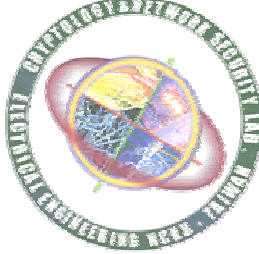
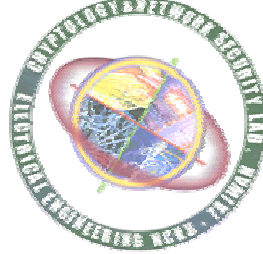
# 網路安全測試平台簡介

報告人:陳培德
國立成功大學電機工程學系 博士候選人
E-mail:peder@crypto.ee.ncku.edu.tw
http://crypto.ee.ncku.edu.tw/
FAX:(06)2743533
2004年4月1日



# 大綱

- 網路安全測試平台規劃與建置
  - 美國Mini-Internet Testbed
  - 我國網路安全測試平台
- Q & A



# 美國Mini-Internet Testbed

- 2003/10/9 ISI (Information Sciences Institute)發佈USC/UCB關於Mini-Internet Testbed消息
  - 學術界
    - UC Berkeley、ISI、SRI、Pennsylvania State University、Purdue University, Princeton University、 UC Davis 、 University of Utah等
  - 工業界
    - Juniper、CISCO、Intel、IBM、HP

# Mini-Internet news

**News from ISI**
University of Southern California School of Engineering
Information Sciences Institute

## USC/UCB 'Mini-Internet' Testbed Will Improve Defenses Against Net Attacks

**October 9, 2003** Last Modified: October 23, 2003

A three-year, $5.46 million grant from the National Science Foundation will establish a testbed to evaluate and improve defenses against Internet-spread computer worms, viruses and denial-of-service attacks, as part of a two-pronged $10.8 million NSF anti-cybercrime initiative.

The University of California, Berkeley and the University of Southern California's Information Sciences Institute (ISI) will partner in the project, called the cyber DEfense Technology Experimental Research network, or DETER.

"With so much of the nation and the world's business now dependent on the Internet," said ISI's Terry Benzel, a nationally recognized expert on cybersecurity who is a DETER co-principal investigator, "we are no longer talking about nuisance pranks and vandalism, but potential losses in the billions of dollars. We need better tools to protect ourselves."

DETER will be a facility where such tools can be tested and perfected. The project's architects will use sophisticated methods to create a closed, isolated network that can credibly represent the makeup and operation of the entire Internet, from routers and hubs to end users' computer desktops.

The DETER testbed will consist of approximately 1,000 computers with multiple network interface cards, located off the actual Internet. Three permanent hardware clusters, or nodes, at UC Berkeley and at ISI's Southern California and Virginia facilities, will serve as the core of the system.

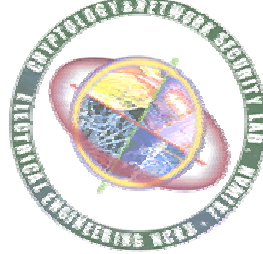
**Press Contact**

Eric Mankin
mankin@usc.edu
(310) 448-9112

**Information Sciences Institute**

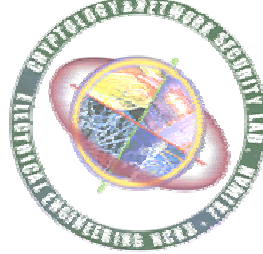
4676 Admiralty Way,
Suite 1001
Marina del Rey, CA 90292
(310) 822-1511
http://www.isi.edu

This isolated mini-Internet will serve as a shared laboratory where researchers from government, industry and academia can test existing and new security technology, using a wide variety of attack techniques.



# Background

- 資金來源
  - NSF、DHS
- 計畫名稱
  - Cyber Defense Technology Experimental Research (DETER) $1億8仟萬 (US$5.46 million)
  - Evaluation Methods for Internet Security Technology (EMIST) $1億7仟萬(US$5.34 million)
- 經費資助時間
  - 2003年9月 ~ 2006年8月



# DETER Project目標

- 建置一個有利於科學實驗且與真實網際網路隔離的Testbed，以避免影響到真實網路運作
- 可提供給政府、學術界、工業界相關研究人員進行新網路安全、攻擊技術研究
- 提供教育訓練資源，培養網安相關人才

# EMIST Project目標

- 對於網路的攻擊和防禦機制，以合乎科學化方式進行精準的測試
- 攻擊場景、攻擊模擬、背景流量, 真實流量的取得, 監控及分析結果的工具
- 在不同攻擊行為下，實驗不同網路環境的參數設定及防禦機制
- 在DETER Testbed進行上述實驗

