ZYNIX FUSION

Product overview

2 de February de 2021

zynix-Fusion is a framework that aims to centralize, standardize and simplify the use of various security tools for pentest professionals. zynix-Fusion (old name: Linux evil toolkit) has few simple commands, one of which is the **init** function that allows you to define a target, and thus use all the tools without typing anything else.

Zynix is a ruby script made for the purpose of being a shortcut, so instead of creating several tools from scratch, it simply uses a range of existing tools.

Is zynix-Fusion better than setoolkit? Yes and no, there are two that serve the same thing and in a different way, the Zynix-Fusion and an automated attack information automation script.

Warning

Warning: I am not responsible for the way that this software will be used by third parties. The purpose of this software is only educational.

:: Considerations ::

§ 1 About use

This script was made to automate the steps of gathering information about web targets, the misuse and responsibility of the user, to report bugs or make suggestions to open a report on github.

§ 2 About simple_scan

Automap was replaced by simple_scan, it is lighter and faster, in addition to being less detectable, now it has different modes of execution that make it possible from a quick and simple execution to more complex modes.

§ 3 About Console

The output of the script can be extremely long, so see if your console, (gnome-terminal, cmd, konsole) is configured to display 1000 lines (I particularly recommend 10,000 lines), for professional purposes it allows the documentation, it records the commands, exits and formats the text.

:: How to work? ::

Zynix works with the idea of providing a personalized (and customizable) command line interface, that is, you will have to type internal zynix commands and pass the parameters, but to avoid having to pass the same parameter several times there is the function **init**, which will globally store these parameters and use them later in various commands automatically.

:: How to use it? ::

There are two types of commands: the internal ones, which are restricted to the back-end system and the usable front-end ones that are used to execute the functions.

red are the functions that do not work at this time or that have been removed.

:: Installation and configuration ::

In order to use zynix it is necessary that you have dependencies installed on your computer, at the moment there is no script that does this, however it is possible to use it without problems in distributions with parrot security, kali linux, back box and fedora security, etc. Soon I will add a script to install the dependencies.

If you use fedora or systems with dnf you can try **sudo dnf group install 'Security lab'**

open your terminal in linux and type:

$ git clone https://github.com/th3void/zynix-fusion.git && cd zynix-fusion && ruby main.rb

To update the program, enter the main folder and type:

$ git pull

:: Kernel functions ::

compress	| Compress files
extract	| Extract files
cover	| Covers your tracks and logs
port_scanner	| Replaced by automap
note	| Create simple notes
search	| Search whois, emails, banner grep
dns_scanner	| Scan for 'A', 'AAAA', 'CNAME', 'MX', 'NS', 'PTR', 'SOA'
dir_scanner	| Brute force for search files and folders
simple_scan	| Runs an automatic scanner with nmap
fakeEmail	| Generate fake emails
call_cpf	| Generate fake cpf
call_rg	| Generate fake rg

call_gem	| Generate fake name (Brazilian, Spanish and Portuquese only)
simple_dump	| Generate return a simples dum with data in txt or xml format
banner	| Shows simple Zynix ascii banner
web_dns	| Shows web dns seekers
linux_files	| Shows useful linux files
linux_folders	| Shows function of linux folders
linux_util	| Shows useful linux commands
tor_search	| Shows tor network searchers
tor_alt	| Shows alternatives to tor