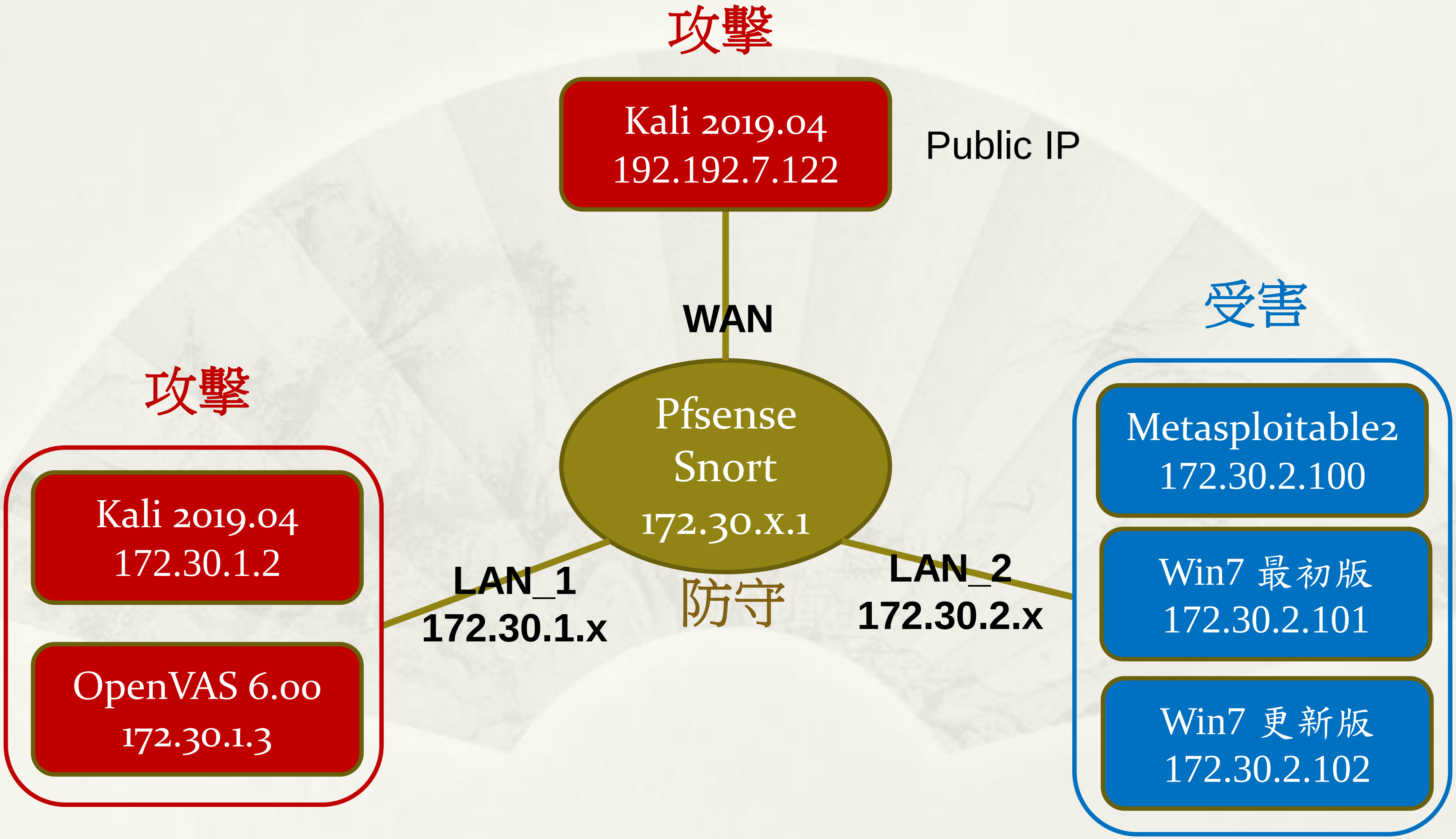
建置資安攻防演練平台
從原理到實作

游子興
台大計中網路組
davisyou@ntu.edu.tw
02-33665008

大綱

- 資安攻防平台架構
  - 攻擊: Kali, OpenVAS
  - 防守: Pfsense, Snort
  - 受害: Metasploitable2, Win7(最初版) + Firefox, Win7(更新版)
- 弱點偵察 Scan
  - Nmap
  - OpenVAS
  - Metasploit
- 攻擊方式
  - Direct Attack 直接攻擊
  - Client Side Attack 用戶端攻擊
  - Privilege Escalation 權限提升
- 防守工具
  - 防火牆: pfsense
  - IPS: 以 Snort 為例