# 目前兩種主要的防禦重點項目

- Distributed Denial of Service Attacks
- Worm Defenses

# 2003年我國政府單位遭受攻擊位居全球前五名

**Overt Digital Attacks - Top 20 attacked Governments**

**Top 20 - January 2003**

| Rank | Country | Code | Attacks |
|---|---|---|---|
| 1 | Brazil | BR | 47 |
| 2 | China | CN | 22 |
| 3 | Taiwan | TW | 19 |
| 4 | United States | US | 17 |
| 5 | Argentina | AR | 6 |
| 6 | Australia | AU | 6 |
| 7 | United Kingdom | GB | 6 |
| 8 | Turkey | TR | 5 |
| 9 | Egypt | EG | 4 |
| 10 | Costa Rica | CR | 3 |
| 11 | Jordan | JO | 3 |
| 12 | Korea, South | KR | 3 |
| 13 | Mexico | MX | 3 |
| 14 | Thailand | TH | 3 |
| 15 | Venezuela | VE | 3 |
| 16 | Ecuador | EC | 2 |
| 17 | Germany | DE | 2 |
| 18 | Indonesia | ID | 2 |
| 19 | Iran | IR | 2 |
| 20 | Peru | PE | 2 |
| | Others | | 16 |

**Top 20 - Last 12 Months**

| Rank | Country | Code | Attacks |
|---|---|---|---|
| 1 | China | CN | 203 |
| 2 | United States | US | 192 |
| 3 | Brazil | BR | 172 |
| 4 | Turkey | TR | 120 |
| 5 | Taiwan | TW | 92 |
| 6 | Australia | AU | 68 |
| 7 | Mexico | MX | 60 |
| 8 | Nigeria | NG | 59 |
| 9 | Colombia | CO | 42 |
| 10 | United Kingdom | GB | 36 |
| 11 | Argentina | AR | 35 |
| 12 | Peru | PE | 35 |
| 13 | Bolivia | BO | 29 |
| 14 | El Salvador | SV | 27 |
| 15 | India | IN | 26 |
| 16 | Malaysia | MY | 25 |
| 17 | Morocco | MA | 21 |
| 18 | Poland | PL | 21 |
| 19 | Philippines | PH | 20 |
| 20 | Korea, South | KR | 19 |
| | Others | | 282 |

