

摔不壞的雞蛋籃

網站集中化的安全保障



敦陽科技 楊伯瀚

貼心小提醒

發問沒有
送小禮物

會後也沒
有大抽獎



不要跑錯
場次喔！



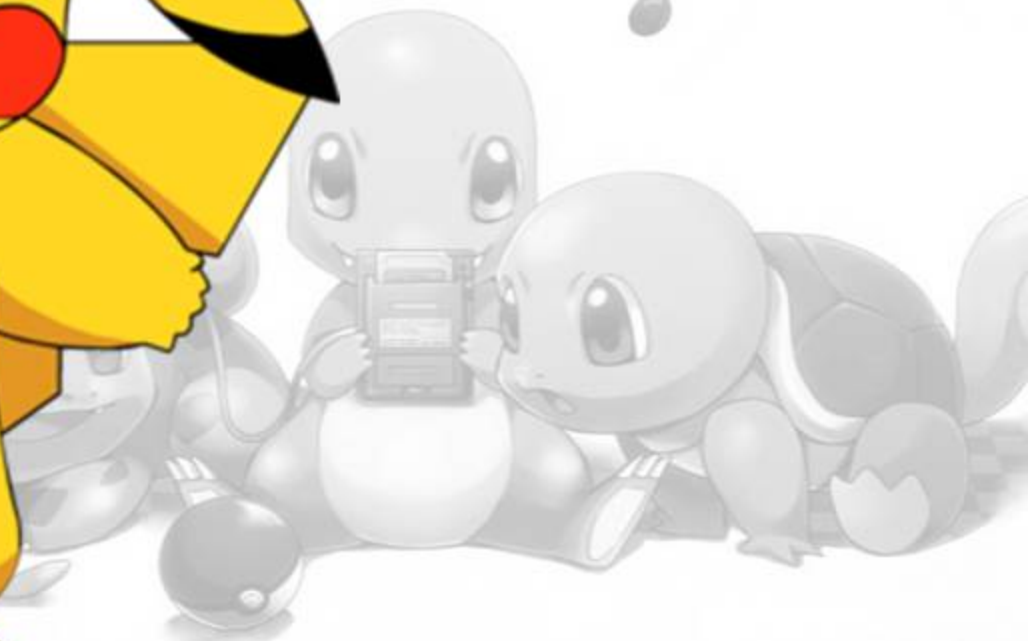
貼紙小招

發問沒

送

會後

有六



雲端雞蛋籃



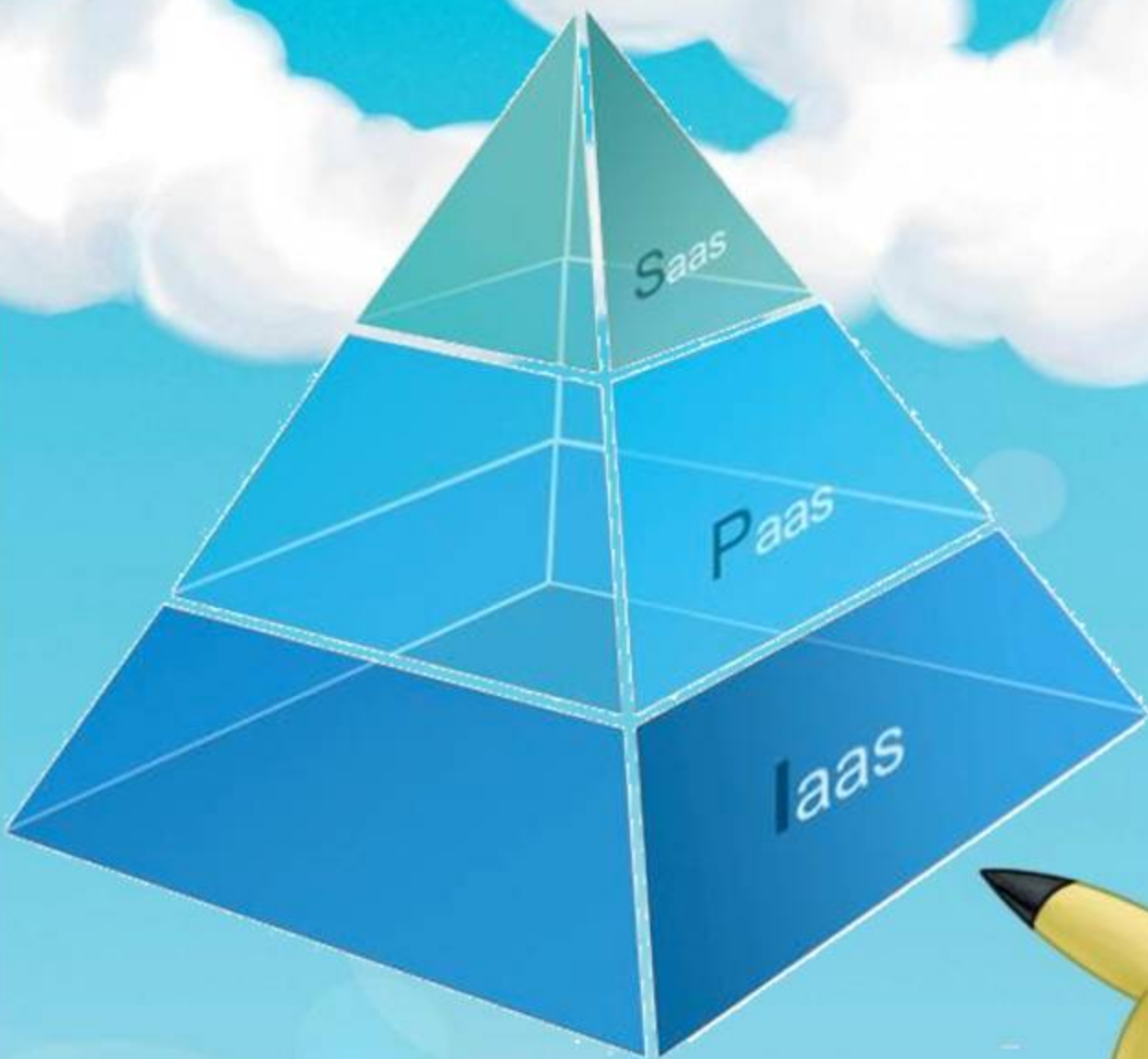
識者不能瞞

七層山海關

洩洪挽狂瀾

雲端雞蛋籃





UCaaS

Daas

OTT

X...

Y...o

Z...aaS

CPaaS

FaaS

Haas

DDoS...aaS

DBaaS

SDN
SDWAN

Crime...aaS



■ 論 程 式 的 止 確

你死了以後就在雲端



■ 論...程式的正確



塔位雲
...aaS

《啟事》
塔位商品上架說明

1. 塔位商品上架說明

2. 塔位商品上架說明

3. 塔位商品上架說明

4. 塔位商品上架說明

5. 塔位商品上架說明

6. 塔位商品上架說明

7. 塔位商品上架說明

8. 塔位商品上架說明

9. 塔位商品上架說明

10. 塔位商品上架說明

11. 塔位商品上架說明

12. 塔位商品上架說明

13. 塔位商品上架說明

14. 塔位商品上架說明

15. 塔位商品上架說明

16. 塔位商品上架說明

17. 塔位商品上架說明

18. 塔位商品上架說明

19. 塔位商品上架說明

20. 塔位商品上架說明

21. 塔位商品上架說明

22. 塔位商品上架說明

23. 塔位商品上架說明

24. 塔位商品上架說明

25. 塔位商品上架說明

26. 塔位商品上架說明

27. 塔位商品上架說明

28. 塔位商品上架說明

29. 塔位商品上架說明

30. 塔位商品上架說明

31. 塔位商品上架說明

32. 塔位商品上架說明

33. 塔位商品上架說明

34. 塔位商品上架說明

35. 塔位商品上架說明

36. 塔位商品上架說明

37. 塔位商品上架說明

38. 塔位商品上架說明

39. 塔位商品上架說明

40. 塔位商品上架說明

41. 塔位商品上架說明

42. 塔位商品上架說明

43. 塔位商品上架說明

44. 塔位商品上架說明

45. 塔位商品上架說明

46. 塔位商品上架說明

47. 塔位商品上架說明

48. 塔位商品上架說明

49. 塔位商品上架說明

50. 塔位商品上架說明

51. 塔位商品上架說明

52. 塔位商品上架說明

53. 塔位商品上架說明

54. 塔位商品上架說明

55. 塔位商品上架說明

56. 塔位商品上架說明

57. 塔位商品上架說明

58. 塔位商品上架說明

59. 塔位商品上架說明

60. 塔位商品上架說明

61. 塔位商品上架說明

62. 塔位商品上架說明

63. 塔位商品上架說明

64. 塔位商品上架說明

65. 塔位商品上架說明

66. 塔位商品上架說明

67. 塔位商品上架說明

68. 塔位商品上架說明

69. 塔位商品上架說明

70. 塔位商品上架說明

71. 塔位商品上架說明

72. 塔位商品上架說明

73. 塔位商品上架說明

74. 塔位商品上架說明

75. 塔位商品上架說明

76. 塔位商品上架說明

77. 塔位商品上架說明

78. 塔位商品上架說明

79. 塔位商品上架說明

80. 塔位商品上架說明

81. 塔位商品上架說明

82. 塔位商品上架說明

83. 塔位商品上架說明

84. 塔位商品上架說明

85. 塔位商品上架說明

86. 塔位商品上架說明

87. 塔位商品上架說明

88. 塔位商品上架說明

89. 塔位商品上架說明

90. 塔位商品上架說明

91. 塔位商品上架說明

92. 塔位商品上架說明

93. 塔位商品上架說明

94. 塔位商品上架說明

95. 塔位商品上架說明

96. 塔位商品上架說明

97. 塔位商品上架說明

98. 塔位商品上架說明

99. 塔位商品上架說明

100. 塔位商品上架說明

塔位自由轉讓平台



自己塔位自己上傳/自己管理
早期預購 / 自由平台交易 / 輕鬆比價 / 滿足您更多需求





(主機代管→環境代管)
基礎架構服務化(IaaS)



