

# Deep Exploit

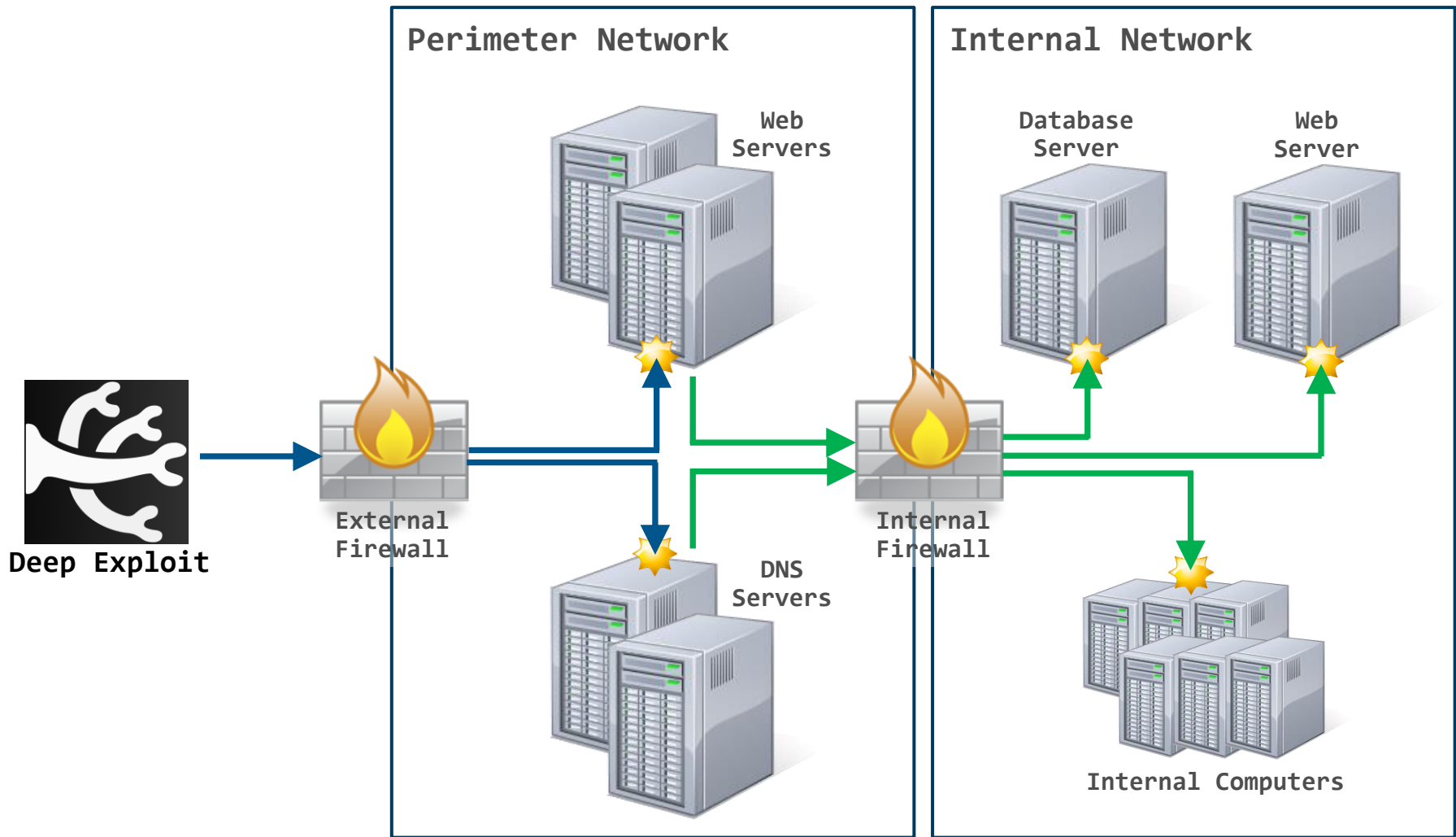
- Fully automated penetration test tool -

