


**Live Cyber Attack Lab**  Watch our IR team detect & respond to a rogue insider trying to steal data! Choose a Session ►

[SUPPORT](#)[COMMUNITY](#)[SERVICES](#)

1-877-292-8767

[SEARCH](#)

# What is Metasploit? The Beginner's Guide

DATA SECURITY

[Inside Out Security Blog](#) » [Data Security](#) » [What is Metasploit? The Beginner's Guide](#)



This site uses cookies to provide you with a better browsing experience. Further information may be found in the [Varonis Site Privacy Policy](#)

Penetration testing allows you to answer the question, “How can someone with malicious intent mess with my network?” Using pen-testing tools, white hats and DevSec professionals are able to **probe networks and applications for flaws and vulnerabilities** at any point along the production and deployment process by hacking the system.

One such **penetration testing** aid is the Metasploit Project. This Ruby-based open-source framework allows testing via command line alterations or GUI. It can also be extended through coding to act as an add-on that supports multiple languages.

## Get the Free Pen Testing Active Directory Environments EBook

First Name\*

Last Name\*

Email\*

☐ I agree to receive communications from Varonis.\*

You can unsubscribe from these communications at any time. For more information on our privacy practices, and how we're committed to protecting your information, please review our [privacy policy](#).

[Download Now](#)

*“This really opened my eyes to AD security in a way defensive work never did.”*



This site uses cookies to provide you with a better browsing experience. Further information may be found in the [Varonis Site Privacy Policy](#)

# What is the Metasploit Framework and How is it Used?

The Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers. Because it's an open-source framework, it can be easily customized and used with most operating systems.

With Metasploit, the **pen testing team** can use ready-made or custom code and introduce it into a network to probe for weak spots. As another flavor of **threat hunting**, once flaws are identified and documented, the information can be used to address systemic weaknesses and prioritize solutions.

## A Brief History of Metasploit

The Metasploit Project was undertaken in 2003 by H.D. Moore for use as a Perl-based portable network tool, with assistance from core developer Matt Miller. It was fully converted to Ruby by 2007, and the license was acquired by Rapid7 in 2009, where it remains as part of the Boston-based company's repertoire of IDS signature development and targeted remote exploit, fuzzing, anti-forensic, and evasion tools.

Portions of these other tools reside within the Metasploit framework, which is built into the Kali Linux OS. Rapid7 has also developed two proprietary OpenCore tools, Metasploit Pro, Metasploit Express.

This framework has become the go-to exploit development and mitigation tool. Prior to Metasploit, pen testers had to perform all probes manually by using a variety of tools that may or may not have supported the platform they were testing, writing their own code by hand, and introducing it onto networks manually. Remote testing was virtually unheard of, and that limited a security specialist's reach to the local area and companies spending a fortune on in-house IT or security consultants.