**2003年1月份**

**計有19次攻擊**

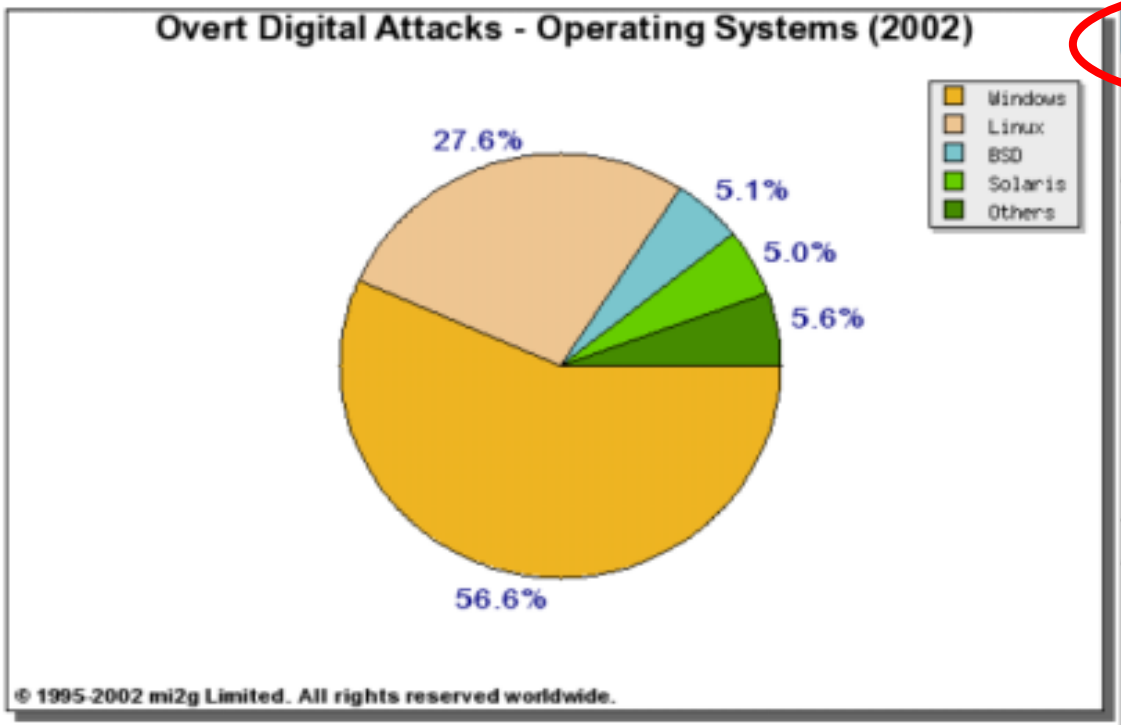
**2003年總共**

**計有92次攻擊**

**資料來源：mi2g**

# 微軟系統為駭客主要攻擊對象

## Operating Systems - Top attacked OS (2002)




| Rank | Operating System | Attacks |
|---|---|---|
| 1 | Windows | 49527 |
| 2 | Linux | 24189 |
| 3 | BSD | 4490 |
| 4 | Solaris | 4395 |
| 5 | Unknown | 3369 |
| 6 | Unix | 783 |
| 7 | AIX | 254 |
| 8 | IRIX | 193 |
| 9 | SCO Unix | 187 |
| 10 | MacOS | 79 |
| 11 | HP-UX | 24 |
| 12 | Compaq Tru64 | 12 |
| 13 | OS/2 | 11 |
| 14 | Novell | 6 |
| 15 | Digital Unix | 3 |
| 16 | VM | 2 |
| 17 | OS/390 | 1 |



資料來源：mi2g

媒體 大成報 記者 王雪玲 版別 B4 日期 2004/3/24

