Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

WordPress Exploit Framework

Nessa aula, vamos instalar um WordPress Exploit Framework, que é uma toolkit escrita em Ruby que é específica para fazer a exploit em sites em WordPress.

Primeiramente, precisamos instalar os seus pré-requisitos:

```
# apt-get install build-essential patch

# apt-get install ruby-dev zlib1g-dev liblzma-dev
```

Depois, baixar o programa completo em seu Kali e rodar:

```
# git clone https://github.com/rastating/wordpress-exploit-framework.git

# cd wordpress-exploit-framework/

# bundle install
```

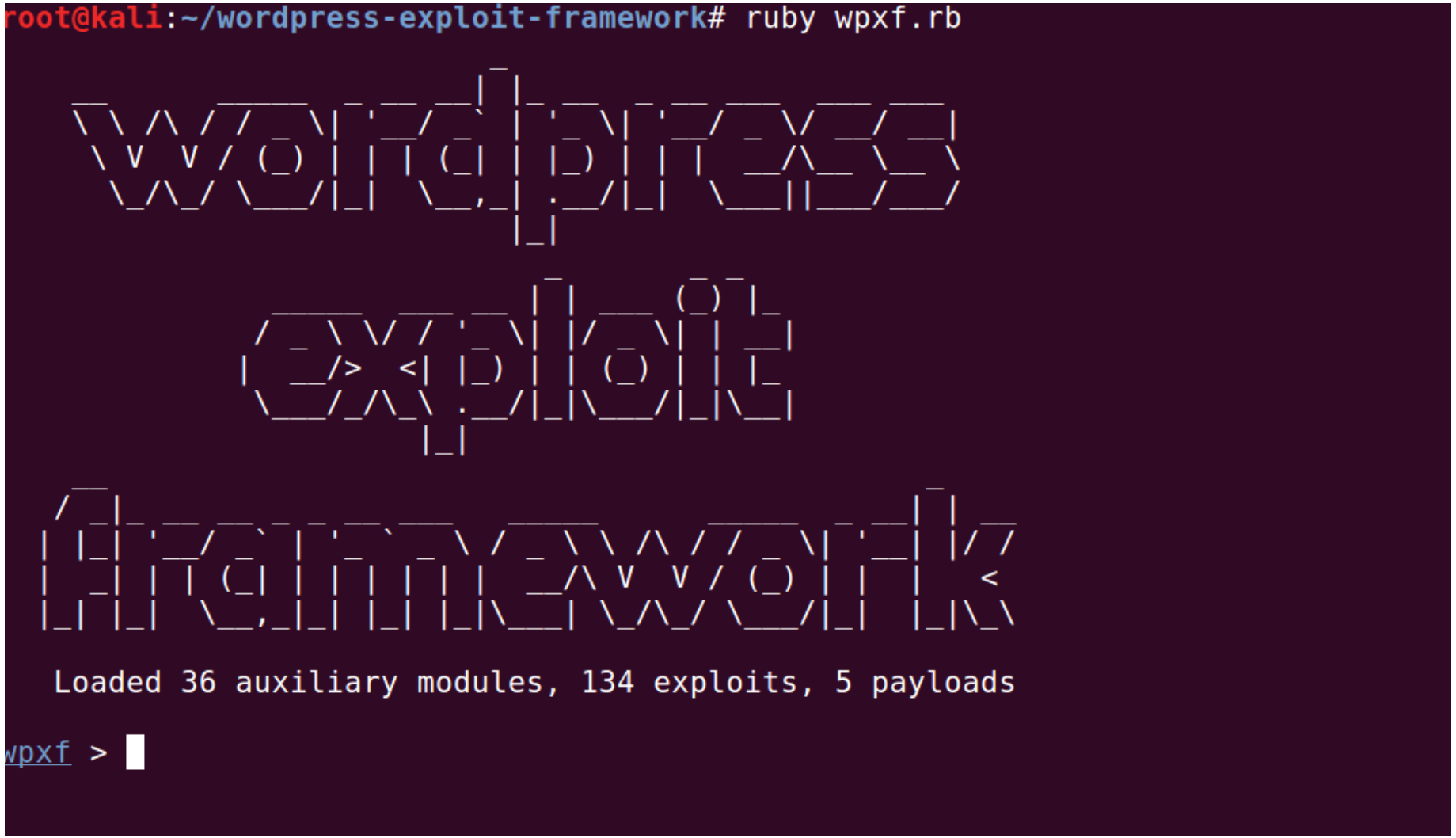
Rode o programa com o comando abaixo:

```
# ruby wpxf.rb
```

WordPress Exploit Framework

```
root@kali:~/wordpress-exploit-framework# ls
CONTRIBUTING.md  Gemfile            LICENSE   README.md  wpxf.rb
data             github_updater.rb  modules   spec
env.rb           lib                payloads  VERSION
root@kali:~/wordpress-exploit-framework# bundle install
Don't run Bundler as root. Bundler can ask for sudo if it is needed, and
installing your bundle as root will break this application for all non-root
users on this machine.
Fetching gem metadata from https://rubygems.org/
Fetching version metadata from https://rubygems.org/
Resolving dependencies...
Installing colorize 0.8.1
Installing diff-lcs 1.3
Installing ffi 1.9.17 with native extensions
Installing mime-types-data 3.2016.0521
Installing mini_portile2 2.1.0
Installing require_all 1.4.0
Using rspec-support 3.5.0
Using rubyzip 1.2.0
Installing slop 4.4.1
Using bundler 1.12.5
Installing ethon 0.10.1
Installing mime-types 3.1
```

WordPress Exploit Framework



Quias expliot estão disponiveis?

- bind_php: carrega um script que irá ligar a uma porta específica e permitir que o WPXF estabeleça um shell remoto.
- custom: carrega e executa um script PHP personalizado.
- download_exec: baixa e executa um arquivo executável remoto.

- exec: executa um comando shell no servidor remoto e retorna a saída para a sessão WPXF.
- reverse_tcp: envia um script que estabelecerá um shell TCP reverso.