P.A.K.U.R.I

Penetration test Achieve Knowledge Unite Rapid Interface
Operation with Ten-key

2019/11/2
AVTOKYO HIVE
@01ra66it

Background

Are you feeling stronger just by installing Kali linux?

- There are so many tools in kali linux that you can't take advantage of them.
- Beginners are often happy with the results of the installation.

metasploit
EeEF
BURPSUITE PROFESSIONAL
Nessus vulnerability scanner
COMMANDO
JOHN
MATRIX
HOT TOYS 1/6TH SCALE COLLECTIBLE FIGURE

I used to think so...

As beginner pentester

- Beginners do not know how to work.
- Scan and enumerate command options are difficult.

As senior pentester

- I want beginners to learn work quickly.
- Systematic human resource development is difficult with Pentest.
- I want to have a successful experience with beginners.
- I don't want to be the only person who knows how work works through my (long) experience.

As manager

- It is very difficult to read the engineer's work status from the console screen.
- Similarly, it is difficult to evaluate the work of engineers.
- Accurate management is impossible unless people of any skill level can understand it.

I want to solve the problems of each position.

What is PAKURI ?

Penetration test

Achieve

Knowledge

Unite

Rapid

Interface

What is PAKURI ?

- Automate work with OSS obtained from Github. Reduce manual mistakes.
- Visualize work progress with OSS obtained from Github.
- Front-end operation is only possible with the numeric keypad.
- C2 Server (Communication & Collaboration)

Why PAKURI ?

- This tool uses a good part of many OSS.
- In short, copycat.
- If you say copycat in Japanese slang, it is “Pakuru”.

Why raven?

- Raven is a symbol of knowledge.
- Raven uses anything when building a nest.

Concept

- I chose the tools installed on Kali Linux and the OSS released on Git as an active pen tester.
- PAKURI is a virtual environment built on the concept of “Everyone can do it easily”.

Features

- Scan
  - nmapAutomator (https://github.com/21y4d/nmapAutomator.git)
  - AutoRecon (https://github.com/Tib3rius/AutoRecon.git)
  - OpenVAS
- Visualize
  - Faraday (https://github.com/infobyte/faraday.git)

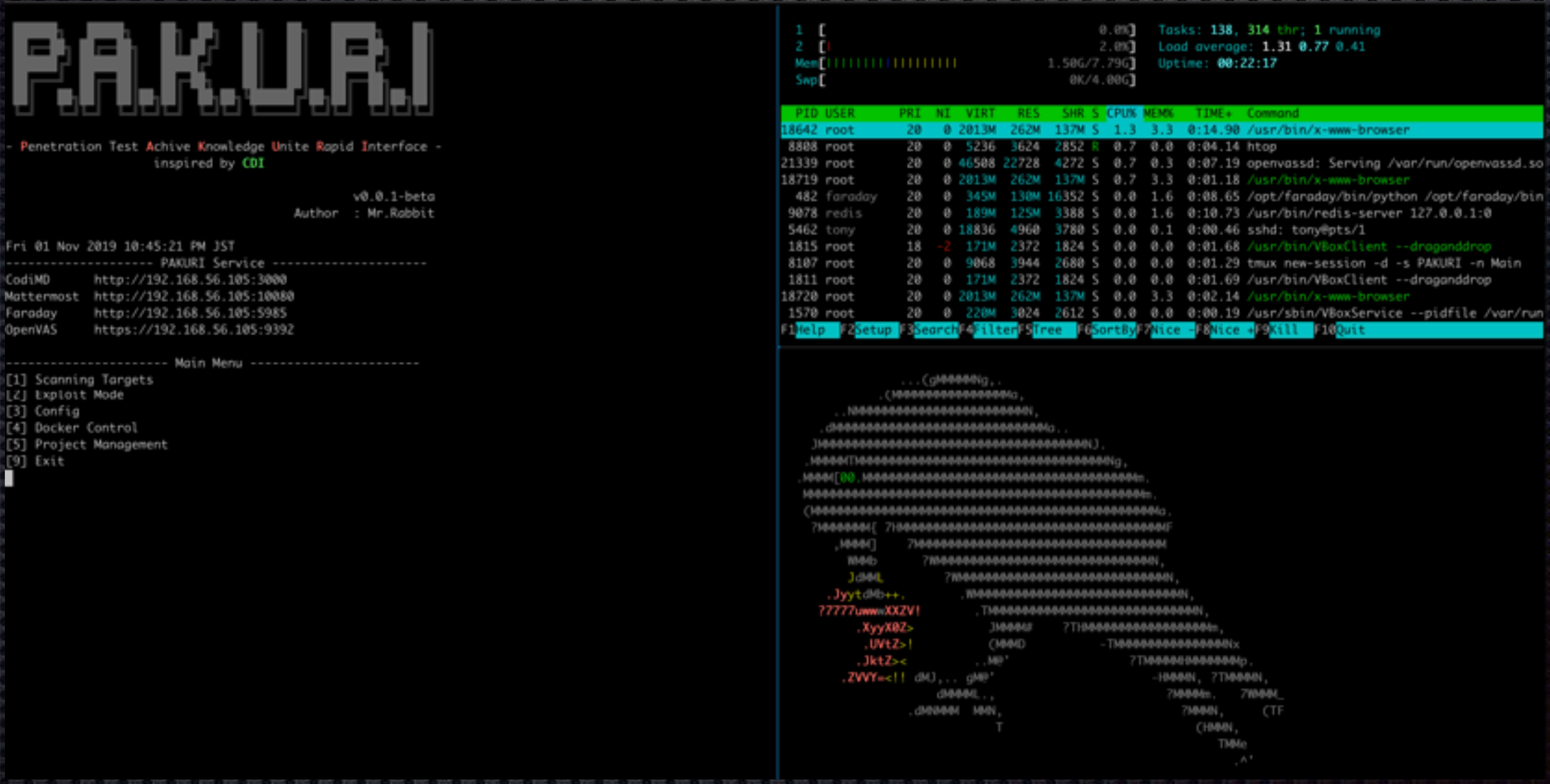
Features

- C2 Server
  - Communication
    - Mattermost (https://github.com/mattermost/mattermost-docker.git)
  - Collaboration
    - CodiMD (https://github.com/hackmdio/docker-hackmd.git)

Features

- Front-end operation
  - PAKURI
- Other
  - oh-my-tmux (https://github.com/gpakosz/.tmux.git)
  - oh-my-zsh (https://github.com/robbyrussell/oh-my-zsh.git)
  - htop
- CUI-GUI switching