August 9<sup>th</sup>, 2018

Black Hat USA 2018 Arsenal

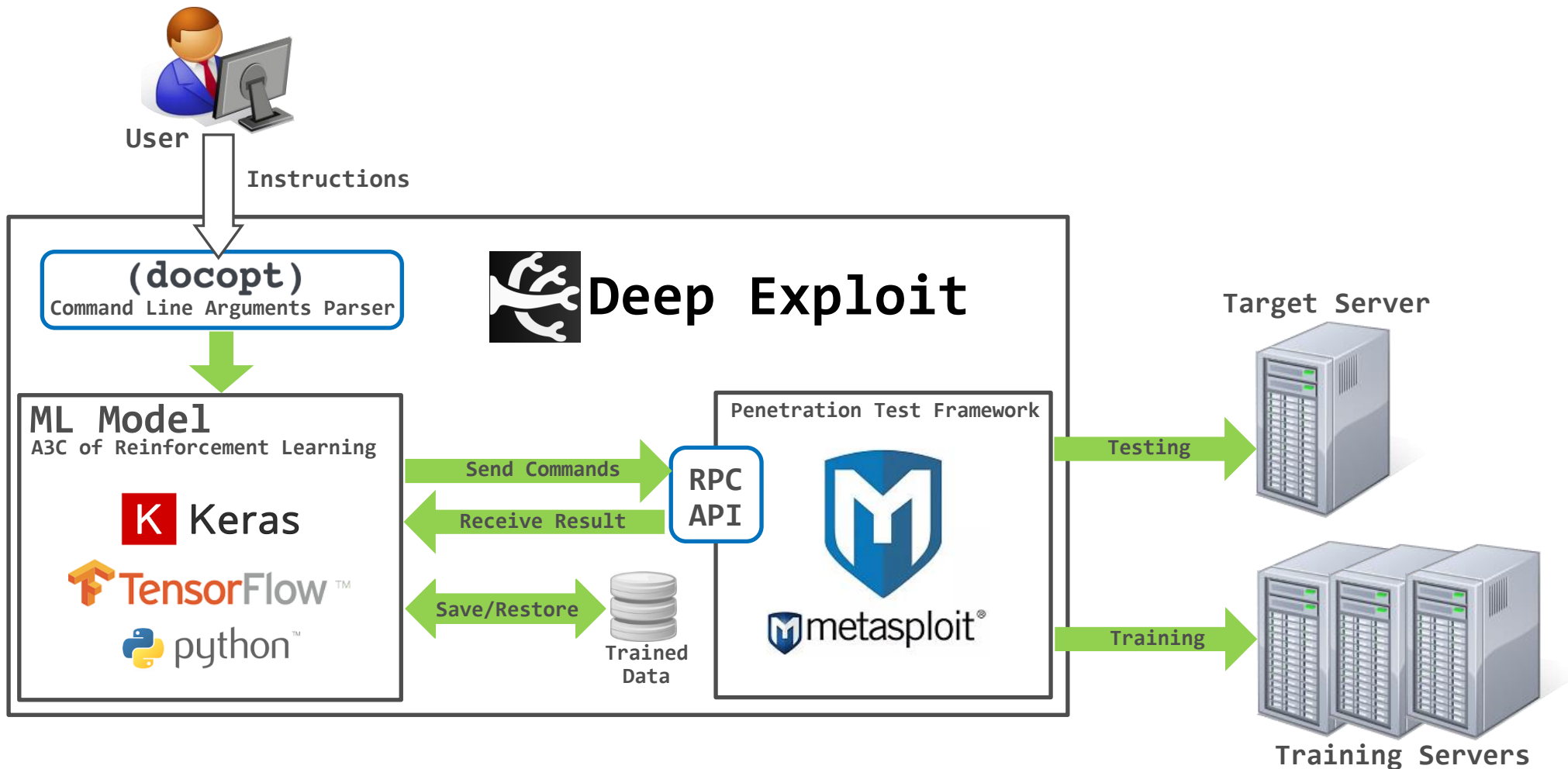
Presented by Isao Takaesu

# What is Deep Exploit?



Exploiting the servers on perimeter & internal networks.

