

# Metasploit Framework User Guide

Version 3.1



<http://www.metasploit.com/>

---

# Contents

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>Introduction</b>                      | <b>3</b>  |
| <b>2</b> | <b>Installation</b>                      | <b>4</b>  |
| 2.1      | Installation on Unix . . . . .           | 4         |
| 2.2      | Installation on Windows . . . . .        | 4         |
| 2.3      | Platform Caveats . . . . .               | 5         |
| 2.4      | Supported Operating Systems . . . . .    | 5         |
| 2.5      | Updating the Framework . . . . .         | 5         |
| <b>3</b> | <b>Getting Started</b>                   | <b>6</b>  |
| 3.1      | The Console Interface . . . . .          | 6         |
| 3.2      | The GUI Interface . . . . .              | 7         |
| 3.3      | The Command Line Interface . . . . .     | 8         |
| 3.4      | The Web Interface . . . . .              | 8         |
| <b>4</b> | <b>The DataStore</b>                     | <b>9</b>  |
| 4.1      | Global DataStore . . . . .               | 9         |
| 4.2      | Module DataStore . . . . .               | 10        |
| 4.3      | Saved DataStore . . . . .                | 10        |
| 4.4      | DataStore Efficiency . . . . .           | 10        |
| 4.5      | DataStore Variables . . . . .            | 11        |
| 4.5.1    | LogLevel . . . . .                       | 11        |
| 4.5.2    | MsfModulePaths . . . . .                 | 11        |
| <b>5</b> | <b>Using the Framework</b>               | <b>12</b> |
| 5.1      | Choosing a Module . . . . .              | 12        |
| 5.2      | Exploit Modules . . . . .                | 12        |
| 5.2.1    | Configuring the Active Exploit . . . . . | 12        |
| 5.2.2    | Verifying the Exploit Options . . . . .  | 13        |
| 5.2.3    | Selecting a Target . . . . .             | 13        |
| 5.2.4    | Selecting the Payload . . . . .          | 13        |
| 5.2.5    | Launching the Exploit . . . . .          | 14        |
| 5.3      | Auxiliary Modules . . . . .              | 14        |
| 5.3.1    | Running an Auxiliary Task . . . . .      | 14        |

|          |  |           |
|----------|--|-----------|
| 5.4      | Payload Modules . . . . .              | 14        |
| 5.4.1    | Generating a Payload . . . . .         | 14        |
| 5.5      | Nop Modules . . . . .                  | 16        |
| 5.5.1    | Generating a NOP Sled . . . . .        | 16        |
| <b>6</b> | <b>Advanced Features</b>               | <b>17</b> |
| 6.1      | The Meterpreter . . . . .              | 17        |
| 6.2      | PassiveX Payloads . . . . .            | 17        |
| 6.3      | Chainable Proxies . . . . .            | 18        |
| 6.4      | Win32 UploadExec Payloads . . . . .    | 18        |
| 6.5      | Win32 DLL Injection Payloads . . . . . | 19        |
| 6.6      | VNC Server DLL Injection . . . . .     | 19        |
| <b>7</b> | <b>More Information</b>                | <b>21</b> |
| 7.1      | Web Site . . . . .                     | 21        |
| 7.2      | Mailing List . . . . .                 | 21        |
| 7.3      | Developers . . . . .                   | 21        |
| <b>A</b> | <b>Security</b>                        | <b>22</b> |
| A.1      | Console Interfaces . . . . .           | 22        |
| A.2      | Web Interface . . . . .                | 22        |
| <b>B</b> | <b>General Tips</b>                    | <b>24</b> |
| B.1      | Tab Completion . . . . .               | 24        |
| B.2      | Secure Socket Layer . . . . .          | 24        |
| <b>C</b> | <b>Licenses</b>                        | <b>25</b> |