(主機代管→環境代管)
基礎架構服務化(IaaS)



IBM

RackSpace

HiCloud

Ora

旁注攻擊 Cloud

AWS

Azure

公有

私有

流量癱瘓

(主機代管 云代管)

基礎架構服務化 (IaaS)

代管機房



郵件主機



網站



資料庫



AD主機

只允許
連上網站



入侵偵測



程式閘道



防火牆



第二套防火牆



防毒牆



SSLVPN



代管機房



郵件主機



網站



資料庫



AD主機



感染



竊聽



劫持
篡改

資安設備
管不到



入侵偵測

程式閘道



防火牆



第二套防火牆

防毒牆

SSLVPN



虛擬環境 更難偵測



V郵件主機



V網站



V資料庫



V-AD主機



感染



竊聽



劫持
篡改



入侵偵測

程式闢道



防火牆



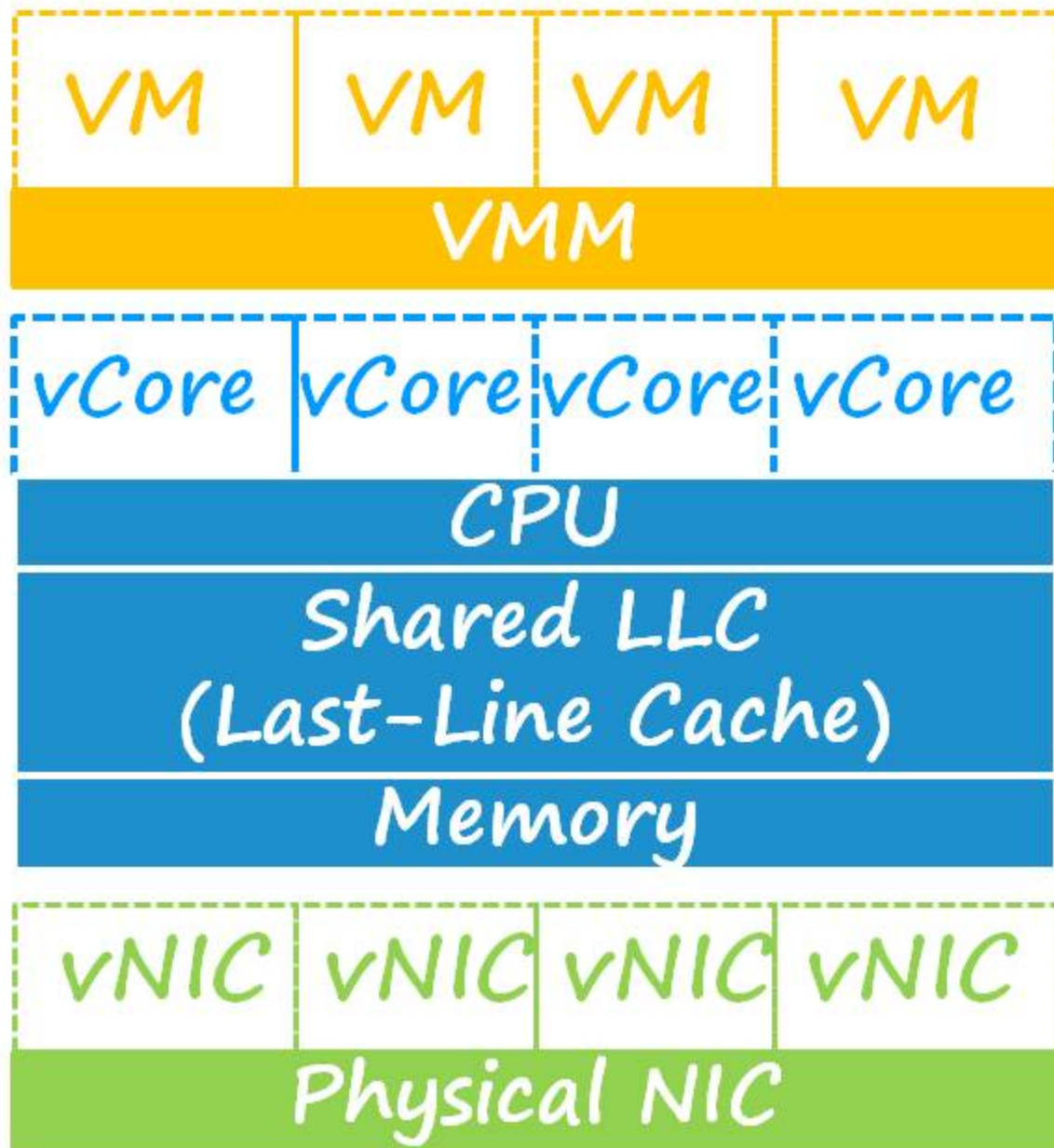
第二套防火牆

防毒牆

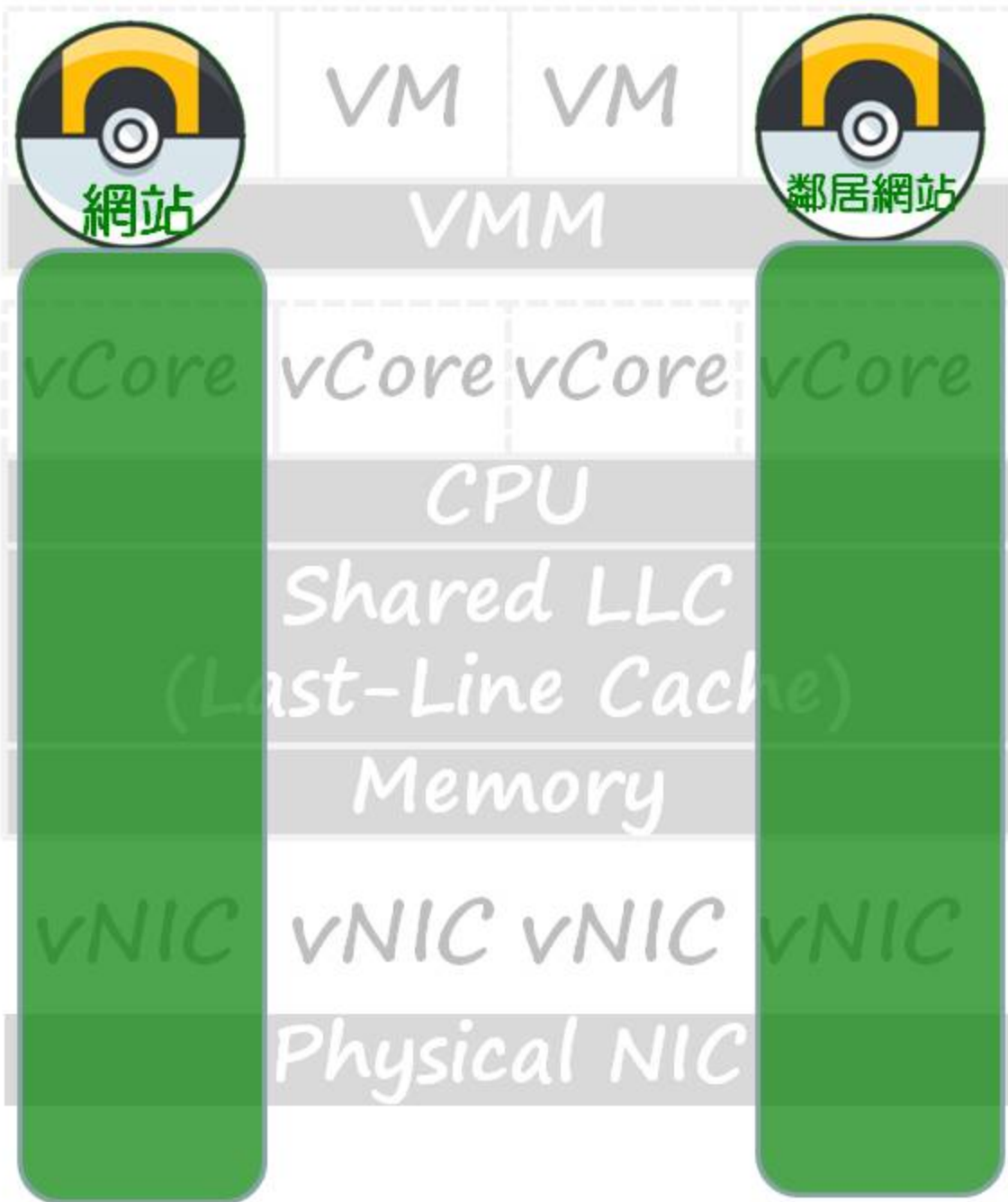
SSLVPN

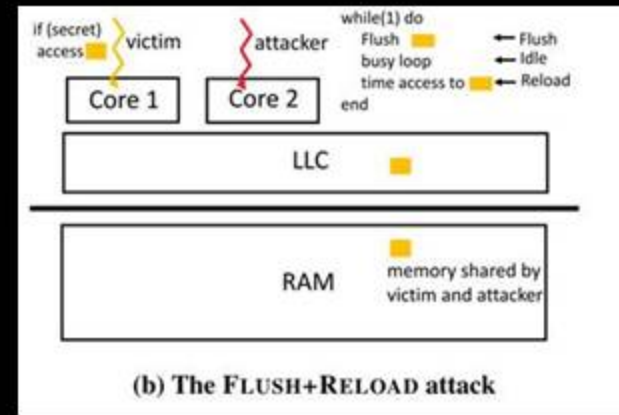
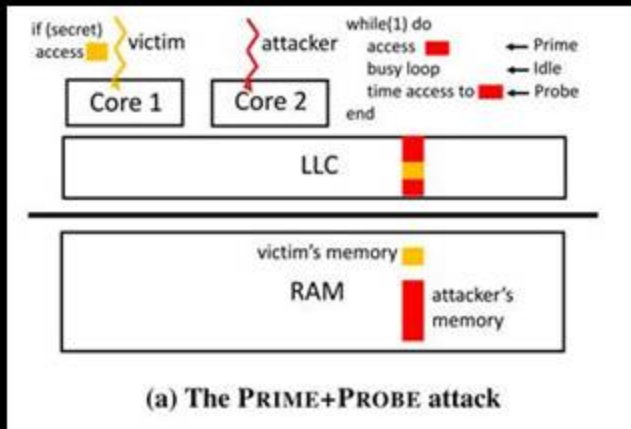