Overview

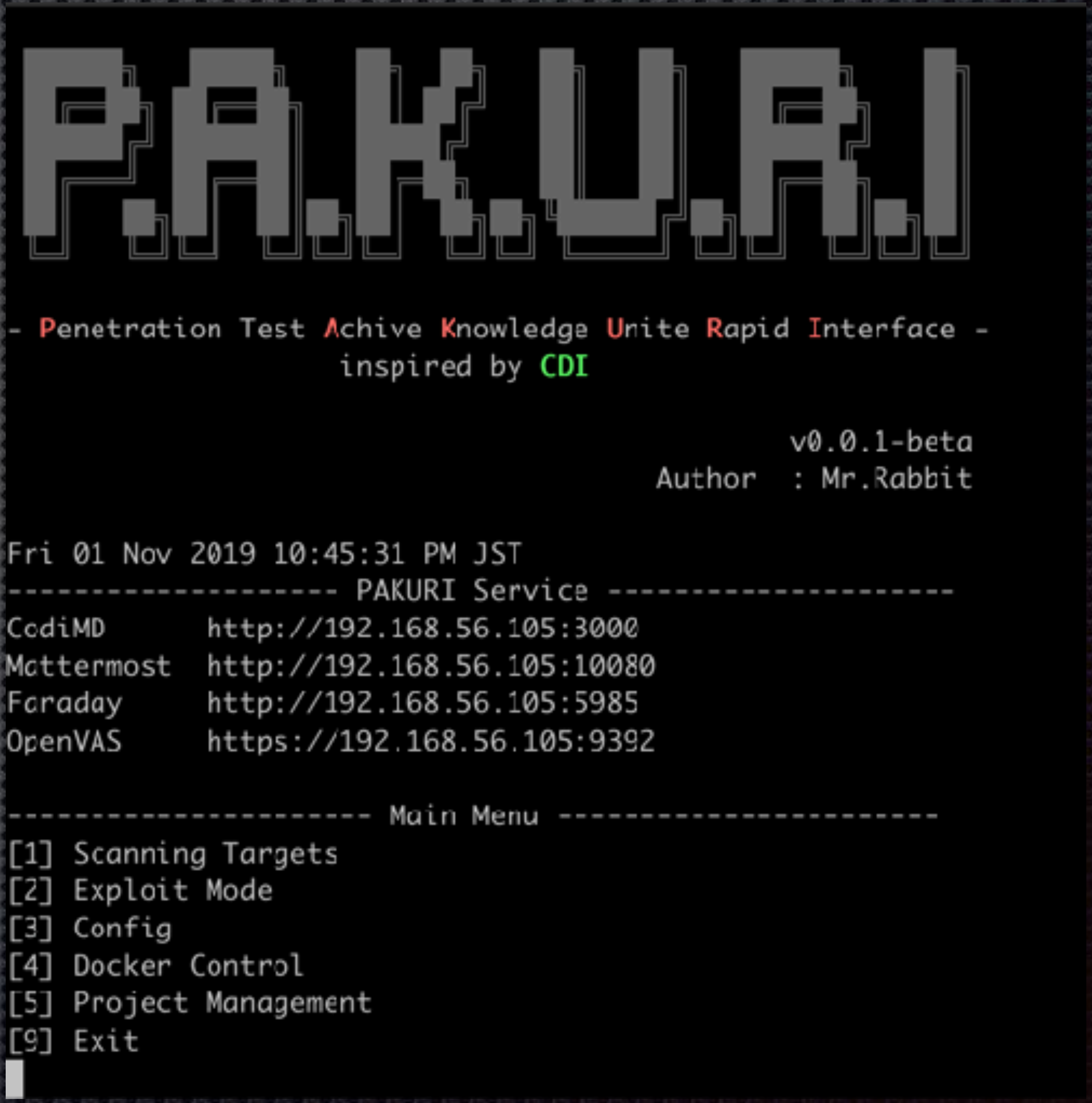


```
P.A.K.U.R.I

- Penetration Test Achive Knowledge Unite Rapid Interface -
                  inspired by CDI

                                        v0.0.1-beta
                                   Author  : Mr.Rabbit

Fri 01 Nov 2019 10:45:21 PM JST
-------------------- PAKURI Service --------------------
CodiMD      http://192.168.56.105:3000
Mattermost  http://192.168.56.105:10080
Faraday     http://192.168.56.105:5985
OpenVAS     https://192.168.56.105:9392

--------------------- Main Menu ----------------------
[1] Scanning Targets
[2] Exploit Mode
[3] Config
[4] Docker Control
[5] Project Management
[9] Exit
```

```
  1  [                              0.0%]   Tasks: 138, 314 thr; 1 running
  2  [|                             2.0%]   Load average: 1.31 0.77 0.41
  Mem[|||||||||||||||||||    1.50G/7.79G]   Uptime: 00:22:17
  Swp[                          0K/4.00G]

  PID USER      PRI  NI  VIRT   RES   SHR S CPU% MEM%   TIME+  Command
18642 root       20   0 2013M  262M  137M S  1.3  3.3  0:14.90 /usr/bin/x-www-browser
 8808 root       20   0  5236  3624  2852 R  0.7  0.0  0:04.14 htop
21339 root       20   0 46508 22728  4272 S  0.7  0.3  0:07.19 openvassd: Serving /var/run/openvassd.so
18719 root       20   0 2013M  262M  137M S  0.7  3.3  0:01.18 /usr/bin/x-www-browser
  482 faraday    20   0  345M  130M 16352 S  0.0  1.6  0:08.65 /opt/faraday/bin/python /opt/faraday/bin
 9078 redis      20   0  189M  125M  3388 S  0.0  1.6  0:10.73 /usr/bin/redis-server 127.0.0.1:0
 5462 tony       20   0 18836  4960  3780 S  0.0  0.1  0:00.46 sshd: tony@pts/1
 1815 root       18  -2  171M  2372  1824 S  0.0  0.0  0:01.68 /usr/bin/VBoxClient --draganddrop
 8107 root       20   0  9068  3944  2680 S  0.0  0.0  0:01.29 tmux new-session -d -s PAKURI -n Main
 1811 root       20   0  171M  2372  1824 S  0.0  0.0  0:01.69 /usr/bin/VBoxClient --draganddrop
18720 root       20   0 2013M  262M  137M S  0.0  3.3  0:02.14 /usr/bin/x-www-browser
 1570 root       20   0  220M  3024  2612 S  0.0  0.0  0:00.19 /usr/sbin/VBoxService --pidfile /var/run
F1Help  F2Setup F3SearchF4FilterF5Tree  F6SortByF7Nice -F8Nice +F9Kill  F10Quit
```