## Who Uses Metasploit?

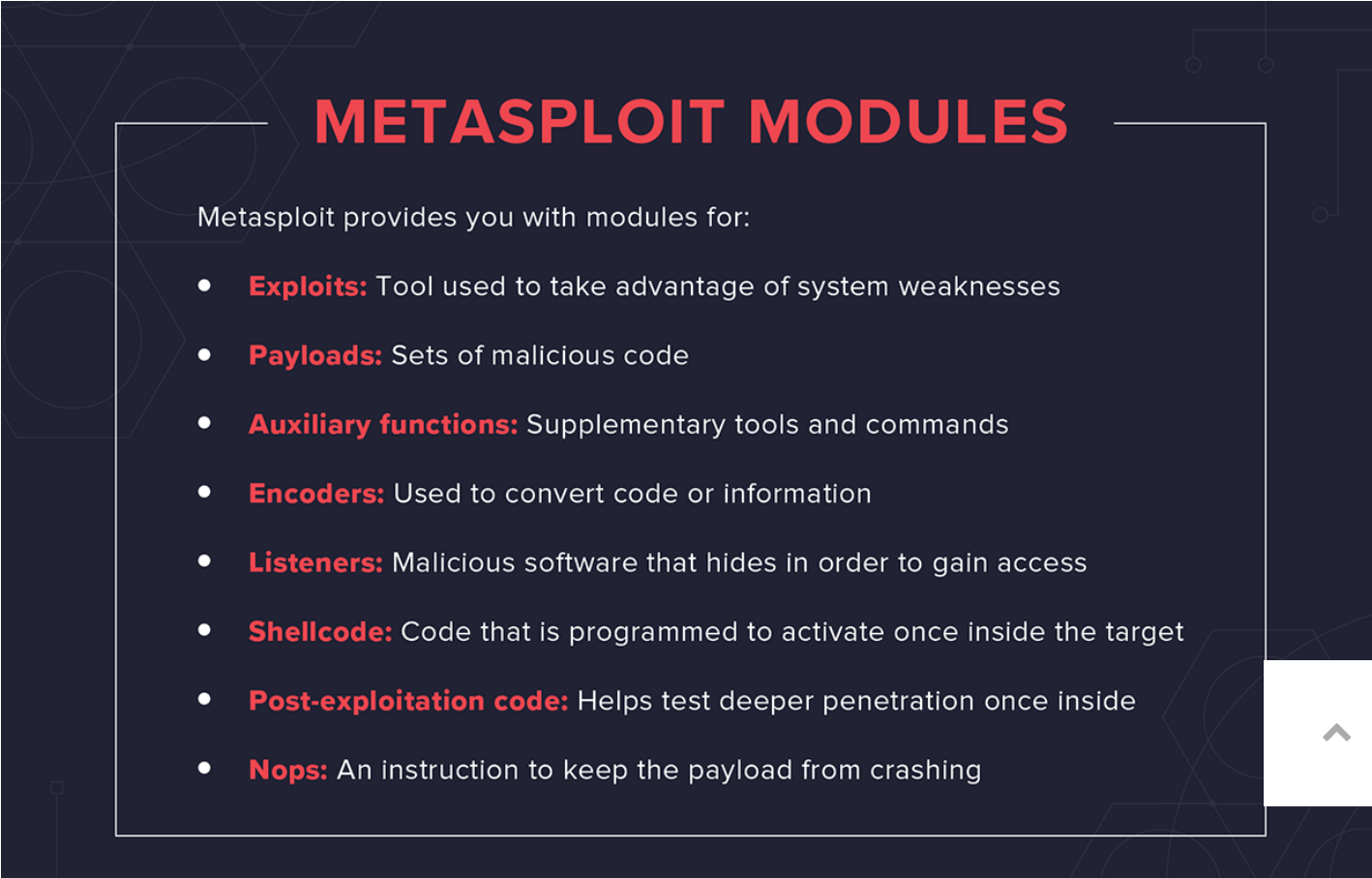
Due to its wide range of applications and open-source availability, Metasploit is used by everyone in the evolving field of **DevSecOps pros to hackers**. It's helpful to anyone who needs an easy to install, reliable tool that gets the job done regardless of which platform or language is used. The software is

This site uses cookies to provide you with a better browsing experience. Further information may be found in the [Varonis Site Privacy Policy](#)

Metasploit now includes more than 1677 exploits organized over 25 platforms, including Android, PHP, Python, Java, Cisco, and more. The framework also carries nearly 500 payloads, some of which include:

- Command shell payloads that enable users to run scripts or random commands against a host
- Dynamic payloads that allow testers to generate unique payloads to evade antivirus software
- Meterpreter payloads that allow users to commandeer device monitors using VMC and to take over sessions or upload and download files
- Static payloads that enable port forwarding and communications between networks

## Metasploit Uses and Benefits

An infographic titled "METASPLOIT MODULES" in large red capital letters. Below the title, it states "Metasploit provides you with modules for:" followed by a bulleted list of eight module types, each with a red header and a description. The background is dark blue with faint geometric patterns. A white upward-pointing arrow is in the bottom right corner of the infographic area.

