New Project

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.

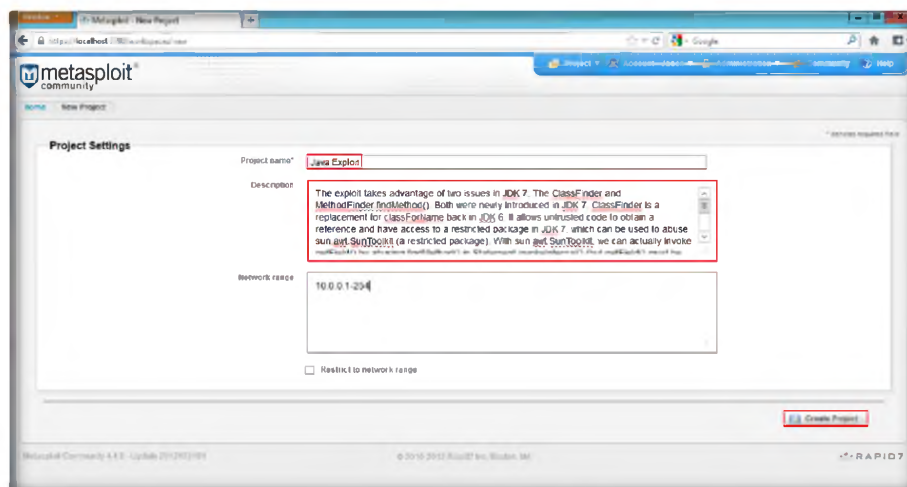


FIGURE 3.16: Metasploit Project Settings

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

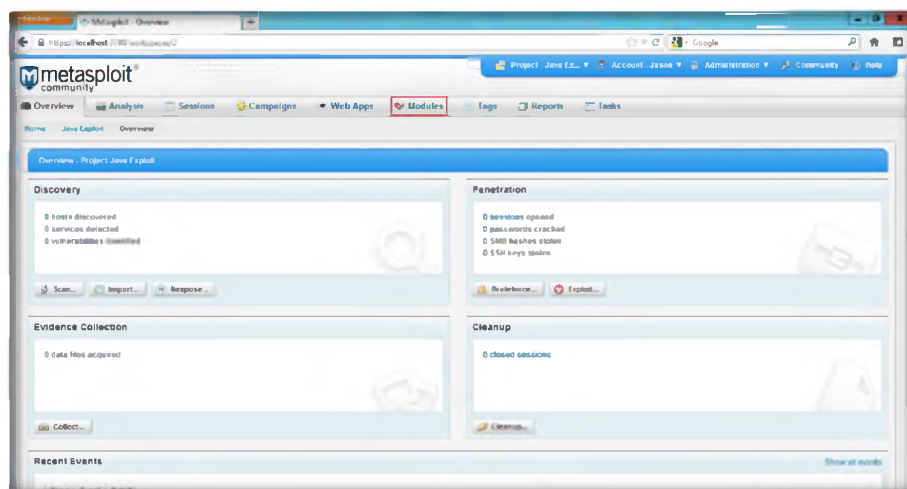


FIGURE 3.17: Metasploit Modules Tab

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.

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.