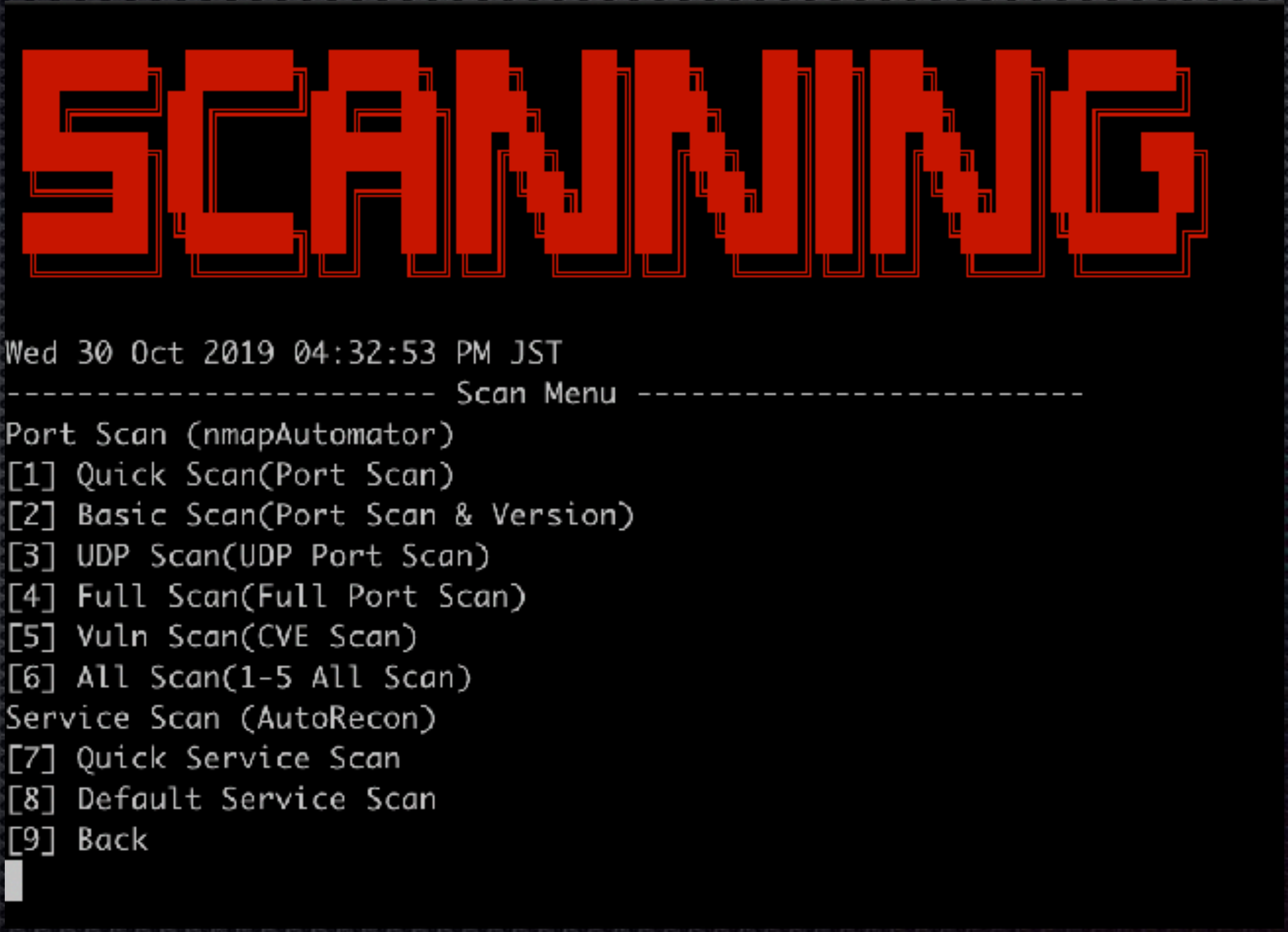
Main

- Scanning Targets
- Exploit Mode
- Config
- Docker Control
- Project Management



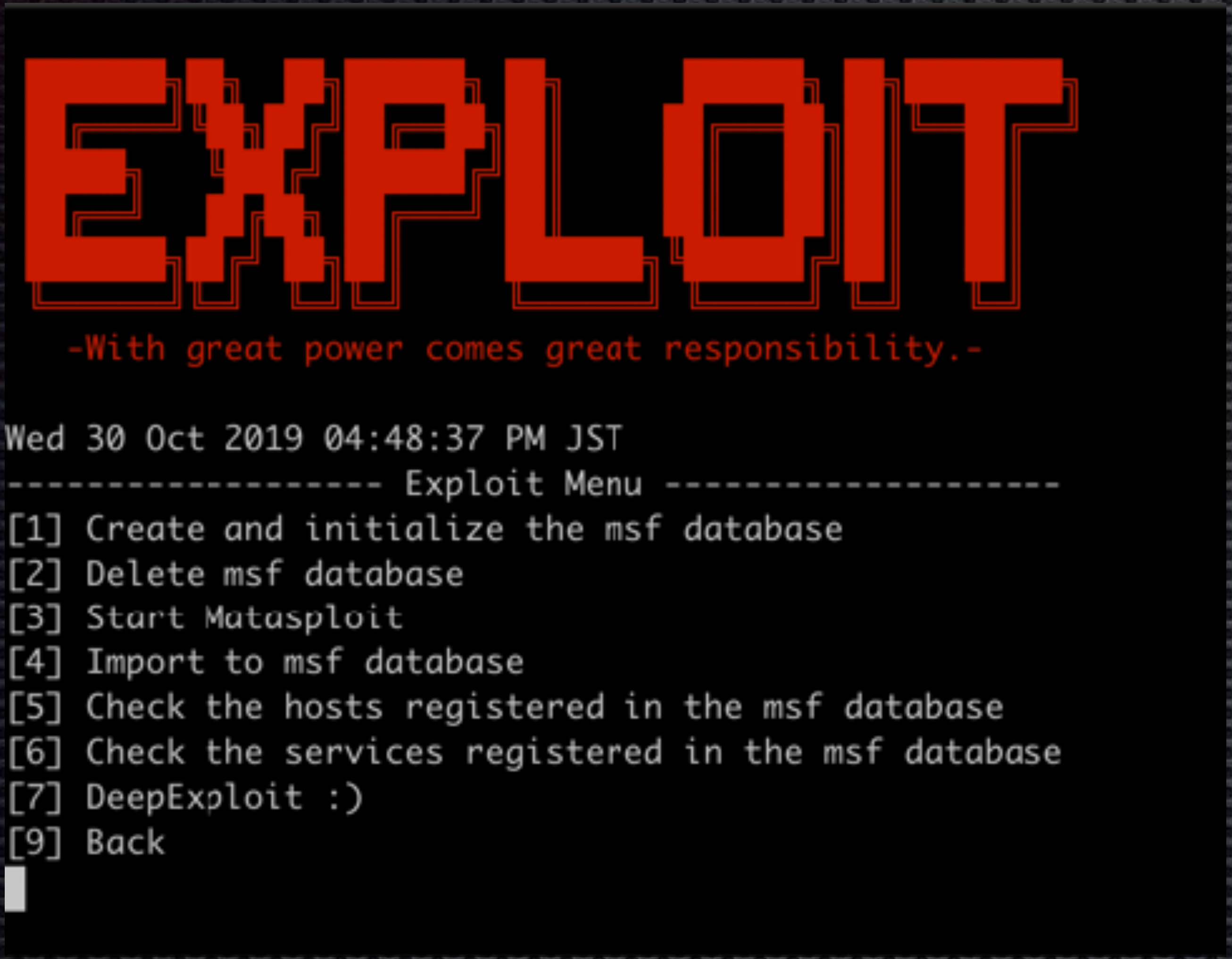
```
- Penetration Test Achive Knowledge Unite Rapid Interface -
                    inspired by CDI

                                               v0.0.1-beta
                                      Author  : Mr.Rabbit

Fri 01 Nov 2019 10:45:31 PM JST
-------------------- PAKURI Service --------------------
CodiMD        http://192.168.56.105:3000
Mattermost    http://192.168.56.105:10080
Faraday       http://192.168.56.105:5985
OpenVAS       https://192.168.56.105:9392

---------------------- Main Menu ----------------------
[1] Scanning Targets
[2] Exploit Mode
[3] Config
[4] Docker Control
[5] Project Management
[9] Exit
```