虛擬環境



虛擬環境 共享硬體





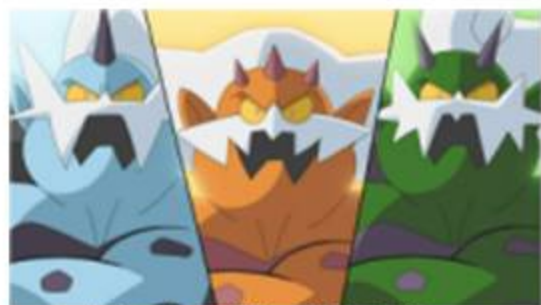
參考資料：

A Measurement Study on Co-residence Threat inside the Cloud

CATalyst: Defeating last-level cache side channel attacks in cloud computing



虛擬環境 共享硬體



VM

VM



VMM

vCore

vCore

vCore

vCore

CPU

Shared LLC

(Last-Line Cache)

Memory

vNIC

vNIC

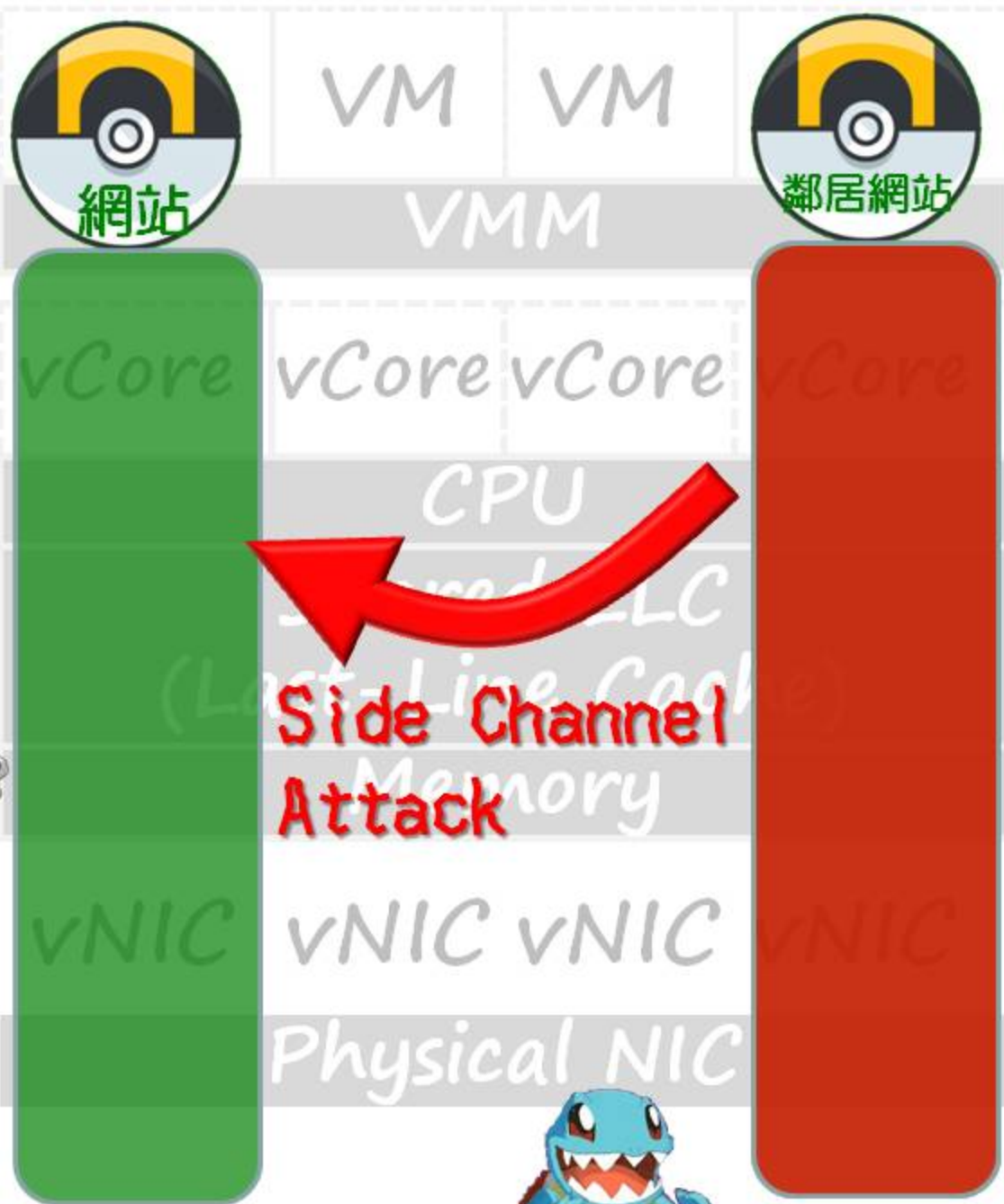
vNIC

vNIC

Physical NIC



虛擬環境 共享硬體



虛擬環境 共享硬體



VM



VM

vCore

vCore

vCore

vCore



Attack

Memory

vNIC

vNIC

vNIC

vNIC

Physical NIC

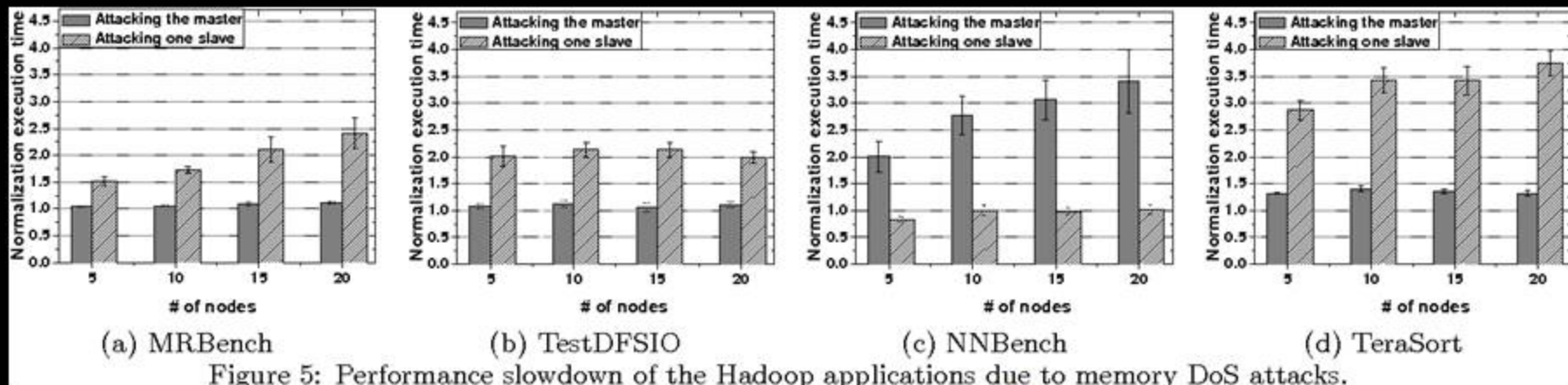


Figure 5: Performance slowdown of the Hadoop applications due to memory DoS attacks.

參考資料：

DoS Attacks on Your Memory in the Cloud
 Memory DoS Attacks in Multi-tenant Clouds



虛擬環境 共享硬體



VM

VM

VMM



vCore

vCore

vCore

vCore

CPU

Shared LLC
(Last-Line Cache)

