Raptor Waf

Raptor Web Application Firewall

Antonio Costa - CoolerVoid - coolerlair[aT]gmail[DOt]com

November 12, 2015

Whoami

Author:

- Antonio Costa ”CoolerVoid” is a Computer Programmer who loves the Hacker culture, he work as a system analyst at CONVISO for four years. Antonio working with code review, pentest and security research with focused on Secure Web Applications and Reverse Engineering. He also has been speaking at in some Brazilian Security Conferences such as YSTS, OWASP Florianopolis and Bsides Sao Paulo.

Introduction

Software Information:

- Raptor is a Open Source Tool, your focus is study of attacks and find intelligent ways to block attacks.
- Raptor held by GPL v3 license

Introduction

Why this tool is made in C language ?

- C have a high delay time for writing and debugging, but no pain no gain, have a fast performance, addition of this point, the C language is run at any architecture like Mips,ARM and others... other benefits of C, have good and high profile to write optimizations, if you think write some lines in ASSEMBLY code with AES-NI or SiMD instructions, i think is good choice.
- Why you not use POO ? in this project i follow ”KISS” principe: http://pt.wikipedia.org/wiki/Keep_It_Simple
- C language have a lot old school dudes like a kernel hackers...

Introduction

Requirements:

- Need ”GCC” and ”make”
- Current version tested only in Linux.
- Current version run well, but is a BeTa version, you can report bug...

How you can use it

Following this to get, decompress, compile and execute:

- wget git clone https://github.com/CoolerVoid/raptor_waf
- cd raptor_waf; make; bin/Raptor

The Overview

Explain

WAF stands for Web Application Firewall. It is widely used nowadays to detect and defend SQL Injections and XSS...

- You can block XSS, SQL injection attacks and path traversal with Raptor
- You can use blacklist of IPs to block some users at config/blacklist_ip.txt
- You can use IPv6 and IPv4 at communications
- At the future DoS protector, request limit, rule interpreter and Malware detector at uploads.
- At the future SSL/TLS...

Hands On !


Coded by CoolerVoid - coolerlair[at]gmail[dot]com
RAPTOR WAF
RAPTOR WEB APPLICATION FIREWALL v0.01
Options argv:
--host or -h : host to protect
--port or -p : port of host to protect
--redirect or -r : port to redirect HTTP
--wafmode or -w : Waf mode protection level, choice level of protection between 1,2,3 or 4
--log or -o : Write in log file
Config Blacklist at config/blacklist_ip.txt

Hands On !

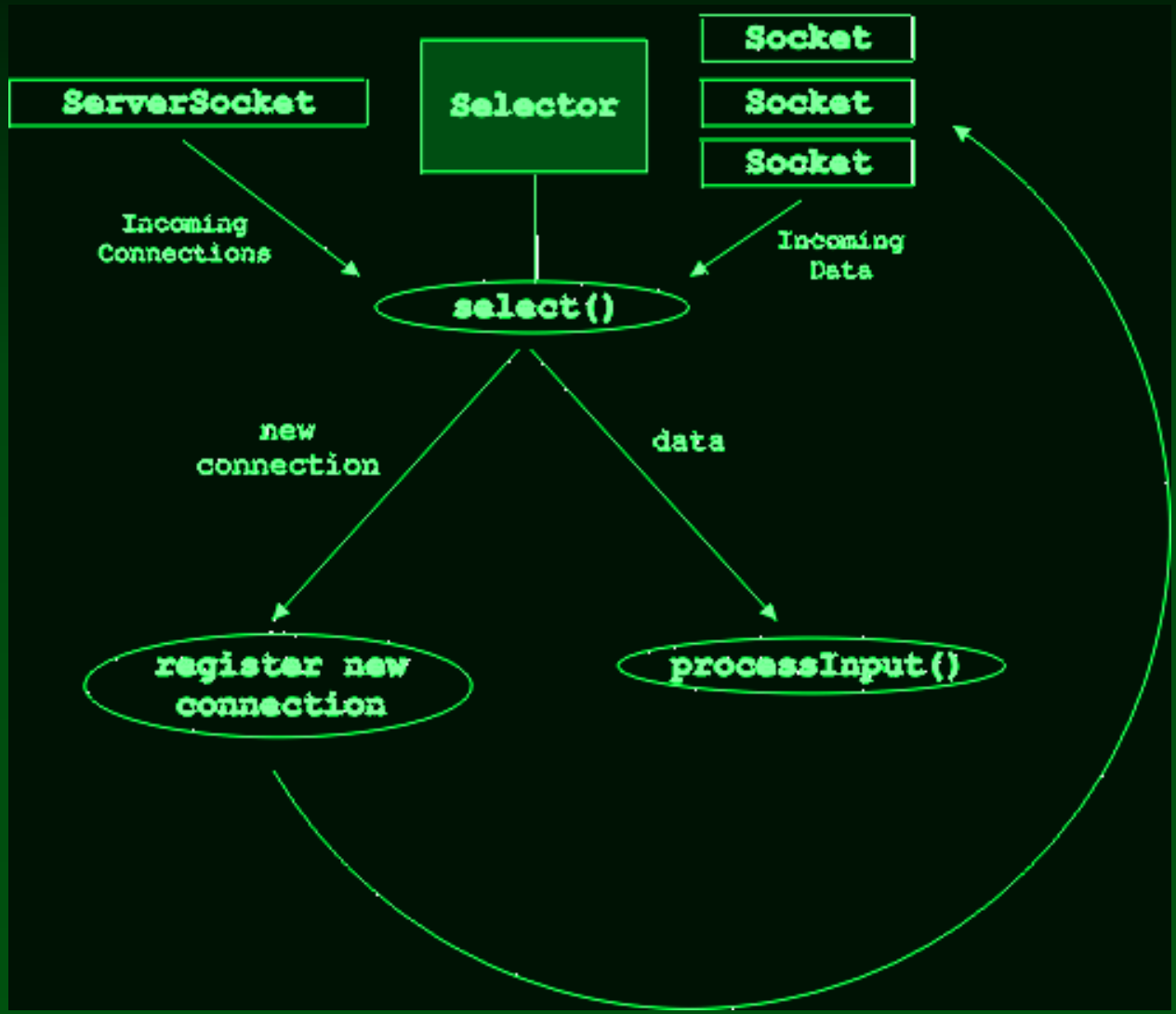
- Follow this command
- bin/Raptor –host Address_of_http_server2Protect -p 80 -r 8886 -w 4 -o logAttacks.txt
- Open the machine of Raptor at any computer of network http://waf_machine:8886
- Copy vulnerable PHP code to your web server directory
- cp doc/test_dfa/test.php /var/www/html
- Ok raptor protect the HTTP server at http://server_ip:8886/test.php

