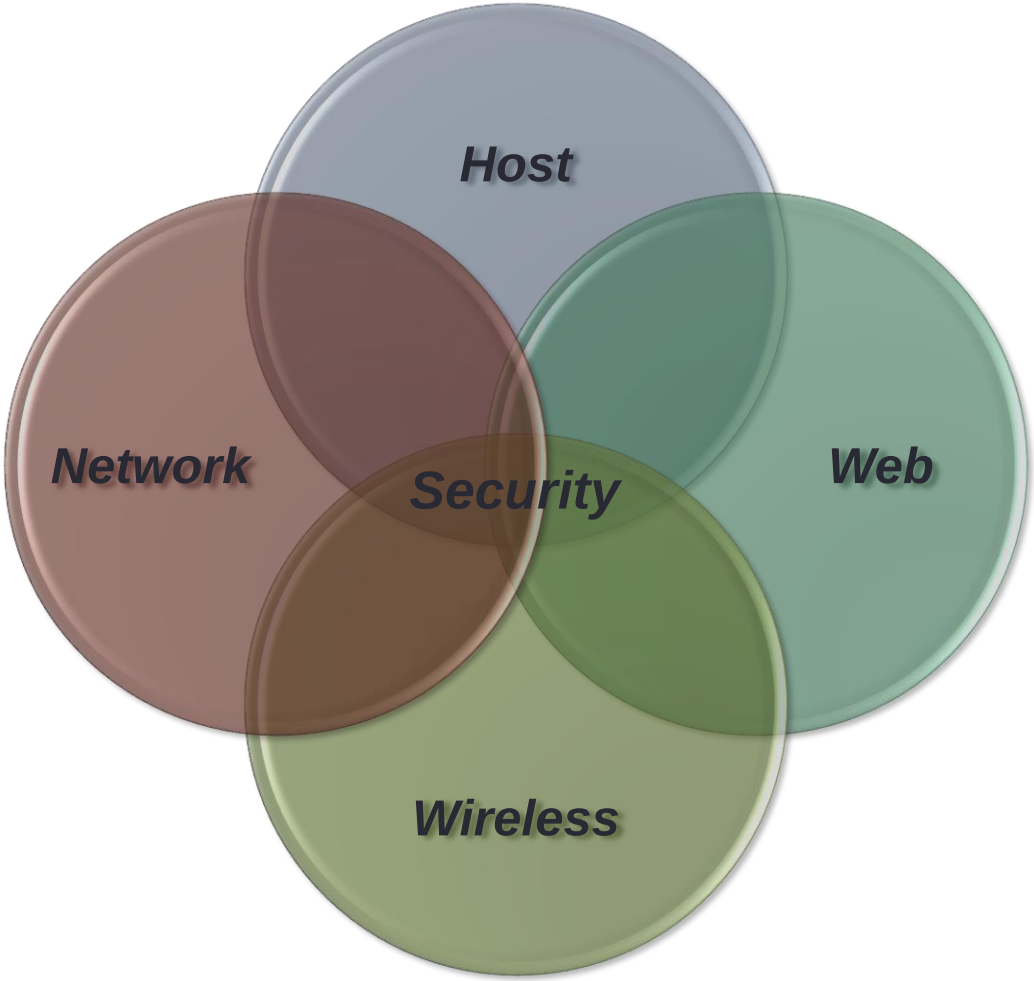
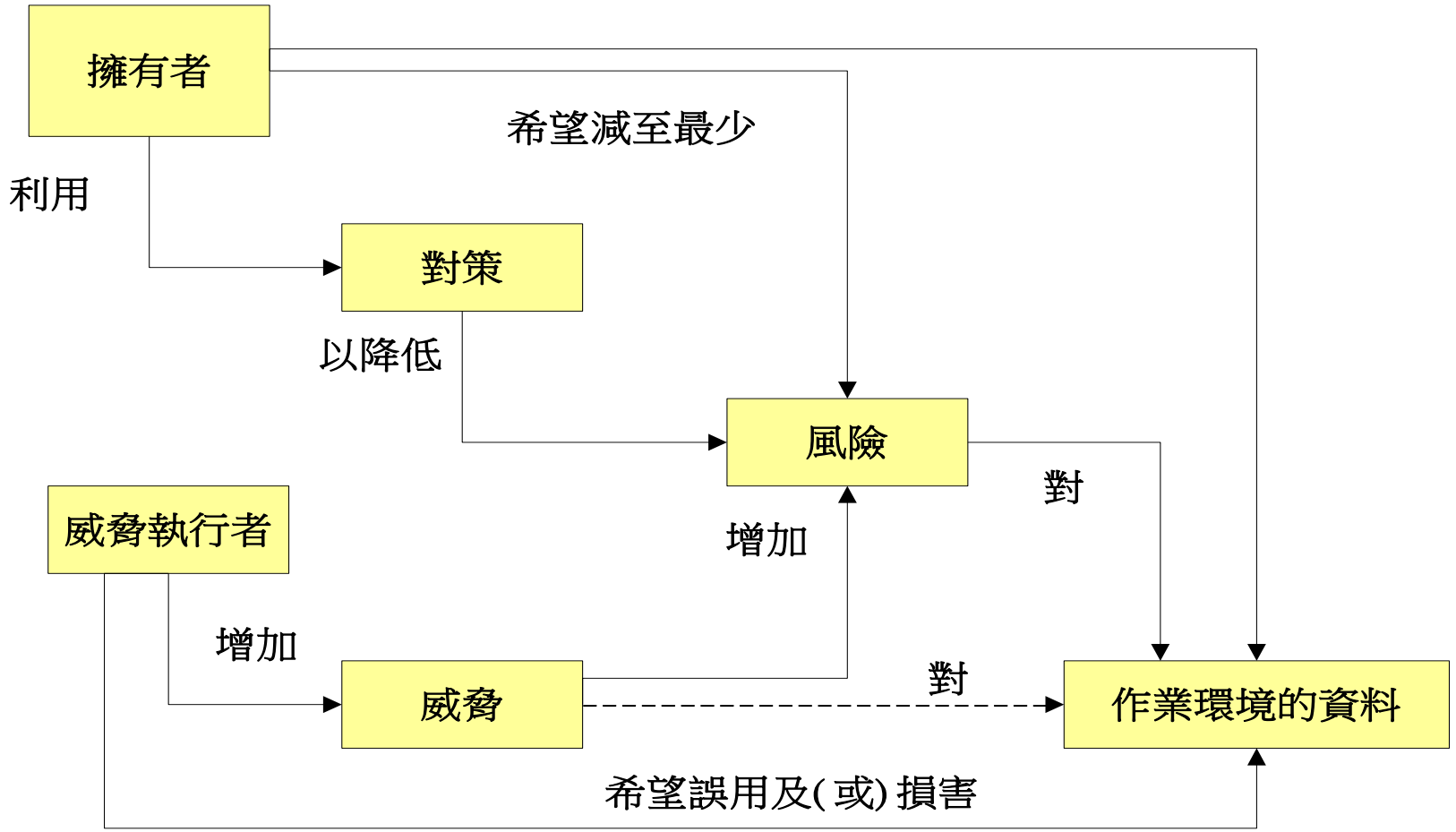
脆弱點的安全管理

網路安全 - 四大領域

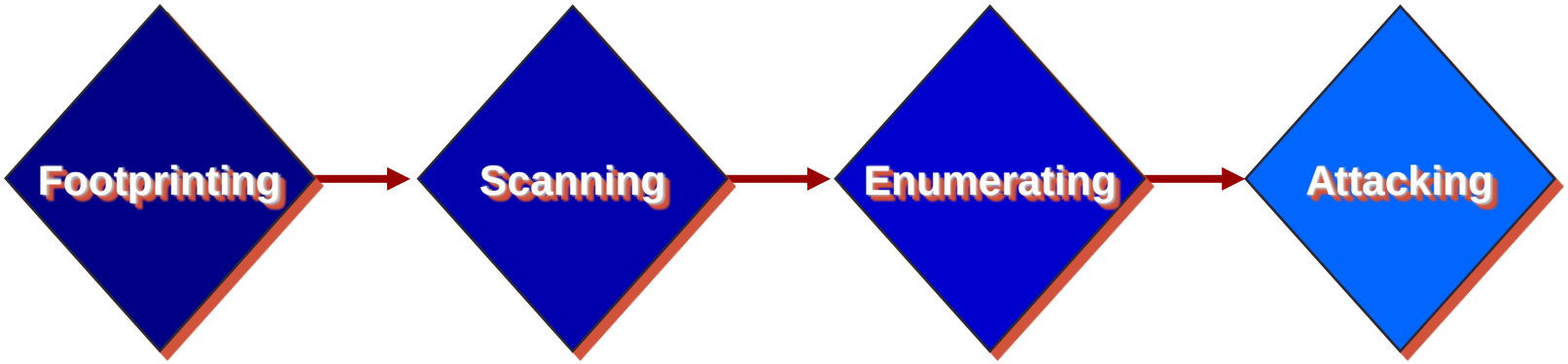


安全概念與關係



資料來源：ISO/IEC JTC 1/SC 27 WG 3 (2005) ISO/IEC WD 15408-1 Figure 1, p.10。

入侵的步驟



資訊安全管理系統技術性控制

- 技術脆弱性管理程序的正確運作對許多組織是不可或缺的，因此需要經常的監控。精確的財產清冊對確保識別潛在相關的技術脆弱性而言是基本的。
- 技術脆弱性管理能被視為變更管理的次功能，同時能利用變更管理的過程與程序。
- 供應商通常面臨儘快發行修補程式的強大壓力。因此，修補程式可能未充分地處理問題與有負面的副作用。同時，在某些案例中，一旦修補程式起作用，解除安裝可能不容易完成。
- 若不可能充分地測試修補程式，例如：因為成本或缺乏資源，依據其他使用者報告的經驗，考慮延後安裝修補程式以評估相關的風險。

網路安全性-脆弱點

- 程式錯誤(Bug)
  - 由於程式中運算邏輯上的流程或設計錯誤，導致程式執行後所得到之結果並 非預期結果，稱之為程式錯誤(Bug)，導致系統或元件不能實現其功能。如果在執行中遇到程式錯誤，可能引起系統或應用程式的失效。
- 脆弱點(Vulnerability)
  - 定義為發生於軟體、韌體及微程式中的 Bug，且若此 Bug 遭利用，會導致資料的機密性、完整性或可用性產生負面影響。因此，若為硬體零件設計不良導致產品外殼損毀等，則不可稱之為漏洞。