Memory

vNIC

vNIC

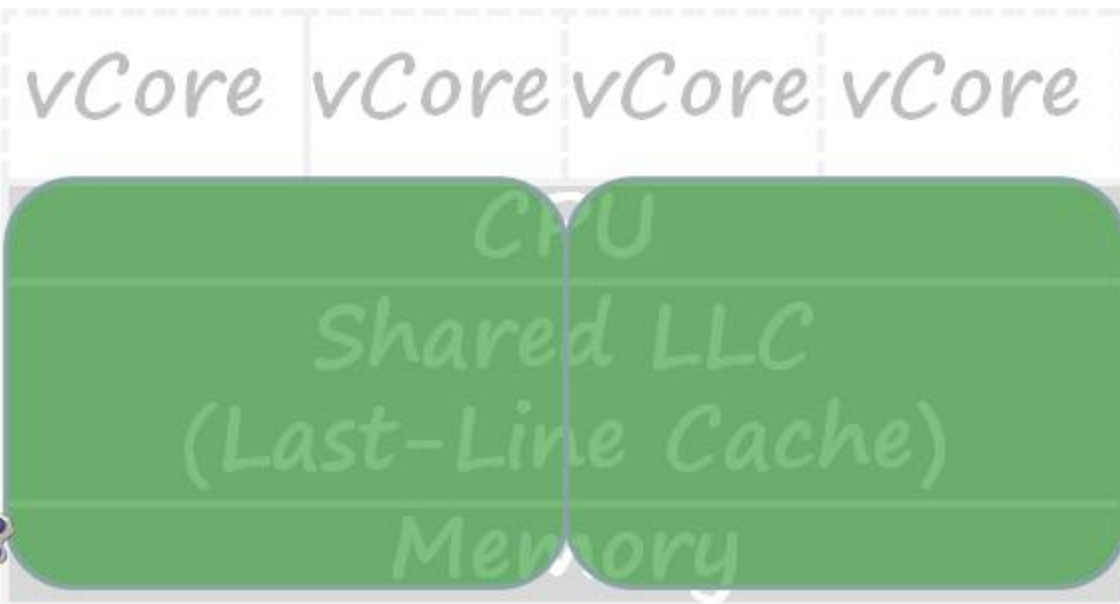
vNIC

vNIC

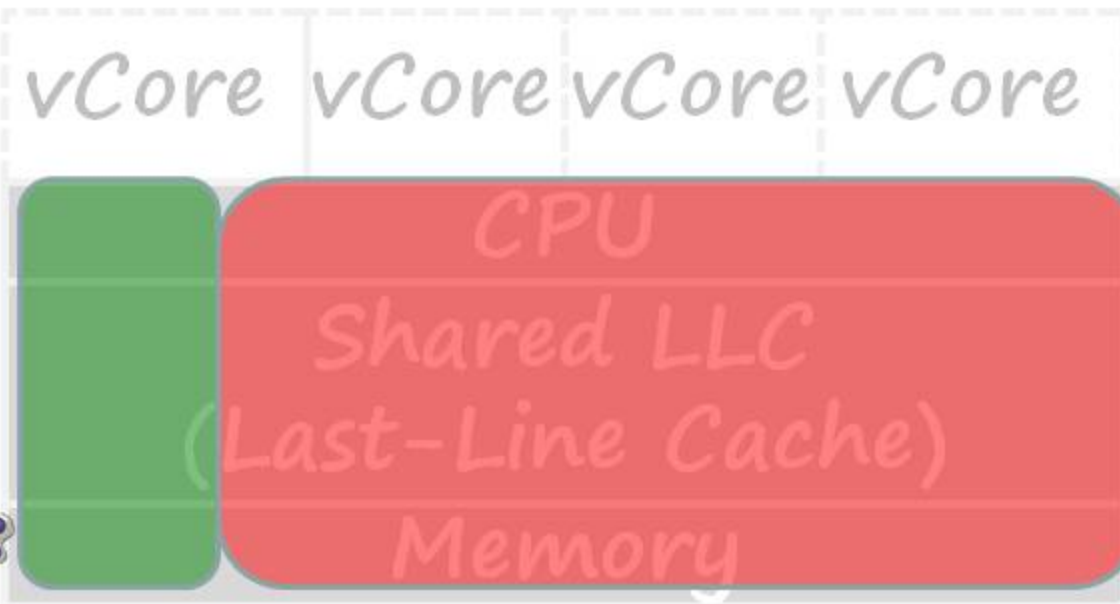
Physical NIC



虛擬環境 共享硬體



虛擬環境 共享硬體



DDoS



虛擬環境 共享機房

跳電



雲端平台



礦機租賃

斷線

DDOS





軟體服務化 (SaaS)
平台服務化 (PaaS)



Slack
(Teamwork)

Shopify
(eCommerce)

Salesforce
(CRM)

SurveyMonkey
(online survey)

Gmail
(mail)

Apple Store
(Software/API)

集中軟體開發
運算與部署

資訊服務
委外

軟體服務化 (SaaS)
平台服務化 (PaaS)

埋置後門

網站漏洞

猜猜樂

中間人
攻擊

資料外洩

平台服務化 (PaaS)

Slack
Team

Shopify
(eCommerce)

Salesforce
(CRM)

Mail
(mail)

Store
(API)

集中軟體開發

資訊服務
委外

服務化 (SaaS)

商業邏輯：

程式運作邏輯：程式規格未想到的漏洞

系統流程漏洞：跨行轉帳、繳款

資源控制：

資訊蒐集：網頁爬蒐、資訊洩露、錯誤訊息

設定管理：系統架構、設定頁、檔案管理

身份驗證：未授權登入、迴避驗證、預設管理密碼

身份權限：水平/垂直權限跳脫、路徑跳脫

登入階段：用戶欺騙

輸入值驗證：

登入階段：偽冒身分、XSRF

身份驗證：暴力登入、脆弱密碼

資料驗證：注入攻擊、跨站腳本攻擊(XSS)

繞過資安設備：迴避防火牆、迴避資安函式庫

敏感回應：

系統錯誤、個人資料、機密資料

網站木馬

用戶端安全：

個人習慣：簡易密碼、共用密碼

內插外插：中間人攻擊、竊聽、瀏覽器側錄



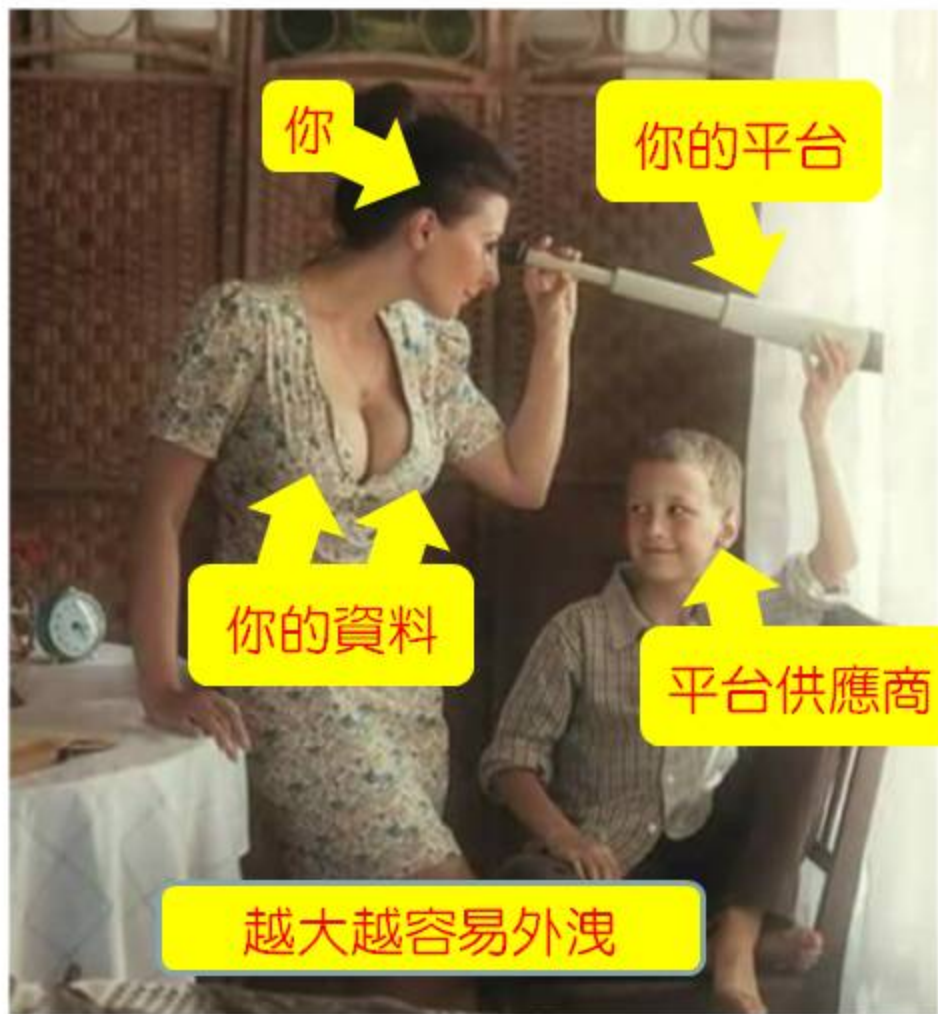
雲端廠商要負責？

完全代管
完全負責？

系統維運
人力不足！



防火牆、IDS/IPS/IDP、系統更新、
SOC監控都到位，怎麼還是防不到？



沒主動駭你
已經佛心了!





黑道開ISI



國家老大哥

網站開發要寫好？

陳之藩：

要謝的人
太多，

還是
謝天吧！



程式煩：

要改的程式
太多，

還是**改天**吧！

網站開發要麻煩嗎？

學校沒教
安全寫作

規格沒說要
資安

介面漂亮
才重要

寫那段的人
離職了

陳之
要
太多，
還是
謝天吧！

程式煩：
改的程式
太多，

這，天吧！

網站開發要麼好？

規檢說要

學校教

安

安全

沒空啦

那段的人
離職了

資安三角不平衡



資安三角不平衡



應用程式傳遞控制 (ADC)

網站防火牆 (WAF) :

正面表列：網址、輸入值、XML格式

負面表列：特徵資料庫

資訊外洩：錯誤訊息、個資、機密

應用層控制 (Application Control) :

系統錯誤、個人資料、機密資料

網站木馬

反DDoS :

L2-L7 Amplification Ddos

HTTP/SSL DDoS



進化吧！防火牆！



進化吧！防火牆！



識者



不能瞞

網頁程式 漏洞



郵件



網站



資料庫



AD主機

設計與 管理疏失



入侵偵測

程式閘道

防火牆

第二套防火牆

防毒牆

SSL VPN





郵件主機



網路



資料庫



AD主機

機敏資訊外洩



入侵偵測



程式閘道



防火牆



第二套防火牆



防毒牆



SSL VPN





網

站

防

火

牆

Handwritten signature



郵件主機



網站



資料庫



AD主機

SSL Offload
HTTP/S, WebSocket, SOAP
HTML, AJAX, JSON, XML

Safe



WAF



入侵偵測



SSL

防火牆



第二套防火牆



防毒牆



SSL VPN



程式管道







正面表列白名單
(毋須依賴廠商更新)