Scanning Targets

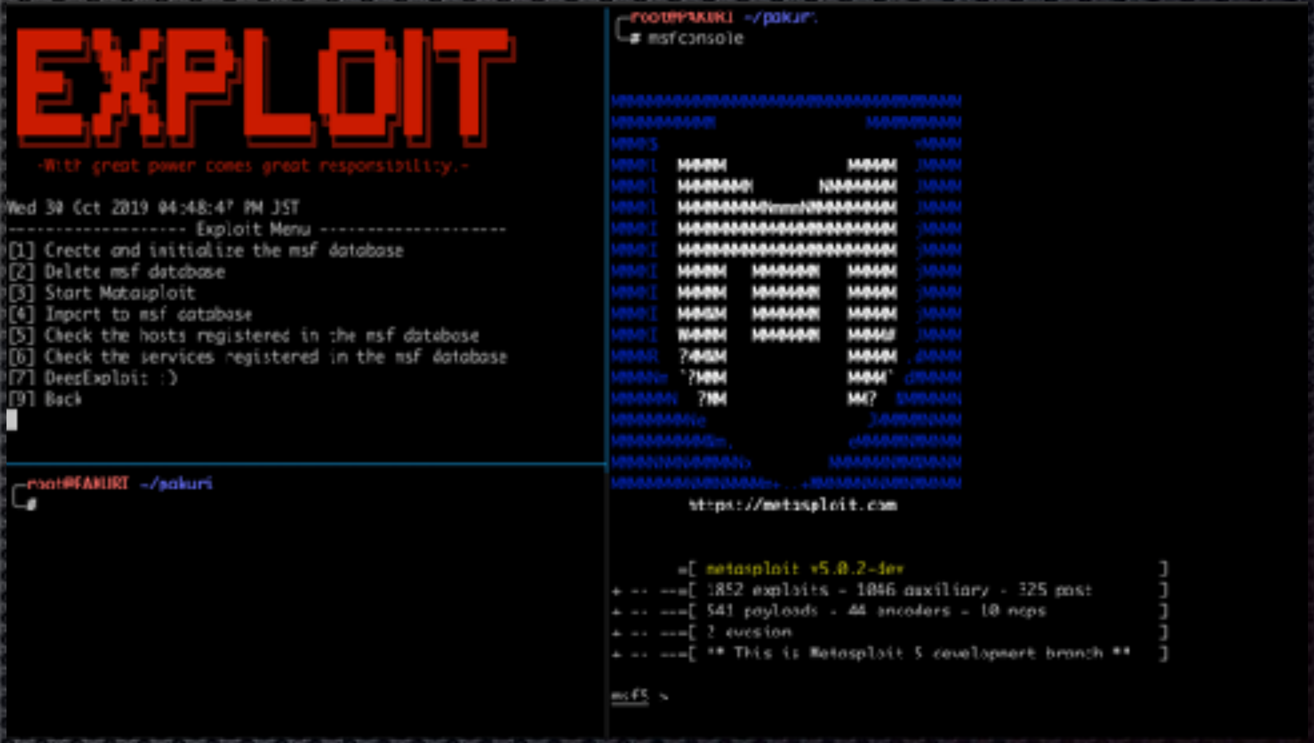


```
Wed 30 Oct 2019 04:32:53 PM JST
------------------------ Scan Menu -------------------------
Port Scan (nmapAutomator)
[1] Quick Scan(Port Scan)
[2] Basic Scan(Port Scan & Version)
[3] UDP Scan(UDP Port Scan)
[4] Full Scan(Full Port Scan)
[5] Vuln Scan(CVE Scan)
[6] All Scan(1-5 All Scan)
Service Scan (AutoRecon)
[7] Quick Service Scan
[8] Default Service Scan
[9] Back
```

Exploit Mode



```
  -With great power comes great responsibility.-

Wed 30 Oct 2019 04:48:37 PM JST
------------------- Exploit Menu --------------------
[1] Create and initialize the msf database
[2] Delete msf database
[3] Start Matasploit
[4] Import to msf database
[5] Check the hosts registered in the msf database
[6] Check the services registered in the msf database
[7] DeepExploit :)
[9] Back
```

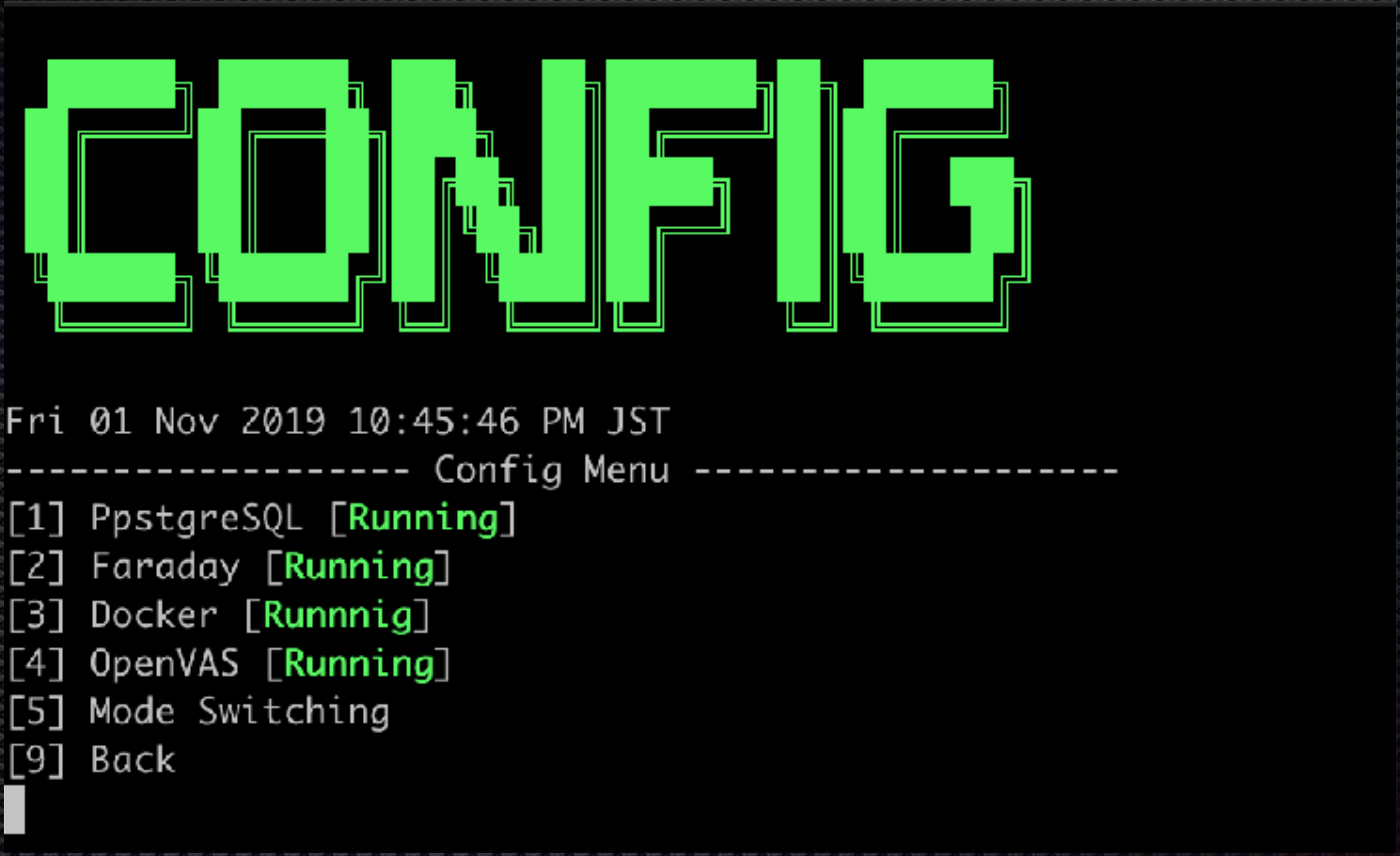


```
  -With great power comes great responsibility.-

Wed 30 Oct 2019 04:48:47 PM JST
------------------- Exploit Menu --------------------
[1] Create and initialize the msf database
[2] Delete msf database
[3] Start Matasploit
[4] Import to msf database
[5] Check the hosts registered in the msf database
[6] Check the services registered in the msf database
[7] DeepExploit :)
[9] Back
```

```
┌─root@FAKURI ~/pakuri
└─#
```

