GyoiThon

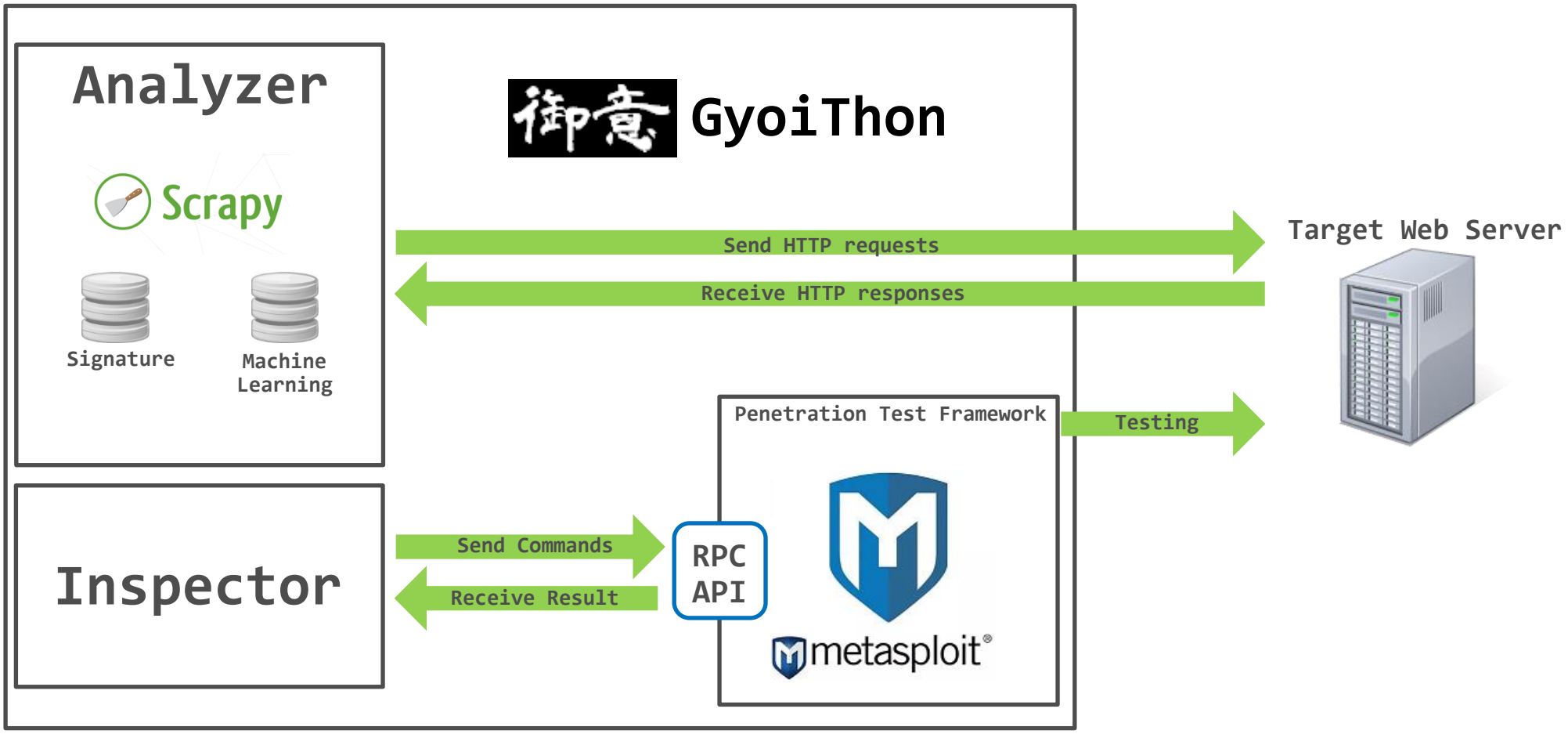
- Fully automated penetration test tool for Web Server -