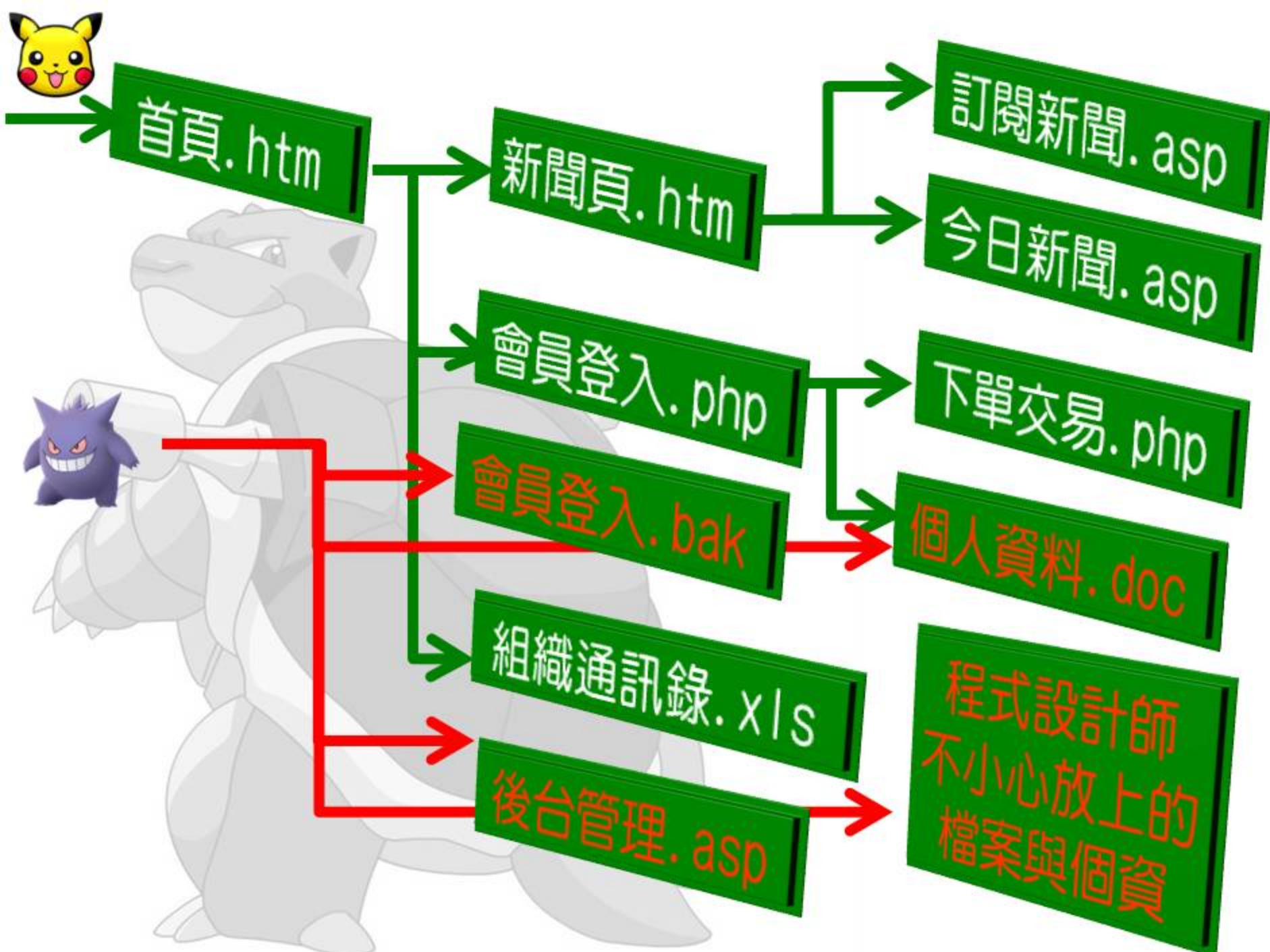
以「行為」為基準
(毋須上百條規則)

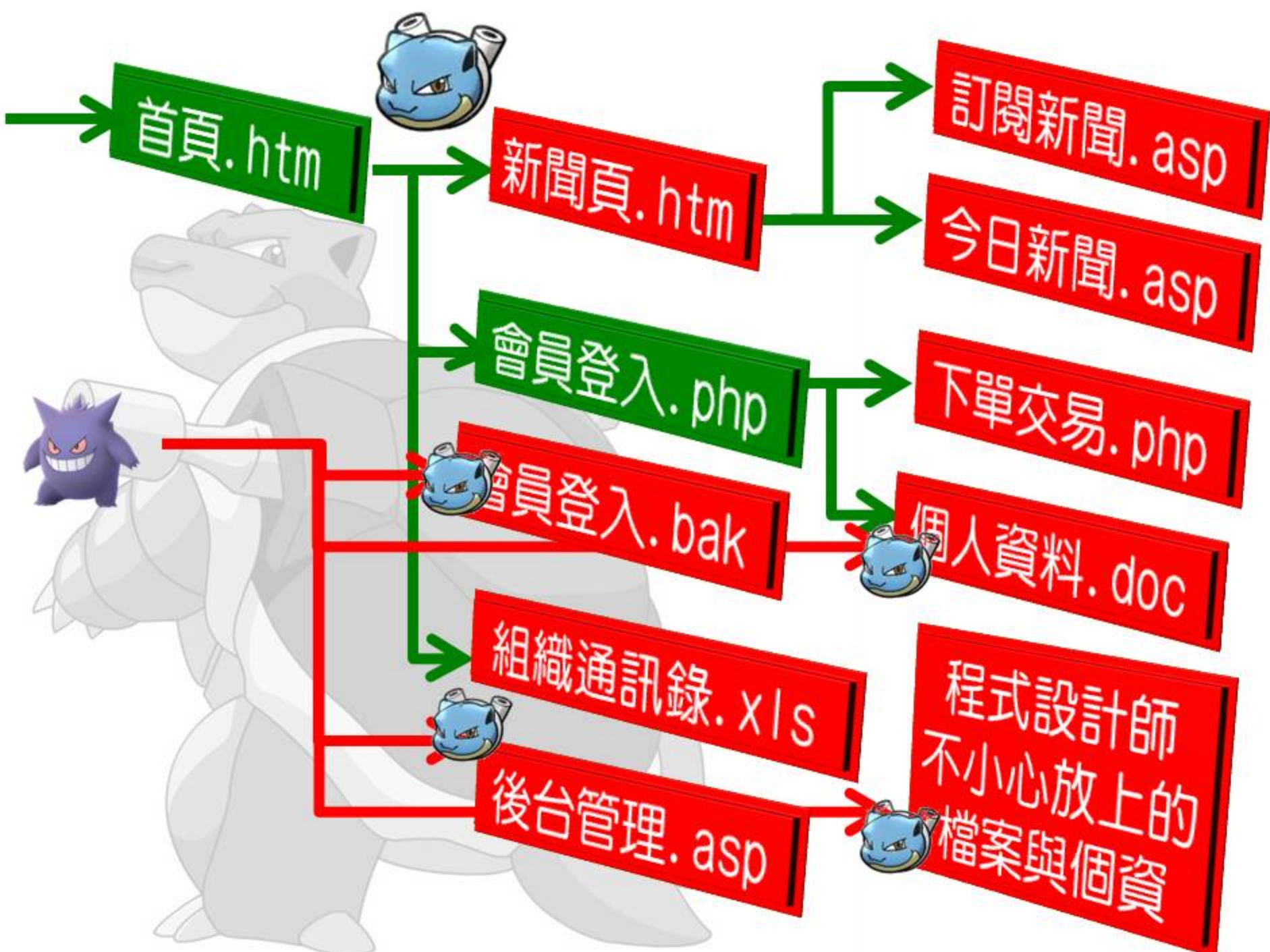
遮蔽程式漏洞

補強設計疏失

阻擋零時差攻擊

資料外洩預警







規定「純數字」
一勞永逸！



Microsoft Internet Explorer window showing a URL: `http://.../list1.asp?c_no=01' and 1=db_name() ;--`. The address bar contains the URL `http://.../list1.asp?c_no=01' and 1=db_name() ;--`. The error message displayed is:

Microsoft OLE DB Provider for ODBC Drivers 錯誤 '80040e07'

[Microsoft][ODBC SQL Server Driver][SQL Server]將 nvarchar 數值 'fxshdb' 轉換成資料型別為 int 的資料行語法錯誤。

/goodweb/list1.asp, 列12

完成 網際網路

只能填身分證號(A11111111)

只能填文數字(8-14)



The image shows a screenshot of a 'User Authentication' dialog box. It has a title bar with the text 'User Authenticati...' and standard window controls. Below the title bar is a menu bar with 'File', 'Edit', and 'View' options. The main area contains two text input fields: the top one is labeled 'Username' and the bottom one is labeled 'Password'. A 'Login' button is located at the bottom right of the dialog box. A blue arrow points from the 'Username' field to the text box on the left.

使用者行為

自動
學習



http://www.unsafe.com/cart/credit.htm - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 我的最愛 記錄

網址(U) http://www.unsafe.com/cart/credit.htm

我的資料:
身分證號:A123456789
密碼:保密
我的客戶:

身分證號	姓名	MASTER卡號	到期日
A123456770	王一	5338746188819585	01/08
A123456761	王二	5492154885755289	04/08
A123456752	王三	5493681591087044	02/09
A123456743	王四	5197241037782077	04/08
A123456734	王五	5457049530618663	06/10
A123456725	王六	5405133926906545	04/08
A123456716	王七	5112152682301976	07/08
A123456770	王八	5151157290226228	04/06
B123456788	王九	5490442135446417	12/08
C123456787	王十	5237600513886110	04/08

資料遮罩
別外露

http://192.168.2.213/cart/credit.htm - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 我的最愛 記錄

網址(U) http://192.168.2.213/cart/credit.htm

Google 搜尋 書籤 拼字檢查 登入

我的資料:
身分證號:A123456789
密碼:保密
我的客戶:

身分證號	姓名	MASTER卡號	到期日
A123456770	王一	xxxxxxxxxxxx9585	01/08
A123456761	王二	xxxxxxxxxxxx5289	04/08
A123456752	王三	xxxxxxxxxxxx7044	02/09
A123456743	王四	xxxxxxxxxxxx2077	04/08
A123456734	王五	xxxxxxxxxxxx8663	06/10
A123456725	王六	xxxxxxxxxxxx6545	04/08
A123456716	王七	xxxxxxxxxxxx1976	07/08
A123456770	王八	xxxxxxxxxxxx6228	04/06
B123456788	王九	xxxxxxxxxxxx6417	12/08
C123456787	王十	xxxxxxxxxxxx6110	04/08



網站防火牆



集中式硬體防護
資安標章/稽核
負面表列(黑名單)
正向表列(白名單)
阻擋未知攻擊
雙向分析
自動學習

使出雙向代理！



A cartoon character wearing a red and black cap and blue clothing is holding a large yellow pennant. The pennant has the Chinese text '使出雙向代理!' written on it in red. The character is pointing upwards with their right hand. The background consists of blue and green vertical stripes.