# 資安中心 成功跑第一

## 將變身網路氣象局 預報網路陰晴風雨

記者
王雪玲／報導

資訊安全已成爲網路時代最重要也最熱門的議題，台灣在資訊安全網路測試平台，就學術界來說，更是領先各國，負責成功大學資訊安全中心建置的成功大學計算機中心主任賴溪松昨(23)日表示，未來目標是希望資訊安全也能像氣象預報一樣，有網路氣象局，預報資安是晴時多雲還是偶陣雨。

今年4月執行，目前已有初步的成果，而美國是去年10月才推動Mini-InternetTestbed，目前還在建置中，尚無成果發表，所以就學術界來說，台灣目前建立的網路安全測試平台可說是世界NO.1。

網路安全測試平台建置的目的，簡單的說就是像真正的病毒一樣，提供一個病毒實驗室，從搜集病毒、了解病毒再提供一套處理病毒的模式，達成安全性分析、支持學術研究發展與教育訓練，讓網管人員更有經驗來處理病毒。

賴溪松指出，最終目標是希望資訊安全通報能像天氣一樣作預報，針對不同資訊安全環境，事先作預報，提供電腦使用者注意，讓病毒的傷害降到最低，但爲避免駭客利用公布的程式漏洞作攻擊，只會作大環境的偵測與預告，不會直接作漏洞提醒。

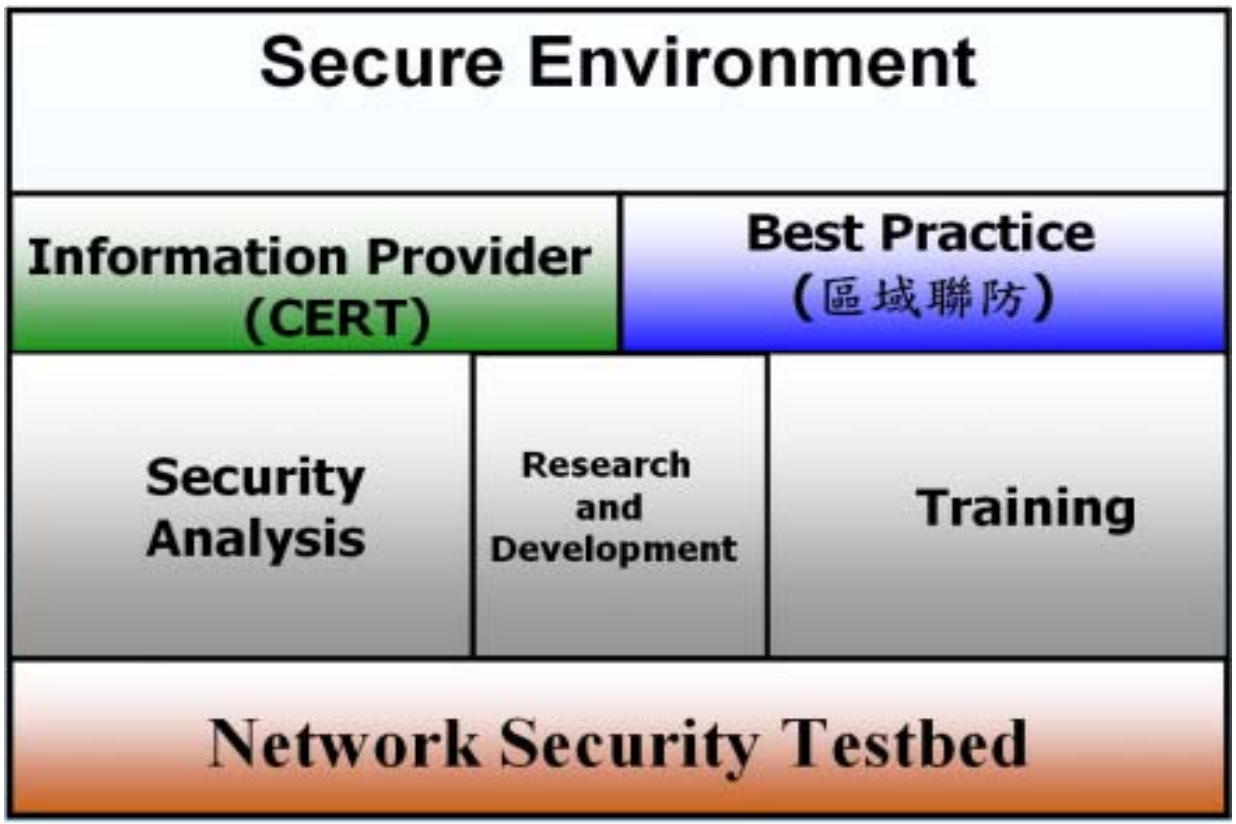
爲吸引駭客進入網路系統以學習駭客活動與行爲，故意隱藏在防火牆後面，所有進出資料都受到監控、捕獲及控制，作爲研究分析入侵者使用工具、方法及動機的研究資料。