脆弱點揭漏

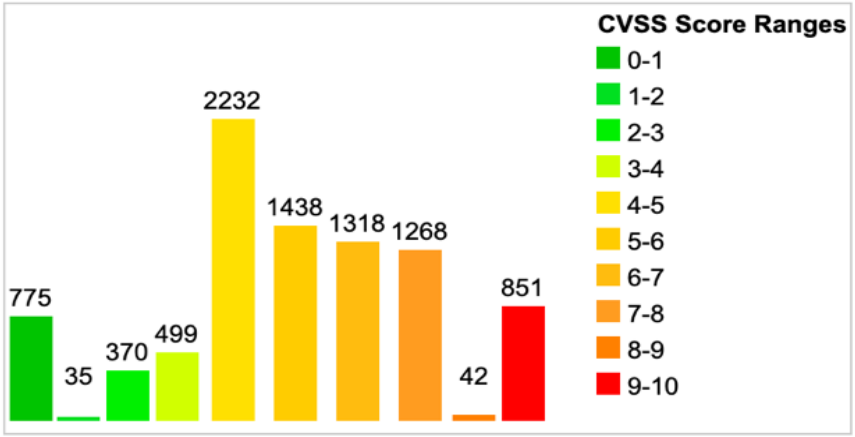
- 通用脆弱點揭露(Common Vulnerabilities and Exposures, CVE)為一個記錄 已知產品漏洞之資料庫，資料庫中記錄產品廠商、產品名稱、漏洞描述及參考源等。
- 此資料庫目前由美國非營利組織 MITRE 所營運維護，且於全世界被廣為 使用，其中亦包含美國官方資安單位等。
- 網址:https://cve.mitre.org/

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	775	8.80
1-2	35	0.40
2-3	370	4.20
3-4	499	5.70
4-5	2232	25.30
5-6	1438	16.30
6-7	1318	14.90
7-8	1268	14.40
8-9	42	0.50
9-10	851	9.60
Total	8828	

Weighted Average CVSS Score: **5.9**

Vulnerability Distribution By CVSS Scores



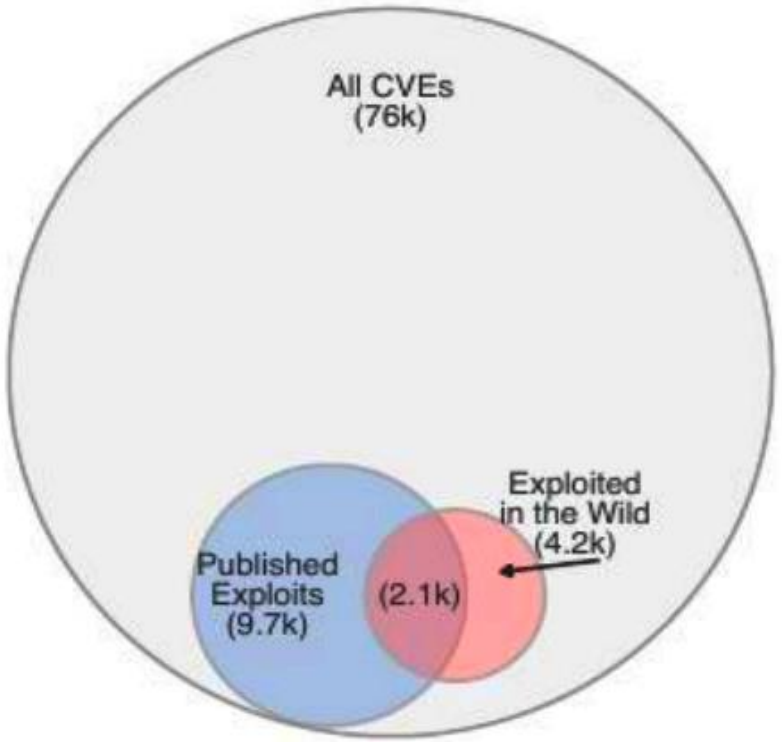
CVE ID

- CVE 編號(CVE ID) 每個記錄在 CVE 中的漏洞皆會被發放一個獨特編號，以利引用時可代表特 定漏洞，該編號則被稱作 CVE 編號(CVE ID)，亦可稱做「CVE Entry」、「CVE」或「CVE number」，且其格式為 CVE-YYYY-NNNN，N 的部分至少 4 碼，最長 則無限制
- 例如 CVE-2017-0144，此 CVE ID 代表的則是 2017 年造成嚴重感染 事件之 WannaCry 勒索軟體，攻入目標主機時所使用之漏洞。

脆弱點與網路安全的關係

	Vendor Name	Number of Vulnerabilities
1	Microsoft	668
2	Google	609
3	Oracle	489
4	Adobe	441
5	Cisco	440
6	IBM	364
7	Debian	360
8	Cpanel	321
9	Redhat	257
10	Jenkins	254
11	Apple	229
12	Canonical	197
13	Fedoraproject	187
14	Qualcomm	171
15	Linux	170
16	Foxitsoftware	162
17	Opensuse	148
18	HP	129
19	Gitlab	119
20	Mozilla	118
21	Netapp	112
22	Apache	108
23	Intel	92
24	SAP	75
25	Magento	72

2019年公開脆弱點揭漏統計



依據統計:2009年至2018年的9年間，在全球被公開揭露的75,976個公開脆弱點中（CVE），約有12.8%的漏洞出現公開的攻擊程式，但在實際的攻擊行動中，只有一半採納了這些公開攻擊程式。

CWE (Common Weakness Enumeration)

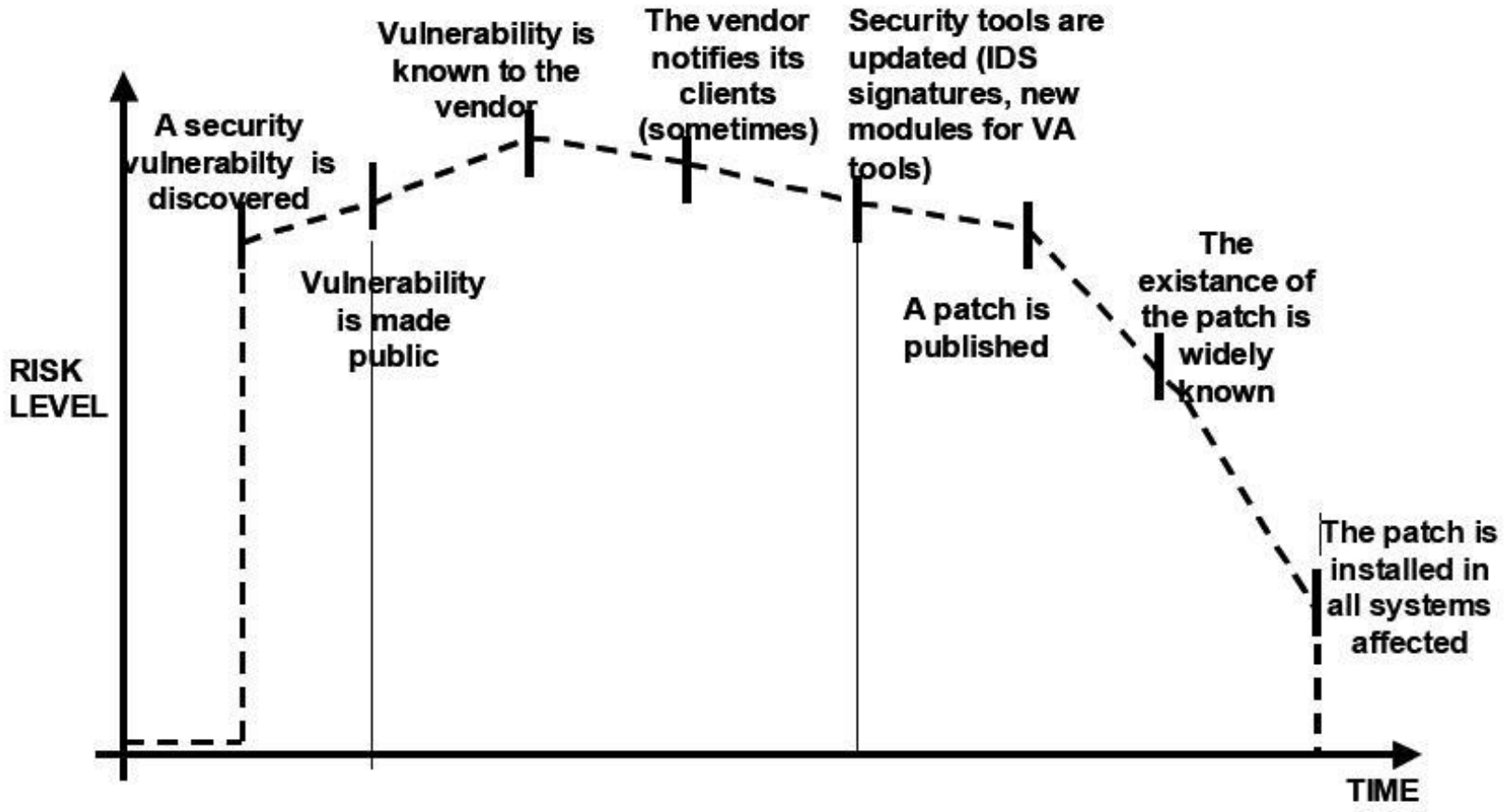
- MITRE 在 2005 年開始發展新的弱點與攻擊的分類概念，目的在於定義軟體缺陷 (Software Weakness)。
- 軟體的缺陷 (Weakness) 與弱點 (Vulnerability) 是不同的，缺陷會導致許多弱點，而弱點將會直接讓攻擊者用於攻擊。MITRE 在 CVE 的基礎上，蒐集許多會產生弱點的真實程式碼，並以缺陷的角度制定了新的分類方法，針對軟體弱點的 CWE 便因此發展出來。

CWSS

- CWSS 使用的 18 項評分因子分為三大類，與風險高低相關的評分因 子會被歸類於 Base Finding Group，與攻擊難易程度相關的評分因子歸類於 Attack Surface Group，而與關某特定環境下相關的評分因子則歸類於 Environmental Group，評

Metric Group	Factors
Base Finding Group	* Technical Impact (TI) * Acquired Privilege (AP) * Acquired Privilege Layer (AL) * Internal Control Effectiveness (IC) * Finding Confidence (FC)
Attack Surface Group	* Required Privilege (RP) * Required Privilege Layer (RL) * Access Vector (AV) * Authentication Strength (AS) * Authentication Instances (AI) * Level of Interaction (IN) * Deployment Scope (SC)
Environmental Group	* Business Impact (BI) * Likelihood of Discovery (DI) * Likelihood of Exploit (EX) * External Control Effectiveness (EC) * Remediation Effort (RE) * Prevalence (P)

脆弱點與風險值的關係


RISK LEVEL
A security vulnerabilty is discovered
Vulnerability is known to the vendor
Vulnerability is made public
The vendor notifies its clients (sometimes)
Security tools are updated (IDS signatures, new modules for VA tools)
A patch is published
The existance of the patch is widely known
The patch is installed in all systems affected
TIME

National Vulnerability Database

- 是美國政府專門用來收集各種資訊系統安全漏洞和弱點資料的資料庫網站，由美國國家標準技術研究所（NIST）負責維護
- SCAP (Security Content Automation Protocol) 的資料儲存庫，SCAP 是一種自動化系統安全和弱點管理、量測與政策相依性檢測的標準，經由SCAP 驗證工具和 SCAP 資料庫的合作，可以將脆弱點管理達到一定程度的自動化
- https://nvd.nist.gov