使出雙向代理！

六層



使出雙向代理！

山海關



郵件主機



網站

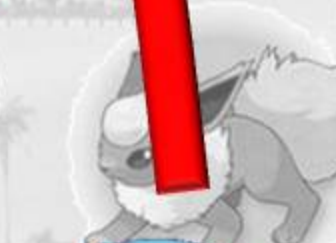


資料庫



AD主機

中間人
盜聽



入侵偵測

防火牆

第二防火牆

防毒牆

SSL VPN

程式門道





郵件



網站



資料庫



AD主機

搶票
搶課
猜密碼

冒用
身份



入侵偵測

程式攔道

防火牆

第二套防火牆

防毒牆

SSLVPN



OWASP Automated Threat

- OAT-001 Carding (卡號測試)
- OAT-002 Token Cracking (偽造優惠券)
- OAT-003 Ad Fraud (廣告詐騙)
- OAT-004 Fingerprinting (應用程式資訊採集)
- OAT-005 Scalping (搶貨)
- OAT-006 Expediting (加速作業)
- OAT-007 Credential Cracking (密碼破解)
- OAT-008 Credential Stuffing (撞庫)
- OAT-009 CAPTCHA Bypass (躲避驗證)
- OAT-010 Card Cracking (破解支付機制)
- OAT-011 Scraping (搜刮資訊)
- OAT-012 Cashing Out (獲得現金)
- OAT-013 Sniping (截止前搶標)
- OAT-014 Vulnerability Scanning (弱點掃描)
- OAT-015 Denial of Service (阻斷服務)
- OAT-016 Skewing (重複點擊影響結果)
- OAT-017 Spamming (垃圾留言、評價)
- OAT-018 Footprinting (探索參數或屬性)
- OAT-019 Account Creation (濫用帳號創建機制)
- OAT-020 Account Aggregation (帳號推理)
- OAT-021 Denial of Inventory (空佔名額)



Selenium

Web Scraper (Chrome extension)

Electron (Chromium + Node.js + Native APIs)

Autolt

SikuliX

Headless Browser

Google Chrome headless (59+)

Firefox headless mode (55/56+)

PhantomJS

HtmlUnit

TrifleJS

Splash

SimpleBrowser

```
10 require('jasmine'),
11 require('karma-chrome-launcher'),
12 require('karma-jasmine-html-reporter'),
13 require('karma-coverage-istanbul-reporter'),
14 require('@angular/cli/plugins/karma')
15 },
16 client:{
17   clearContext: false // leave Jasmine Spec Runner output visible in browser
18 },
19 files: [
20   { pattern: './src/test.ts', watched: false }
21 ]
22 }
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL

