IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A STUDY OF METASPLOIT TOOL

Yash Arya*, Ashwin Bhalotiya, Chiranjeev Sharma, Vikas Kag, Shubhi Snaghvi
Computer Science & Engineering, Acropolis Institute of Technology & Research, indore, India.

ABSTRACT

In this paper, we will discuss about the framework called Metasploit. The framework consists of tools, required libraries, related components, and required user interfaces. The basic purpose of the framework is a module launcher, users can be 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 that it is targeted and the user can interact with the payload using the shell provided to him. Hundreds of exploits and dozens of payload options are available. It is one of the crucial framework as per the security is concerned.

KEYWORDS: Metasploit framework, Architecture, usage, Terminologies.

INTRODUCTION

Metasploit is an open source framework, which works to provide security to the computers. The basic purpose of this framework is that, it will develop and execute the exploit code against the remote target. Using Metasploit we can take advantage of most of the vulnerabilities that subsist in software. Since in older days, the internet grows at much higher rate, the use of it also increases. Today, internet is becoming the need of every individuals and the use of it and its popularity is increasing day by day. It has change the world in many different phases. Thousands of the sites are running on different domains and maintain thousands of confidential information. To retain the security of those information, required to pay some attention on the tools, so that the data hiding can be done and may able to traverse from source to destination confidentially. We require such tool, because it easily utilized the novice user to perform the regression, penetration testing and also they could able to perform patch verification and develop them.

The Metasploit Framework is a tool that collectively combines exploits into one central location ideally for security researchers. Originally developed using the Perl scripting language Metasploit is now currently on its third reincarnation. Version 1.0 was written solely by H.D. Moore using Perl sporting a curses based front -end. Version 2.0, also written in Perl, and included the help of a few additional developers. For Version 3.0, Metasploit received a complete over haul. Written in the powerful scripting language Ruby, Metasploit 3.0 now boasts the power of automation due to the nature of Ruby's status as an object -oriented language. Additionally, Metasploit is considered multi –platform running on most variations of UNIX and Windows [1].

The Metasploit Framework was developed with the intentions of making security experts ' lives easier. The original primary users were considered to be network security professionals, security administrators, product vendors, and other like minded security researches. Each would use the tool within the guidelines of their own discipline; network security professionals for penetration testing, security administrators for patch installation verification, product vendors for regression testing, and other security researchers for perhaps development of other exploits[1].