How it works ?

Raptor is very simple, have three layers reverse proxy, blacklist and Match(using deterministic finite automaton).

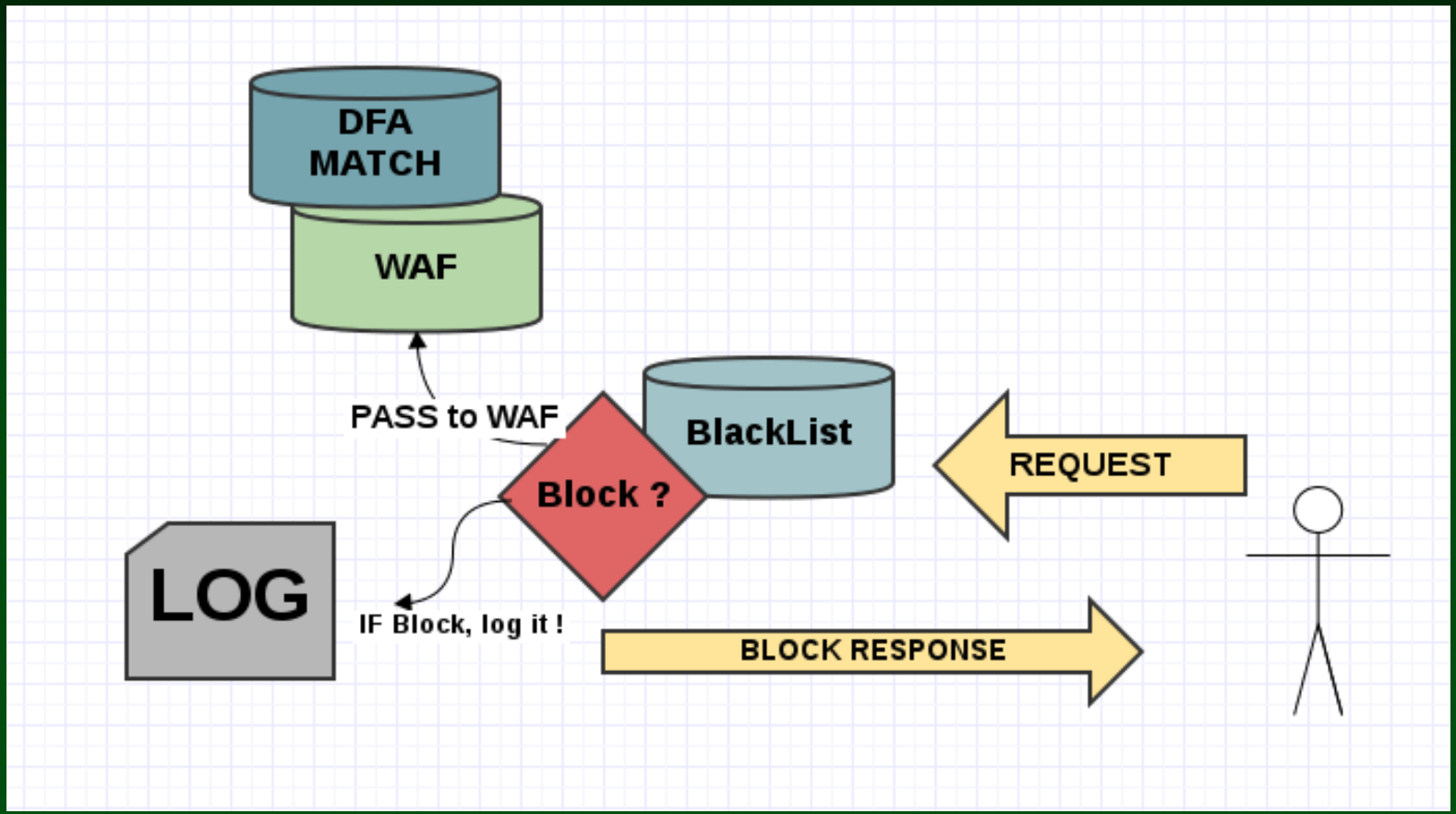
How proxy works ?