August 12th,2018

DEFCON26! DEMO LABS

Presented by MBSD

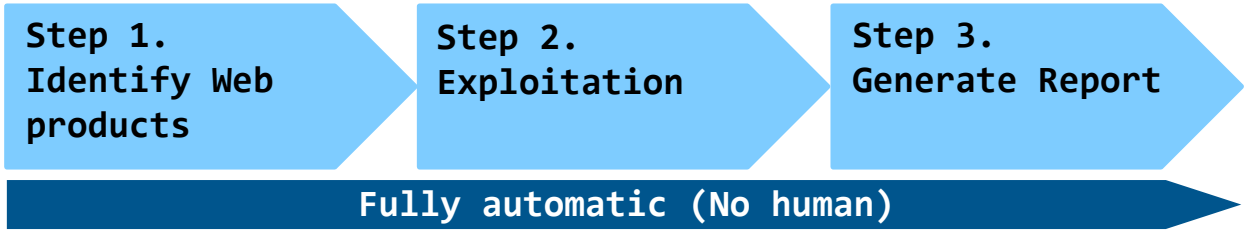
Overview



Analyzer : **Identify Web products name** using Sig + ML.

Inspector : **Execute exploit** the identified Web products.

Processing Flow

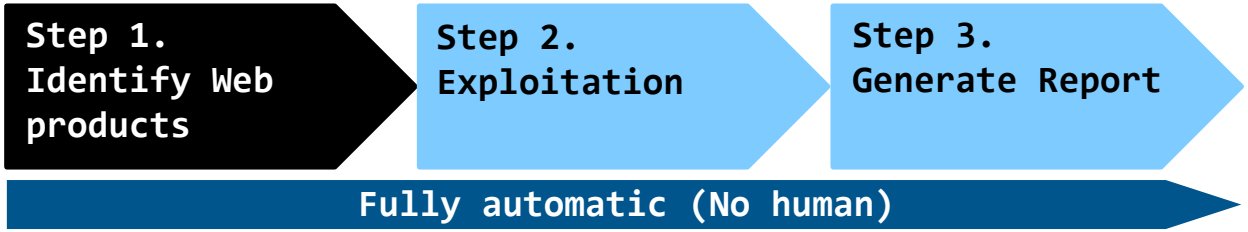


Step 1. Identify Web products

Step 2. Exploitation

Step 3. Generate Report

Processing Flow



Step 1. Identify Web products

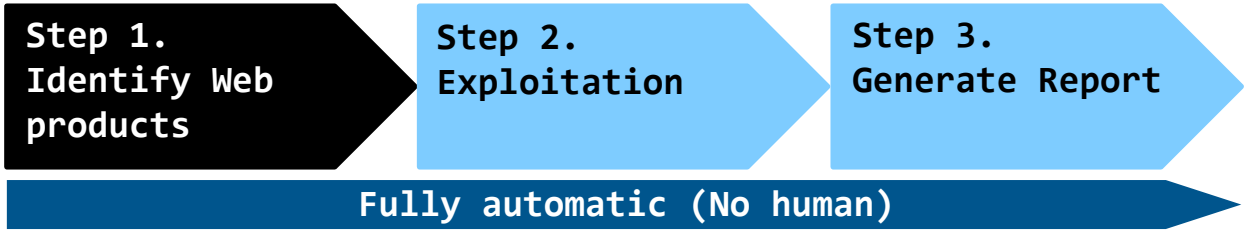
- Gather the HTTP responses by Web crawling.
- Identify the WEB products by **Signature** (Pattern Matching).
- Identify the WEB products by **Machine Learning**.

Step 2. Exploitation

Step 3. Generate Report

Identify Web products using Signature + Machine Learning.