METASPLOIT ARCHITECTURE

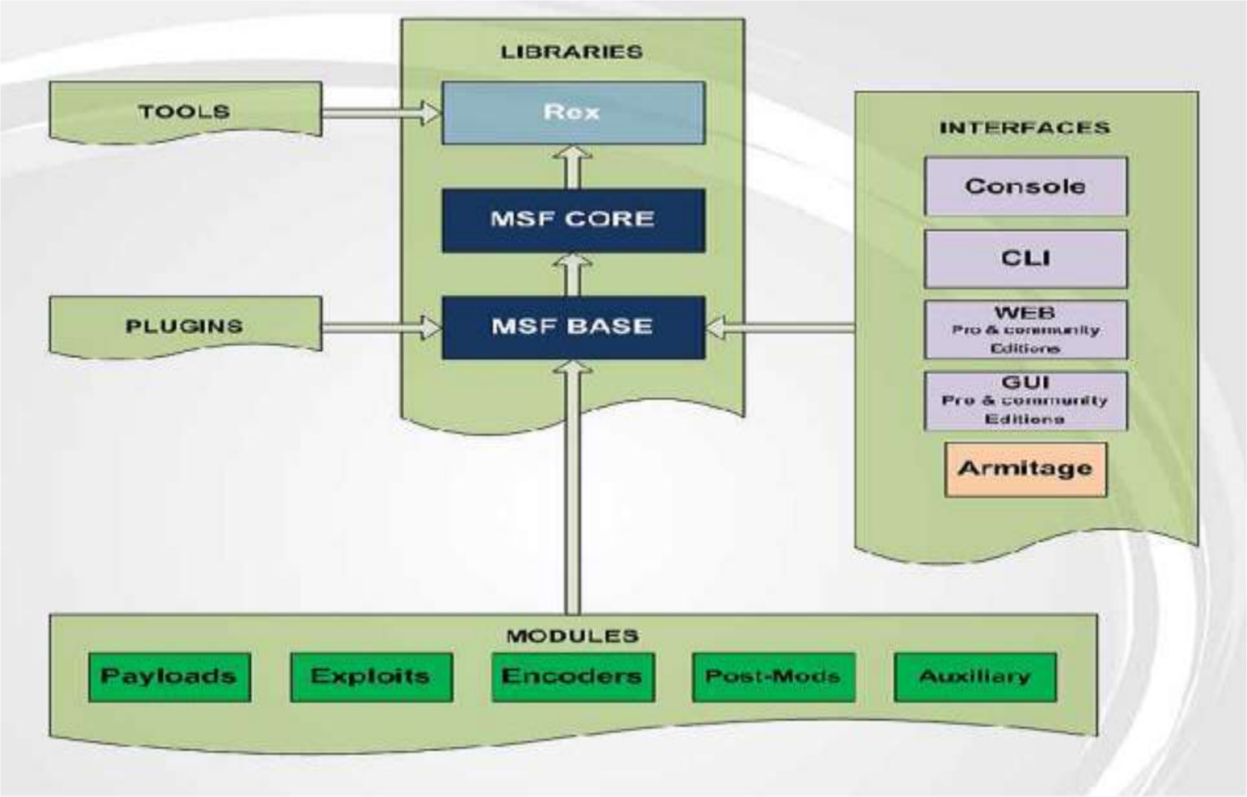

Figure 1: Architecture of Metasploit

Libraries:
1. **Rex:** it is the fundamental library. Most of the task will be perform by this library. It handles the things like sockets and different types of protocols.

2. MSF Core: it provides the application programming interface and also defines the Metasploit framework.

3. MSF Base: for the metasploit framework, this library will provides the It provides the friendly API.
Modules:

Payload: Payload is a piece of code that runs in the target system remotely.

Exploit: Exploit is a piece of software, chunk of data or a sequence of code that takes the advantage of a bug of vulnerability.

Auxiliary modules: This module is used for scanning, fuzzing and doing various tasks.

Encoder: A program which encodes our payloads to avoid anti virus detection.

Interfaces:
Metasploit has different interfaces to ease our tasks. We can do a variety of tasks with these interfaces.

METASPLOIT TERMINOLOGIES

- ✓ **VULNERABILITY/EXPOSURE**:- It is the weakness of the system that allows the attacker to break the truthfulness i.e. integrity of the system. It is one of the concerns of computer security. It may result from weak passwords, software bugs, a computer virus or a script code injection, and a SQL injection.
- ✓ **Exploit:-**is the means by which an attacker/pen tester takes advantage of a flaw within a system (i.e. buffer overflow).
- ✓ **Payload:-**is the code we want the system to execute in the exploit. The MSF allows you to select and deliver various payloads.

USAGE

Now that we come to know the transcript and genesis of Metasploit we can move on to the applications of the product. We will begin to develop the report/ synopsis of some common attacks considering some individual characteristics of the Metasploit Framework. The basic fundamental application of Metasploit is to identify the exploitation applications of remote application. But, it also develops the new ones as well. With the 3.0 iteration of Metasploit, near complete automation is possible in terms of exploiting, scanning, identifying etc.

CONCLUSION

The purpose of this paper was to provide the reader with an understanding of Metasploit such that he/she may use it himself. Metasploit is a powerful tool that like we said time and time again, in the wrong hands can be used for great harm. It provides an abundance of resources for legitimate network security professionals, security administrators, product vendors, and developers to use in a variety of ways. In fact, in its diversity lays the key to its success. However, the only real way to fully understand the intricate design of the Metasploit Framework is to use it. Hopefully, this paper helps others to understand the capabilities of Metasploit and utilize it as a tool for themselves.

REFERENCES

[1] Maynor , D . & Mookhey, K.K. (2007) . Metasploit toolkit for penetration testing, exploit development, and vulnerability assessment [pp. 1-30]. Retrieved from http: / / books.google.com/books?id=bzZG5a1kEw4C&lpg=PA1&ots=36soArIcvd&dq=metasploit&lr&pg=PP1#v=onepage&q&f=false

[2] The Metasploit Project. (2010, October 20).Retrieved from http:/ /www.metasploit.com/

[3] Aharoni, M., Coppola, W., & Kearns, D.(2010, October 15). Metasploit unleashed. Retrieved from http:/ www.offensivesecurity.com/metasploit-unleashed/

[4] Rajani, M.A., Mohamed, A., & Stansbury,H.C. (2006).E-commerce security technologies: an evaluation using them metasploit framework (msf). In formally published manuscript, Computer Science, George Mason University, Fairfax, Virginia. Retrieved from http://www.qatar.cmu.edu/iliano/courses/06S-GMU-ISA767/project/papers/mohamedrajani-stansbury.pdf

[5] Babcock, C. (2008, April 25). In database market, oracle gets bigger, others hang on. Information Week, Retrieved from http://www.informationweek.com/news/software /database_apps/showArticle.jhtml?articleID=207402230

[6] Gates, C., & Ceballos, M. (2009). Oracle penetration testing using the metasploit framework. Proceedings of the BlackHat USA2009, http://www.blackhat.com/presentations /bhusa-09/ GATES/BHUSA09-GatesOracleMetasploit-PAPER.pdf

[7] Silberman, P., & Davis, S. (2009). Metasploit autopsy: reconstructing the scene of the crime. Proceedings of the BlackHat USA 2009, http://www.blackhat.com/presentations/bhusa -09/SILBERMAN/BHUSA09-SilbermanMetasploitAutopsy-PAPER.pdf.