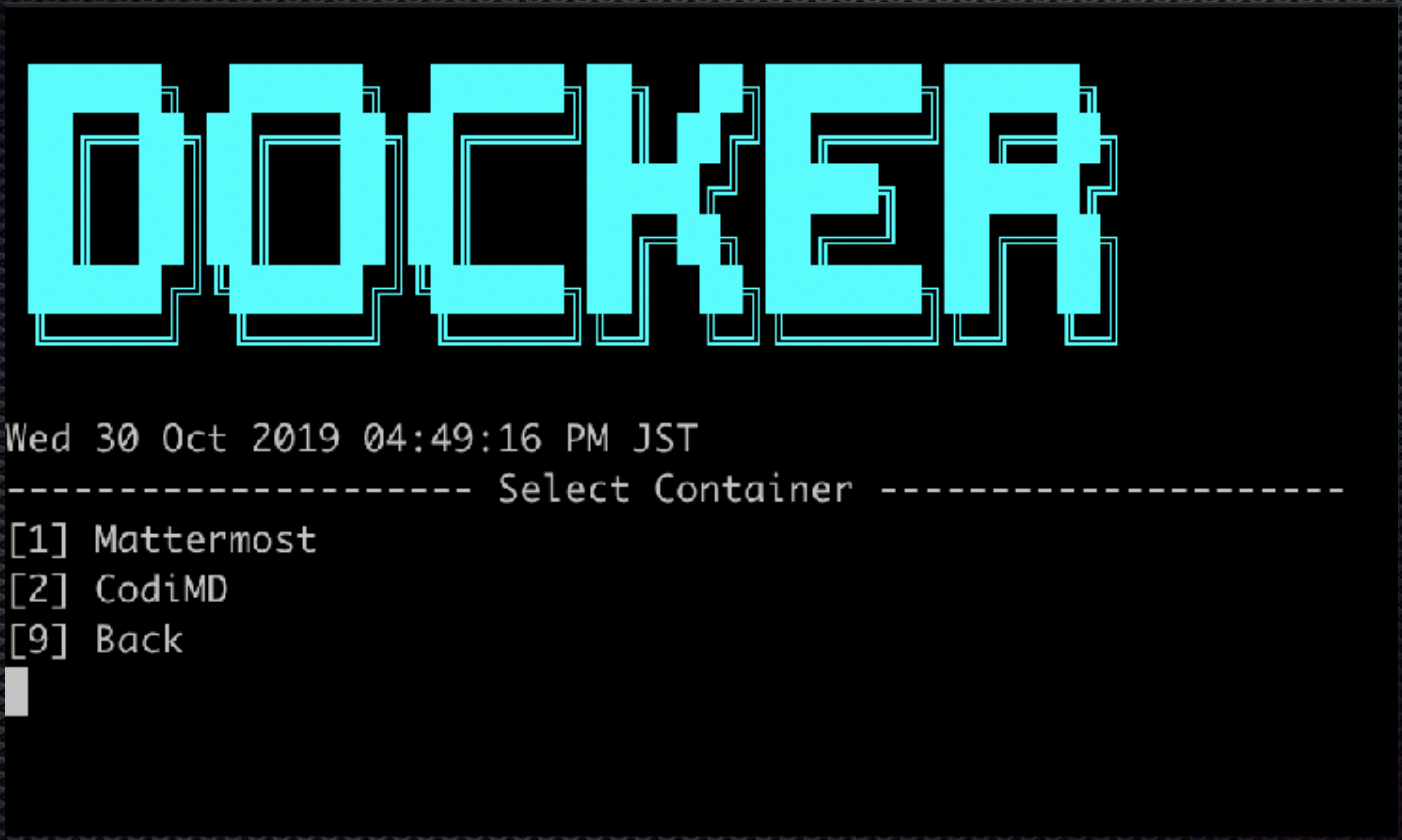
```
┌─root@FAKURI ~/pakuri
└─# msfconsole

         https://metasploit.com


       =[ metasploit v5.0.2-dev                          ]
+ -- --=[ 1852 exploits - 1046 auxiliary - 325 post      ]
+ -- --=[ 541 payloads - 44 encoders - 10 nops           ]
+ -- --=[ 2 evasion                                      ]
+ -- --=[ ** This is Metasploit 5 development branch **  ]

msf5 >
```

Config



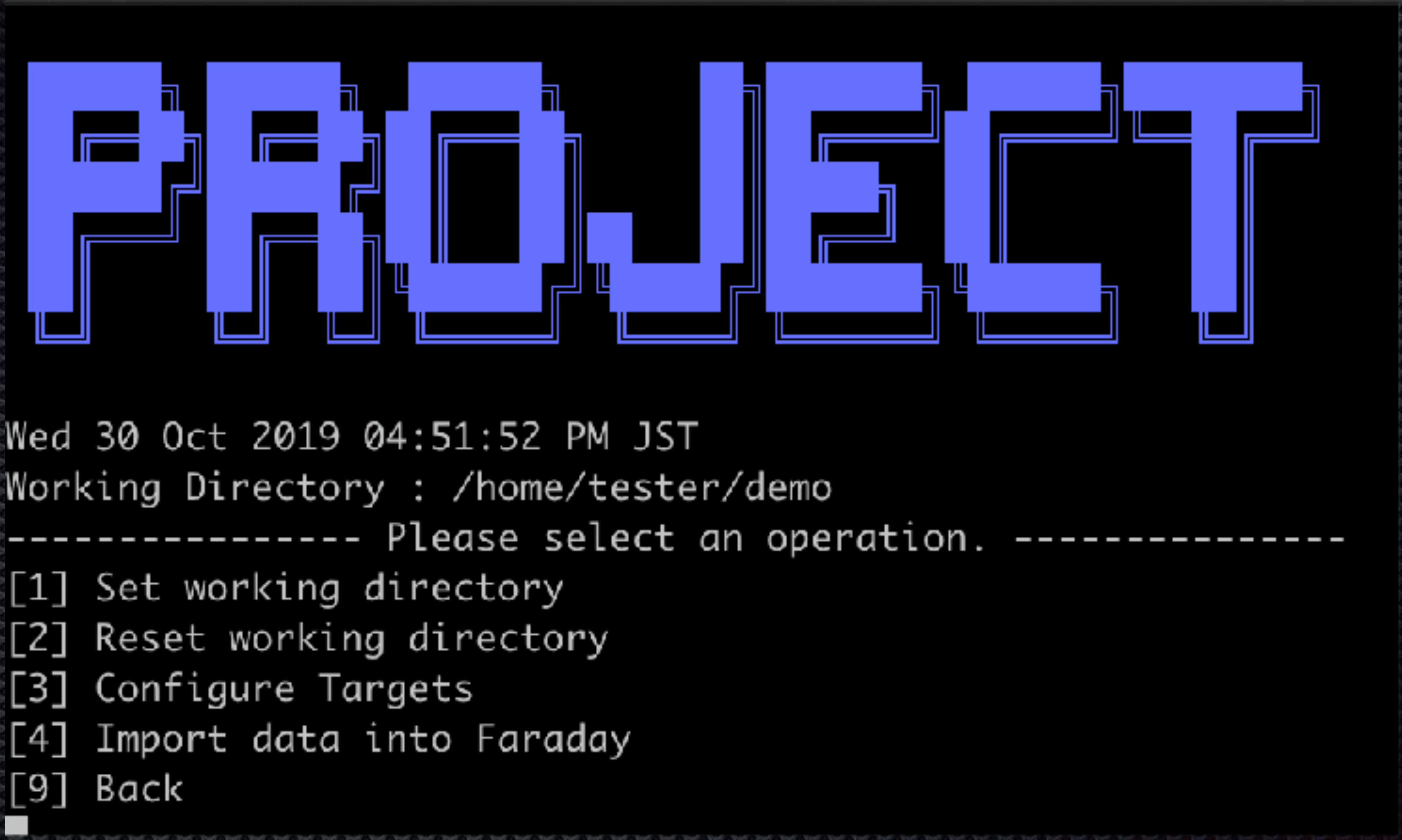
```
CONFIG

Fri 01 Nov 2019 10:45:46 PM JST
------------------- Config Menu --------------------
[1] PpstgreSQL [Running]
[2] Faraday [Running]
[3] Docker [Runnnig]
[4] OpenVAS [Running]
[5] Mode Switching
[9] Back
```