### METASPLOIT MODULES

Metasploit provides you with modules for:

- **Exploits:** Tool used to take advantage of system weaknesses
- **Payloads:** Sets of malicious code
- **Auxiliary functions:** Supplementary tools and commands
- **Encoders:** Used to convert code or information
- **Listeners:** Malicious software that hides in order to gain access
- **Shellcode:** Code that is programmed to activate once inside the target
- **Post-exploitation code:** Helps test deeper penetration once inside
- **Nops:** An instruction to keep the payload from crashing

This site uses cookies to provide you with a better browsing experience. Further information may be found in the [Varonis Site Privacy Policy](#)

All you need to use Metasploit once it's installed is to obtain information about the target either through port scanning, OS fingerprinting or using a vulnerability scanner to find a way into the network. Then, it's just a simple matter of selecting an exploit and your payload. In this context, an exploit is a means of identifying a weakness in your choice of increasingly **harder to defend networks** or system and taking advantage of that flaw to gain entry.

The framework is constructed of various models and interfaces, which include **msfconsole** interactive curses, **msfcli** to alls msf functions from the terminal/cmd, the Armitag graphical Java tool that's used to integrate with MSF, and the Metasploit Community Web Interface that supports remote pen testing.

White hat testers trying to locate or learn from black hats and hackers should be aware that they don't typically roll out an announcement that they're Metasploiting. This secretive bunch likes to operate through virtual private network tunnels to **mask their IP address**, and many use a dedicated VPS as well to avoid interruptions **that commonly plague many shared hosting providers**. These two privacy tools are also a good idea for white hats who intend to step into the world of exploits and pen testing with Metasploit.

As mentioned above, Metasploit provides you with exploits, payloads, auxiliary functions, encoders, listeners, shellcode, post-exploitation code and nops.

You can obtain a Metasploit Pro Specialist Certification online to become a credentialed pen-tester. The passing score to obtain the certification is 80 percent, and the open book exam takes about two hours. It costs \$195, and you can print your certificate out once you're approved.

Prior to the exam, it's recommended that you take the **Metasploit training course** and have proficiency or working knowledge:

- Windows and Linux OS
- Network protocols
- Vulnerability management systems
- Basic pen testing concepts



Obtaining this credential is a desirable achievement for anyone who wants to become a marke pen-tester or security analyst.

This site uses cookies to provide you with a better browsing experience. Further information may be found in the [Varonis Site Privacy Policy](#)

Metasploit is available through open-source installers directly from the Rapid7 website. In addition to the latest version of the Chrome, Firefox, or Explorer browsers, the minimum system requirements are:

### Operating Systems:

- Ubuntu Linux 14.04 or 16.04 LTS **(recommended)**
- Windows Server 2008 or 2012 R2
- Windows 7 SP1+, 8.1, or 10
- Red Hat Enterprise Linux Server 5.10, 6.5, 7.1, or later

### Hardware:

- 2 GHz+ processor
- Minimum 4 GB RAM, but 8 GB is recommended
- Minimum 1 GB disk space, but 50 GB is recommended

You'll have to disable any antivirus software and firewalls installed on your device before you begin, and get administrative privileges. The installer is a self-contained unit that's configured for you when you install the framework. You also have the option of manual installation if you want to configure custom dependencies. Users with the Kali Linux version already have the Metasploit Pro version pre-bundled with their OS. Windows users will go through the install shield wizard.

After installation, upon startup, you'll be faced with these choices:

- Creating database at /Users/joesmith/.msf4/db
- Starting Postgresql
- Creating database users
- Creating an initial database schema



## Learning How to Use Metasploit: Tutorial +

This site uses cookies to provide you with a better browsing experience. Further information may be found in the [Varonis Site Privacy Policy](#)

The ease of learning to use Metasploit depends on your [knowledge of Ruby](#). However, if you have a familiarity with other scripting and programming languages like Python, making the jump to working with Metasploit shouldn't be too difficult to get up to speed. Otherwise, it's an intuitive language that's easy to learn with practice.

Because this tool requires you to disable your own systematic protections and enables the generation of malicious code, you should be aware of the [potential risks involved](#). If possible, keep this utility installed on a separate system than your personal device or any computer that contains potentially sensitive information or access to such information. You should use a dedicated work device when pen-testing with Metasploit.

## Reasons to Learn Metasploit

This framework bundle is a must-have for anyone who is a security analyst or pen-tester. It's an essential tool for discovering hidden vulnerabilities using a variety of tools and utilities. Metasploit allows you to enter the mind of a hacker and use the same methods for probing and infiltrating networks and servers.

