The Metabrik Platform - Rapid Development of Reusable Security Tools

Patrice Auffret

metabrik.org

March 2017

Whoami?

GomoR

- Information security engineer for 15 years
- *Perl* developper for same amount of time
- CPAN author
  - *Net::Packet* (obsolete)
  - *Net::Frame* suite (successor)
  - *Net::Write*
  - *Net::SinFP/Net::SinFP3* (2012: hack.lu, ekoparty, EuSecWest)
  - *Metabrik* (and *Metabrik::Repository*)
- Interests
  - Forensic analysis
  - Network protocols
  - Big data (mining)
  - https://www.sisyphe.io/

What is Metabrik?

The subject of today...

A Pokemon?

Yes, but no.

- Source: http://www.mypokecard.com/fr/Galerie/Pokemon-Metabrik

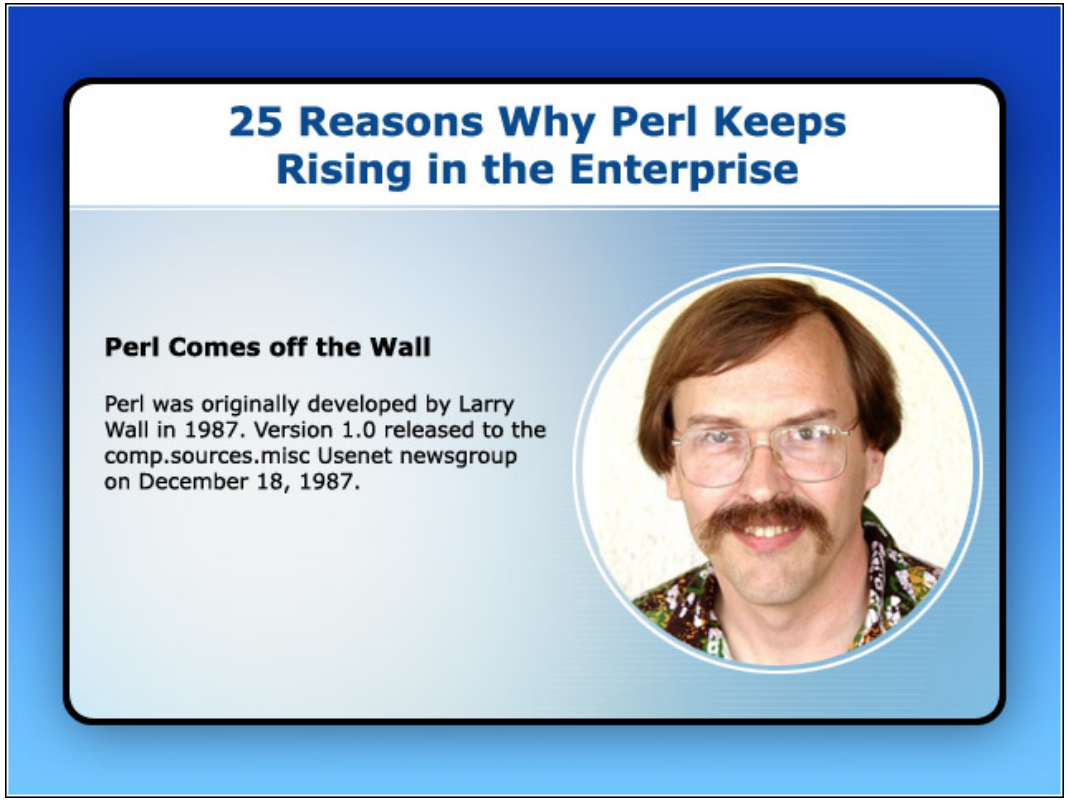
A platform

And much more.

- A *UNIX*-like shell
- A *true* language with a *Read-Eval-Print-Loop*
- Many *Brik*s
  - A development/prototyping platform
  - To build quickly the right tool

A *true* language?

Yes. Kill the troll now. But *Perl* is better than *Python* anyway :)



- Source: eweek - April, 30th 2010

Why?

