PAPER PRESENTATION SLIDES

SREENIDHI INSTITUTE OF SCIENCE AND TECHNOLOGY

Department of Computer Science and Engineering

Technical paper writing and Seminar on

METASPLOIT

By **B.Shashank 16311A05C6**

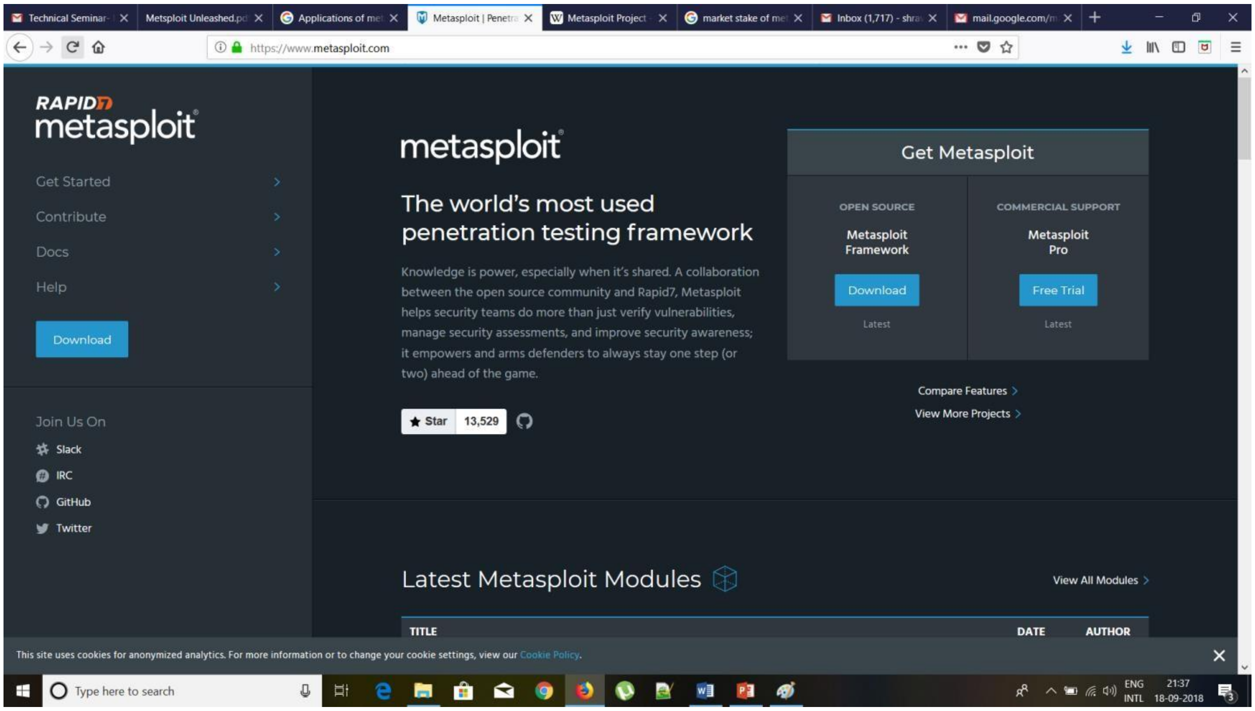
Of

B.Tech CSE IV Year I Semester-**Section E3**

METASPLOIT

INTRODUCTION

- The **Metasploit Tool** is a computer security tool that provides information about security vulnerabilities and aids in penetration testing.
- Its best-known sub-project is the open source **Metasploit Framework**, a tool for developing and executing exploit code against a target machine.
- The Metasploit Project is well known for its tools, some of which are used for penetration testing.



metasploit

The world's most used penetration testing framework

Knowledge is power, especially when it's shared. A collaboration between the open source community and Rapid7, Metasploit helps security teams do more than just verify vulnerabilities, manage security assessments, and improve security awareness; it empowers and arms defenders to always stay one step (or two) ahead of the game.

Get Metasploit

OPEN SOURCE	COMMERCIAL SUPPORT
Metasploit Framework	Metasploit Pro
Download	Free Trial
Latest	Latest

Compare Features >

View More Projects >

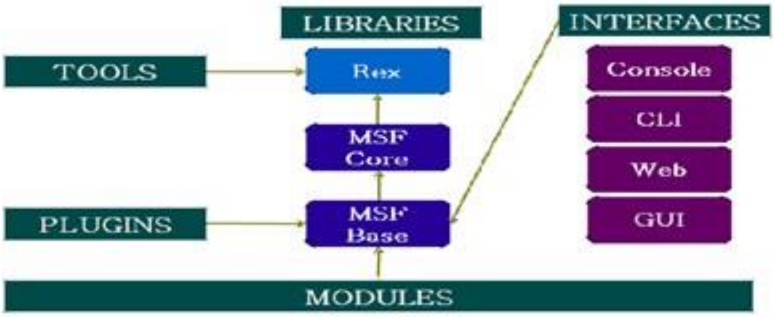
Latest Metasploit Modules

View All Modules >

TITLE	DATE	AUTHOR

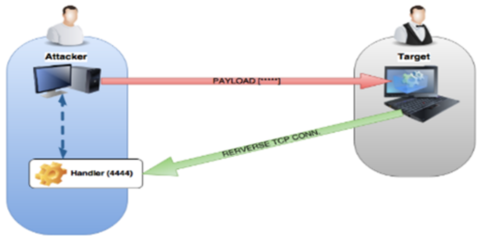
This site uses cookies for anonymized analytics. For more information or to change your cookie settings, view our Cookie Policy.