Question



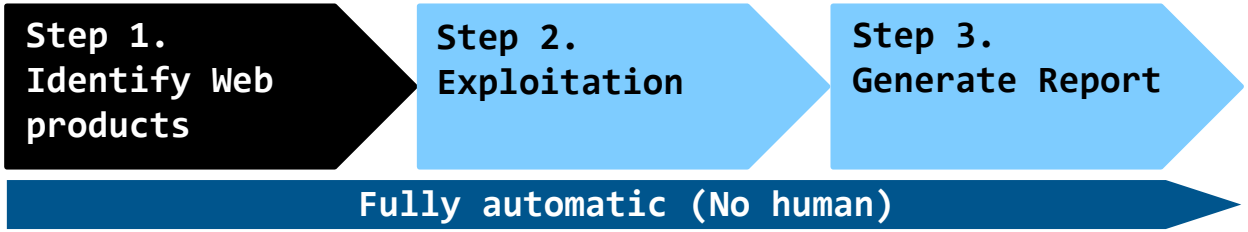

```
HTTP/1.1 200 OK
Date: Tue, 06 Mar 2018 06:56:17 GMT
Server: OpenSSL/1.0.1g
Content-Type: text/html; charset=UTF-8
Set-Cookie: f00e68432b68050dee9abe33c389831e=0eba9cd0f75ca0912b4849777677f
587;  path=/;
Content-Length: 37496
Etag: "409ed-183-53c5f732641c0"

…snip…

<form action="/example/confirm.php">
```

What are included the Web products in this HTTP response?

Answer



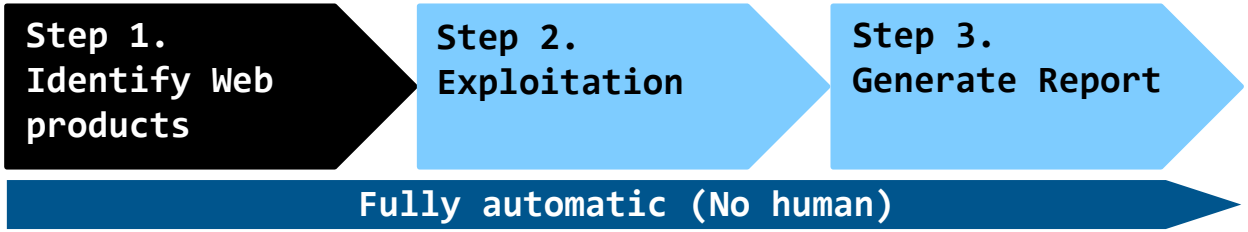

```
HTTP/1.1 200 OK
Date: Tue, 06 Mar 2018 06:56:17 GMT
Server: OpenSSL/1.0.1g
Content-Type: text/html; charset=UTF-8
Set-Cookie: f00e68432b68050dee9abe33c389831e=0eba9cd0f75ca0912b4849777677f
587;  path=/;
Content-Length: 37496
Etag: "409ed-183-53c5f732641c0"

…snip…

<form action="/example/confirm.php">
```

Identify **OpenSSL** and **PHP** using **Signature.**

Answer



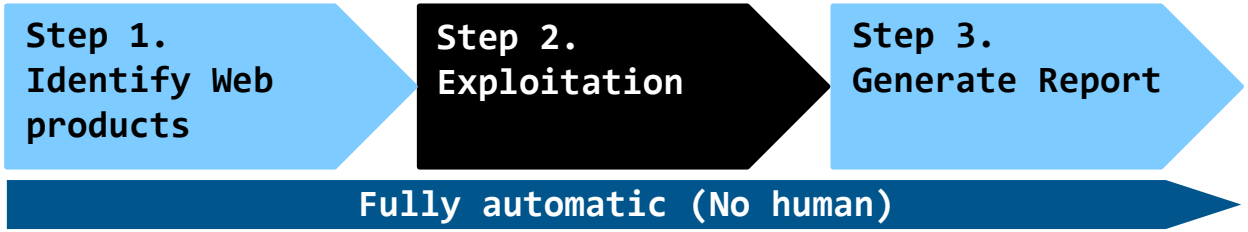

```
HTTP/1.1 200 OK
Date: Tue, 06 Mar 2018 06:56:17 GMT
Server: OpenSSL/1.0.1g
Content-Type: text/html; charset=UTF-8
Set-Cookie: f00e68432b68050dee9abe33c389831e=0eba9cd0f75ca0912b4849777677f
587;  path=/;
Content-Length: 37496
Etag: "409ed-183-53c5f732641c0"

…snip…

<form action="/example/confirm.php">
```