CLI rules

- Everything should be possible via command line
  - Automate all the things
- *Do it once* principle
  - Tired of repeated throw-away scripts
  - Code reusability rules
- *UNIX* shells too simple
  - *Pipe* too limited
  - Needed a powerful language
- Rapid development from a *CLI*
  - Writing scripts is also possible
- Normalized syntax in *human readable* form

Comparison with REbus

Interactive usage versus fully automatic one

- Same goal: normalize tool usage
- REbus: replace the human
  - Not a shell
  - Usage is not so easy
  - Written in *Python*
  - Input/output automation
- Metabrik: help the human
  - Manual input/output
  - Easy *Brik* usage
- Both are using *wrapper*s around existing tools
  - Metabrik does not only use *wrapper*s
  - It tries to use best *Perl* CPAN modules

Demo 1 - The Metabrik Shell (~3 minutes)

- 3 kinds of command lines
  - external
  - *Brik*'s commands
  - *Perl* code (*REPL*)
- 5 *Brik*'s commands
  - *use, set, get, run, help*

Features

Most notable ones

- Shell: builtins
  - cd, alias, ...
- Customizable shell with history handling
  - File *.metabrik_rc*
  - File *.metabrik_history*
- *Metasploit*-like syntax
- Completion for commands, files, variables
- Control keys like *Ctrl+R*

Briks

You have the knowledge, detail is in the *Brik*

- Many *wrapper*s around external programs
  - but not only
- Object-oriented
  - defined by properties like tags, category or attributes
  - a *Brik* may inherit from one or more others
  - Example: *file::psv* inherits from *file::csv*
- Add features to existing tools
  - There is always one lacking
  - Example: *forensic::scalpel*
- A reusable *Perl* module
  - a command line interface
  - a classic interface

brik::tool Brik

Makes a *Brik* easy to use

- Two kind of dependencies
  - System packages
  - *Perl* modules
- Easy to install and use
  - *run brik::tool install database::cvesearch*
  - *use database::cvesearch*
  - *help database::cvesearch*
- Easy to update as
  - *run brik::tool update*

Special variables

Where we keep some *Perl* philosophy

- Example:
  - *run shell::command capture ls /*
  - *my $count = scalar(@$RUN)*
- Input/output handling via $RUN
  - This is the new pipe
  - *Perl* basic data types
  - You sculpt it to your needs
- Other special variables
  - *$SET*
  - *$GET*
  - *$CON, $LOG, $GLO, $SHE*
  - *$USE, $ERR, $MSG, $REF*

Demo 2 - forensic challenge (~3 minutes)

Or how to quickly solve a problem

- Some miscreants kidnapped your cat
- We found an old device on crime-scene
- We have to analyze this data
- File analysis
  - *file::type*
  - *file::compress*
  - *image::exif*
- Extract data
  - *forensic::scalpel*

Metabrik Core and Metabrik Repository

What's the difference?

- Metabrik Core
  - *core::global*
  - *core::shell*
  - *core::log*
  - *core::context*
  - Minimal system and *Perl* modules dependencies
- Metabrik Repository
  - 240+ *Brik*s (and counting)
  - *brik::tool* to manage
  - *brik::search* to search
  - Install dependencies only when needed

brik::tool and brik::search

Your best friends

- Search by tag, command, category or string...
  - *run brik::search tag video*
- *brik::tool* for management
  - create a skeleton of a new *Brik*
    - *run brik::tool create_brik my::first*
  - create a skeleton of a new program
    - *run brik::tool create_tool my_tool.pl*

A *Metatool*

From prototype to industrialisation

- Finalized prototype
  - *run brik::tool create_tool iplocation.pl*
- Shell commands conversion to code

```
# Shell Metabrik
use lookup::iplocation
run lookup::iplocation from_ip 93.184.216.34
```

```
# Perl program
use Metabrik::Core::Context;
my $con = Metabrik::Core::Context->new;

use Metabrik::Lookup::Iplocation;
my $li = Metabrik::Lookup::Iplocation->new_from_brik_init($con);
my $h = $li->from_ip($ip);
```

Demo 3 - automate malware analysis (~3 minutes)

Or how to extract *Indicators of Compromise*

- Use a *VM* as a scapegoat (sacrifice it)
- Take a fingerprint of its memory/process/registry before
- Run a malware
- Take a fingerprint of its memory/process/registry after
- Instrumentalise a *VM* and take a snapshot
  - *system::virtualbox*
- Execute program remotely
  - *remote::winexe*
  - *remote::wmi*
- Perform a diff on a *Windows* machine-state
  - *forensic::volatility*

Demo 4 - bind all *Brik*s together (~5 minutes)

Make it straightforward

- Use all previous *Brik*s to write a new one
- *remote::windiff*
- Automates diffing between two *VM* states

Enlarge your tools

Use more *Briks*

- Code: *lib/Metabrik/Remote/Windiff.pm*
- Improve a tool by yourself from the 240+ *Briks*
  - *run file::csv write $process_diff out.csv*
  - *run client::dns ptr_lookup $ip*
  - *run api::virustotal ipv4_address_report $ip*
  - *run api::shodan host_ip $ip*

Weaknesses of this approach

Or just more work todo?