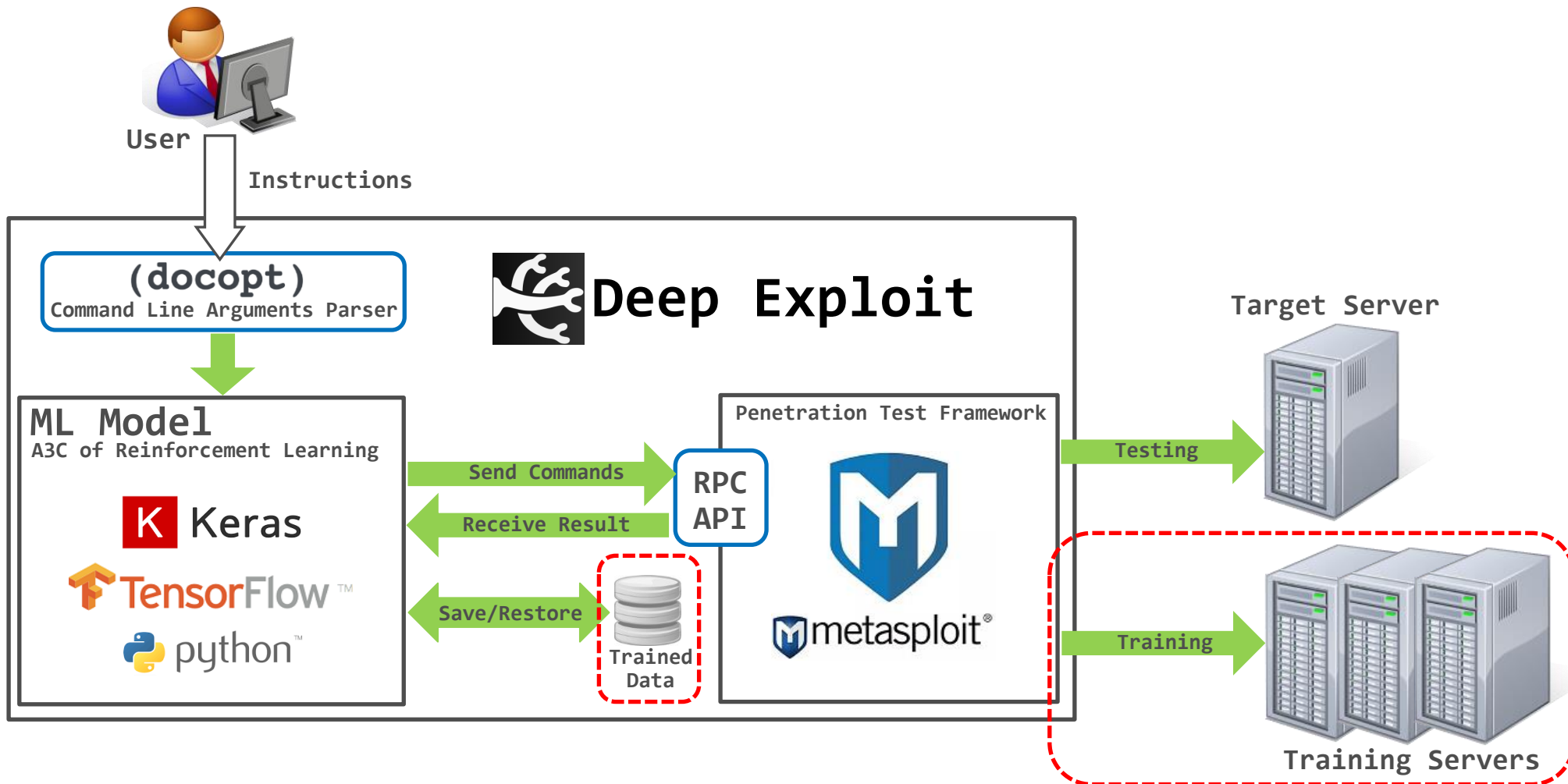
# Overview



**Train** : **Train** how to exploitation by itself.

**Test** : **Execute the exploit** using trained data.

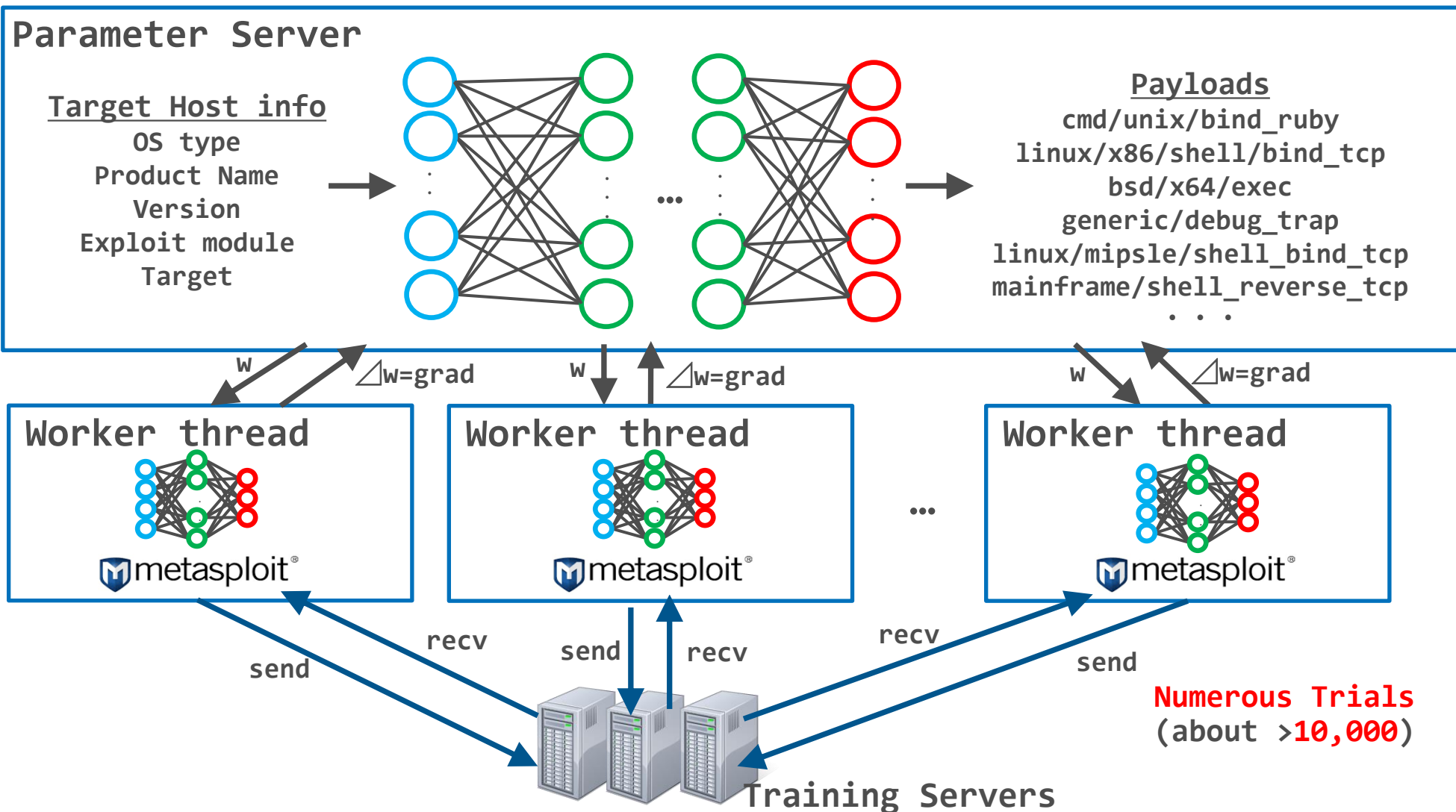
# Overview



**Train : Train how to exploitation by itself.**

**Test : Execute the exploit using trained data.**

# Train the Deep Exploit



Learn how to exploitation while trying numerous exploits.

# Training Movie

~~~~~

postfix exploit/linux/misc/gld\_postfix payload/linux/x86/shell\_bind\_tcp shell

```
[*] 1233/10000 : 009/020 local_thread7 reward:-1 failure 192.168.220.145 (tcp/80:3) unix | unix/webapp/flashchat_upload_exec | php/meterpreter/bind_tcp_uuid | 0
[+] Update LocalBrain weight to ParameterServer.
[*] 1235/10000 : 002/020 local_thread9 reward:-1 failure 192.168.220.145 (tcp/6667) irc | multi/misc/legend_bot_exec | cmd/unix/bind_awk | 0
[*] 1236/10000 : 009/020 local_thread2 reward:-1 failure 192.168.220.145 (tcp/5432) postgresql | linux/postgres/postgres_payload | linux/x86/shell_bind_tcp | 0
[+] Update LocalBrain weight to ParameterServer.