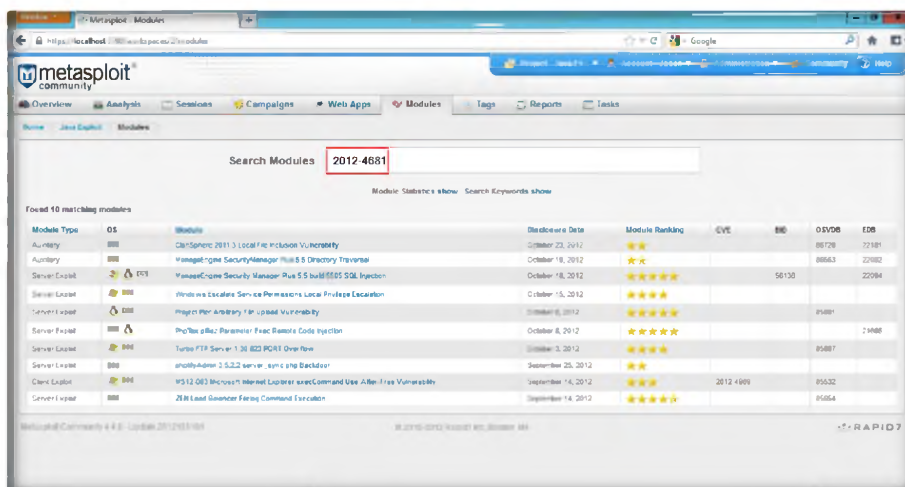


FIGURE 3.18: Metasploit Searching for Java Exploit

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

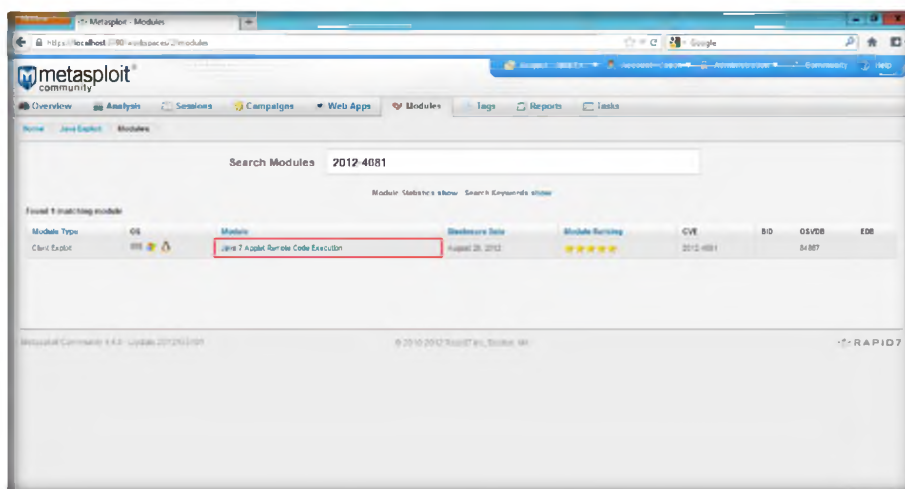


FIGURE 3.19: Metasploit Java 7 Applet Remote Code Execution Exploit found

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**.

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.

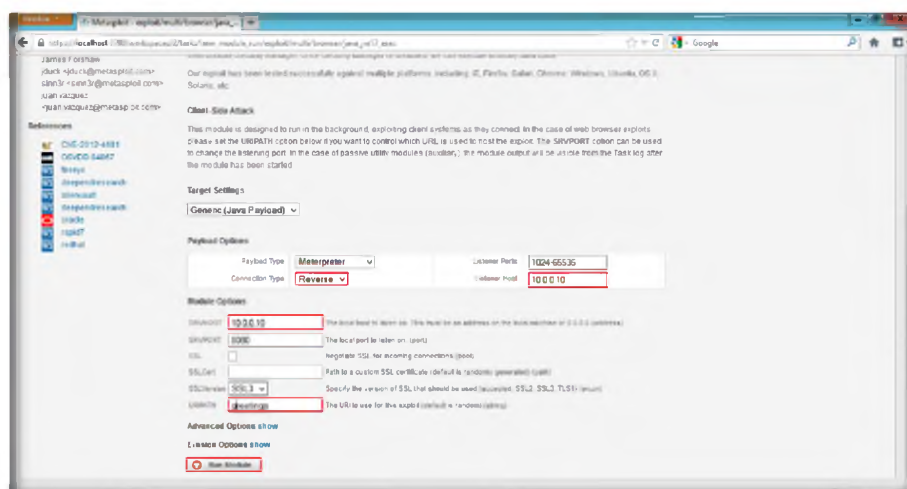


FIGURE 3.20: Metasploit Running Module

23. The task is started as shown in the following screenshot.

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 bruteforce 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.