目前在學術界對網路安全測試平台規劃與建置，台灣算是很早就進行，賴溪松指出，我國網路安全測試平台是由電信國家型計劃作補助，進行NBEN網路安全建置與實驗計劃，從去年5月到

成大資通安全研究中心設計一套Honeypot，故意設計爲有缺陷系統，是研究人員用來作

←成功大學計算機中心主任賴溪松（前）領軍，成大資通安全研究中心率先建立網路安全測試平台。
記者 王雪玲／攝

# 我國網路安全測試平台-定位



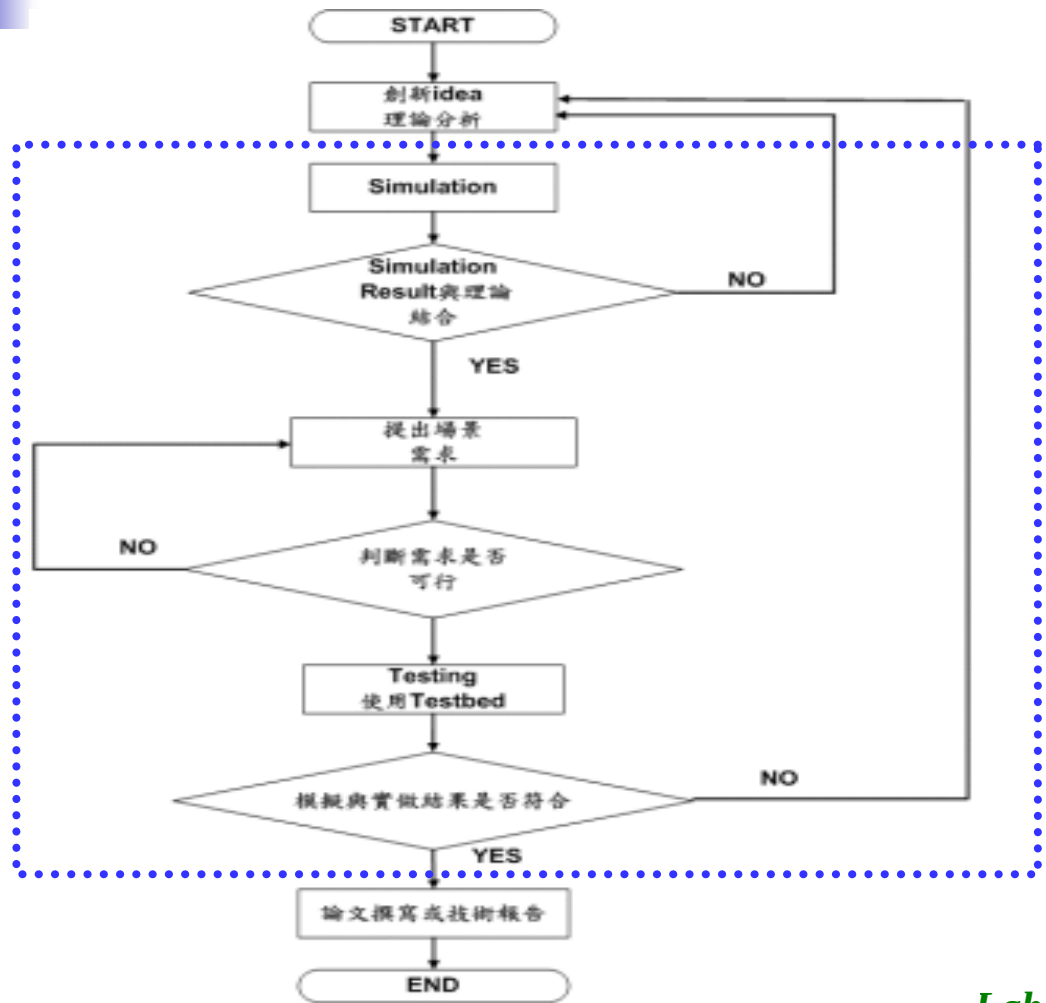
# 網路安全測試平台建置目的-安全性分析

- 以已知的方法或發展未知技術進行各種系統、軟體、駭客攻擊手法等的安全性分析，提供相關漏洞資訊及防範的方法。
- 分析判斷哪些漏洞在國內現有的網路環境架構與系統平台下可能的威脅，以量化、具體化的形式整理此種漏洞對網路架構所造成的衝擊。
- 希望能逐步建立起我國預警的機制，提供給國外CERT、SANS等單位，提升我國在國際間網路安全的地位。

# 網路安全測試平台建置目的-支援學術界研究發展 (1/2)

- 可完整支援我國網路安全相關理論之學術研究實驗。
- 可快速提供實驗環境需求及一套結合理論創建、模擬分析、實驗三項循序進行反覆求證的研究流程，提出相關具體的資料來支持新的理論創建，以增強資安研究的深度。