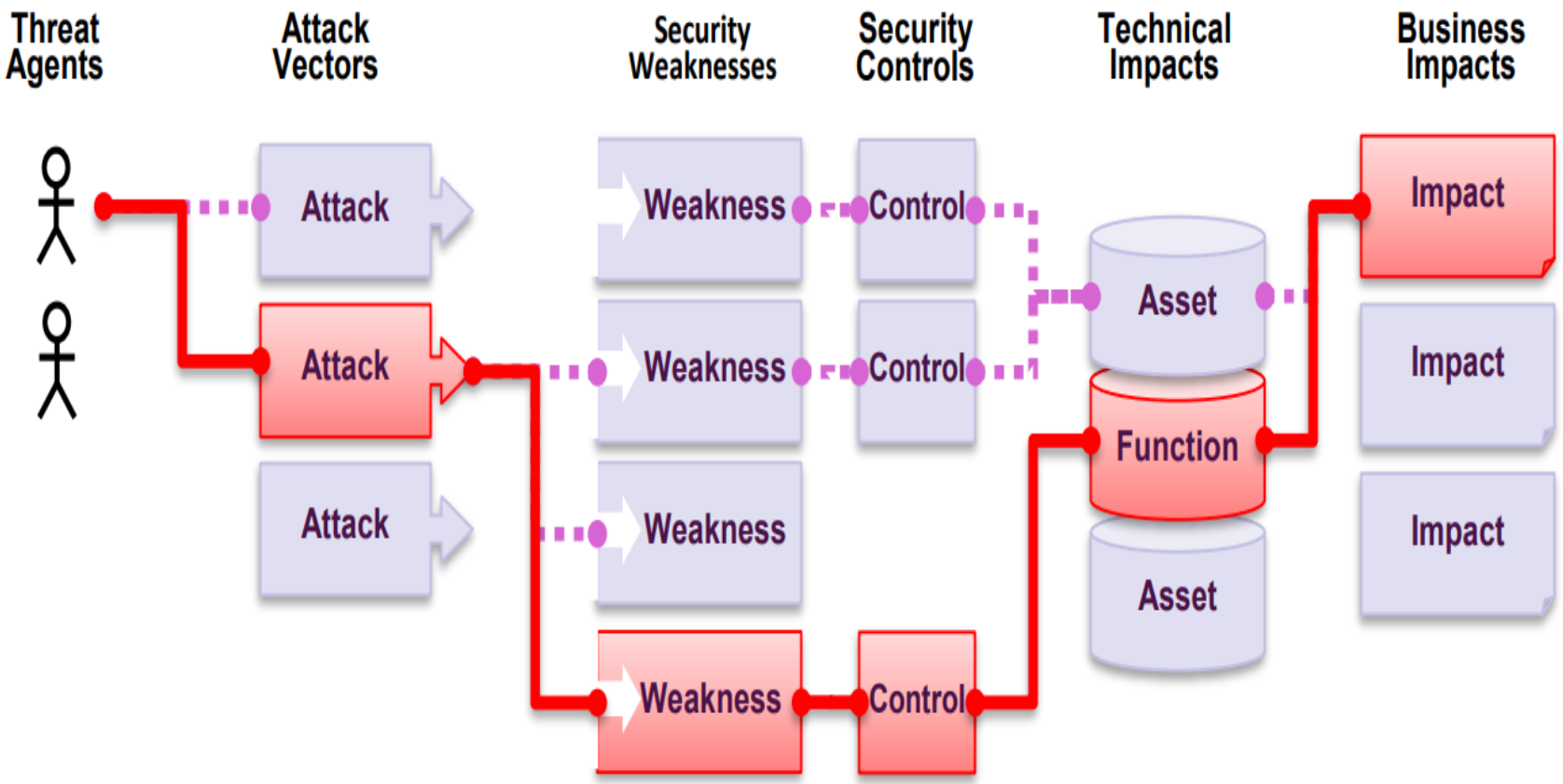
OWASP 計畫簡介

- 開放網路軟體安全計畫，簡稱OWASP（Open Web Application Security Project）是一個開放社群、非營利性組織，全球目前有82個分會，其主要目標是研議協助解決網路軟體安全之標準、工具與技術文件，長期致力於協助政府或企業瞭解並改善應用程式的安全性。美國聯邦貿易委員會（FTC）更強烈建議所有企業務必遵循OWASP所發佈的十大網路弱點防護守則，美國國防部亦將此守則列為最佳實務，就連國際信用卡資料安全技術PCI標準更將其列為必要元件。
- 目前OWASP有30多個進行中的計畫，包括最知名的OWASP Top 10（OWASP十大網路應用系統安全安全弱點）、WebGoat（代罪羔羊）練習平台、安全PHP/Java/ASP.Net等計畫，針對不同的軟體安全問題在進行討論與研究。

OWASP Top 10

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

OWASP(Weakness與安全性的關係)



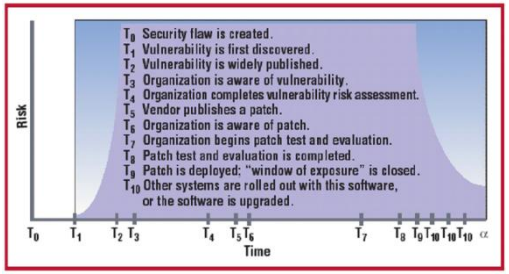
資訊安全管理系統技術性控制

安全性脆弱點生命週期

資料來源：Brykczynski, B. and R. A. Small (2003) Effective security patch management, IEEE Computer, Vol.20, No.1, pp.50~57 。

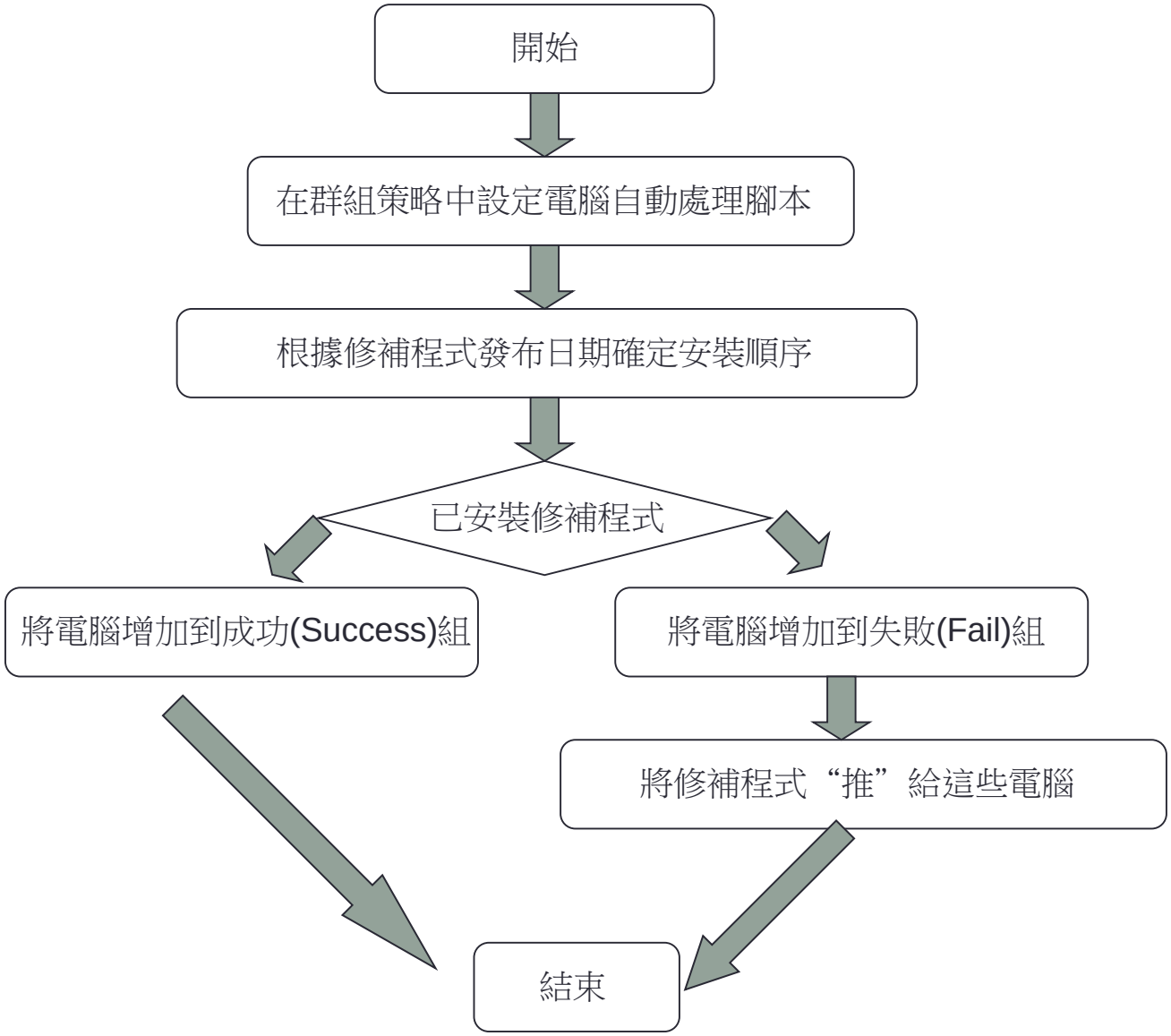
資訊安全管理系統技術性控制

安全性脆弱點生命週期(二)