Docker Control



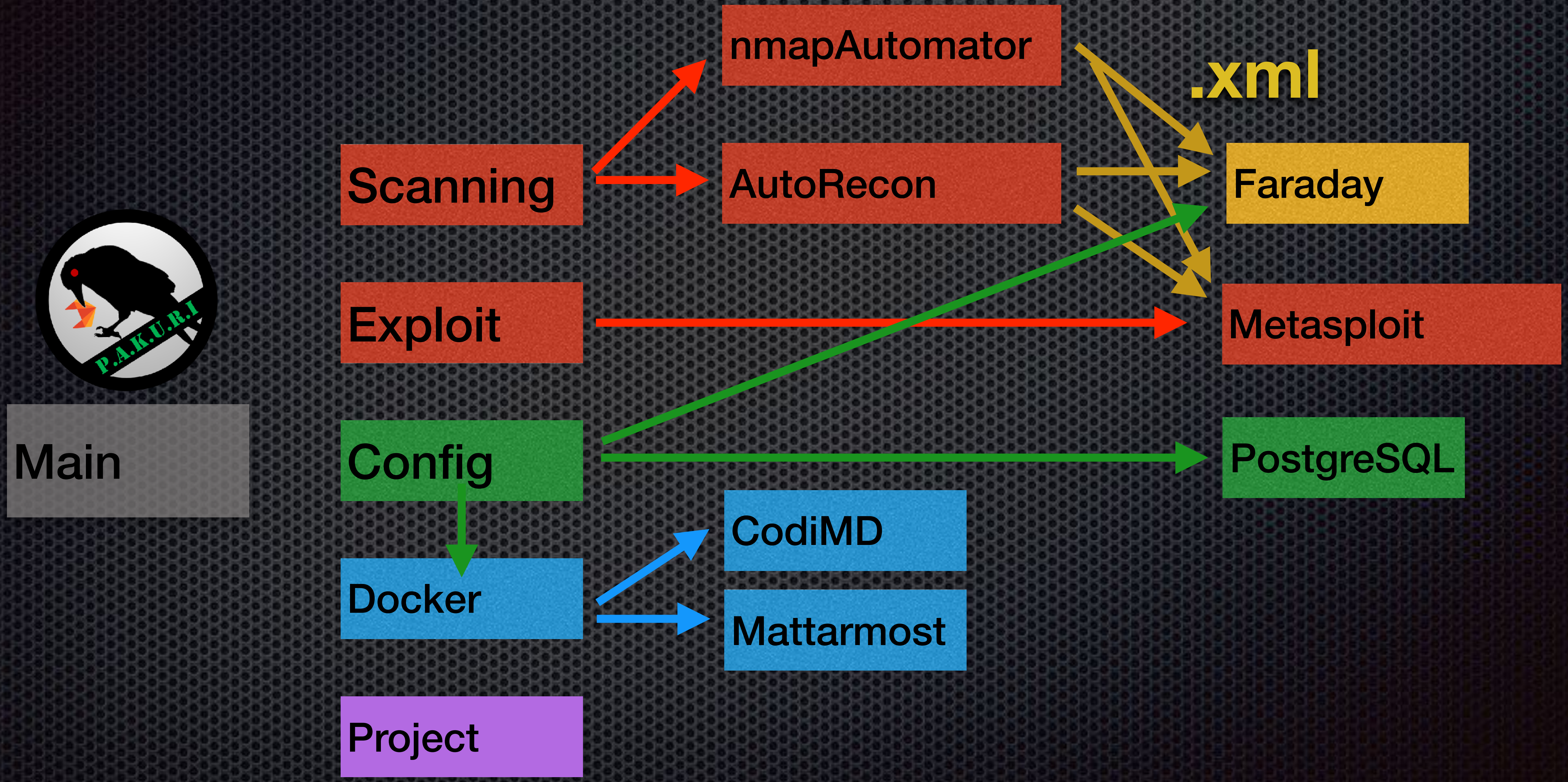
```
Wed 30 Oct 2019 04:49:16 PM JST
--------------------- Select Container ---------------------
[1] Mattermost
[2] CodiMD
[9] Back
```