資安攻防平台



攻擊

Kali 2019.04
192.192.7.122

Public IP

WAN

Pfsense
Snort
172.30.x.1

防守

攻擊

Kali 2019.04
172.30.1.2

OpenVAS 6.00
172.30.1.3

LAN_1
172.30.1.x

LAN_2
172.30.2.x

受害

Metasploitable2
172.30.2.100

Win7 最初版
172.30.2.101

Win7 更新版
172.30.2.102

VM 資源

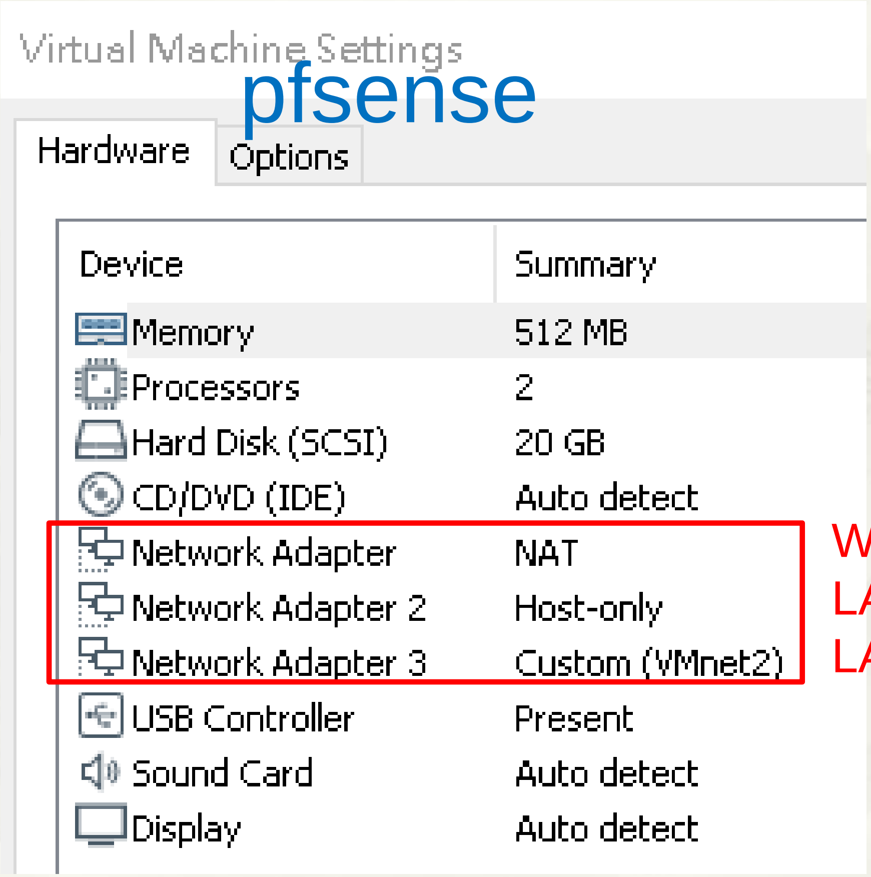
VM	記憶體
Pfsense 2.4.4	512MB
Kali 2019.04	1GB
Metasploitable2	1GB
Win7 最初版	1GB
OpenVAS 6.00 (Option)	2GB

- VM 開啟時
  - I Moved It: 不會變更 uuid & mac address
  - I Copied It: 會變更 uuid & mac address

資安攻防平台
Vmware 網路設定

Mode	VMnet	網卡	IP	DHCP	Internet
Bridge	VMnet0	目前上網網卡	Layer2	N/A	N/A
Host-only	VMnet1	VMware Network Adapter VMnet1	192.168.x.1	Yes	No
NAT	VMnet8	VMware Network Adapter VMnet8	192.168.x.1	Yes	Yes
	VMnetX	N/A	N/A	No	No

