

Filesystem And Libraries a11y.text Filesystem And Libraries Understanding the Metasploit

Architecture a11y.text Understanding the Metasploit Architecture One can more easily understand the Metasploit architecture by taking a look under its hood. In learning how to use Metasploit, take some time to make yourself familiar with its filesystem and libraries. In Kali Linux, Metasploit is provided in the metasploit-framework package and is installed in the

/usr/share/metasploit-framework directory, the top-level of which is shown below. The Metasploit filesystem Metasploit Filesystem a11y.text Metasploit Filesystem The MSF filesystem is laid out in an intuitive manner and is organized by directory. Some of the more important directories are briefly outlined below. data a11y.text data The data directory contains editable files used by Metasploit to store binaries required for certain exploits, wordlists, images, and more. root@kali : ~ # ls

```
/usr/share/metasploit-framework/data/ cpuinfo      ipwn      meterpreter snmp
webcam
```

```
eicar.com      isight.bundle mime.yml      sounds      wmap
eicar.txt      john.conf    msfcrawler   SqlClrPayload wordlists
emailer_config.yaml lab          passivex     templates
exploits       logos       php          vncdll.x64.dll
```

```
flash_detector markdown_doc post      vncdll.x86.dll documentation a11y.text documentation
As its name suggests, the documentation directory contains the available documentation for the framework. root@kali : ~ # ls /usr/share/metasploit-framework/documentation/ changelog.Debian.gz
CONTRIBUTING.md.gz developers_guide.pdf.gz README.md
```

```
CODE_OF_CONDUCT.md copyright      modules lib a11y.text lib The lib directory contains the
“meat” of the framework code base. root@kali : ~ # ls /usr/share/metasploit-framework/lib/
```

```
anemone      msfenv.rb      rbmysql.rb sqlmap
anemone.rb   net            rex          tasks
enumerable.rb postgres      rex.rb      telephony
metasm       postgres_msf.rb robots.rb   telephony.rb
```

metasploit rabal snmp windows_console_color_support.rb

msf rbmysql snmp.rb modules a11y.text modules The modules directory is where you will find the actual MSF modules for exploits, auxiliary and post modules, payloads, encoders, and nop generators. root@kali : ~ # ls /usr/share/metasploit-framework/modules/ auxiliary encoders exploits nops payloads post plugins a11y.text plugins As you will see later in this course,

Metasploit includes many plugins , which you will find in this directory. root@kali : ~ # ls

/usr/share/metasploit-framework/plugins/ aggregator.rb ips_filter.rb openvas.rb sounds.rb

alias.rb komand.rb pcap_log.rb sqlmap.rb

auto_add_route.rb lab.rb request.rb thread.rb

beholder.rb libnotify.rb rssfeed.rb token_adduser.rb

db_credcollect.rb msfd.rb sample.rb token_hunter.rb

db_tracker.rb msgrpc.rb session_notifier.rb wiki.rb

event_tester.rb nessus.rb session_tagger.rb wmap.rb

ffautoregen.rb nexpose.rb socket_logger.rb scripts a11y.text scripts The scripts directory

contains Meterpreter and other scripts. root@kali : ~ # ls /usr/share/metasploit-framework/scripts/

meterpreter ps resource console tools a11y.text tools The tools directory has various useful

command-line utilities. root@kali : ~ # ls /usr/share/metasploit-framework/tools/ context dev exploit

hardware memdump modules password recon Metasploit Libraries a11y.text Metasploit Libraries

There are a number of MSF libraries that allow us to run our exploits without having to write

additional code for rudimentary tasks, such as HTTP requests or encoding of payloads. Some of the most important libraries are outlined below. Rex a11y.text Rex The basic library for most tasks

Handles sockets, protocols, text transformations, and others SSL, SMB, HTTP, XOR, Base64,

Unicode Msf::Core a11y.text Msf::Core Provides the “basic” API Defines the Metasploit

Framework Msf::Base a11y.text Msf::Base Provides the “friendly” API Provides simplified

APIs for use in the Framework Throughout this course, we will touch upon how to use other

tools directly within Metasploit. Understanding how things are stored and related to the Metasploit

filesystem will help you in using the msfconsole and the other Metasploit interfaces. Next

[Modules and Locations](#) [Prev](#) [Metasploit Architecture](#)