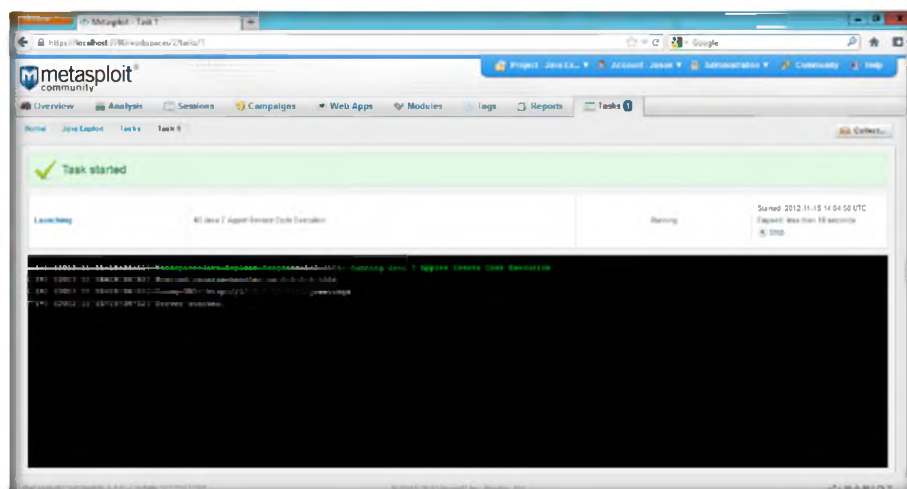


FIGURE 3.21: Metasploit Task Started

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.

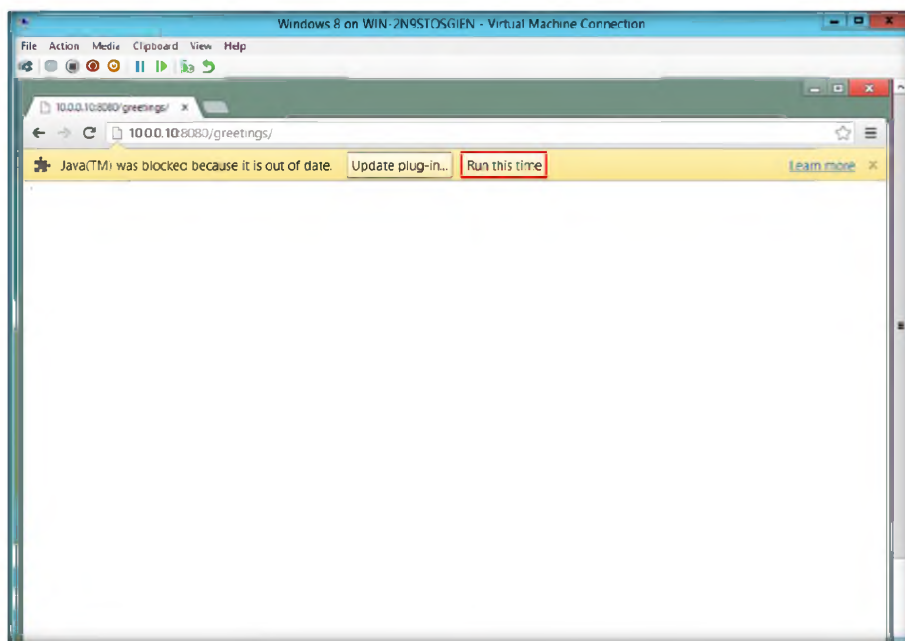


FIGURE 3.22: Windows 8 Virtual Machine – Running the Exploit

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.

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.

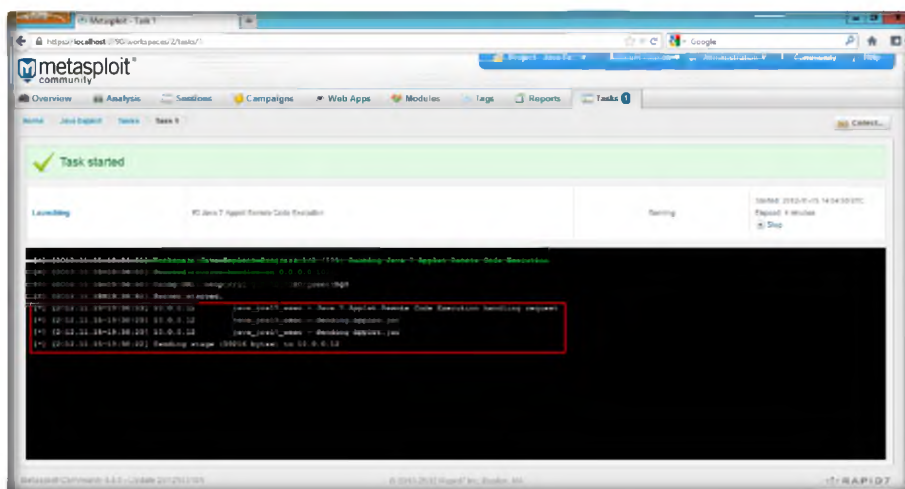


FIGURE 3.23: Metasploit Capturing the reverse connection of targeted machine

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.