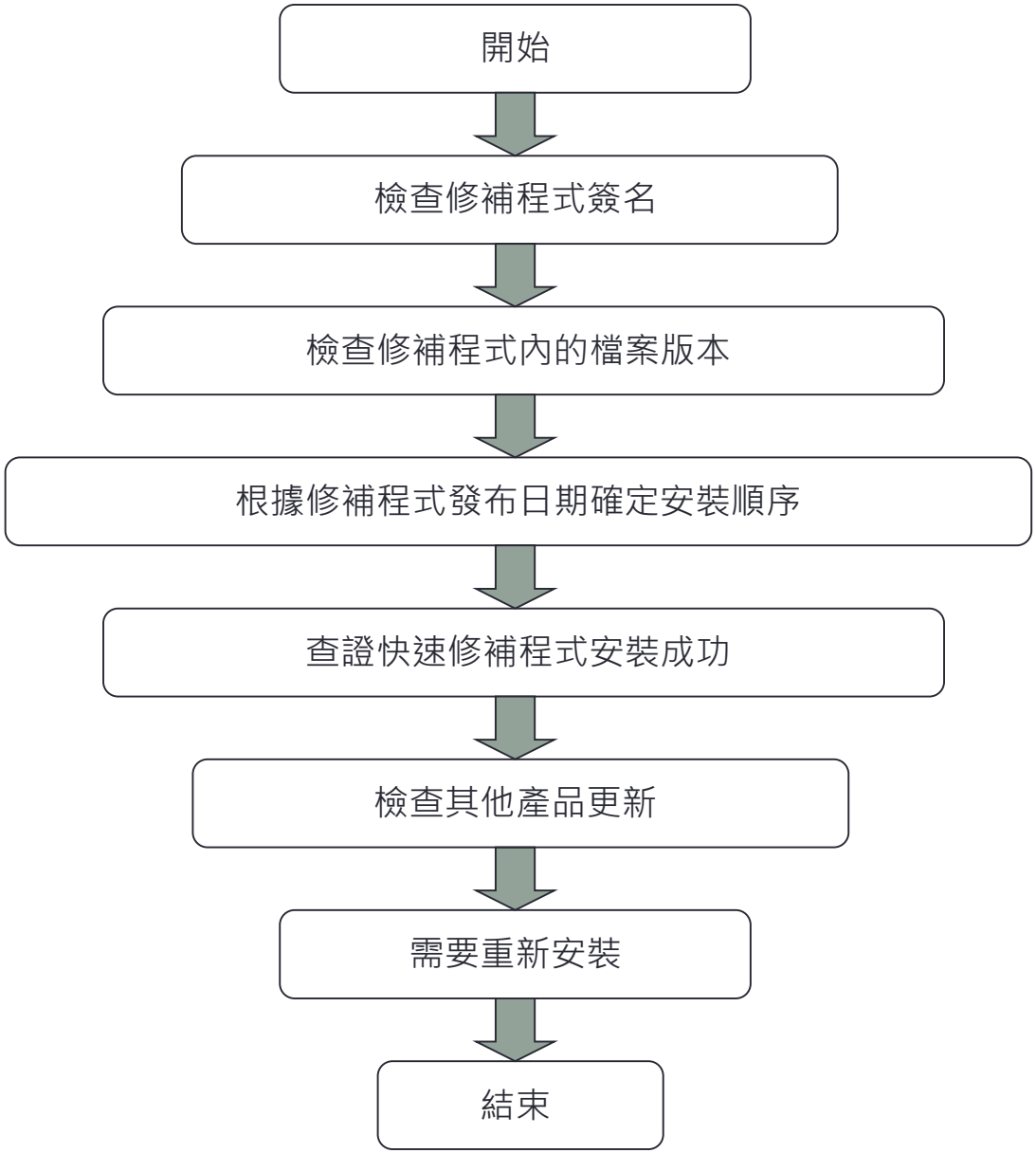


- T0 = 導致安全性缺點的缺陷產生。
- T1 = 發現弱點。早期公開發現的安全性缺點。
- T2 = 發現弱點。廣泛公開發現的安全性缺點。
- T3 = 發現弱點。組織察覺的的安全性缺點。
- T4 = 組織完成安全性缺點風險評鑑。
- T5 = 軟體廠商公告可用以解決缺點的新安全性相關軟體更新及對策。
- T6 = 組織察覺可用以解決缺點的新安全性相關軟體更新及對策。
- T7 = 組織進行安全性相關軟體更新測試。
- T8 = 核准變更要求。
- T9 = 確認部署軟體更新。
- T10 = 持續性安全性修補程式部署。

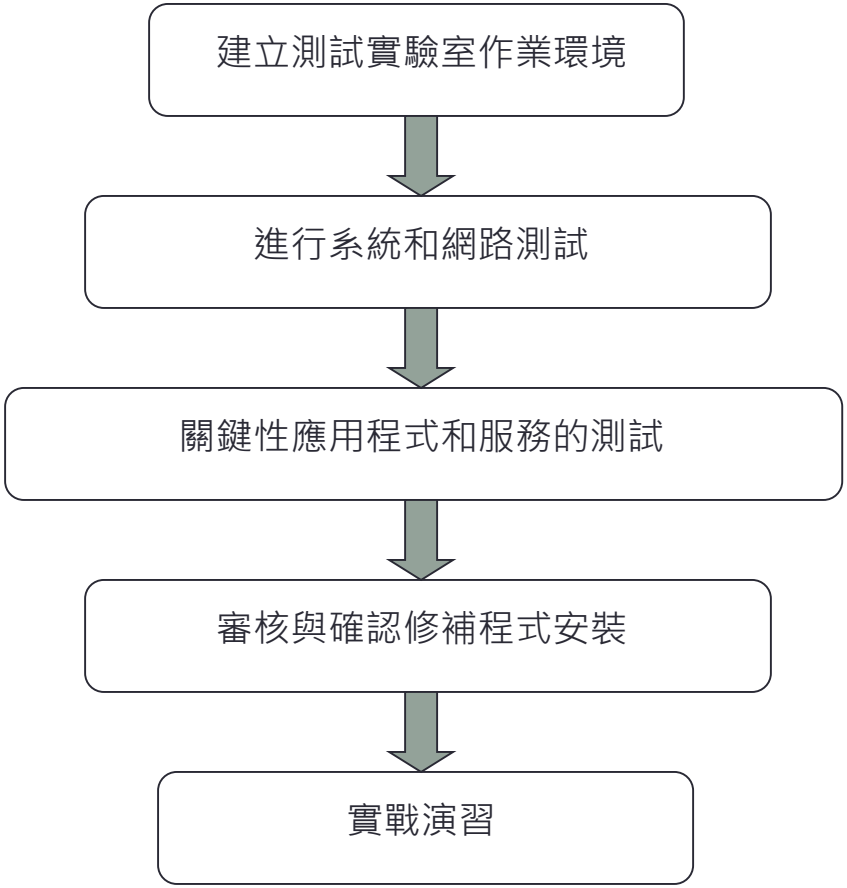
資訊系統組態管理實作


開始
在群組策略中設定電腦自動處理腳本
根據修補程式發布日期確定安裝順序
已安裝修補程式
將電腦增加到成功(Success)組
將電腦增加到失敗(Fail)組
將修補程式“推”給這些電腦
結束

資訊系統組態管理


開始
檢查修補程式簽名
檢查修補程式內的檔案版本
根據修補程式發布日期確定安裝順序
查證快速修補程式安裝成功
檢查其他產品更新
需要重新安裝
結束

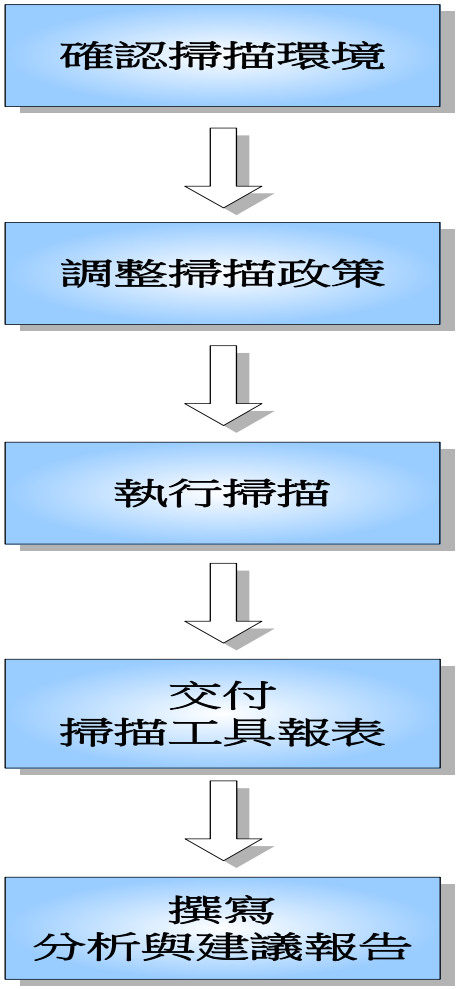
資訊系統組態管理實作



弱點掃描

- 弱點掃描 (Vulnerability Scanner, VS)
  - 弱點掃描是一種透過自動化工具的方式，針對系統上「已知」的漏洞進行檢測。
    檢測人員會事先與企業討論欲檢測的目標或範圍，以弱點評估工具快速的掃描，工具會將檢測到的漏洞產出報表作為參考。
- 常見可掃描的類型包含：
  - 作業系統漏洞
  - 網路設備漏洞
  - WEB 應用程式漏洞
  - 資料庫主機漏洞
- 由於弱點掃描是針對資料庫中已知的漏洞來做檢測，因此對於尚未被發現的系統漏洞，或是操作邏輯上的漏洞就無法檢測出。另外不同工具檢測的技術不同，也可能造成不一樣的結果。因此，弱點掃描仍需要請專業的人員來協助判讀，並將誤判的內容加以排除，才能找出系統真正的漏洞，並提早修補或改善。

弱點掃瞄評估服務執行程序



(1)確認掃描範圍
(2)確認掃描時間
(3)目標主機資訊搜集

(1)依照所得資訊調整Internet Scanner的
Scan Policy
(2)選擇其他輔助掃描工具

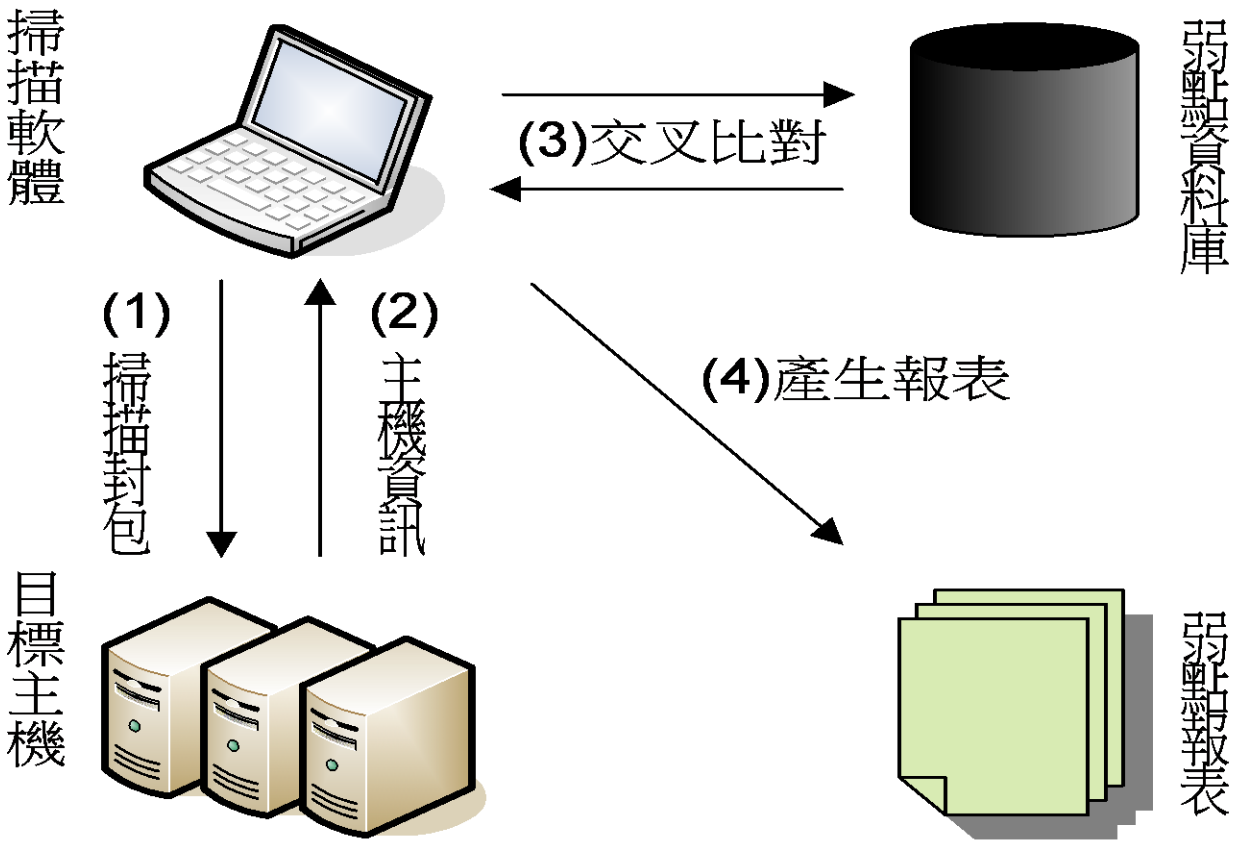
(1)在目標主機同一網段進行掃描
(2)檢查相關系統或應用程式的版本資訊
(3)檢查掃描所得結果確認是否為誤判
(4)測試掃描所得之帳號密碼

