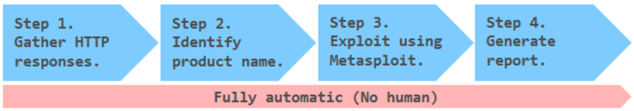
GyoiThon

- Next generation penetration test tool for the Web Server -

Isao Takaesu Masuya Masafumi Toshitsugu Yoneyama
Mitsui Bussan Secure Directions, Inc.

1. Overview

GyoiThon is a **growing penetration test tool using Machine Learning**. GyoiThon **identifies the software installed on web server** (OS, Middleware, Framework, CMS, etc...) based on the learning data. After that, it **executes valid exploits** for the identified software using Metasploit. Finally, it **generates reports** of scan results. GyoiThon executes the above processing **automatically**.



User's operation only inputs the top URL of the target web server in GyoiThon. You can identify vulnerabilities of the web servers without taking time and effort.

2. Processing flow

Step1. Gather HTTP responses.

GyoiThon gathers several HTTP responses of target website while **crawling**.

The following are example of HTTP responses gathered by GyoiThon.

```
HTTP/1.1 200 OK
Date: Tue, 06 Mar 2018 06:56:17 GMT
Content-Type: text/html; charset=UTF-8
Set-Cookie: f00e68432b68050dee9abe33c389831e=0eba9c
d0f75ca0912b4849777677f587; path=/;
Content-Length: 37496
```

Example 1

```
HTTP/1.1 200 OK
Date: Tue, 06 Mar 2018 04:19:19 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 11819

 ...snip...

<script src="/core/drupal.js?v=8.3.1"></script>
```

Example 2

Step2. Identify product name.

GyoiThon identify product name installed on web server using **two methods**.

<Based on Machine Learning>

By using Machine Learning (**Naive Bayes**), GyoiThon identifies software based on a **combination of slightly different features** of each software (Apache, Joomla!, TYPO, Drupal etc.,). Naive Bayes learns using the training data. Unlike the signature base, Naive Bayes is stochastically identified based on various features included in HTTP response when it cannot be identified software in one feature.

```
Set-Cookie: f00e68432b68050dee9abe33c389831e=0eba9cd0
f75ca0912b4849777677f587;
```

Example 1

GyoiThon can identify the CMS **Joomla!**.
This is because GyoiThon learns features of Joomla! such as "**Cookie name** (f00e6 ... 9831e)" and "**Cookie value** (0eba9 ... 7f587). In our survey, Joomla! uses **32 lower case letters as the Cookie name and Cookie value** in many cases.

```
Joomla!@(Set-Cookie: [a-z0-9]{26,32}=.*);
Joomla!@(Set-Cookie: .*=[a-z0-9]{26,32});
Word Press@(X-Pingback):.*xmlrpc.php[¥r¥n]
Word Press@(<body class=["']home ).*
```

Training data (one example)

<Based on String matching>

Of course, GyoiThon can identify software by **string matching** also used in traditional penetration test tools. Examples are shown below.

```
<script src="/core/drupal.js?v=8.3.1"></script>
```

Example 2

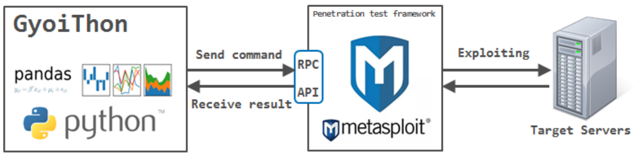
GyoiThon can identify the CMS **Drupal**.
It is very easy.

```
Drupal@(drupal¥.js¥?v=¥d¥.¥d¥.¥d)
Word Press@<.*=(.*/wp-).*/.*>
```

String matching pattern (one example)

Step3. Exploit using Metasploit.

GyoiThon executes exploit corresponding to the identified software using Metasploit. And it checks whether the software is affected by the vulnerability.

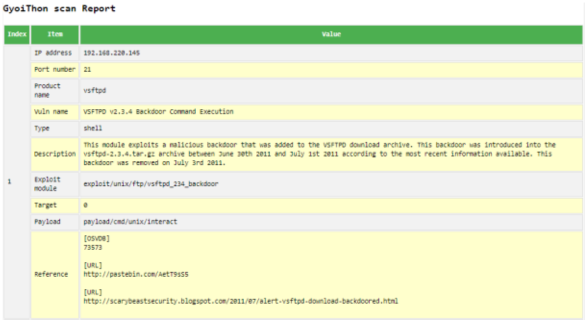


```
[*] exploit/multi/http/joomla_http_header_rce, target:
0, payload: generic/shell_reverse_tcp, result: failure
[*] exploit/multi/http/joomla_http_header_rce, target:
0, payload: php/bind_perl, result: failure

...snip...

[*] exploit/unix/webapp/joomla_akeeba_unserialize,
target: 0, payload: generic/shell_reverse_tcp, result:
failure
[*] exploit/unix/webapp/joomla_akeeba_unserialize,
target: 0, payload: php/bind_perl, result: bingo!!
```

Running sample

Step4. Generate scan report.

GyoiThon generates a report that summarizes vulnerabilities.



GyoiThon scan Report

Index	Item	Value
1	IP address	192.168.220.145
	Port number	21
	Product name	vsftpd
	Vuln name	VSFTPD v2.3.4 Backdoor Command Execution
	Type	shell
	Description	This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.
	Exploit module	exploit/unix/ftp/vsftpd_234_backdoor
	Target	0
	Payload	payload/cmd/unix/interact
	Reference	[OSVDB] 73573 [URL] http://pastebin.com/AetT9sS5 [URL] http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

Sample report

3. Demonstration

```
msf >
msf > load msgrpc ServerHost=192.168.16.148 ServerPort=55553 User=test Pass=test1234
[*] MSGRPC Service:  192.168.16.148:55553
[*] MSGRPC Username: test
[*] MSGRPC Password: test1234
[*] Successfully loaded plugin: msgrpc
msf >
```

https://youtu.be/jmi43eZOE9w

More information / Source code

https://github.com/gyoisamurai/GyoiThon

Contact us

➢ Isao Takaesu
gyoiler3@gmail.com
https://twitter.com/bbr_bbq

About MBSD

Mitsui Bussan Secure Directions, Inc. is a leading Japanese provider of IT security solutions. We offer a wide range of solutions including vulnerability assessment, incident response, cyber training and managed security service.

https://www.mbsd.jp/en/