ARCHITECTURE

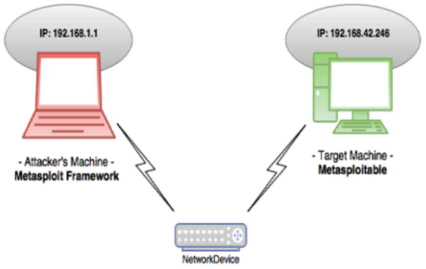


WORKING

Creating Payload -



Demo Setup -



PREREQUISITES

- Some of the hardware Prerequisites that should be considered are
  - Hard Drive Space: The recommended amount of space needed is 40 gigabytes.
  - Processors Capabilities: Faster Processor(500MHz recommended).
  - RAM: 1GB or more.
- It is highly recommended that you set up a virtual machine using a product such as VirtualBox, VirtualPC, or the free VMware Server.
- We will also perform an installation of Microsoft's free SQL Server 2005 Express.
- This will allow us to use some of the different SQL modules in Metasploit.

APPLICATIONS

1. Information Gathering

- The foundation for any successful penetration test is solid information gathering.
- Failure to perform proper information gathering will have you flailing around at random, attacking machines that are not vulnerable and missing others that are.
- Some of the features within the Metasploit framework that can assist with the information gathering effort.

- *Port Scanning*
- *Scanning*
- *Password Sniffing*
- *Creating Your Own TCP Scanner*

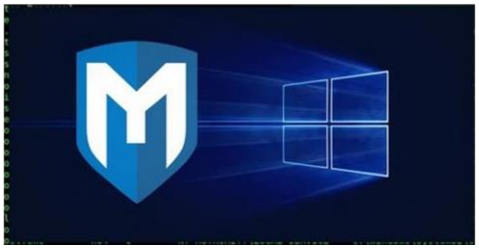
12

APPLICATIONS

2. Vulnerability Scanning

- Vulnerability scanning will allow you to quickly scan a target IP range looking for known vulnerabilities
- Some of the vulnerability scanning capabilities that the Metasploit Framework can provide.

- *Login Check*
- *Authentication*
- *Web Scanner*



13

CONCLUSION

- Metasploit is a powerful tool and it is one of those classics that you should always have in your toolbox.
- One of Metasploit’s biggest issues for Metasploit tool is that it is not multithreaded, but this is fixed in Metasploit Pro.
- It is best suitable for peoples from security domain.
- As it is an open source, It provides access to all exploit classes and methods.

References

1 Metasploit-Beginners-threat-free-best-class/dp/1788295978/httpwwwtuto0a-20

2 Metasploit-Penetration-Testers-David-Kennedy/dp/159327288X/httpwwwtuto0a-20

3 Mastering-Metasploit-Second-Nipun-Jaswal/dp/1786463164/httpwwwtuto0a-20

4 Metasploit-Penetration-Testing-Cookbook-Second/dp/1782166785/httpwwwtuto0a-20 [5]Mastering-

Nexpose-Metasploit-Lab-Based-Approach/dp/0128010444/httpwwwtuto0a-20

6 "Kali Linux Tools Listing | Penetration Testing Tools"

7 http://sectools.org/sploits.html

8 "Armitage vs Cobalt Hooked Strike"

[9]M. Abadi, A. Agarwal, P. Barham, E. Brevdo, Z. Chen, C. Citro, G. S. Corrado,A. Davis, J. Dean, M. Devin, et al. Tensorflow: Large-scale machine learning on heterogeneous distributed systems. arXiv preprint arXiv:1603.04467, 2016

[10]A. J. Aviv, B. Sapp, M. Blaze, and J. M. Smith. Practicality of accelerometer sidechannels on smartphones. In Proceedings of the 28th Annual Computer Security Applications Conference, pages 41–

50. ACM, Orlando, 2012

[11]Bergadano F, Gunetti D, Picardi C (2002). User authentication through keystroke dynamics. ACM Transactions on Information and System Security

(TISSEC), 5(4):367–397.

[12]L. Cai and H. Chen. On the practicality of motion based keystroke inference attack. In International Conference on Trust and Trustworthy Computing, pages 273–290. Springer, Vienna, 2012

13 Clarke NL, Furnell SM, Lines BM, Reynolds PL (2003). Keystroke dynamics on a mobile handset: a feasibility study. Inf Manag Comput Secur 11(4):161–166

14 Giuffrida C, Majdanik K, Conti M, Bos H (2014, July). I sensed it was you: authenticating mobile users with sensor-enhanced keystroke dynamics. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 92–111). Springer, Cham

15 Huang X, Lund G, Sapeluk A (2012). Development of a typing behaviour recognition mechanism on android. In IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) (pp. 1342-1347). IEEE

[16]P. Kang, S.-s. Hwang, and S. Cho. Continual retraining of keystroke dynamicsbased authenticator. In International Conference on Biometrics, pages 1203–1211. Springer, Seoul, 2007

[17]Killourhy K, Maxion R (2010) Why did my detector do that?!. In International Workshop on Recent Advances in Intrusion Detection (pp. 256-276). Springer, Berlin, Heidelberg.

[18]X. Liu, Z. Zhou, W. Diao, Z. Li, and K. Zhang. When good becomes evil: Keystrokeinference with smartwatch. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pages 1273–1285. ACM,
Denver, 2015

19 "Month of Kernel Bugs – Broadcom Wireless Driver Probe Response SSID Overflow

20 https://subscription.packtpub.com/book/networking_and_servers/9781788990615/6/ch06lvl1sec39/generating-manual-reports