```
1: @angular/cli
~/projects/angular-excel tests ng test
05 05 2017 19:02:56.567:WARN [karma]: No captured browser, open http://localhost:9876/
05 05 2017 19:02:56.578:INFO [karma]: Karma v1.4.1 server started at http://0.0.0.0:9876/
05 05 2017 19:02:56.579:INFO [launcher]: Launching browser ChromeHeadless with unlimited concurrency
05 05 2017 19:02:56.625:INFO [launcher]: Starting browser Chrome
05 05 2017 19:02:57.098:INFO [HeadlessChrome 0.0.0 (Linux 0.0.0)]: Connected on socket lqEu6...
HeadlessChrome 0.0.0 (Linux 0.0.0): Executed 23 of 23 SUCCESS (0.982 secs / 0.963 secs)
```







應 用 層 控 制



郵件主機

資料庫

AD主機

無帳號系統

員工資料.doc
交易記錄.log
信用卡號.xls
自拍影片.jpg



L7

身份驗證
我來作



入侵偵測

程式攔道

防火牆

第二套防火牆

防毒牆

SSL VPN



A screenshot of an F5 Secure Logon web form. The form includes the F5 logo at the top left, followed by the title "Secure Logon". Below the title are three input fields: "Username" with the value "jrahm", "Password" with masked characters "*****", and "Domain" with the value "devcentral". A "Logon" button is positioned at the bottom of the form.



郵件主機



有帳號系統



資料庫



AD主機

身份冒用

猜密碼



L7

強化驗證



入侵偵測



防火牆



第二套防火牆



防毒牆

程式攔道

SSL VPN



▶ 請輸入帳號及密碼登入企業入口網站!

▶ 帳號:

▶ 密碼:



插入
CAPTCHA

▶ 請輸入帳號及密碼登入企業入口網站!

▶ 帳號:

▶ 密碼:

登入



我不是機器人



reCAPTCHA
隱私權 · 條款

雙因子驗證
(2FA)



L7

用戶憑證

設備憑證

TOKEN

OTP

Callout Push

username
password

<input checked="" type="radio"/> Duo Push
<input type="radio"/> Phone Call
<input type="radio"/> Passcode
<input type="text"/>
Login

Windows or Linux

Authentication Proxy

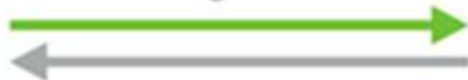
Active Directory or RADIUS



Auth Proxy Access to
Outbound Port 443 HTTPS



5



6

3

2





郵件主機



交易系統



資料庫



AD主機

搶票
搶課



L7

機器人檢查



入侵偵測



程式闖道



防火牆



第二套防火牆



防毒牆



SSL VPN



登入



訂購頁

交易網站

登入



交易網站

訂購頁
JavaScript

登入



訂購買

JavaScript



機器人特徵？

- Known Bad Bots
- Known Good bots -> Reverse DNS lookup Check
- 有沒有 Keyboard 活動
- 有沒有 Mouse 活動
- 有沒有其他人為活動
- 檢查瀏覽器載入插件
- 計算開啟的新連線數量
- 計算每個連線的新請求數量



交易網站

登入



訂購頁

JavaScript



機器人特徵？

產生設備ID



產生一次性



追蹤碼



訂購頁

交易網站

登入



訂購頁

JavaScript



訂購頁 交易網站



機器人特徵？

訂購



產生設備ID
產生一次性
追蹤碼

計算頻率

驗證追蹤碼



登入



訂購頁

JavaScript

機器人特徵？

產生設備ID
產生一次性
追蹤碼

訂購



計算頻率

驗證追蹤碼



訂購頁 交易網站



登入



交易網站

訂購頁

JavaScript

機器人特徵？

訂購

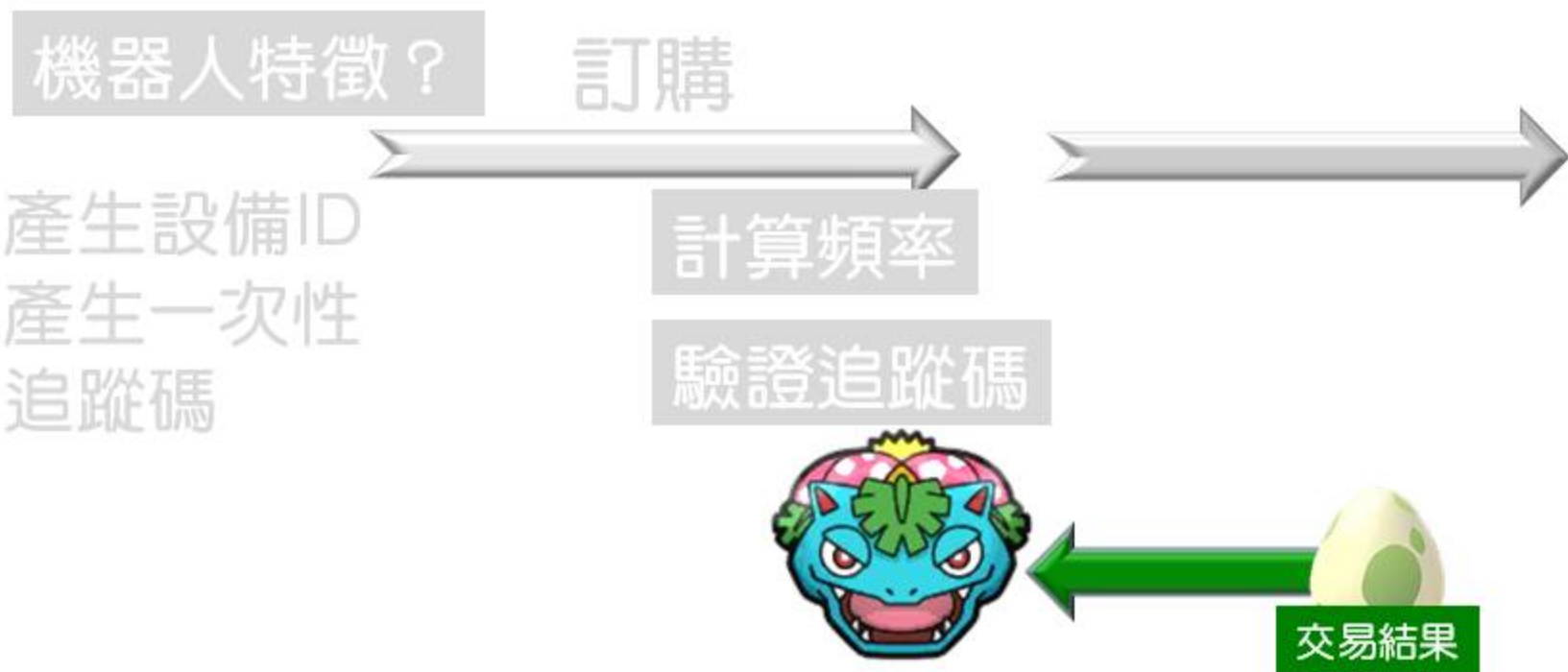
產生設備ID
產生一次性
追蹤碼

計算頻率

驗證追蹤碼



交易結果



登入



交易網站

訂購頁

JavaScript

機器人特徵？

訂購

產生設備ID
產生一次性
追蹤碼

計算頻率

驗證追蹤碼



交易結果

JavaScript

重設追蹤碼

登入



訂購頁

JavaScript



交易網站