# 網路安全測試平台建置目的-支援學術界研究發展 (2/2)

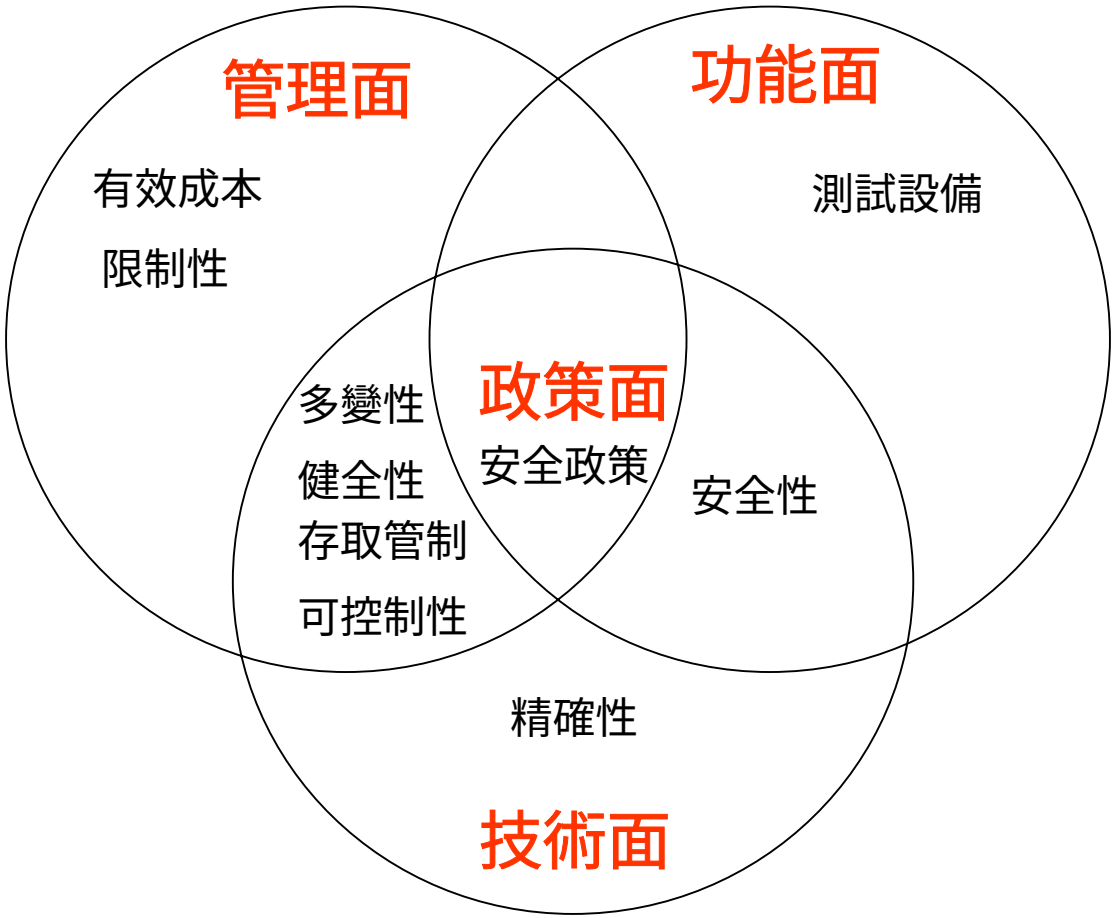


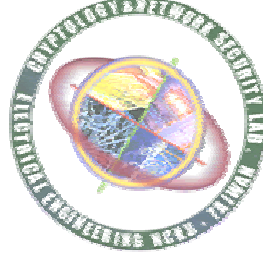

虛線部分為在測試平台環境中進行

# 網路安全測試平台建置目的-教育訓練

- 提供網路安全事件的真實重現，培養網管人員或相關技術人員可在不同網安事件重現過程中反覆的訓練，學習與加強網安事件發生時的應變能力過程經驗。
- 編撰成教育訓練教材及網安事件處理建議流程等資訊，提供給不同單位學習與防護的依據。
- 定期舉辦資安講座及規劃課程，以培訓國內資安人才和降低我國網路安全事件的發生。

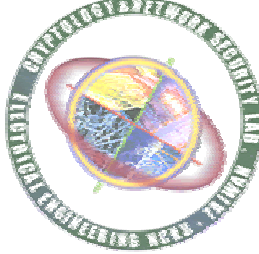
# 建置網路安全測試平台之需求





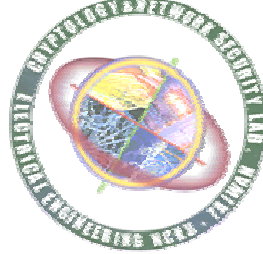
# 現有設備

| 設備名稱 | 數量 |
|---|---|
| PC (Pentium 4 2.4G MHZ 256 RAM 80GB) | 50 |
| Cisco Catalyst 3750 | 3 |
| Cisco Router 2610 | 4 |
| Cisco PIX 515 | 1 |
| Netscreen 204 | 1 |
| McAfee IntruShield 1200 | 1 |
| Cisco Aironet 1100 Series AP | 2 |
| Cisco Aironet 350 Series Client Adapters | 8 |



# 現有技術報告成果

- Real-time Monitoring your enemy via Honeypot
- Distributed Denial of Service: Attack & Prevention  A Case Study
- Experience with “Swiss Knife”
- A Practical experience of securing IIS server
- Performance Evaluation of Password Recovery Toolkits



# 現有技術報告成果 (cont.)

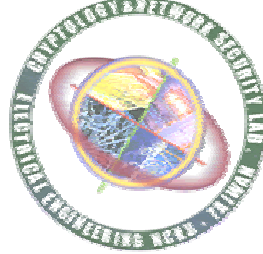
- Experience with IP Spoofing via Dsniff
- Experience with Hijacking attack and its prevention
- A Practical Experience of Securing Apache Server
- Domain Fingerprint with Net Tools
- DDoS攻擊在NS-2模擬軟體的研究與實作
- Honeynet之整合測試報告

# 國內外TestBed規模比較

| Project Name | Time | Testbed | Partner | Budget | Support Department |
|---|---|---|---|---|---|
|  DETER /EMIST | **2003/10/9** 發表 | **DETER Testbed** | **Academic** The University of California、Berkeley and University of Southern California's Information Sciences Institute (ISI)<br>**Industry:**Juniper, CISCO, Intel, IBM,HP | **DETER** $1 億 8 仟萬 **EMIST** $1 億 7 仟萬 | NSF 和 DHS |
|  NBEN 網路安全建置與實驗計畫 | **2003/5~ 2004/4** | **Nework Security Testbed** | **Academic** 成功大學、台灣大學、交通大學、中山大學、中正大學 、東華大學、清華大學、中央大學 | 1220 萬 | NTP 電信國家型科技計畫 |