使用ISAM系統產生中文報表

※此報表僅為參考用，並未過濾誤判

提供整體安全建議

弱點掃瞄工作流程



系統脆弱點的掃描

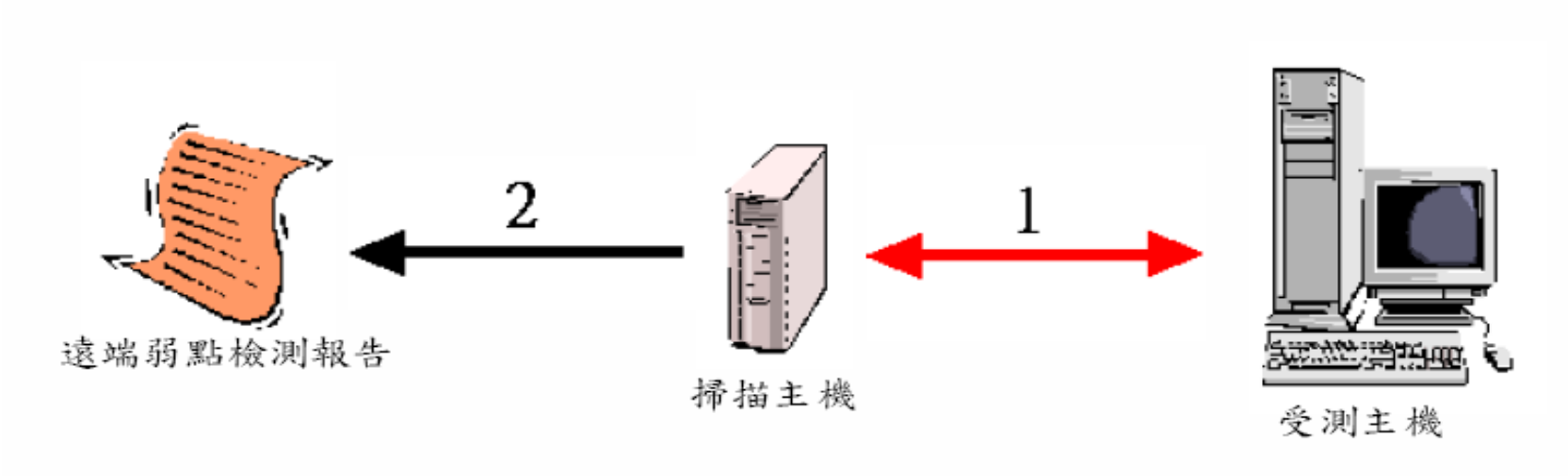
- 掃描的步驟
- 系統脆弱點的掃描工具
- 系統常見的脆弱點

掃描的步驟

- 第1階段：發現目標主機或網路。
- 第2階段：發現目標後進一步搜集目標資訊，包括作業系統類型、運行的服務以及服務軟體的版本等。如果目標是一個網路，還可以進一步發現該網路的拓撲結構、路由設備以及各主機的資訊。
- 第3階段：根據搜集到的資訊判斷或者進一步測試系統是否存在安全漏洞。

系統脆弱點的掃描

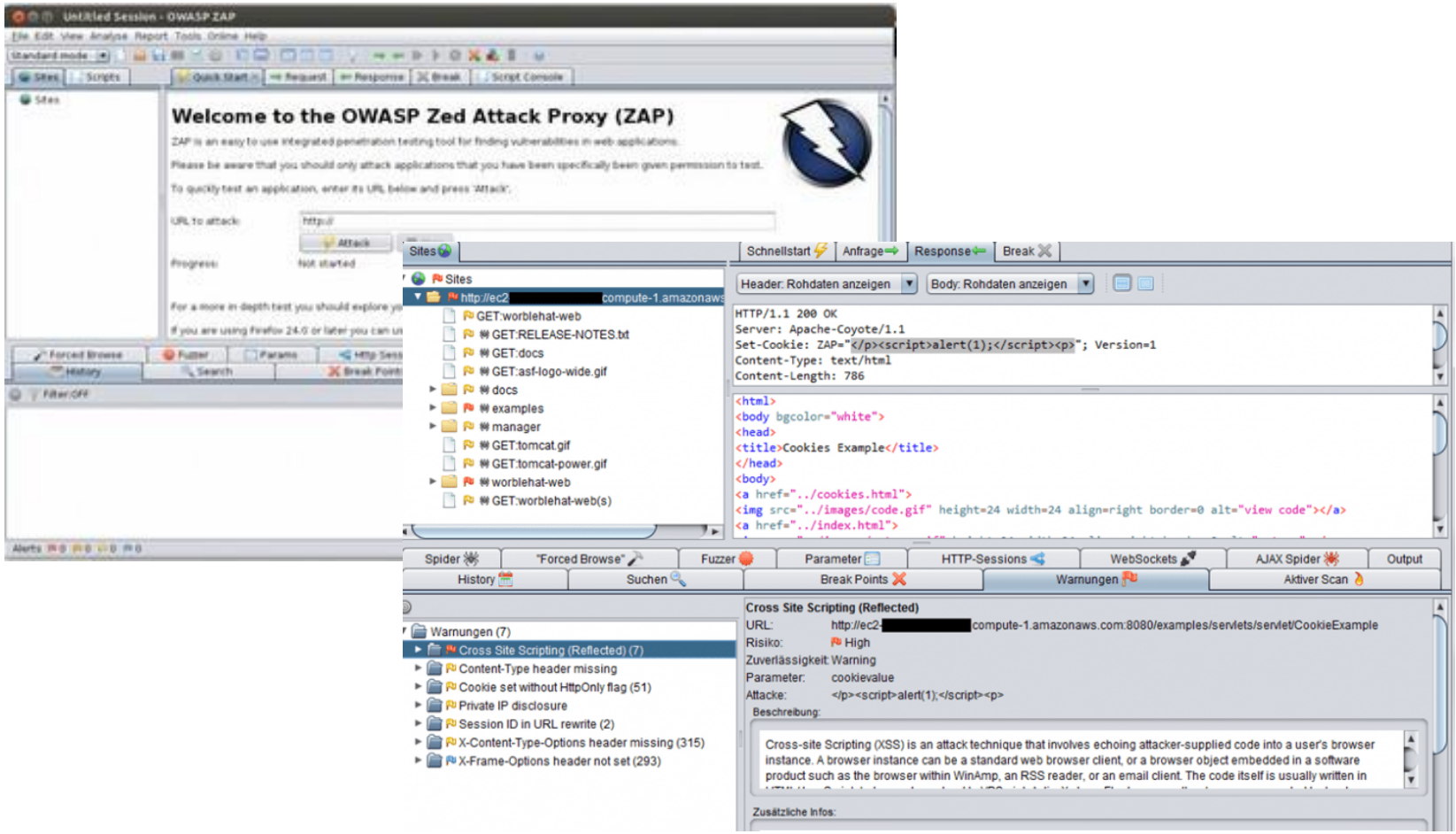
- 掃描主機透過網路對受測主機作遠端弱點檢測。
- 按照檢測的結果產生遠端弱點檢測報告，系統管理者藉此報告以作為未來系統補強的方向。



系統脆弱點的掃描的項目

- PING掃射（Ping sweep）、
- 作業系統探測（Operating system identification）
- 探測存取控制規則（firewalking）
- 埠掃描（Port scan）
- 漏洞掃描（Vulnerability scan）
- 攻擊框架程式應用
  - Metasploit, Core Impact等

OWASP ZAP

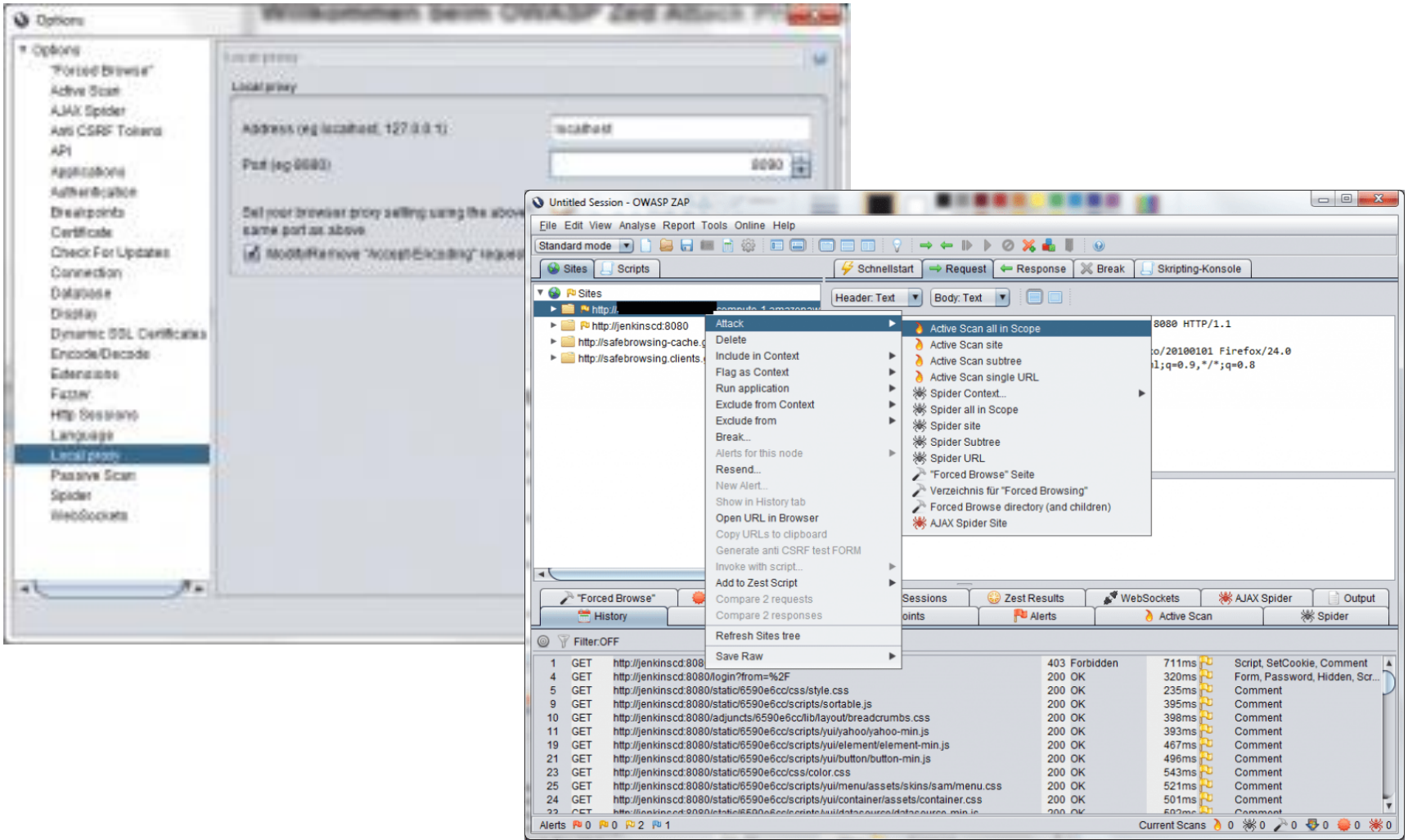

Untitled Session - OWASP ZAP
Welcome to the OWASP Zed Attack Proxy (ZAP)
Sites
Schnellstart
Anfrage
Response
Break
Header: Rohdaten anzeigen
Body: Rohdaten anzeigen
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: ZAP=" <script>alert(1);</script> "; Version=1
Content-Type: text/html
Content-Length: 786
<html>
<body bgcolor="white">
<head>
<title>Cookies Example</title>
</head>
<body>