機器人特徵？

訂購

產生設備ID
產生一次性
追蹤碼

計算頻率

驗證追蹤碼



交易結果

JavaScript

重設追蹤碼





郵件主機



網站



資料庫



AD主機

側錄



插入混淆碼



L7



入侵偵測



程式閃避



防火牆

木馬



第



防火牆

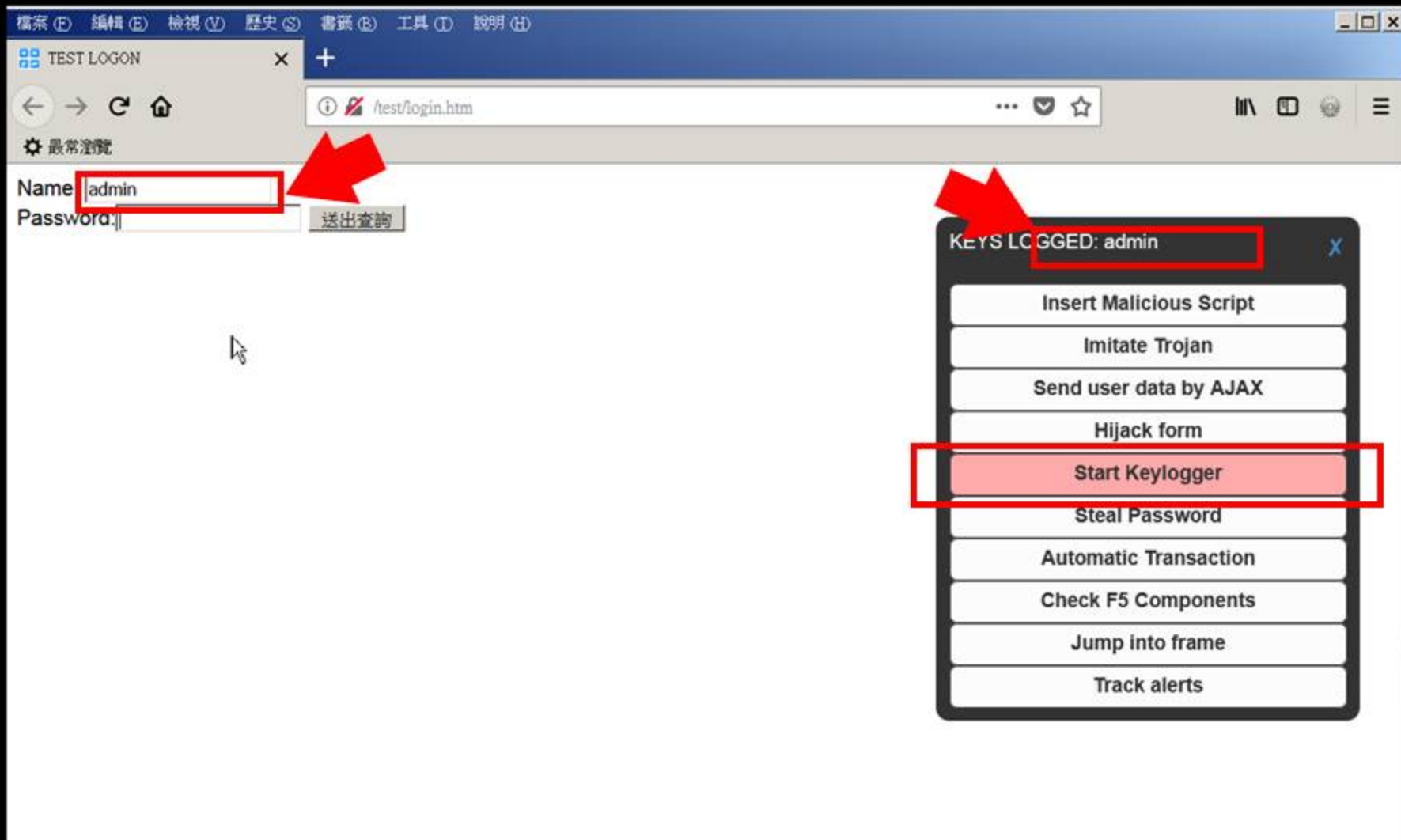


防毒牆



SSLVPN





檔案 (F) 編輯 (E) 檢視 (V) 歷史 (S) 書籤 (B) 工具 (T) 說明 (H)

TEST LOGON x +

← → ↻ 🏠 ... 📑 ☆

⚙️ 最常瀏覽

Name

Password:

KEYS LOGGED: ardhdnnimxxi

- Insert Malicious Script
- Imitate Trojan
- Send user data by AJAX
- Hijack form
- Start Keylogger**
- Steal Password
- Automatic Transaction
- Check F5 Components
- Jump into frame
- Track alerts

javascript
混淆



郵件主機



網站



資料庫



AD主機

網址稼接

竊聽

篡改

七層
加密



L7

偵測

釣魚

網站



入侵偵測

程式閃避



防火牆

第

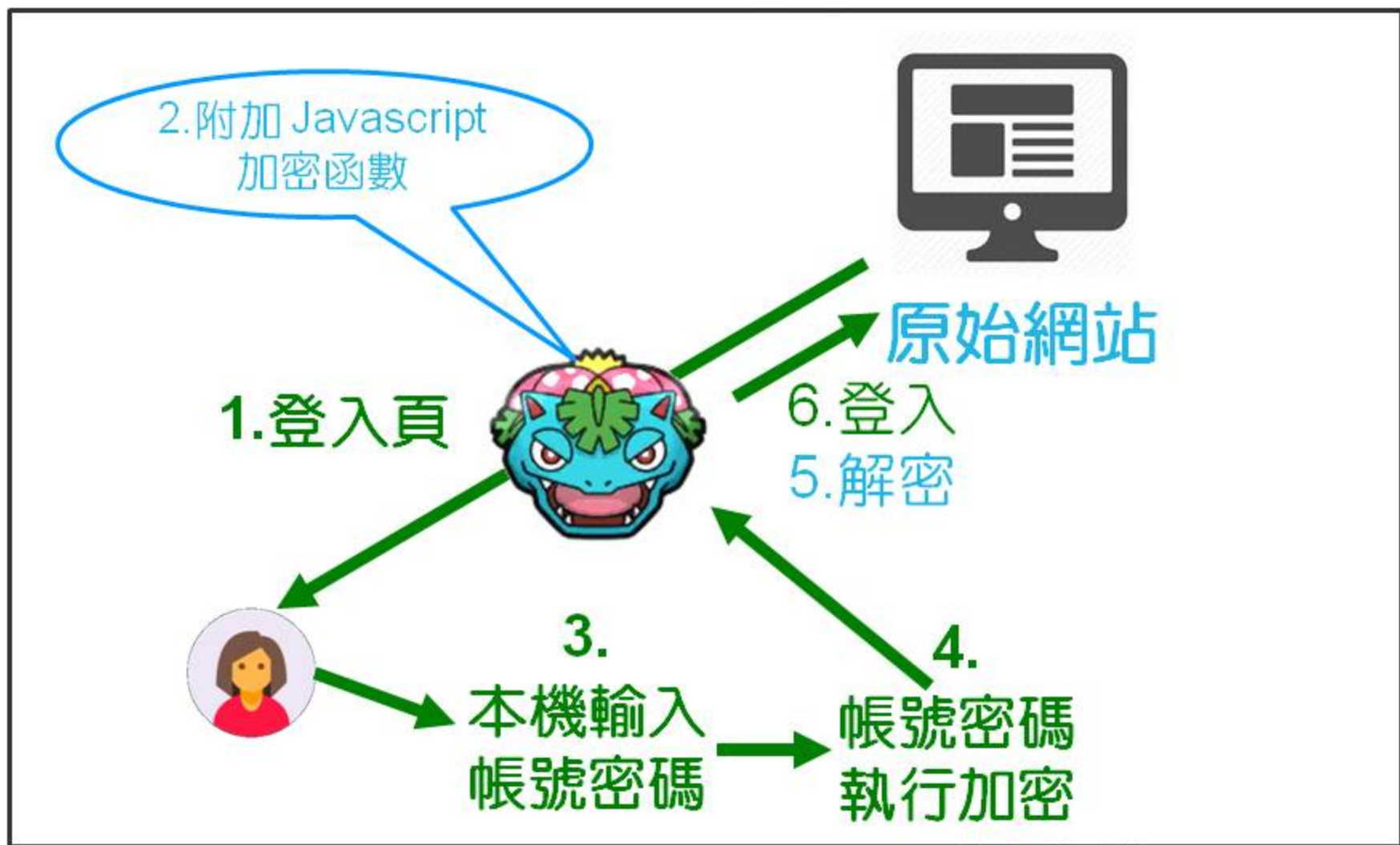
火牆



SSL VPN



網路釣魚與網址嫁接



應用層控制

快取 (Cache)

壓縮 (Compression)

前端網頁最佳化 (FEO)

依照國家或地區提供不同回應

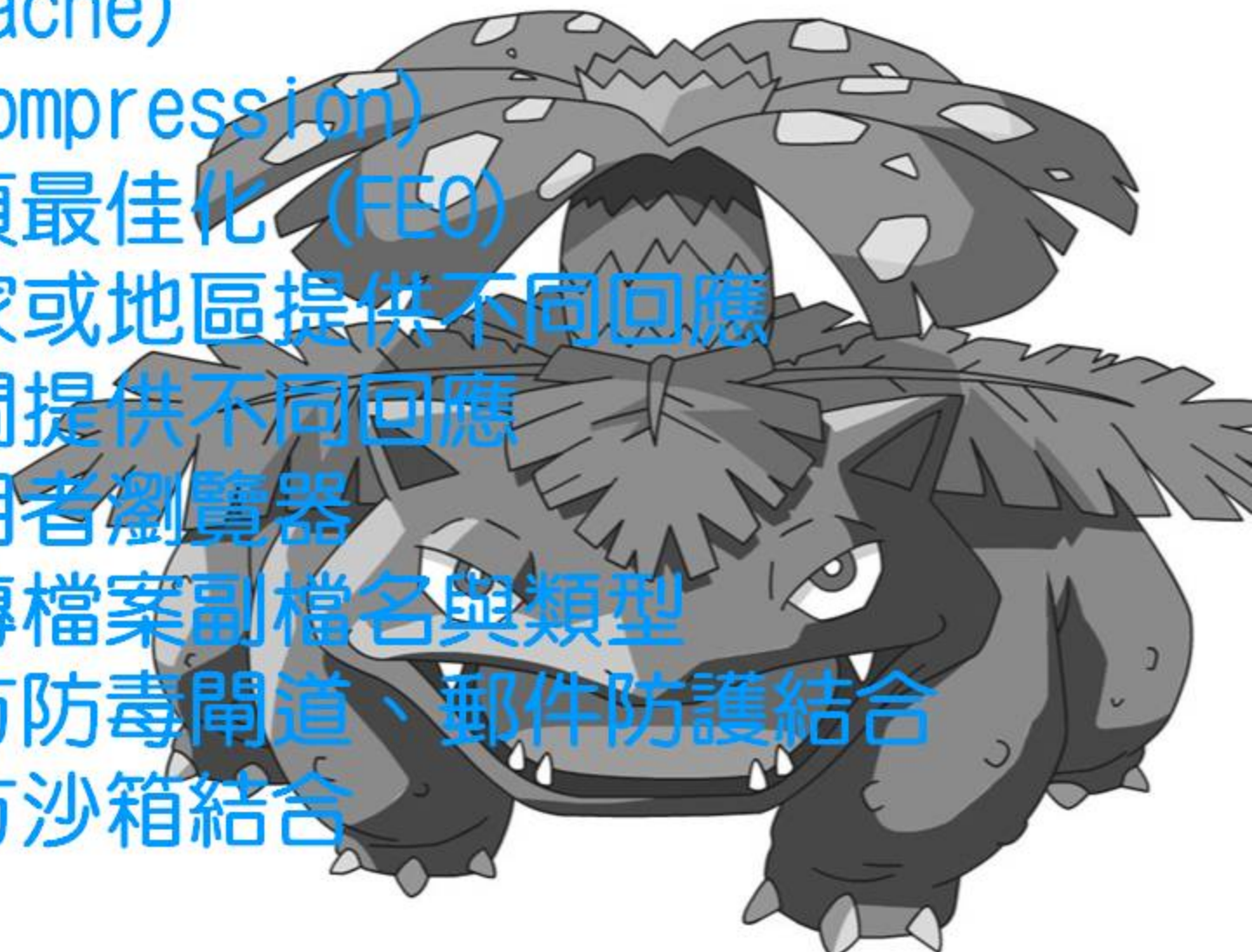
依照時間提供不同回應

識別使用者瀏覽器

限制上傳檔案副檔名與類型

與第三方防毒閘道、郵件防護結合

與第三方沙箱結合





擋住！化成肉盾！



洩洪



挽狂瀾



郵件主機

網站

資料庫

AD主機

應用層

DDoS



系統層



DDoS

網路層



入侵偵測

程式攔道

防火牆






二套防火牆

防毒牆

SSL VPN

DDoS



L7	 Application		Slowloris, Slow Post/GET, HTTP GET/POST floods, ...
L6	 Session	 SSL	DNS UDP floods, DNS query floods, DNS NXDOMAIN floods SSL floods, SSL renegotiation, ...
L5		 DNS, NTP	
L4	 Network		SYN/UDP/Conn. floods, PUSH and ACK floods, ICMP/Ping floods, Teardrop, Smurf Attacks, ...
L3			
L2			





反 D D O S

Call Me

S



反 D D O S

Call Me

SO



反 D D O S

Call Me

SOD



反 D D O S

提供



OWASP Taiwan Chapter
The Open Web Application Security Project



The HoneyNet Project
Taiwan Chapter

DEMAND **SOFT**
ND

反

0

S



郵件主機



站



資料庫



AD主機

SynFlood

TCP/UDP Flood

Reflection

DDoS



入侵偵測

程式攔道

防火牆

第二套防火牆

防火牆

SSL VPN





郵件主機



網站



資料庫



AD主機

已知特徵資料
IP信譽



SoD

SynCookie
Surge Queue
TCP Offload
TCP Optimization

QoS
Rate Control
Dynamic ACL



防火牆



第二套防火牆



防毒牆



SSL VPN



柱式南坦

入侵



限制連線頻率



系統漏洞

大量搜尋商品
CC攻擊 (i frame)
CC攻擊 (Proxy)
洋蔥網路
防毒牆



入侵偵測
程式闖道



防火牆



第二套防火牆



SSSEVPN

AD主機

快問快答



郵件主機



資料庫



AD主機

系統漏洞

SoD



入侵偵測

防火牆

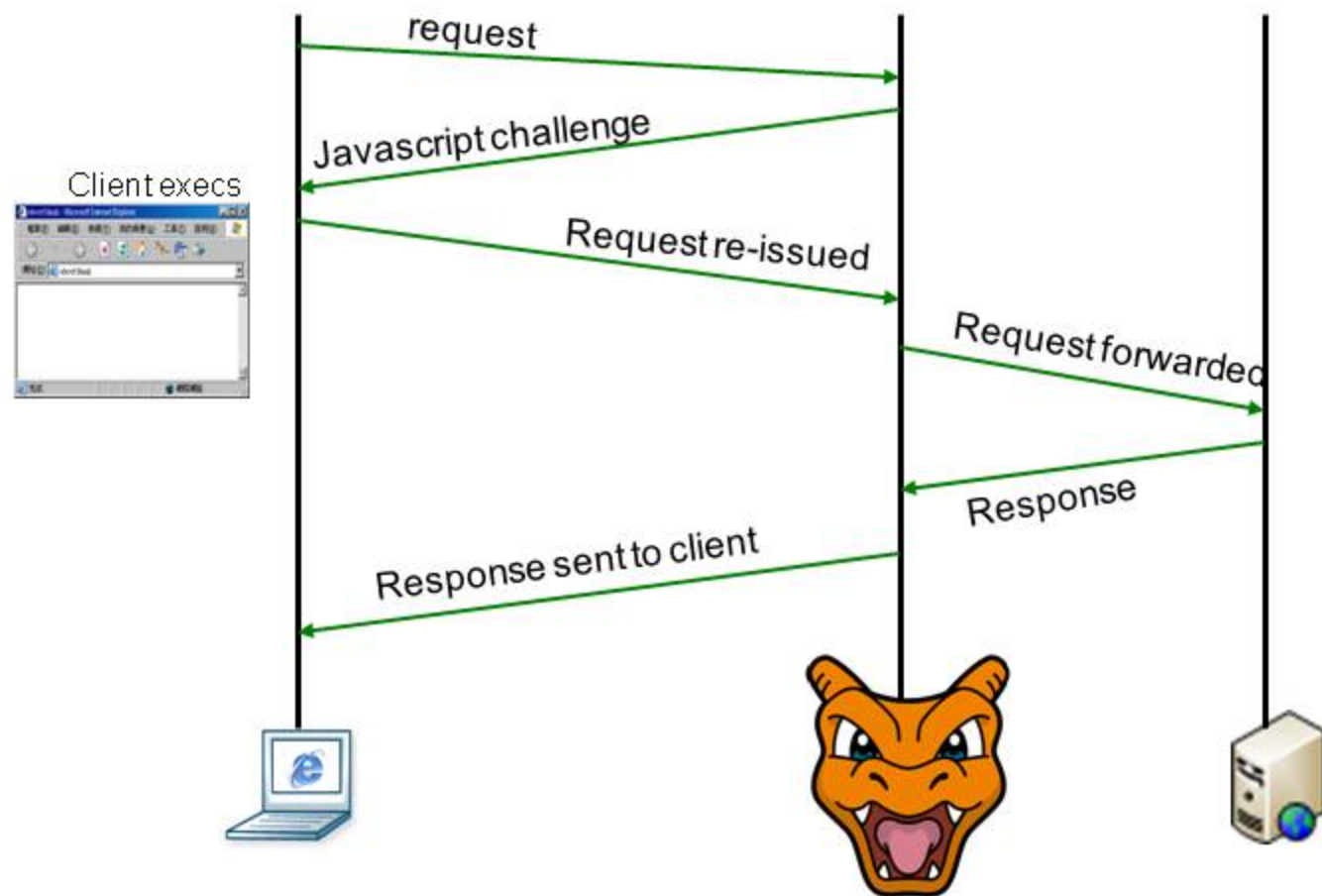
第二套防火牆

防毒

SSL VPN



以 JavaScript 辨識是否為正常瀏覽器



反DDoS

同時部署不同方案
因應不同手法



雲端雞蛋籃



識者不能瞞

七層山海關

洩洪挽狂瀾

蛋雞蛋籃

讓懶懶的來

識者不能瞞

七層山海關

洩洪挽狂瀾



成功因素
在人

「雲端」顧問有兩種



「雲端」顧問有兩種



「雲端」顧問有兩種



你需要另一種...



要專業

熟知雲端系統，排除架構問題
具備開發能力，協助研發人員修正
熟知攻擊手法，了解邏輯面問題



WAF

會交際

資安、系統與研發的三向溝通
責任_{推卸}歸屬與工作協調



L7

拍馬屁

沒有長官/資安政策支持 = 不用作



SoD

lucifer.yang
小老鼠 sti.com.tw

資安解決方案規劃

網頁防火牆

資料庫稽核

資料防洩

資安服務

滲透測試

弱點掃描

緊急應變

程式碼檢測

資安強化SOP



有沒有
問題？