[*] 1238/10000 : 004/020 local_thread8 reward:-1 failure 192.168.220.145 (tcp/6667) irc | multi/misc/xdh_x_exec | cmd/unix/bind_awk | 0
[+] Update LocalBrain weight to ParameterServer.
[*] 1238/10000 : 000/020 local_thread10 reward:-1 failure 192.168.220.145 (tcp/2121) proftpd | linux/ftp/proftpd_sreplace | linux/x86/shell_bind_tcp | 0
[*] 1239/10000 : 011/020 local_thread1 reward:-1 failure 192.168.220.145 (tcp/23) telnet | linux/telnet/telnet_encrypt_keyid | linux/x86/shell_bind_tcp | 1
[*] 1232/10000 : 009/020 local_thread3 reward:-1 failure 192.168.220.145 (tcp/53) bind | windows/antivirus/trendmicro_serverprotect_createbinding | generic/custom | 0
[+] Update LocalBrain weight to ParameterServer.
[*] 1229/10000 : 003/020 local_thread4 reward:10 bingo!! 192.168.220.145 (tcp/25) postfix | linux/misc/gld_postfix | linux/x86/shell_bind_tcp | 0
[+] Update LocalBrain weight to ParameterServer.
[*] Thread: local_thread4, Trial num: 6, Step: 4, Avg step: 8.9
[*] 1240/10000 : 002/020 local_thread5 reward:-1 failure 192.168.220.145 (tcp/80:1) apache | linux/http/apache_continuum_cmd_exec | linux/x86/shell_bind_tcp | 0
```