Project Management

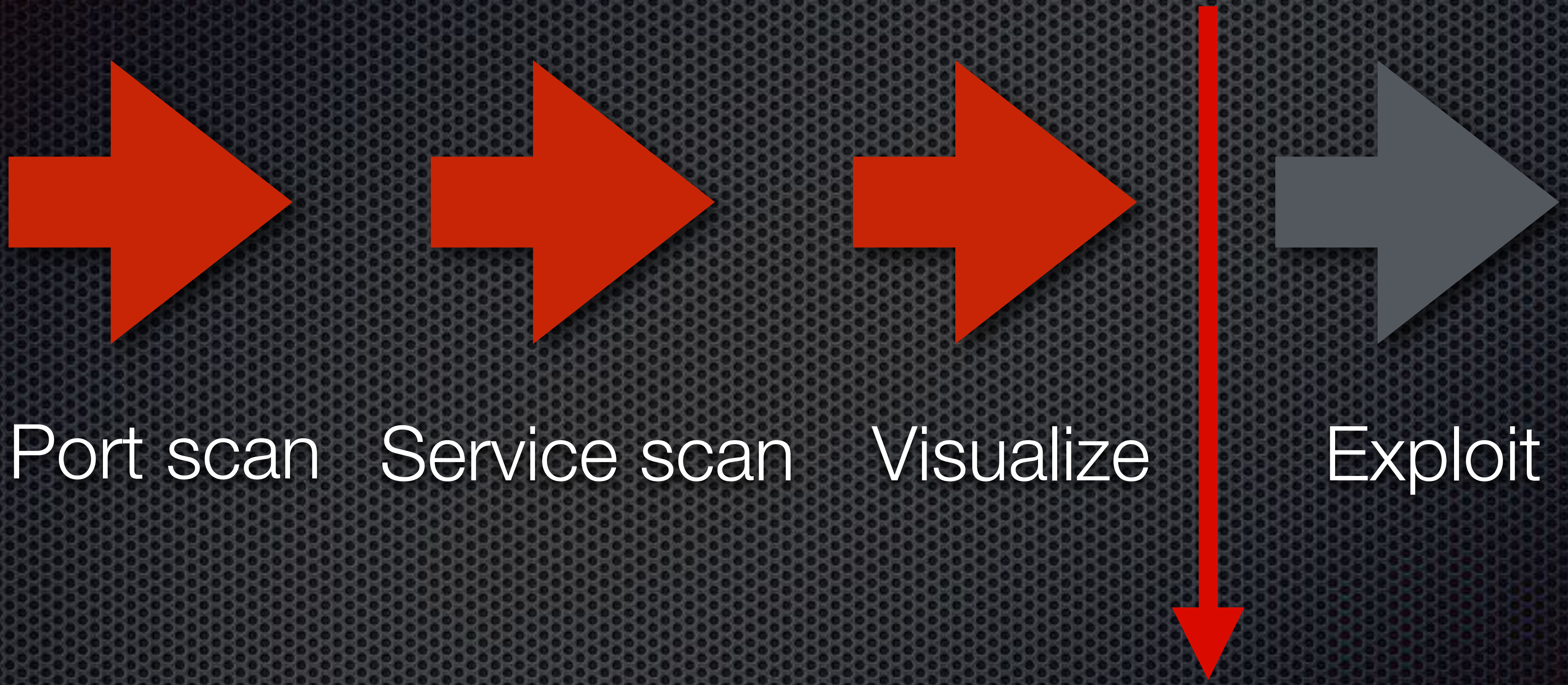


```
Wed 30 Oct 2019 04:51:52 PM JST
Working Directory : /home/tester/demo
---------------- Please select an operation. ---------------
[1] Set working directory
[2] Reset working directory
[3] Configure Targets
[4] Import data into Faraday
[9] Back
```

System overview

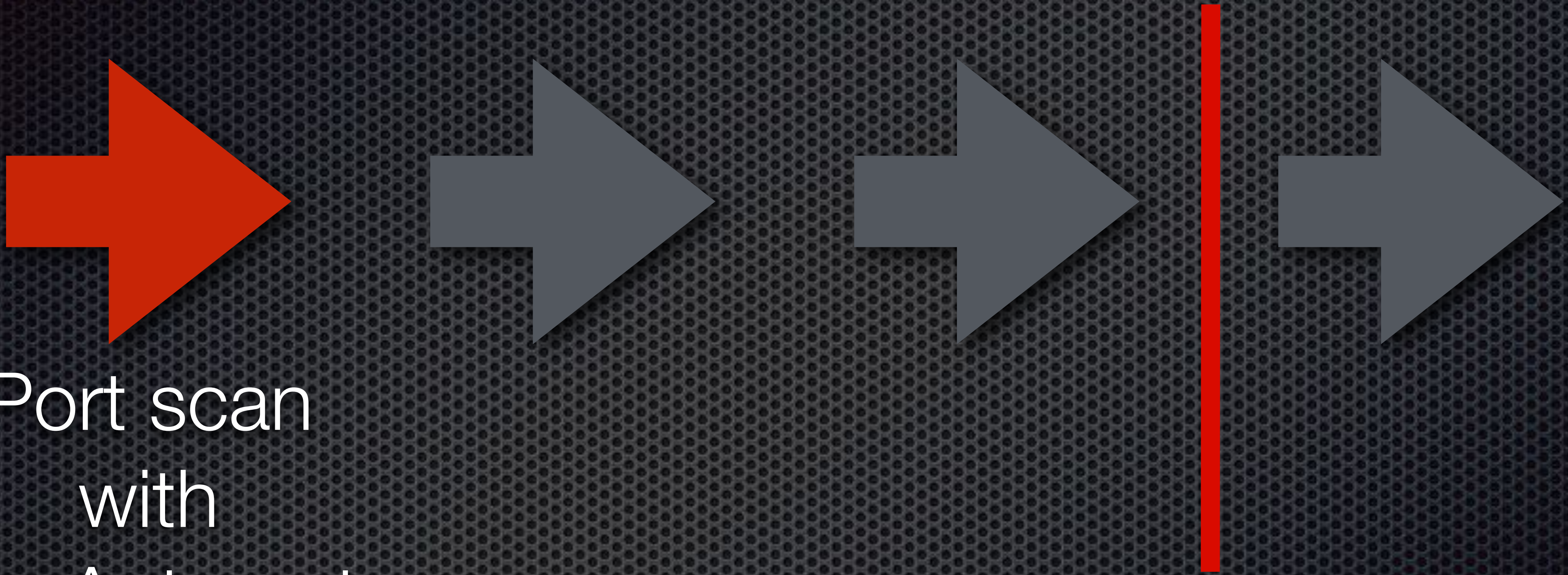


Flow



Scan ports and services, visualize results.
To this point, I want to support with PAKURI.

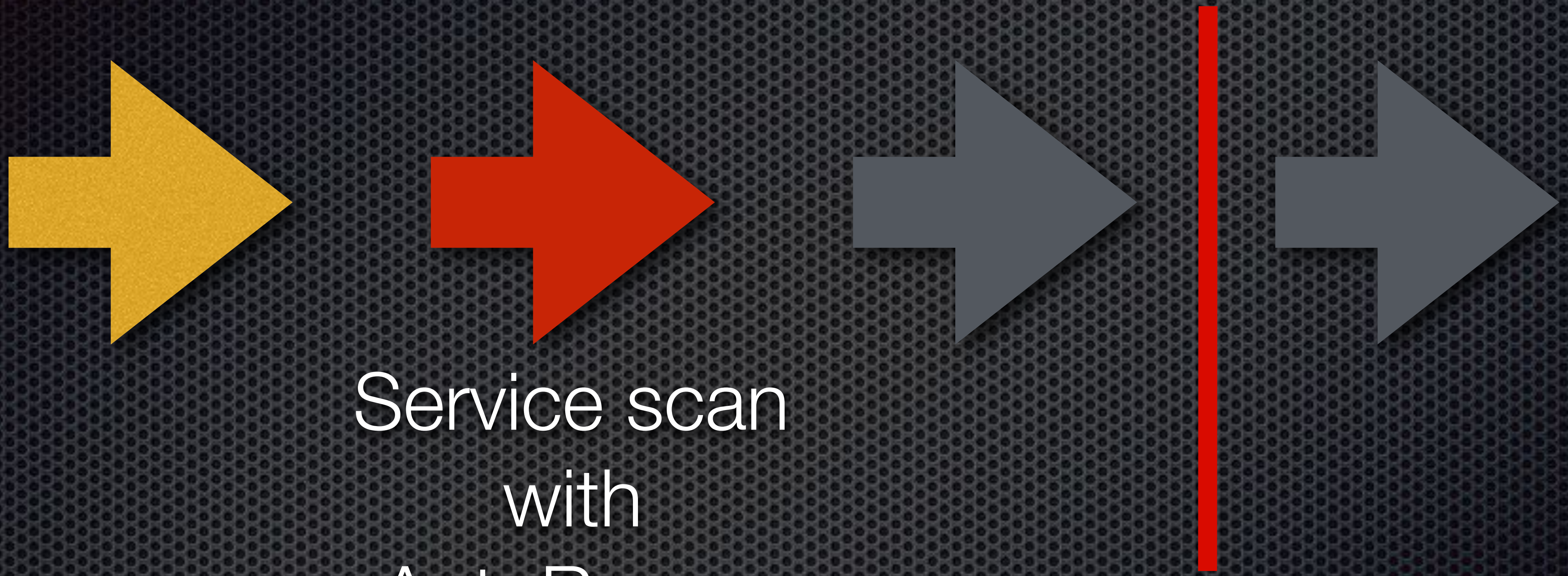
Flow



Port scan
with
nmapAutomator

There are many tools for port scanning.
Use the most convenient nmapAutomator.