<img src="../images/code.gif" height=24 width=24 align=right border=0 alt="view code">
<a href="../index.html">
GET:worblehat-web
GET:RELEASE-NOTES.txt
GET:docs
GET:asf-logo-wide.gif
docs
examples
manager
GET:tomcat.gif
GET:tomcat-power.gif
worblehat-web
GET:worblehat-web(s)
Spider
"Forced Browse"
Fuzzer
Parameter
HTTP-Sessions
WebSockets
AJAX Spider
Output
History
Suchen
Break Points
Warnungen
Aktiver Scan
Warnungen (7)
Cross Site Scripting (Reflected) (7)
Content-Type header missing
Cookie set without HttpOnly flag (51)
Private IP disclosure
Session ID in URL rewrite (2)
X-Content-Type-Options header missing (315)
X-Frame-Options header not set (293)
Cross Site Scripting (Reflected)
URL: http://ec2-[redacted]compute-1.amazonaws.com:8080/examples/servlets/servlet/CookieExample
Risiko: High
Zuverlässigkeit: Warning
Parameter: cookievalue
Attacke: <script>alert(1);</script>
Beschreibung:
Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in
Zusätzliche Infos:

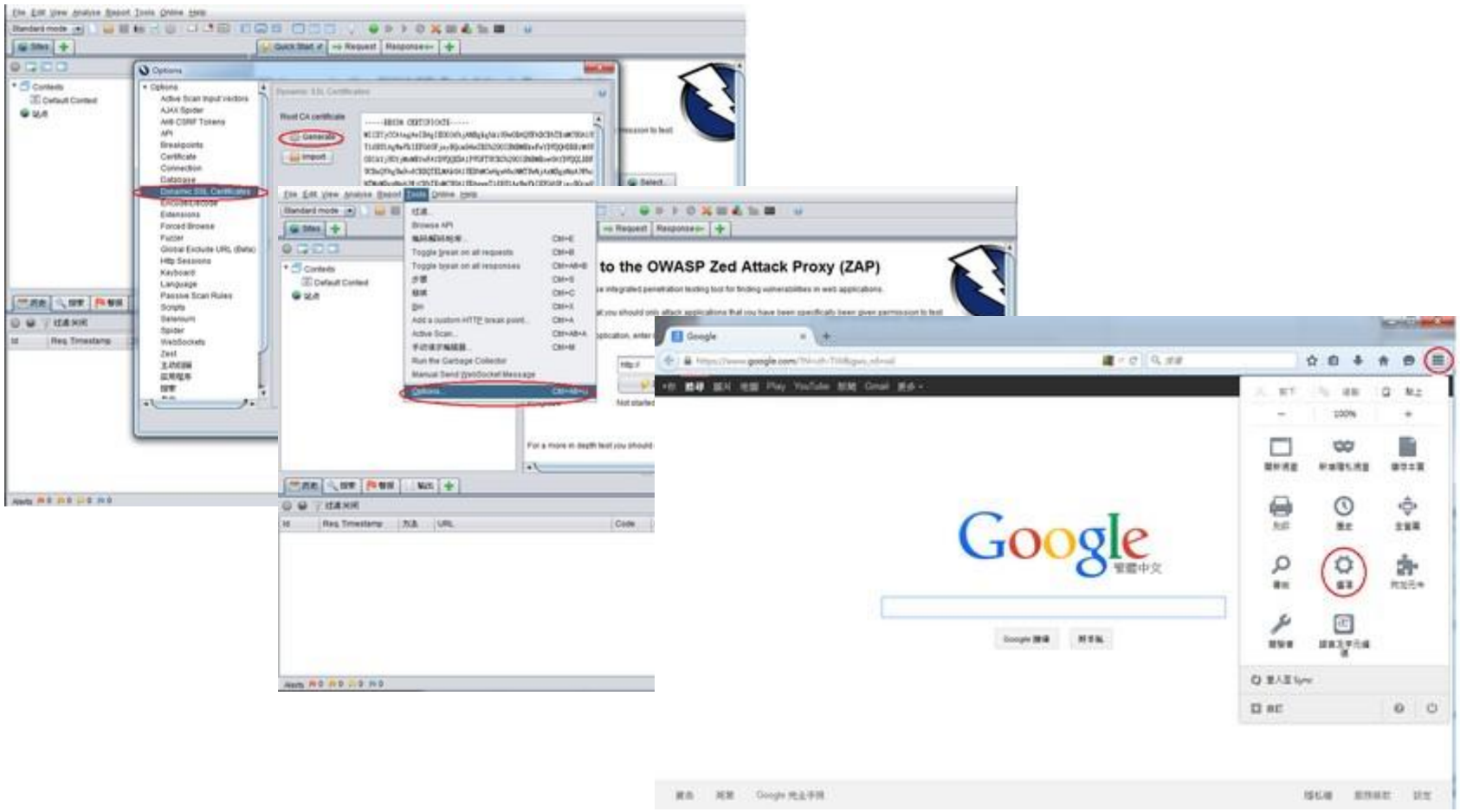
設定ZAP為代理主機(Proxy)

- 設定ZAP為Proxy目的是使用ZAP去記錄網路封包以及更改請求(Request)參數來進行測試，先在 瀏覽器設定使用ZAP為Proxy，因此Request便會經過ZAP再到網頁程
- **ZAP -> Tools -> Options -> Local Proxy.**

設定ZAP為代理主機(Proxy)

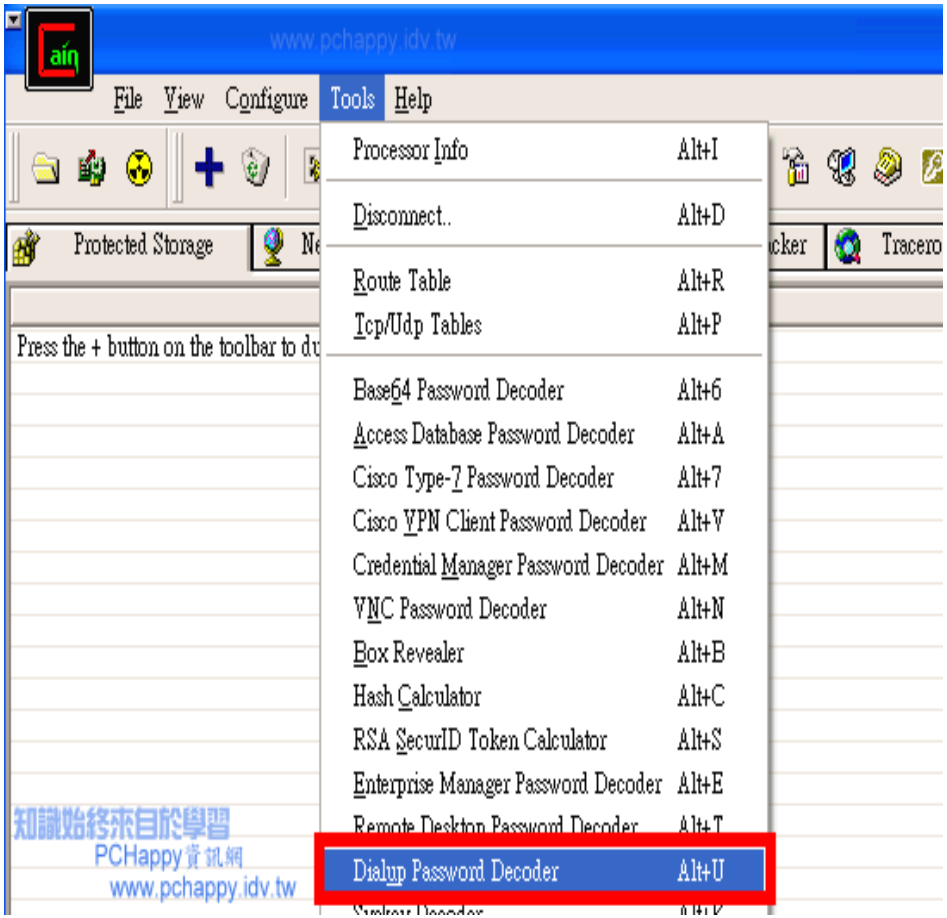


ZAP SSL憑證

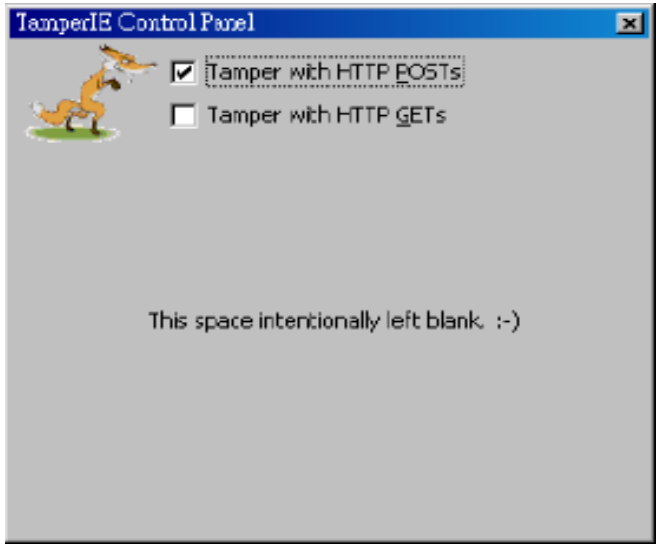

Options
Dynamic SSL Certificates
Root CA certificate
Generate
Import
to the OWASP Zed Attack Proxy (ZAP)
Google