~~~~~

**BINGO!!!**

~~~~~

vsftpd exploit/unix/ftp/vsftpd\_234\_backdoor payload/cmd/unix/interact shell

```
[*] 1241/10000 : 010/020 local_thread7 reward:-1 failure 192.168.220.145 (tcp/80:3) unix | unix/webapp/flashchat_upload_exec | php/meterpreter/bind_tcp_uuid | 0
[*] 1242/10000 : 003/020 local_thread9 reward:-1 failure 192.168.220.145 (tcp/6667) irc | multi/misc/legend_bot_exec | cmd/unix/bind_awk | 0
[*] 1243/10000 : 010/020 local_thread2 reward:-1 failure 192.168.220.145 (tcp/5432) postgresql | linux/postgres/postgres_payload | linux/x86/shell_bind_tcp | 0
[*] 1244/10000 : 005/020 local_thread8 reward:-1 failure 192.168.220.145 (tcp/6667) irc | multi/misc/xdh_x_exec | cmd/windows/bind_ruby | 0
[*] 1245/10000 : 001/020 local_thread10 reward:-1 failure 192.168.220.145 (tcp/2121) proftpd | linux/ftp/proftpd_sreplace | linux/x86/shell_bind_tcp | 0
[*] 1234/10000 : 000/020 local_thread6 reward:10 bingo!! 192.168.220.145 (tcp/21) vsftpd | unix/ftp/vsftpd_234_backdoor | cmd/unix/interact | 0
[*] Thread: local_thread6, Trial num: 7, Step: 1, Avg step: 12.7
[*] 1249/10000 : 003/020 local_thread5 reward:-1 failure 192.168.220.145 (tcp/80:1) apache | linux/http/apache_continuum_cmd_exec | linux/x86/shell_bind_tcp | 0
[*] 1249/10000 : 010/020 local_thread3 reward:-1 failure 192.168.220.145 (tcp/53) bind | windows/antivirus/trendmicro_serverprotect_createbinding | windows/shell/reverse_tcp_uuid | 0
```