**Here's a diagram of a typical Metasploit architecture:**



This site uses cookies to provide you with a better browsing experience. Further information may be found in the [Varonis Site Privacy Policy](#)

# Metasploit Step-by-Step

We'll begin a brief tutorial of an easy exploit by assuming that you have the basic system and OS requirements. In order to set up a testing environment, you're going to need to download and install [Virtualbox](#), [Kali](#), and [Metasploitable](#) to create a virtualized hacking machine. You can download and install Windows XP or above in order to create a third virtual machine for this exploit.

**Once you have your testing tools installed, you'll want to open your Metasploit console. It will look like this:**




This site uses cookies to provide you with a better browsing experience. Further information may be found in the [Varonis Site Privacy Policy](#)



One shortcut is to type “help” into the console, which will bring up a list of Metasploit commands and their descriptions. It should look like this:



This site uses cookies to provide you with a better browsing experience. Further information may be found in the [Varonis Site Privacy Policy](#)

A powerful and useful tool, to begin with, is the Armitage GUI, which allows you to visualize targets and recommend the best exploits to access them. This tool also shows advanced post-exploit functions for deeper penetration and further testing. To select it from the console, go to Applications – Exploits – Armitage. 

Once you've got the form field on your screen, enter the host, port number, user ID, and password. Type 'enter' after all fields are completed and you'll be ready to initiate your exploit.

This site uses cookies to provide you with a better browsing experience. Further information may be found in the [Varonis Site Privacy Policy](#)

# Resources to Learn Metasploit

One great thing about the open-source community is the commitment to resource pooling and information sharing. It's the modern embodiment of why the internet was created in the first place. It enables borderless collaboration and promotes flexibility.

To that end, we offer a list of resources that will allow you to realize the full extent of Metasploit's promise.

One of the best resources, and the first place you should visit, is Metasploit's own extensive [knowledge base](#). There, you'll find quick start guides, metamodules, exploits, and vulnerability identification and fixes. You can also learn about different types of credentials and how to obtain them.

Another helpful resource is the [Varonis Cyber Workshop](#). It offers a range of tutorials and sessions with security industry experts.

Penetration testing is essential for rooting out vulnerabilities and preventing networks from exploits and hacks. By working with a data-driven and results-oriented cybersecurity company like [Varonis](#) and employing a framework like Metasploit, you'll have an edge when it comes to protecting your networks.



## JEFF PETTERS

Jeff has been working on computers since his Dad brought home an IBM PC 8086 with dual disk drives. Researching and writing about data security is his dream job.

## — RELATED POSTS —



This site uses cookies to provide you with a better browsing experience. Further information may be found in the [Varonis Site Privacy Policy](#)

DATA SECURITY, INCIDENT RESPONSE

## Threat Update #14 – Post-Ransomware Recovery

DATA SECURITY

## What is Role-Based Access Control (RBAC)?

CYBERSECURITY NEWS, DATA SECURITY, THREAT DETECTION

## Watch: Varonis ReConnect! Defending Against Today's Spookiest Malware

# Does your **cybersecurity** start at the heart?

Get a highly customized data risk assessment run by engineers who are  
obsessed with data



**SCHEDULE NOW**

This site uses cookies to provide you with a better browsing experience. Further information may be found in the  
[Varonis Site Privacy Policy](#)

	SOLUTIONS	PLATFORM	COMPANY	RESOURCES	PARTNERS
Français	Remediation	How It	About	Free	Technology
Deutsch	&	Works	Varonis	Security	Partners
日本	Governance	How to Buy	Varonis Life	Training	Channel
語	Security	How to Use	Careers	Analyst	Partners
Русский	Analytics	It	Customers	Reports	Partner
Português	Data	Real Results	Investor	Whitepapers	Portal
	Classification	ROI	Relations	Guides	
	Ransomware	Integrations	Brand	Videos	
	Insider		Contact Us	Events	
	Threats				
	External				
	Threats				

© 2020 Inside Out Security | Policies | Certifications



This site uses cookies to provide you with a better browsing experience. Further information may be found in the [Varonis Site Privacy Policy](#)