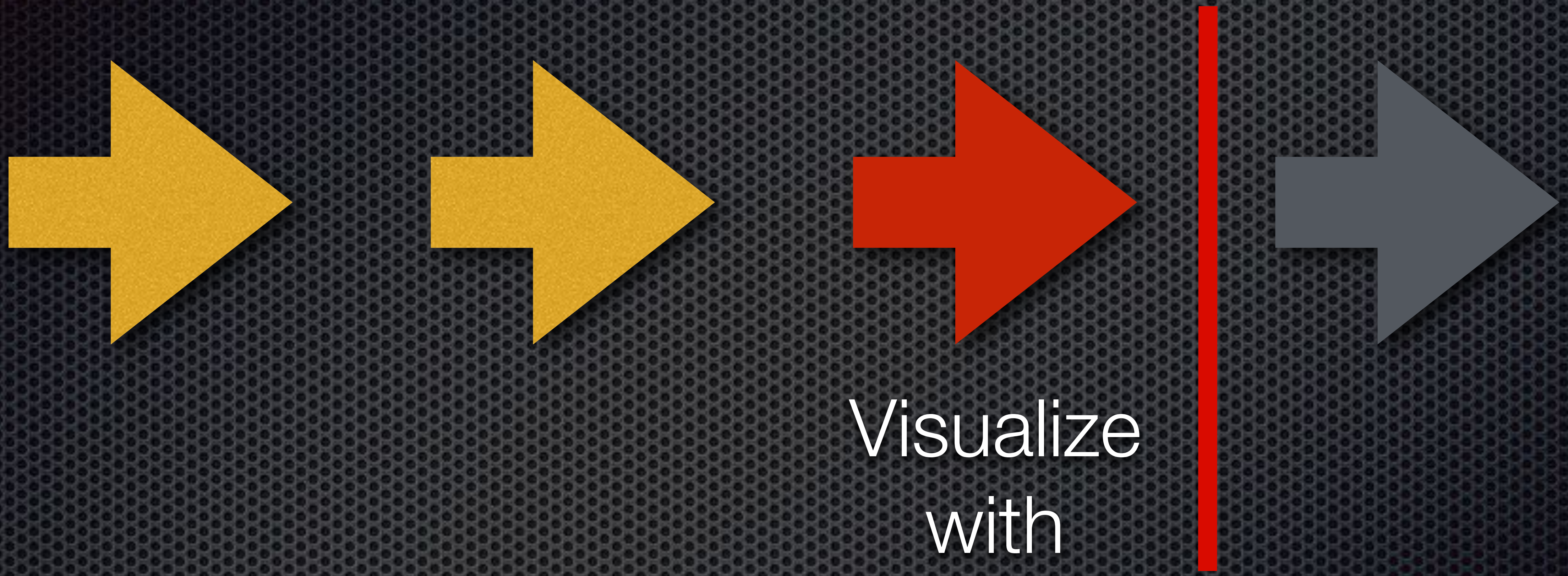
Flow



Service scan with AutoRecon

Service scans are more complex and more diverse than port scans. Scan support using AutoRecon.

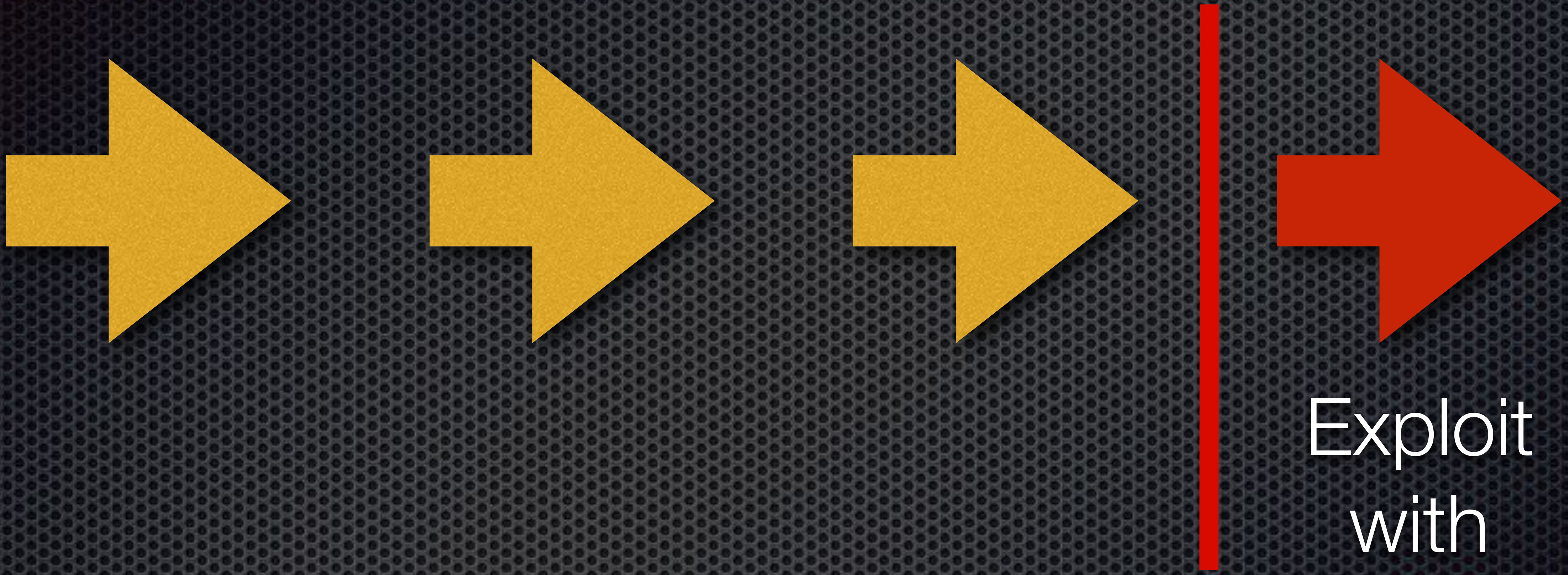
Flow



Visualize with Faraday

Only the resulting text-based data can miss important points.

Flow (extra)



Exploit
with
Metasploit

Visualization makes it easier to find prominent vulnerabilities. This makes it easy to exploit.

Summary

- Beginner
  - You should do your best without fear.
- Senior
  - Leave tasks that can be automated to beginners.
- Manager
  - Use visualization to make accurate decisions.

Thank you!

Please give me advice and feedback.

@PAKURI9
@01ra66it

pakuri.pentest@gmail.com