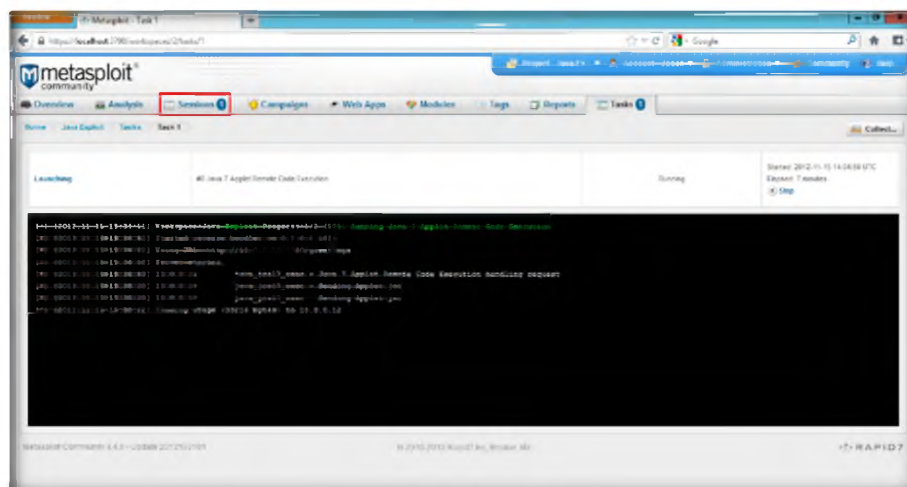


FIGURE 3.24: Metasploit Session tab

28. Click the captured session to view the information of a target machine as shown in the following screenshot.

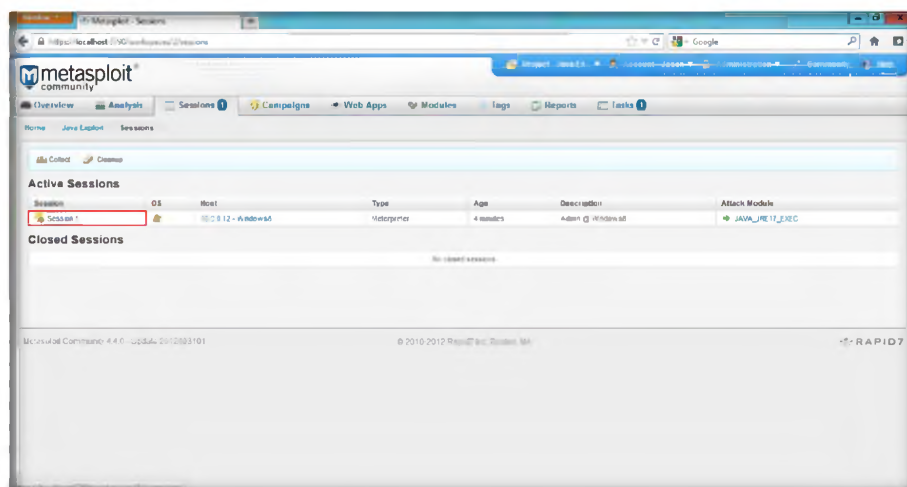


FIGURE 3.25: Metasploit Captured Session of a Target Machine

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.

29. 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.

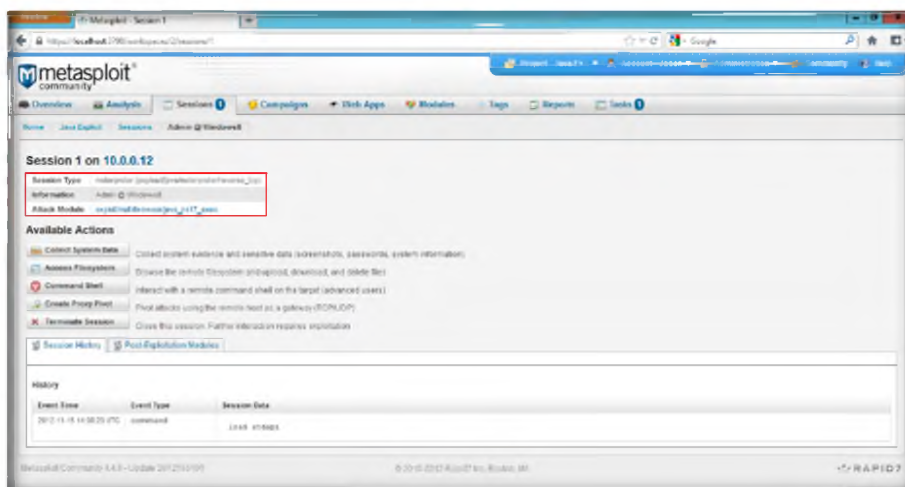


FIGURE 3.26: Metasploit Target Machine System information

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.