Proxy using the select() function to check multiple sockets, at the future change to use libevent(signal based is very fast)



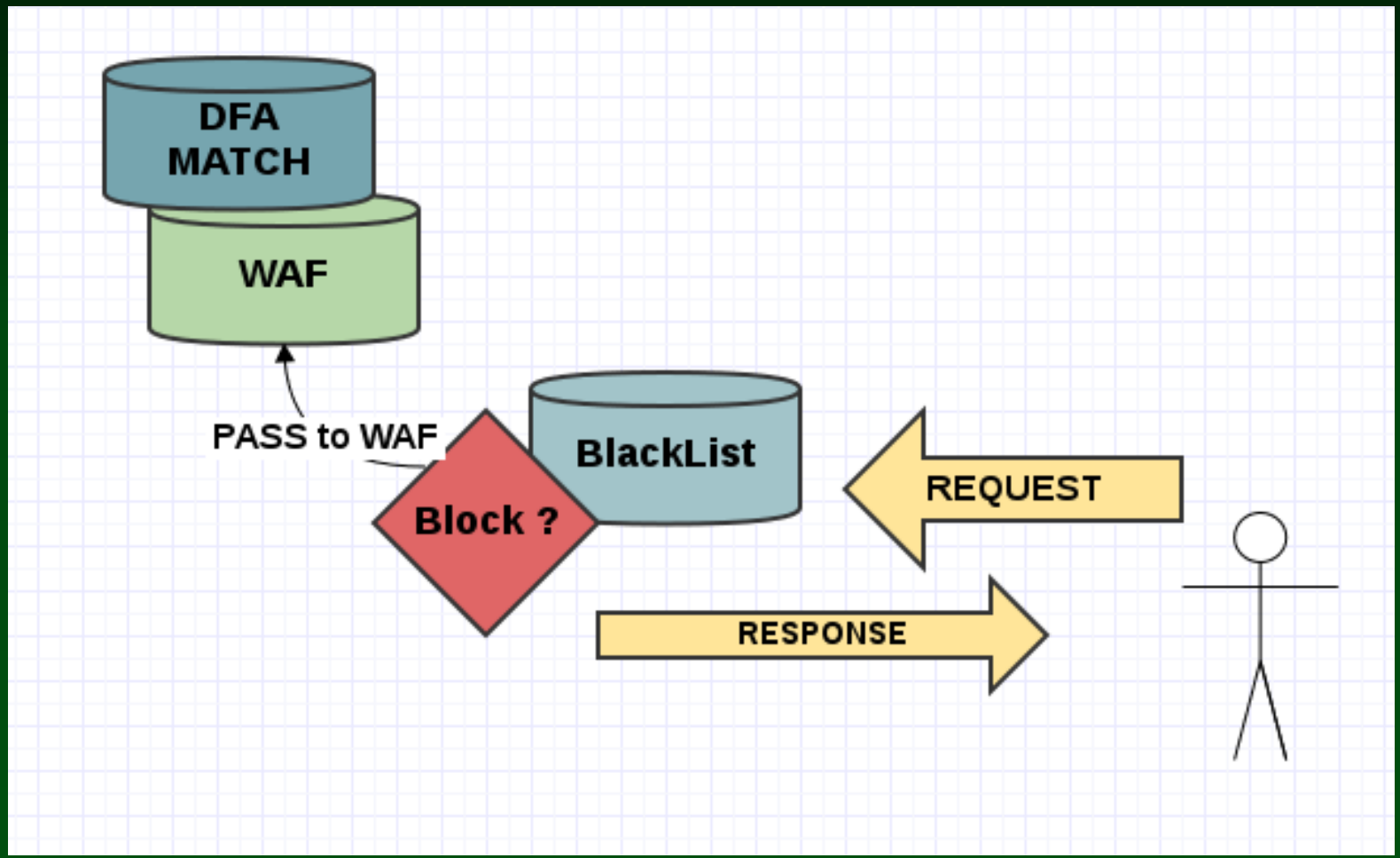
How it works ?