~~~~~

**BINGO!!!**

~~~~~

telnet exploit/linux/telnet/telnet\_encrypt\_keyid payload/linux/x86/shell\_bind\_tcp shell

<https://youtu.be/8ht4y9tboNY>

# Processing Flow

**Step 1.  
Intelligence  
Gathering**

**Step 2.  
Exploitation**

**Step 3.  
Post-Exploitation**

**Step 4.  
Generate Report**

**Fully automatic (No human)**

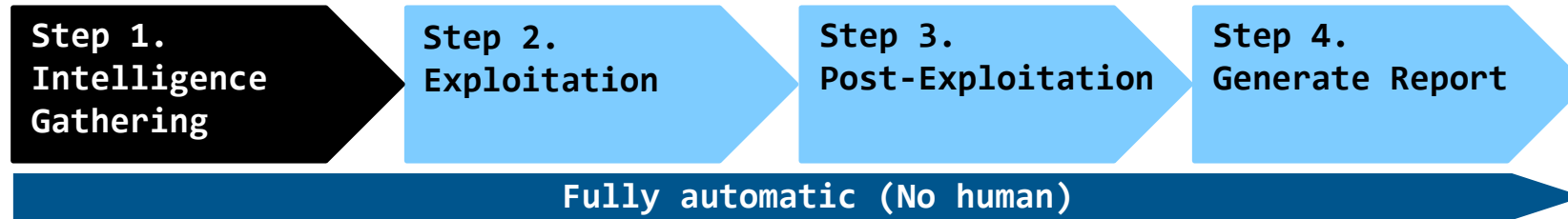
**Step 1. Intelligence Gathering**

**Step 2. Exploitation**

**Step 3. Post-Exploitation**

**Step 4. Generate Report**

# Step 1. Intelligence Gathering



## Step 1. Intelligence Gathering

- Identify open ports, products by port scanning.
- Analyze gathered HTTP responses and identify products on the WEB ports.

## Step 2. Exploitation

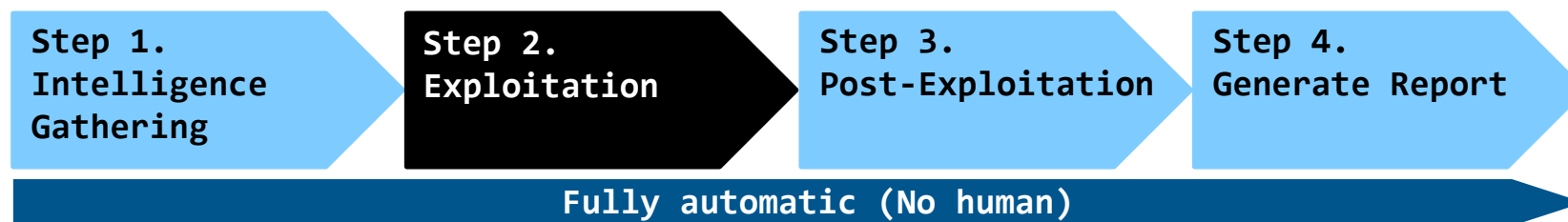
## Step 3. Post-Exploitation

## Step 4. Generate Report

Gathering target server info using Nmap, WEB Crawling.



# Step 2. Exploitation



Step 1. Intelligence Gathering

Step 2. Exploitation

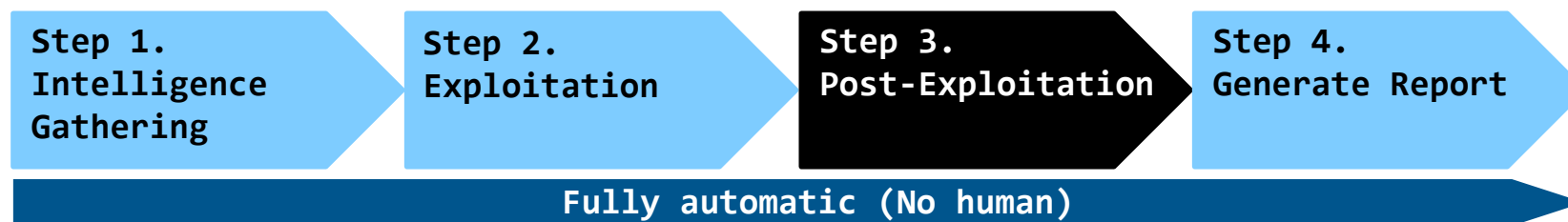
- Open session between “Deep Exploit” and front server (=compromised server).

Step 3. Post-Exploitation

Step 4. Generate Report

Open session between “Deep Exploit” and front server.

# Step 3. Post-Exploitation



Step 1. Intelligence Gathering

Step 2. Exploitation

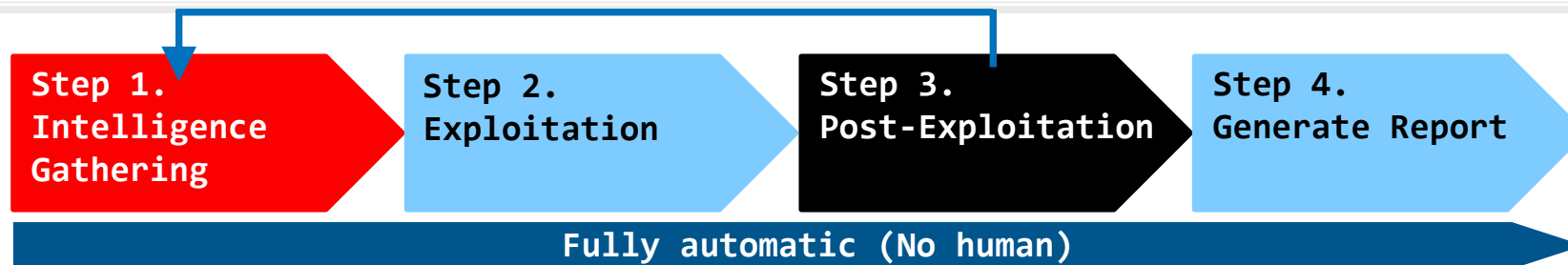
Step 3. Post-Exploitation

- Pivoting and execute the exploit to internal server via compromised server.

Step 4. Generate Report

Pivoting and execute the exploit to internal server.

# Step 3. Post-Exploitation



Step 1. Intelligence Gathering

Step 2. Exploitation

Step 3. Post-Exploitation

- Pivoting and execute the exploit to internal server via compromised server.

Step 4. Generate Report

If detect new server, repeat Step1-3 in new server.