30. To access the files of the target system, click **Access Filesystem**.

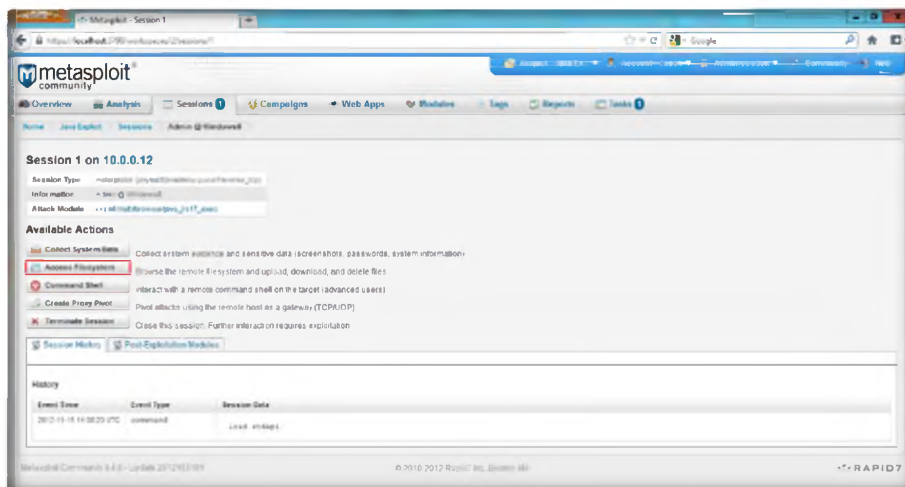


FIGURE 3.27: Metasploit Accessing Filesystem of a Target Machine

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.

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.