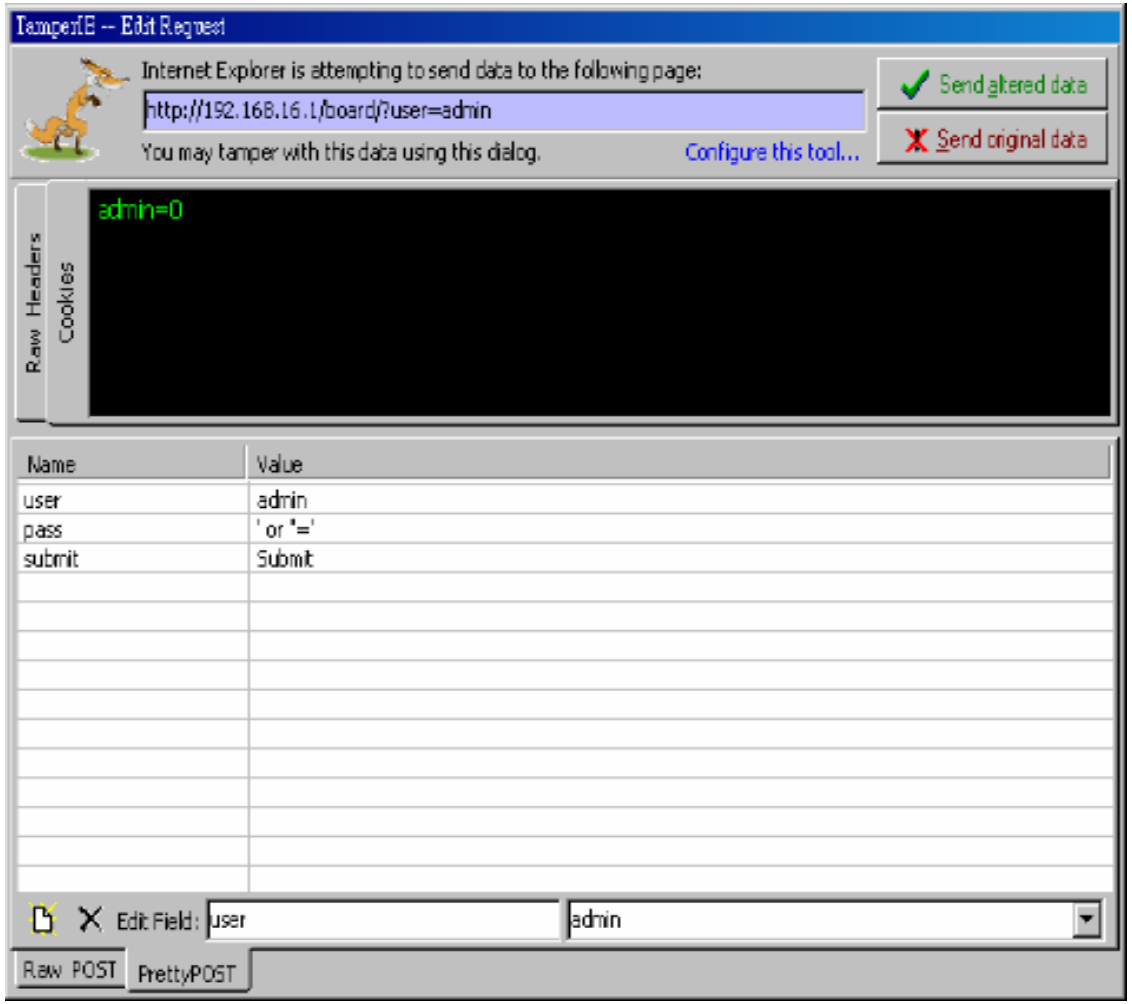
Cain & Abel

- oxid.it 發佈的Cain & Abel軟體，。Cain & Abel是一款專為微軟作業系統設計的密碼復原(竊取)軟體
- 主要透過ARP Spoofing的技巧，欺騙特定電腦假冒自己成中間人，以取得電腦與Gateway間傳遞的封包，並進而得到帳號密碼等資訊。
- 該軟體的限制為只能監聽到同一區域網路下的主機。



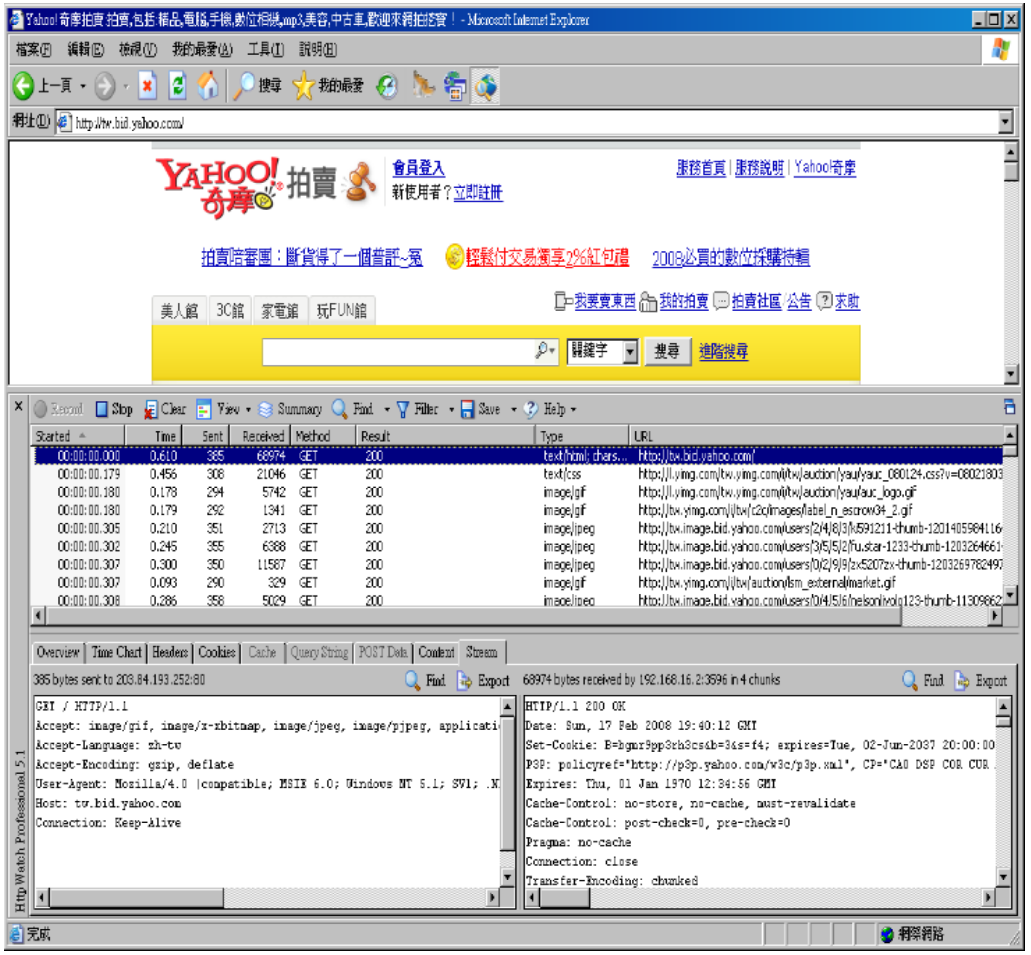
TamperIE -檢測跨網站腳本漏洞





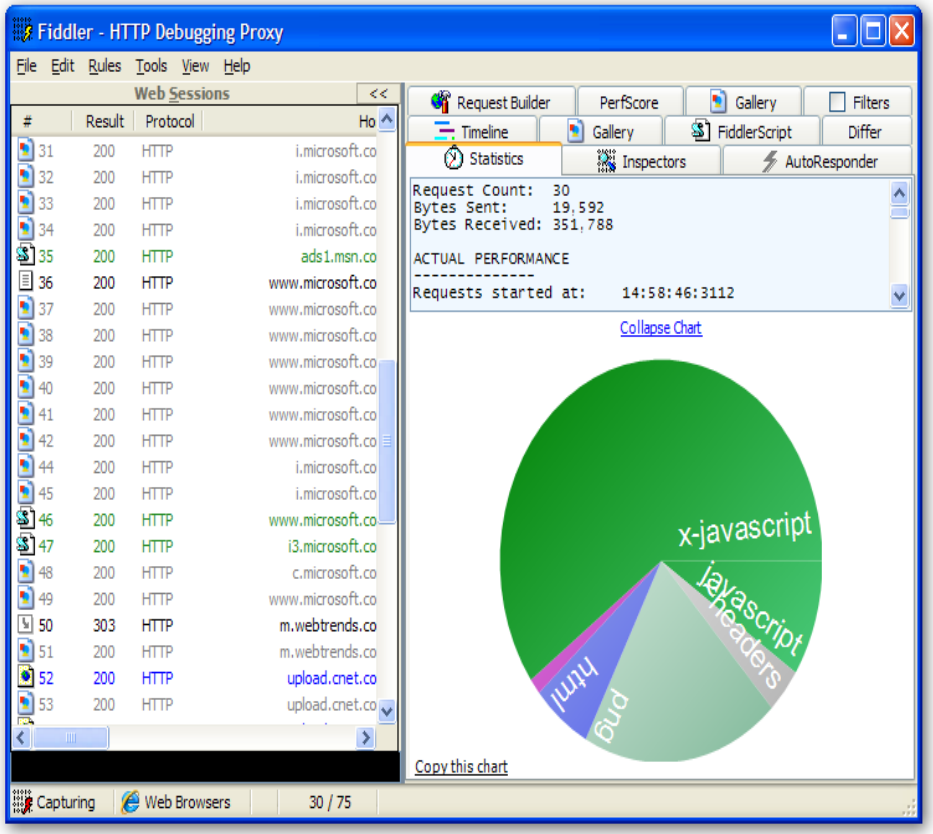
HTTPWatch

- HttpWatch是一款IE介面中的外掛程式，他可以幫我們分析上網時的流量細節，幫我們抓出某個網頁中有哪些連結、連線速度、檔案類型與連線狀態，方便我們找出哪些連線是否壞掉或速度過慢
- 網頁設計者可以輕易找出網站問題或進行安全性或效能調校。此外，更可方便網管人員查看網頁是否包藏啥木馬或病毒程式，以及更多進階訊息。