# Step 4. Generate Report

Step 1.  
Intelligence  
Gathering

Step 2.  
Exploitation

Step 3.  
Post-Exploitation

Step 4.  
Generate Report

Fully automatic (No human)

Step 1. Intelligence Gathering

Step 2. Exploitation

Step 3. Post-Exploitation

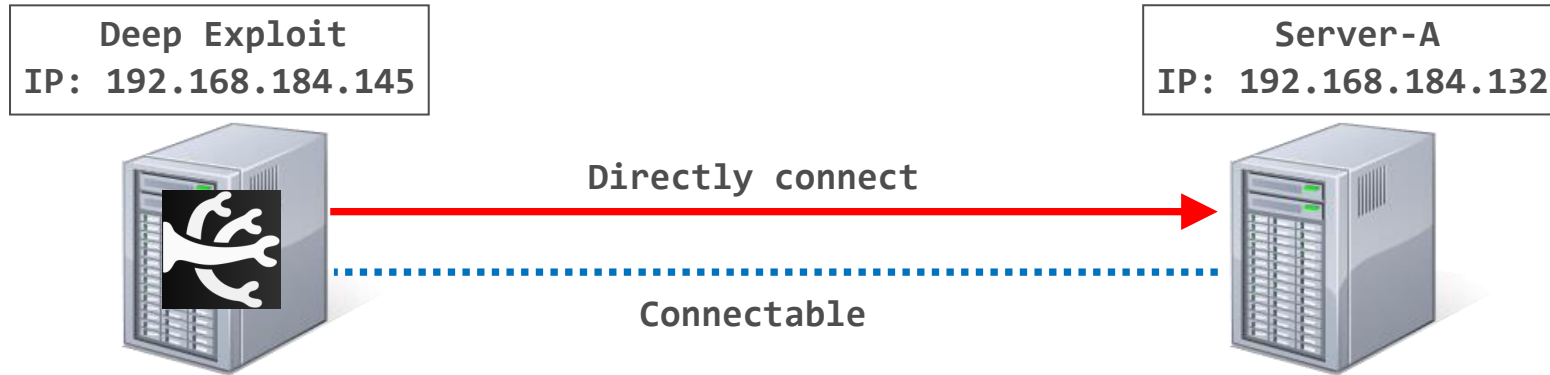
Step 4. Generate Report

- **Create the report** of penetration test.

| Deep Exploit scan Report |                   |                                                                                                                                                                                                                                                                                                          |
|--------------------------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Index                    | Item              | Value                                                                                                                                                                                                                                                                                                    |
| 1                        | IP address        | 192.168.220.145                                                                                                                                                                                                                                                                                          |
|                          | Port number       | 21                                                                                                                                                                                                                                                                                                       |