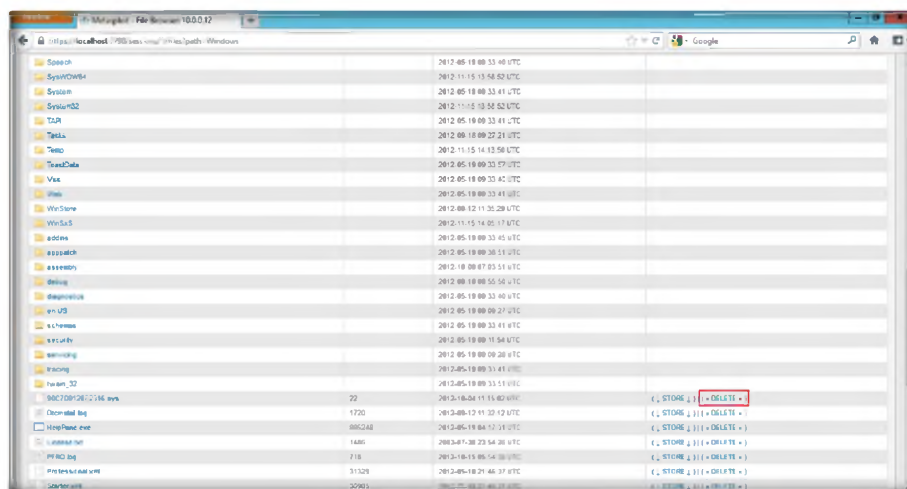


FIGURE 3.28: Metasploit Modifying Filesystem of a Target Machine

32. You can also launch a command shell of the target machine by clicking **Command Shell** from sessions captured.

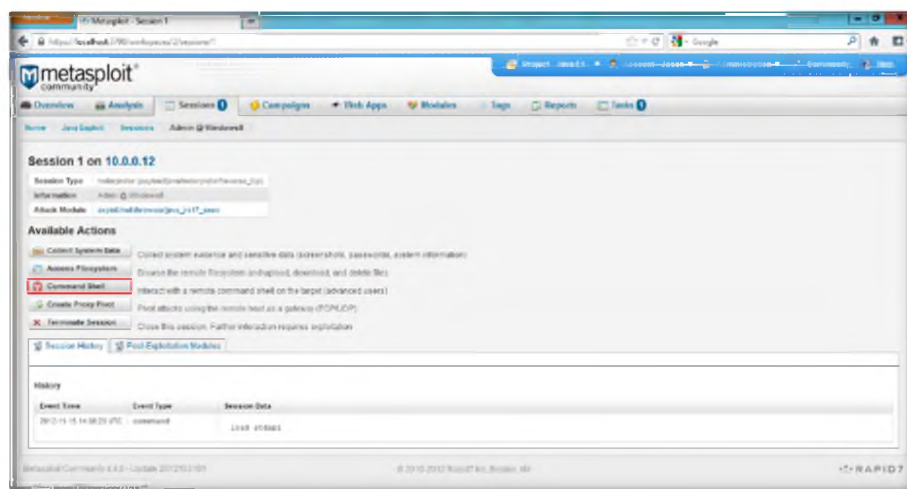


FIGURE 3.29: Metasploit Launching Command Shell of Target Machine

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.

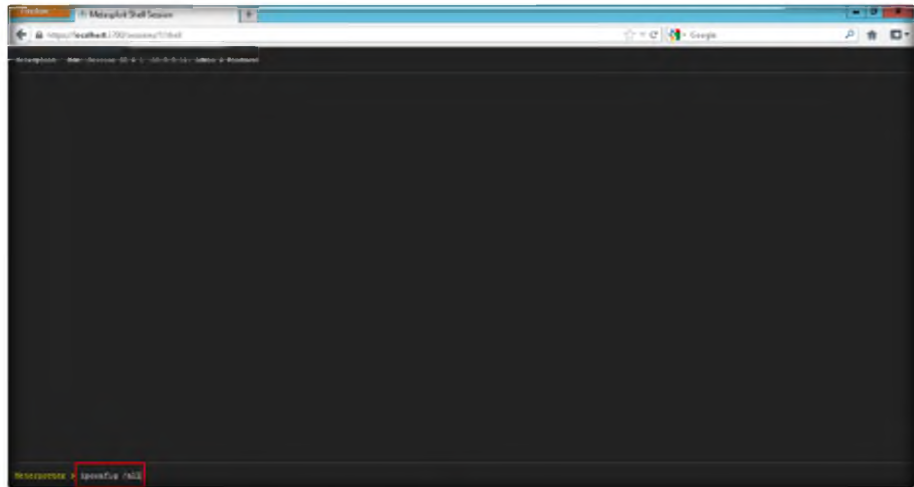


FIGURE 3.30: Metasploit IPCONFIG command for Target Machine

34. The following screenshot shows the IP address and other details of your 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.

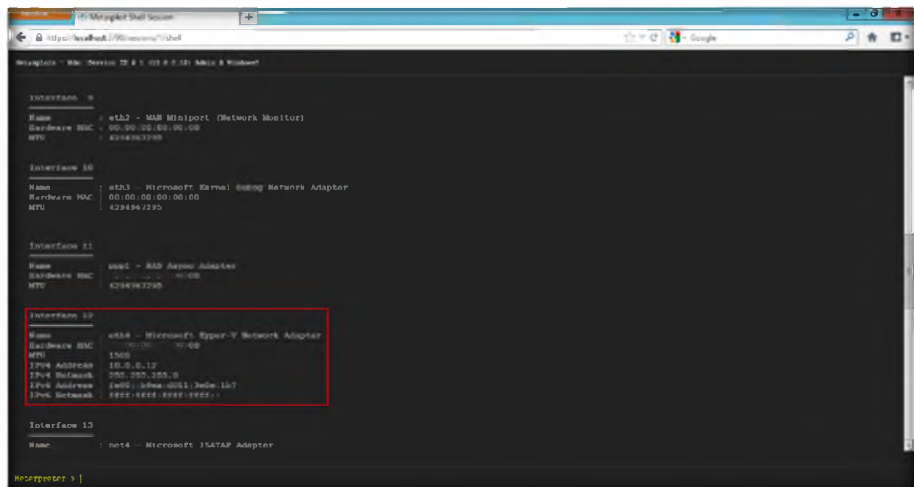


FIGURE 3.31: Metasploit Target Machine IP Address in Metasploit Command Shell

35. Click the **Go back one page** button in Metasploit browser to exit the 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.

Module 12 – Hacking Webservers

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.

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.

