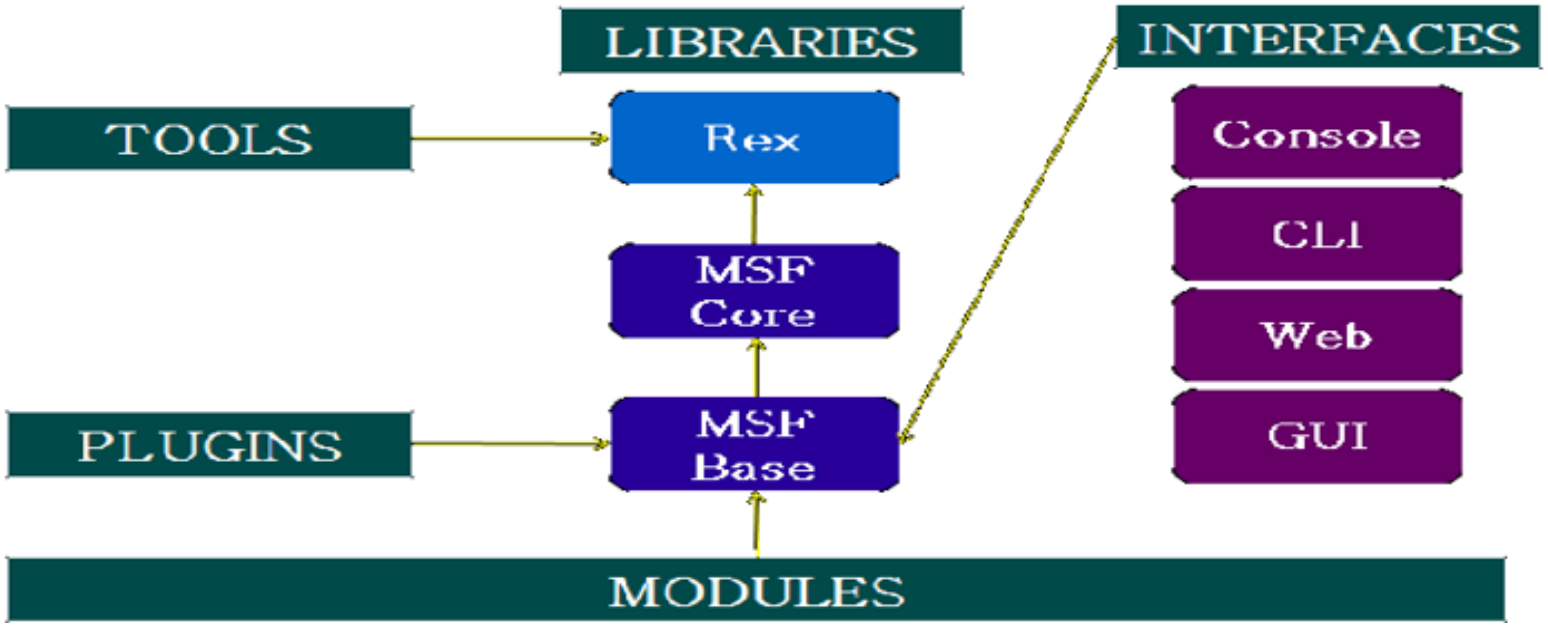
# METASPLOIT

presented by
B Shashank
CSE-E3
16311A05C6

# 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.

# ARCHITECTURE



# WORKING OF METASPLOIT

The basic steps for exploiting a system using the Tool include:

- Choosing and configuring an *exploit.*
- Optionally checking whether the intended target system is susceptible to the chosen exploit;
- Choosing,creating and configuring a *payload*
- Choosing the encoding technique so that the intrusion-prevention system (IPS) ignores the encoded payload;
- Executing the exploit.

# 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.
- 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.

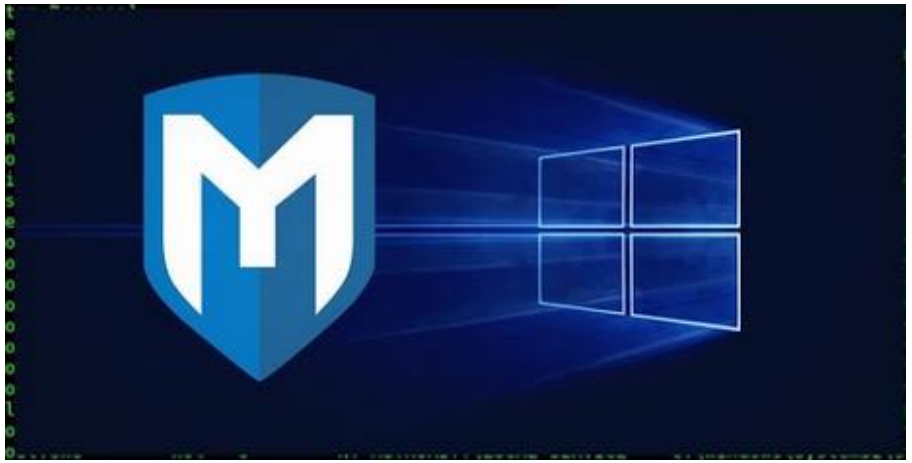
  - *Port Scanning*
  - *Scanning*
  - *Password Sniffing*

# 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*



# FUTURE PROSPECTS OF METASPLOIT

- With the Metasploit 3.5.0 release , Metasploit is going to head first into web application security.
- Most of it's development work is focused on the web application testing capabilities of Metasploit
- Users are still investing resources into exploit coverage for a Metasploit Platform.
- The presence of Rapid7 behind the Metasploit Project has dramatically increased the acceptance of this tool within corporate environments.

# MARKET STAKE OF METASPLOIT

- Metasploit's self-proclaimed quest is to help IT pros verify the security of the software they buy or write.

- Since Metasploit is open source, it's hard to tell how many people use it. A rough estimate that 90,000 this year--by tracking the unique IP addresses of people who've downloaded the latest version.

# 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.


Thank
you