If someone send a request, Raptor do address analysis...
Address blacklisted ? block !



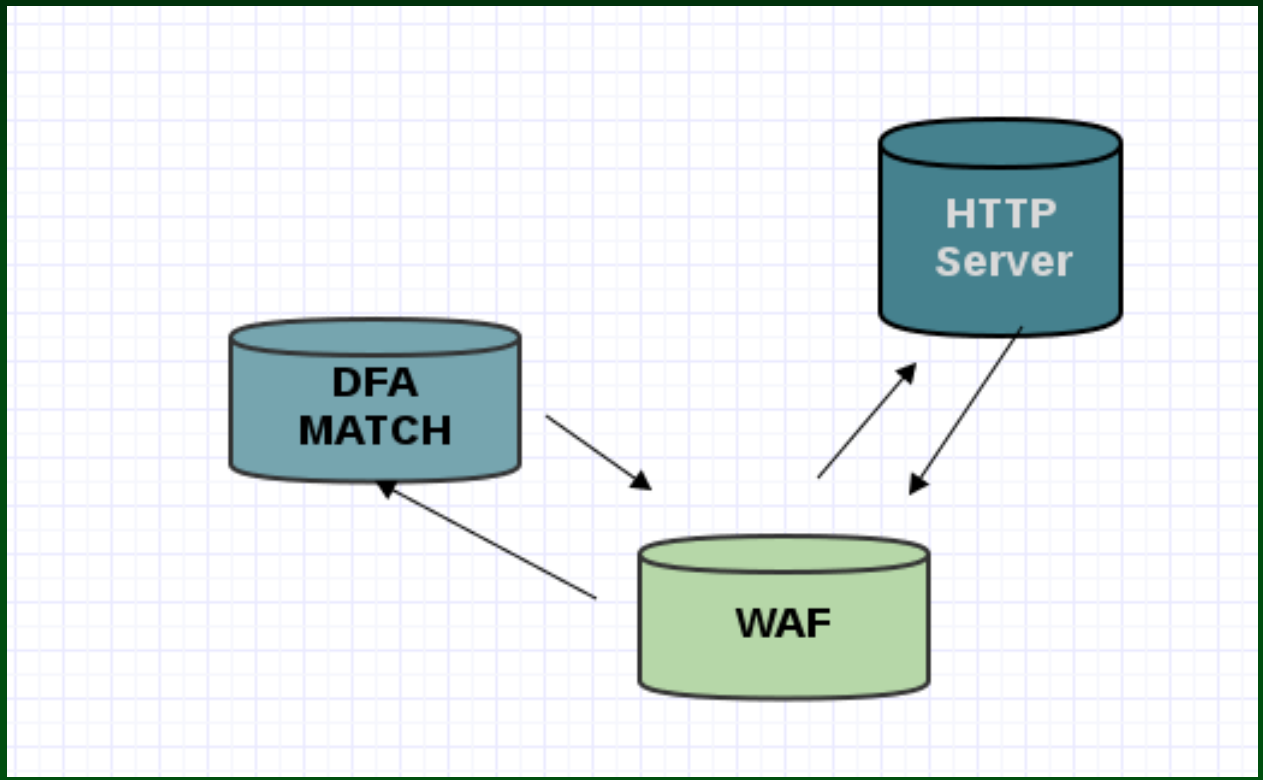
How it works ?

If deterministic finite automaton and Blacklist don’t match, Raptor don’t block



How it works ?

Raptor get a Request with GET or POST method and make some analysis to find dirt like a sql injection, cross site scripting...



External match string mode

- At directory config have a file of lists of rules
- You can match string with diferent algorithms
- You can choice with argument –match or -m
- Choice one option between Karpe Rabin, DFA or Boyer Moore Horspool

The End ?

Greets

- contact: coolerlair[at]gmail[dot]com
- acosta@conviso.com.br
- my parents and friends...
- https://conviso.com.br/index.php/EN

at construction...