# 現有成果比較

| Project Name | Result |
|---|---|
|  DETER / EMIST | ▪建置Testbed - 64 node at ISI-west (2004年1月)<br>▪N/A |
|  NBEN網路安全建置與實驗計畫 | ▪第一階段網路測試平台建置(2003年5月~2003年8月)<br>▪第二階段網路安全測試平台建置(2003年9月 2004年2月)<br>▪針對TCP/IP協定弱點進行為主進行不同作業平台及伺服器的安全性問題進行不同場景測試。<br>▪針對共同主題DDoS攻擊進行研究與測試。<br>▪重現重大事件場景：DDoS Attack、SQL Slammer、Blaster。<br>▪Honeypnet環境建置<br>▪IPTrackback技術追蹤DDoS攻擊來源。<br>▪DDoS攻擊回復機制<br>▪教育訓練教材及技術報告(總共19份) |



# 未來規劃

- 擴增至150台電腦
- 建置部分網路環境提升至10G
- 增購無線網路安全設備
- 購買NetScreen-IDP 500 (入侵偵測與防禦系統)

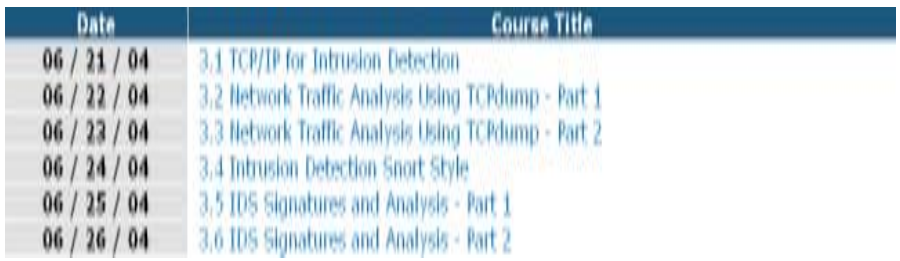
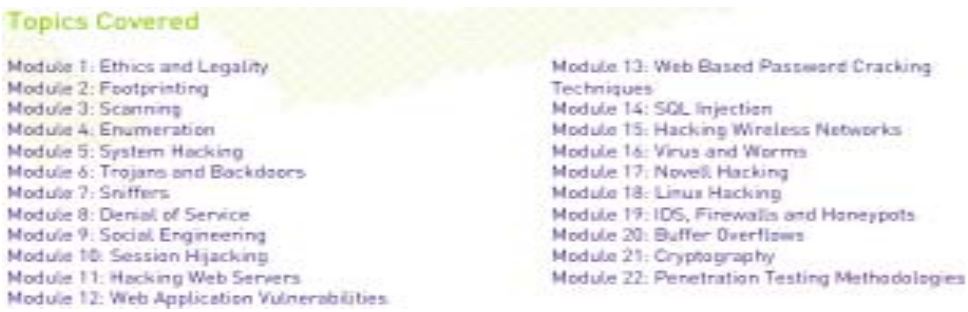
# 教育訓練

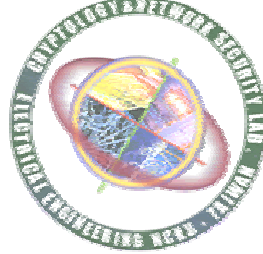
- 每年7月舉辦資安課程 (免費，每年約30~40名)
  - TCP/IP介紹
  - 基礎密碼學
  - 網路安全管理工具應用
  - 電腦病毒與蠕蟲
  - 防駭工具應用分析等
    - 建議由老師推薦新研究生來接受短期訓練

# 教育訓練 (cont.)

- 每年8月份開始開始舉辦資安課程 (中高階課程收費)
  - 安全性程式設計
  - 路由器高階安全攻防課程
  - CISSP 安全認證課程等
- 資安訓練教材製作編撰