Identify **joomla!** and **Apache** using **Machine Learning.**

Processing Flow



Step 1. Identify Web products

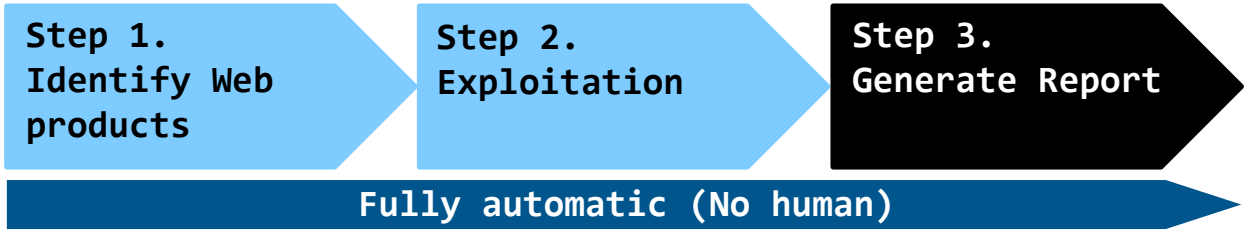
Step 2. Exploitation

- **Execute exploit** the identified Web products.
- **Open session** between **"GyoiThon" and target Web server**.

Step 3. Generate Report

Open session between "GyoiThon" and target Web server.

Processing Flow



Step 1. Identify Web products

Step 2. Exploitation

Step 3. Generate Report

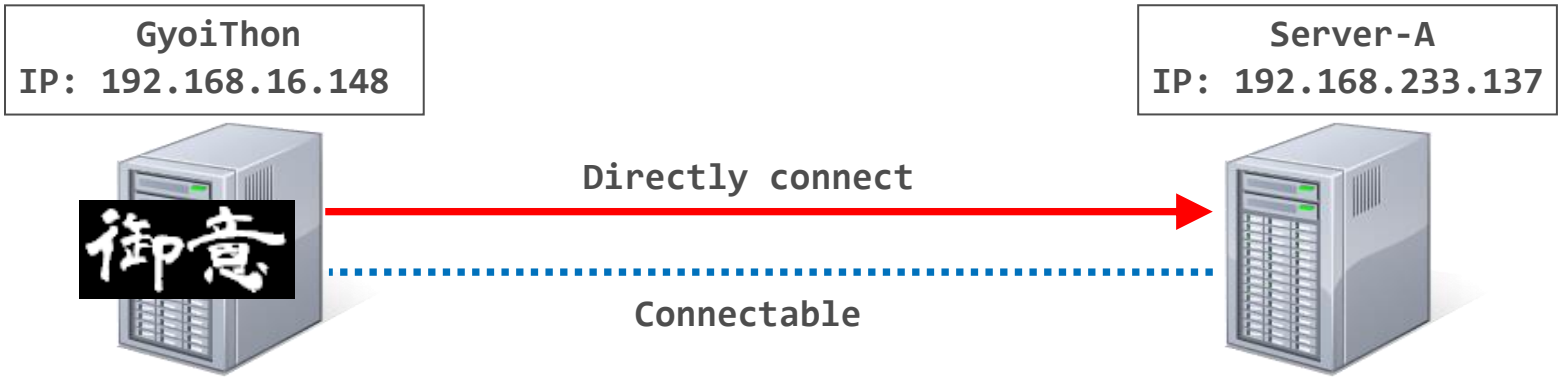
- **Create the report.**

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

Demonstration

Scenario. Single target server



・Demo movie

https://youtu.be/jmi43eZOE9w

Resource

- Source codes & Usage

https://github.com/gyoisamurai/GyoiThon

Who we are

Company	:	MBSD - Mitsui Bussan Secure Directions, Inc.
Established	:	2001
Head office	:	Tokyo, Japan
Paid in capital	:	JPY 400 Mil (100% subsidiary of Mitsui & Co., Ltd)
Employees	:	256
Industry affiliations	:	Leading companies in Japan, such as telecoms, banks, retailers, internet business, and the governments.
Businesses	:	Professional security services to protect business from cyber attacks.
Services	:	Vulnerability Assessment/Penetration test (Web/NW/IoT..) Managed Security Services, Incident Response & Handling, GRC Consulting, Research & Development.

THANK YOU!

Reference all source codes and document:
https://github.com/gyoisamurai/GyoiThon