- Relies on *incomplete* tools
  - *Volatility* is based on reverse engineering Windows
  - *WMI* too...and we found some parsing bugs
- Depends on the ability to snapshot a VM memory
  - What if we wanted to use a physical machine?
- No *live* analysis
- And approach already taken by VolatilityBot
  - *https://github.com/mkorman90/VolatilityBot*
  - (But requires a *Python* agent to be installed)

Now for a better approach

Have you heard about sysmon?

- Monitors Windows system changes like
  - Loading of drivers and images
  - Registry changes
  - Filesystem changes
  - Process accesses
  - ...and more
- Live stream through Windows Event logs

Collect all the things

Sysmon and network

- Put everything into an *Elasticsearch* storage
  - *Winlogbeat* for Windows Event logs
  - *tcpdump*-like to capture network traffic
    - (but no live stream yet)

Understanding malwares without l33t skills (1/2)

Automate all the things now.

- We need remote capabilities for
  - Sysmon
  - Windows Defender
  - Upload/download
- We need local capabilities for
  - Interacting with *Elasticsearch*
  - Performing forensic analysis on pcap files

Understanding malwares without l33t skills (2/2)

Automate all the things now.

- Sysmon + Winlogbeat
  - *remote::sysmon, remote::winsvc, forensic::sysmon*
- Elasticsearch
  - *server::elasticsearch, client::elasticsearch*
- tcpdump
  - *client::tcpdump*
- smbclient + winexe
  - *client::smbclient, remote::winexe, remote::windefend*
- New *Brik remote::sandbox*

remote::sysmon && forensic::sysmon

- *remote::sysmon*
  - Generate configuration (full logging by default)
  - Deploy/undeploy sysmon agent to remote host with *remote::winexe*
  - Update configuration on remote host
- *forensic::sysmon*
  - A *client::elasticsearch* child
  - Queries everything
  - Saves state as CSV files
  - Performs diff analysis on CSV files

Give me malware to test :)

You have a spambox, do you?

- Acquire malware sample from browsing your spambox
- But automated, of course
  - And there is a *Brik* for that: *client::imap*

Demo 5 - Acquire malware sample (~2 minutes)

- Use *client::imap Brik*

Demo 6 - the *remote::sandbox Brik* (~8 minutes)

- Sysmon + winlogbeat + Elasticsearch are ready
- Will use *remote::sandbox* and *client::tcpdump*
- Take a snapshot from collected events from Elasticsearch
- We have to disable the antivirus before executing malware

Demo 7 - pcap to Elasticsearch (~3 minutes)

- Explore pcap data with *forensic::pcap*

Analysis conclusion

We have to, at some point, conclude.

- A ZIP file containing a ZIP containing a JS file
- A JS using WScript to download PNG images
- Images are in fact executable files
- We now have some IOCs
  - MD5 sums (or whatever your want)
  - A registry key
  - IP addresses
  - Domain names and URLs
- (And we didn't looked at the a.doc file)

Some of the best *Briks*

For some catagories

- api::*
  - splunk, ...
- client::*
  - elasticsearch, mongodb, redis, rest, openssh, twitter, splunk, ...
- server::*
  - rest, snmp, dns, ...
- proxy::*
  - http, ssh2tcp, ...
- www::*
  - shorten, google, ...
- lookup::*
  - iplocation, oui, ...
- network::*
  - nmap, linux::iptables, sinfp3, ...

Conclusion

- Reaching the 250 *Brik*s milestone...
- Everything becomes a *Perl* variable
- Automate all the things from *CLI*
- Add missing features to existing tools
- Normalization brings easeness
- Shell unification too
- Understand the philosophy and play
- POLL: who would be interested in a workshop?

Question(s)?

Metabrik
There is a Brik for that.

- Code available on: *http://trac.metabrik.org/*
- Howto install: *https://www.metabrik.org/metabrik/install/*
- Docker: *docker pull metabrik/metabrik*
- Twitter: @Metabrik
- Twitter: @PatriceAuffret