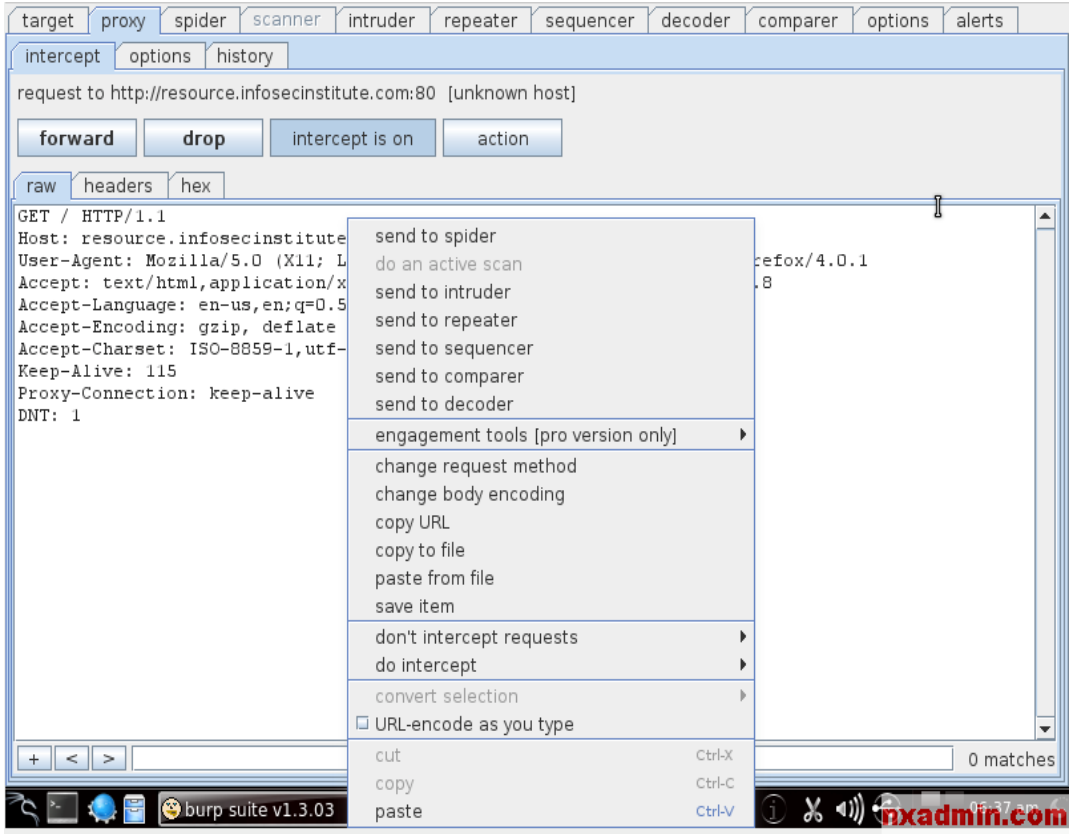
Fiddler

- 免費工具，可以用來觀看 HTTP 通訊的傳遞內容與方法
- 對於網頁程式設計師及網路管理人員的偵錯軟體



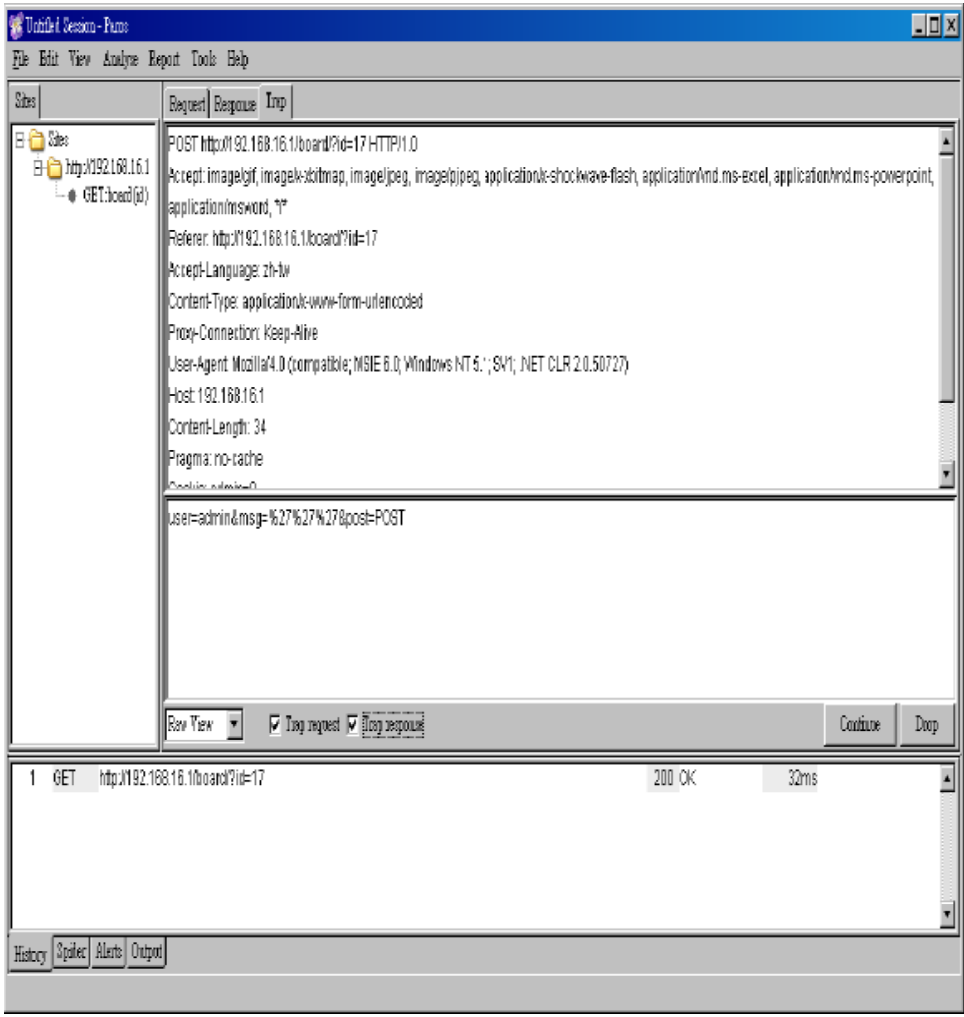
burp suite

- 可以用來檢視，請求跟觀看HTTP的傳輸內容，簡單的說就是web弱點檢測工具是一套自動化的檢測工具
- 基本上就是網路在進行 Request 時，會攔下相關的請求資訊，若確定資訊 OK 才會進行 Forward 的動作，當然也可以進行封包的修改。
- 有提供 Spider 的功能進行網站爬蟲，以及透過 Intruder 進行參數等資訊的測試，一般會應用在密碼猜測，且可同時應用多個參數，以不同的組合進行測試。而 Repeater 是 Intruder 的手動測試，可以直接取的 Response ，Decoder 則會產生 URL Encode 等編碼進行攻擊，最後更能透過 Compare 進行比較。



PAROS PROXY

- 網頁資料Proxy
- 許多客戶自己開發的網站應用網頁都有SQL injection、cross-site scripting、session cloning等問題。駭客可以利用特殊的Web proxy對這些網站應用網頁送出特製的資料，以便找出漏洞或者入侵系統。
- 網站資料Proxy是架設在攻擊者的瀏覽器和目標網站中間，所有的HTTP或HTTPS的要求和回應都會被送到proxy，藉此駭客得以仔細研究這些封包資訊，包括在網頁傳送中的cookies、hidden form變數，並可以修改這些變數後再送出。 Paros Proxy可以在Windows和Linux平台上操作（需要Java Runtime的環境），而Paros是這類型Web proxy中的最佳工具，它功能齊全，也讓它成為強大的駭客工具
- Paros也具備網站弱點掃描和偵測能力，對於一些常見的網頁應用程式攻擊，像是SQL injection、cross-site scripting，Paros都可以進行檢測。而Paros甚至能夠檢測出不安全的網頁元件，像是未簽署的ActiveX 控制項目，另外Paros可以偵測出來自惡意網頁伺服器端，針對瀏覽器漏洞的攻擊。



WIKTO

- WIKTO
  - 網站弱點掃描器與Google Hacking 工具
  - Web伺服器弱點掃描工具。一個放在網際網路上的Web應用程式為企業提供了許多商機，但也提供駭客們許多機會進行入侵。
  - 在去年，數以千計有問題的phpBB網站，以及許多利用AWStats這支CGI工具來統計主機流量資料的站台，紛紛淪為駭客的階下囚。除了這幾個著名的漏洞外，也有越來越多Web script漏洞一一被找出來。試試看Wikto這個令人激賞的檢測工具，來協助你找出這些已知或未知的漏洞。
  - Wikto是由一家位於南非的資安服務公司Sensepost所開發的，Wikto是建構在著名Nikto網頁掃描器的Perl script上，並且具備Windows GUI與許多功能。 和Nikto一樣，Wikto能夠檢測數千種有問題的網頁script程式、常見的設定錯誤，以及問題版本。
  - Wikto還增加了HTTP Fingerprinting功能，能夠藉由分析網頁伺服器的回應結果，來辨識出許多Web伺服器的類型。甚至，如果是網頁管理者刻意地改變網頁伺服器的Banner來躲避駭客偵查，Wikto亦可檢測出真實的伺服器類型。對於一個所謂的白帽者（White hat)而言，這真是非常強大的新功能。

SQL Injector安全測試

- (HP) Scrawlr
- NBSI
- HDSI
- Pangolin
- Absinthe
- DataThief
- SQL Power Injector
- Sqlget
  - http://www.infobyte.com.ar/
- sqlmap
- http://sqlmap.sourceforge.net/
  - sqldumper

Brute Force Attack

- THC-Hydra
  - http://www.thc.org/thc-hydra/
- Brutus AET2
  - http://www.hoobie.net/brutus/
- Unsecure
- ObiWaN
- Cain & Abel
- Authforce
- WebCracker
- Lophtcrack

Code Review

- 以程式對原始碼作靜態分析，取代傳統人工檢查
  - Microsoft Source Code Analyzer (ASP)
  - CodeScan (ASP/PHP)
  - CodeSecure (PHP/JSP)
  - Ounce (Java/.NET)
  - Pixy (PHP)
  - Fortify SCA (.NET/Java)
  - SWAAT (PHP)
  - Spike PHP Security Audit Tool (PHP)

Web Vulnerability Scan

- 以Web Vulnerability Scanner 進行掃描
  - 定期掃描
  - 驗收外包專案時
  - 新AP 上線前
  - 修改程式後
  - 更新signature 後

- Nikto
- Wikto
- Commercial
- (HP) SPI Dynamics - WebInspect
- (IBM) Watchfire -AppScan
- Acunetix - Web Vulnerability Scanner
- N-Stalker - Web Application Security Scanner

Web Application Firewall

- 可較有效阻擋Web 層攻擊之資安設備
- 代理模式處理SSL 加解密, 因此可分析https 加密封包
- 由“行為”模式判斷是否為攻擊
- 雙向保護，輸入及輸出資料皆進行檢查
- 設定較繁瑣, 需AP 開發人員配合

攻擊框架滲透工具應用

- 常見攻擊框架滲透工具
  - Metasploit
  - ImmunityCANVAS
  - CoreImpact

Metasploit

- Metasploit是一款開源的安全漏洞檢測工具。由於Metasploit是免費的工具，因此安全工作人員常用Metasploit工具來檢測系統的安全性
  - MetasploitFramework(MSF)是2003年以開放源代碼方式發佈、可自由獲取的開發框架，這個環境為滲透測試、shellcode編寫和漏洞研究提供了一個可靠的平台。它集成了各平台上常見的溢出漏洞和流行的shellcode，並且不斷更新，最新版本的MSF包含了180多種當前流行的操作系統和應用軟件的exploit，以及100多個shellcode。作為安全工具，它在安全檢測中起到不容忽視的作用，並為漏洞自動化探測和及時檢測系統漏洞提供有力的保障。
- Metasploit的安裝文件可以到官方網站進行下載。
- http://metasploit.com/framework/

Metasploit滲透測試系統

- 滲透測試(penetration testing)工具內建許多可用來入侵與攻擊的模組
- 採用Ruby程式語言開發，蒐集了各作業系統平台常見的系統漏洞攻擊程式，包括緩衝溢位攻擊，以及針對目標作業環境所夾帶的攻擊碼
- Metasploit可在Windows 、Linux、MacOS X等作業系統下使用
- Metasploit於最新版本中提供了圖形介面程式

- 謝謝您的參與！

Turn Knowledge Into Valuable Services …