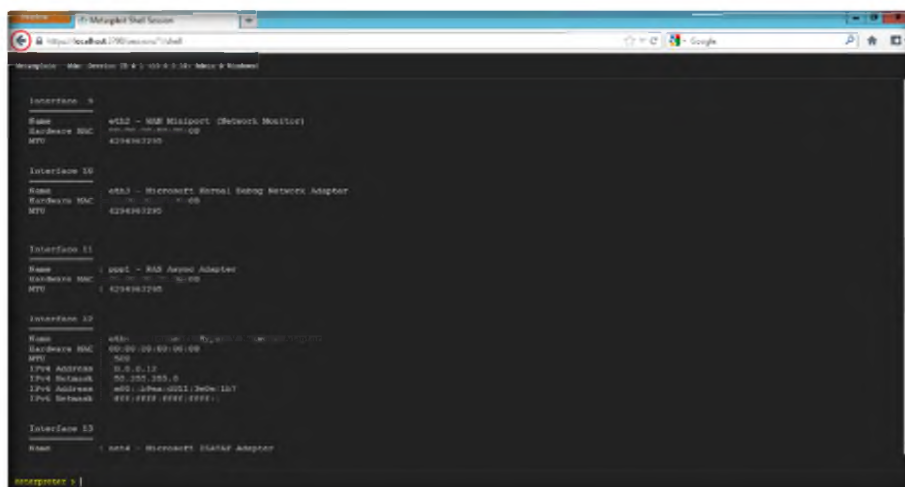


FIGURE 3.32: Metasploit closing command shell

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

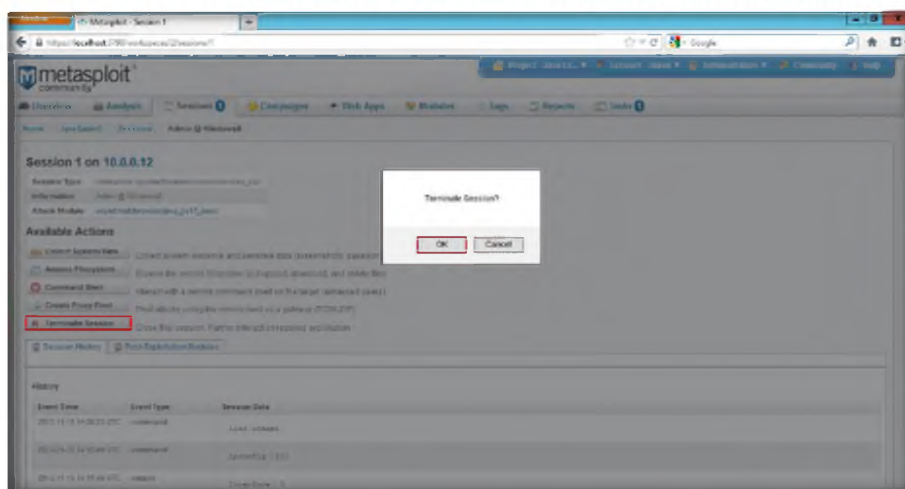


FIGURE 3.33: Metasploit Terminating Session

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.

37. It will display **Session Killed**. Now from the **Account** drop-down list, select **Logout**.

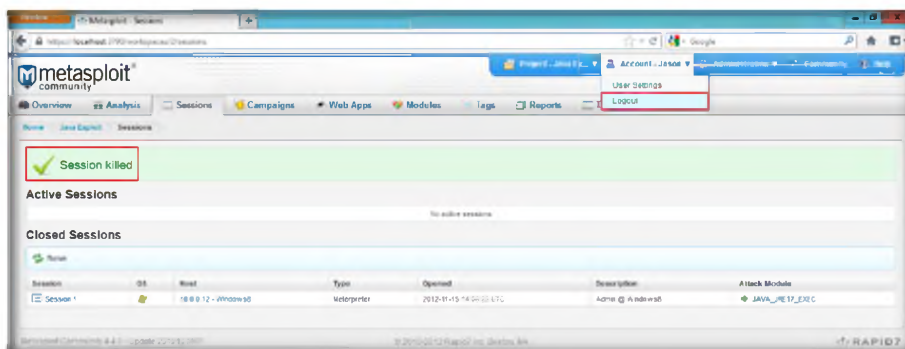


FIGURE 3.34: Metasploit Session Killed and Logging out

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	Output: Interface Information <ul style="list-style-type: none"> Name: eth4-Microsoft Hyepr-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::

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