|                          | Source IP address | 192.168.220.150                                                                                                                                                                                                                                                                                          |
|                          | 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]<br>73573<br>[URL]<br><a href="http://pastebin.com/AetT9sS5">http://pastebin.com/AetT9sS5</a><br>[URL]<br><a href="http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html">http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html</a> |

# Demonstration

## Scenario 1. Single target server

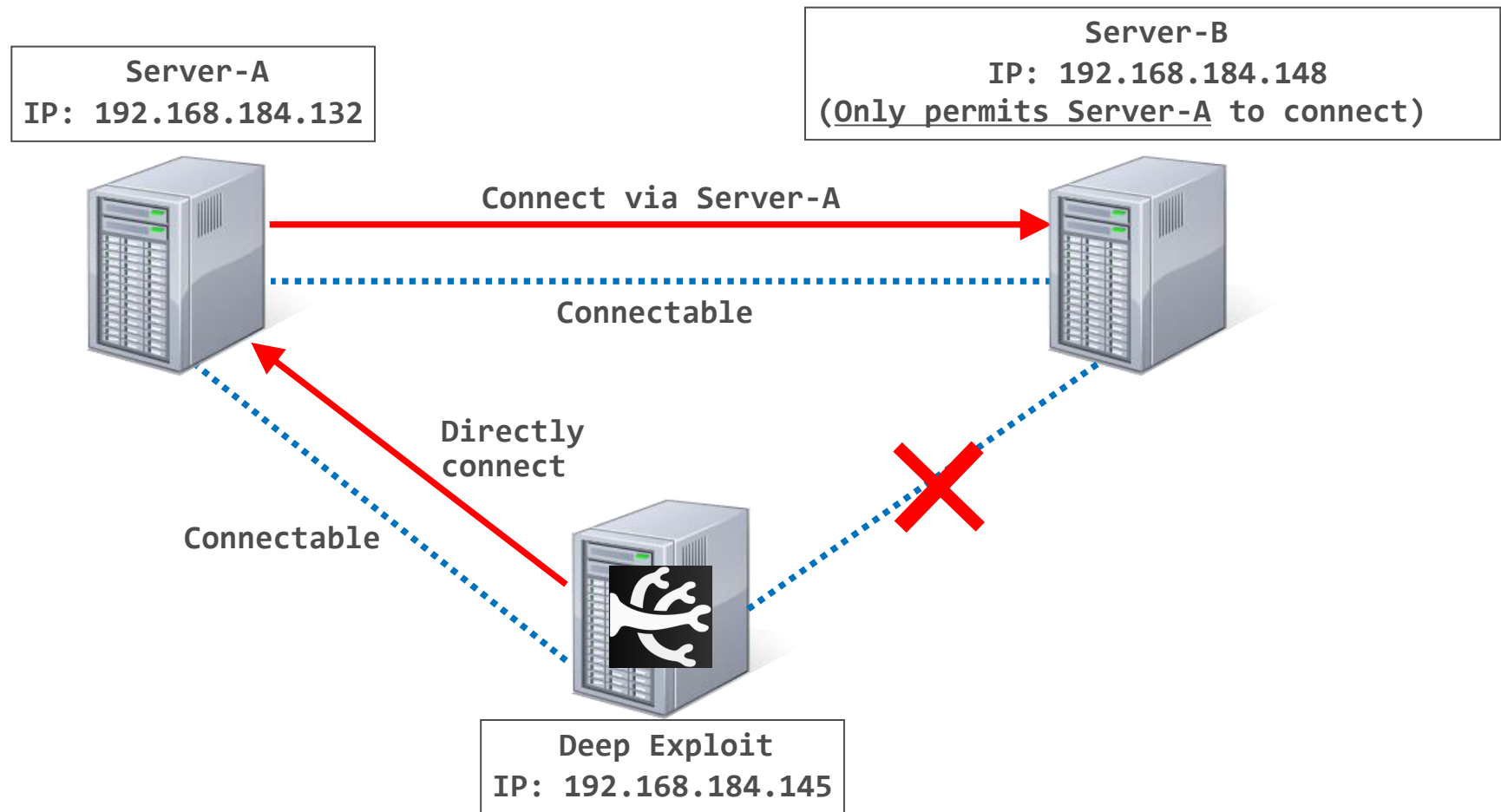


• Demo movie

<https://youtu.be/mgEOBIM4omM>

# Demonstration

## Scenario 2. Exploitation via compromised server (=Server-A)

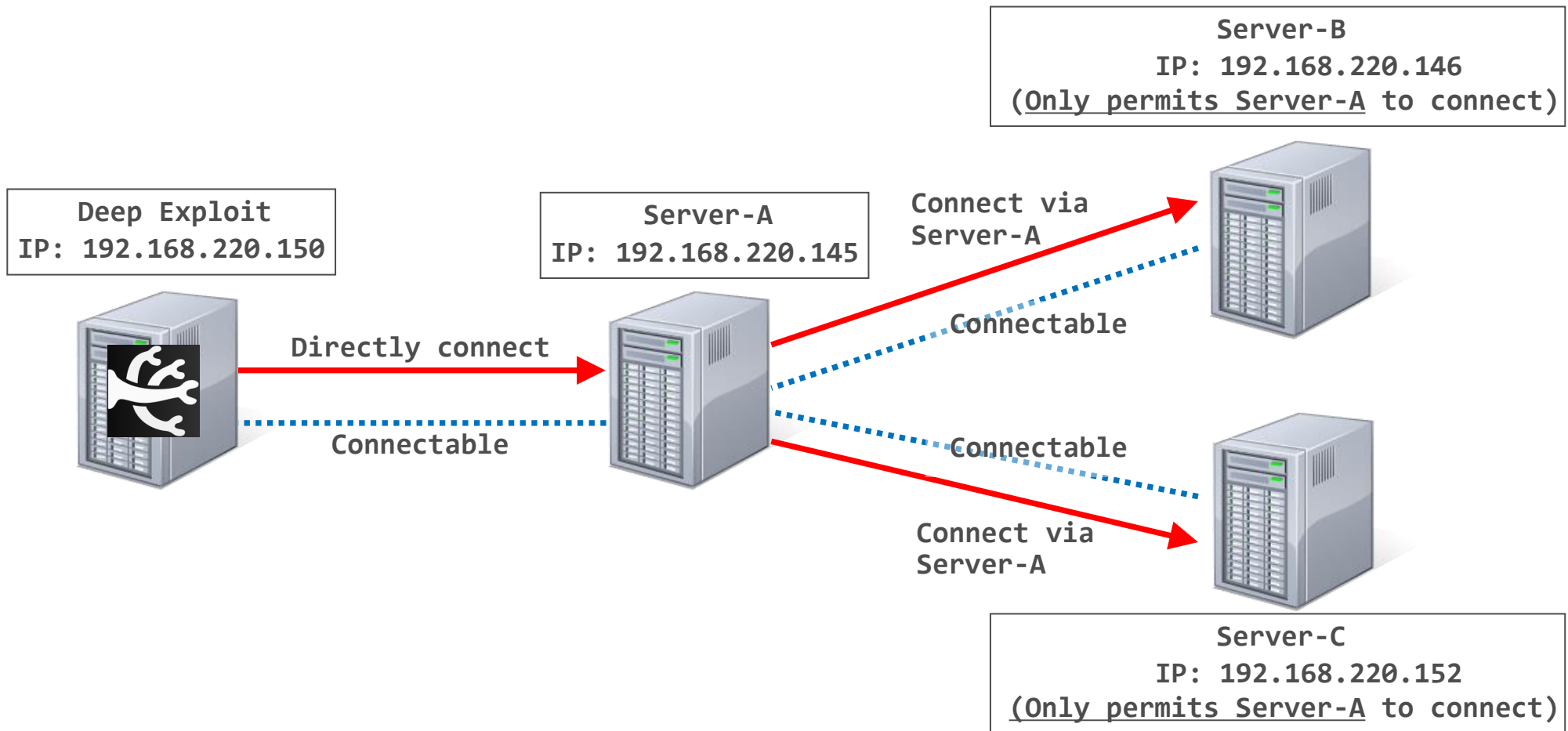


• Demo movie

<https://youtu.be/DsBN0GBjJNg>

# Demonstration

## Scenario 3. Deep penetration



• Demo movie

<https://youtu.be/s-Km-BE8NxM>

# Resource

- Source codes & Usage

[https://github.com/13o-bbr-bbq/machine\\_learning\\_security/tree/master/DeepExploit](https://github.com/13o-bbr-bbq/machine_learning_security/tree/master/DeepExploit)





# 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..)<br>Managed Security Services, Incident Response & Handling,<br>GRC Consulting, Research & Development. |

# THANK YOU!

**Reference all source codes and document:**

**[https://github.com/13o-bbr-bbq/machine\\_learning\\_security/](https://github.com/13o-bbr-bbq/machine_learning_security/)**