# 教育訓練 – 國外教育訓練機構比較

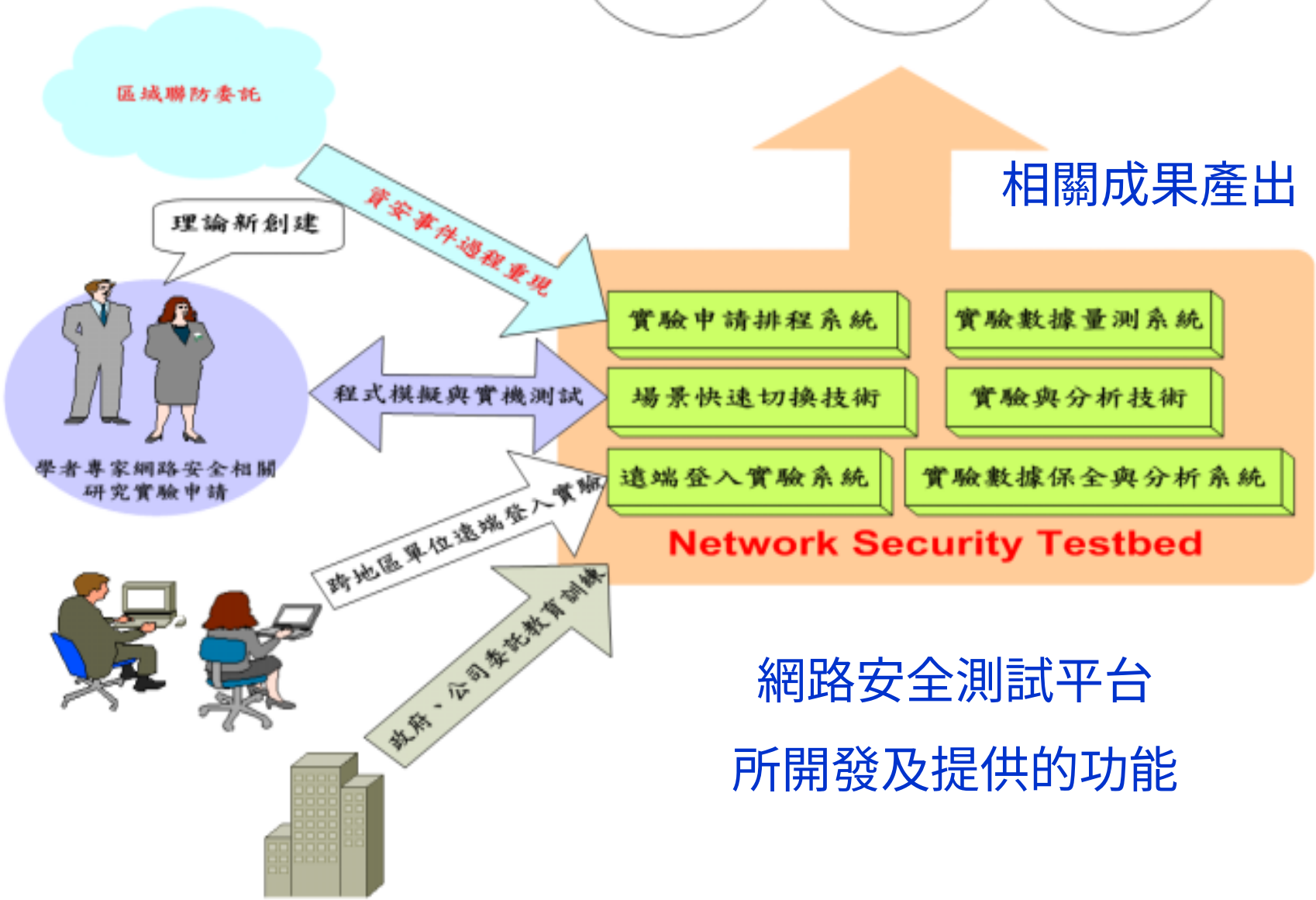
| 公司 | 課程 | 費用 |
|---|---|---|
| SANS |  | 六天<br>US$3095 |
| Microtrain |  | 五天<br>US$1950 |
| 成大<br>Testbed | 上述課程均可講授，且可開授中高階課程 | 尚待評估 |



# 教育訓練–初步規劃課程

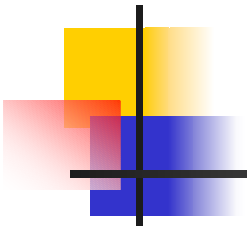
| | | | | | | |
|---|---|---|---|---|---|---|
| 高階安全性管理課程 | CISSP安全認證課程 | BSI/ISO 17799安全管理實務 | Microsoft安全性管理架構 | Microsoft安全性環境之設計與規劃 | 企業安全性風險評估與管理:理論與實務 | 企業級IPV6網路環境規劃與建置 |
| 高階技術課程 | 路由器高階安全攻防課程 | Windows作業系統安全性分析 | Linux作業系統安全性分析 | Windows SA Server實務 | Linux 安全性技術: Firewall、VPN | 安全性程式設計 |
| 中階課程 | 路由器基本課程 | Windows作業系統課程模組 | Linux作業系統課程模組 | Linux Server課程模組 | 進階駭客攻防實務 | IPV6網路環境建置 |
| 初階課程 | 網路安全基本課程 | | | | | |

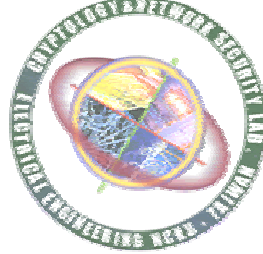
我們可以服務的對象




網路安全測試平台

所開發及提供的功能





# Q & A