資安攻防平台
Pfsense 網路設定



Virtual Machine Settings

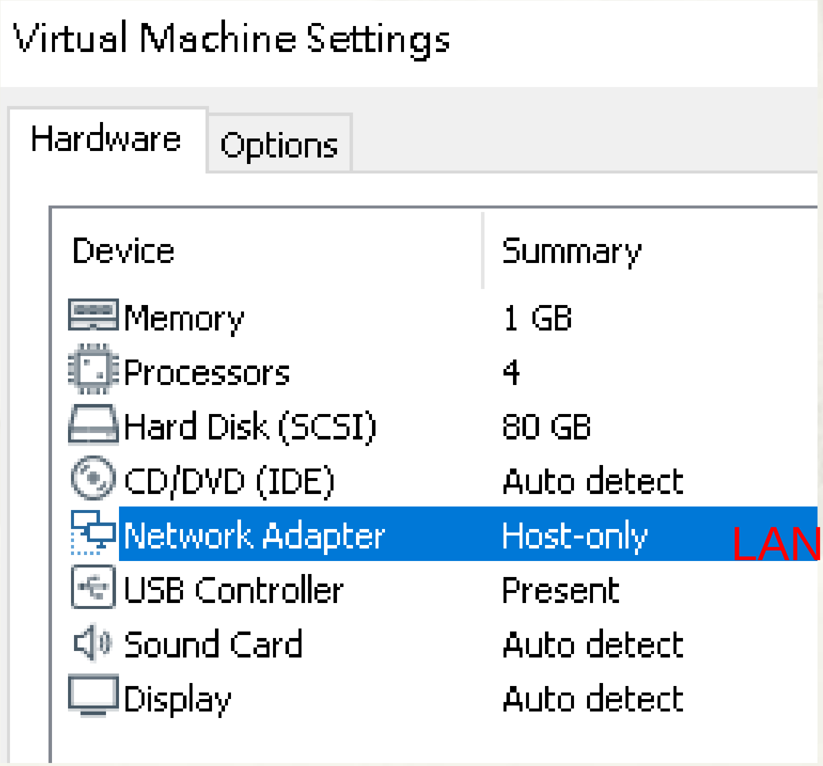
pfsense

Device	Summary
Memory	512 MB
Processors	2
Hard Disk (SCSI)	20 GB
CD/DVD (IDE)	Auto detect
Network Adapter	NAT
Network Adapter 2	Host-only
Network Adapter 3	Custom (VMnet2)
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

WAN
LAN_1
LAN_2

資安攻防平台
Pfsense 網路設定

Kali
OpenVAS



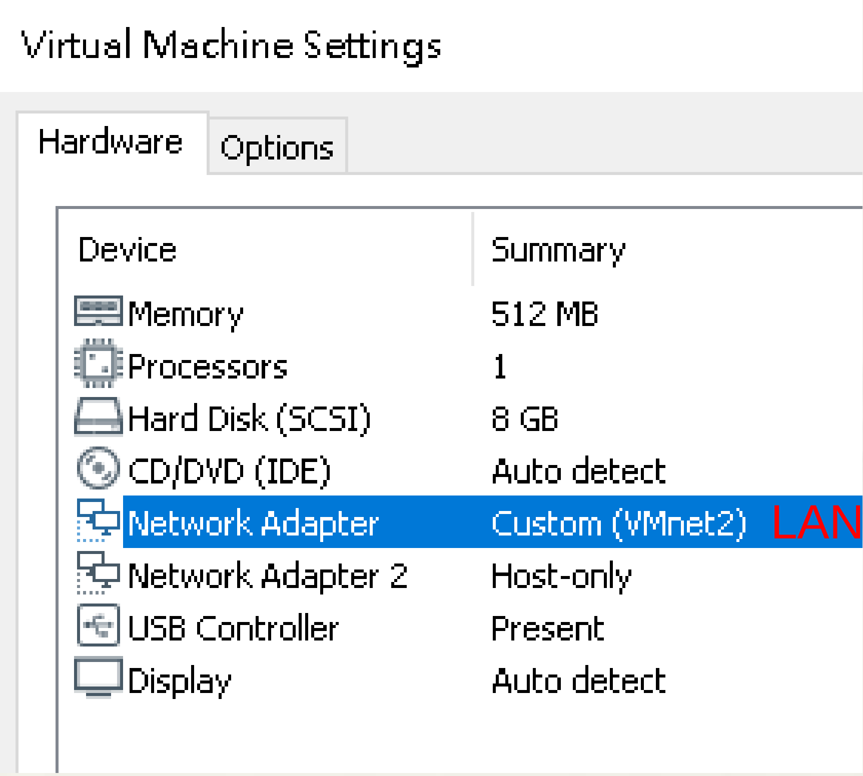
Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	1 GB
Processors	4
Hard Disk (SCSI)	80 GB
CD/DVD (IDE)	Auto detect
Network Adapter	Host-only
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

LAN_1

Metasploitable2
Win7 最初版



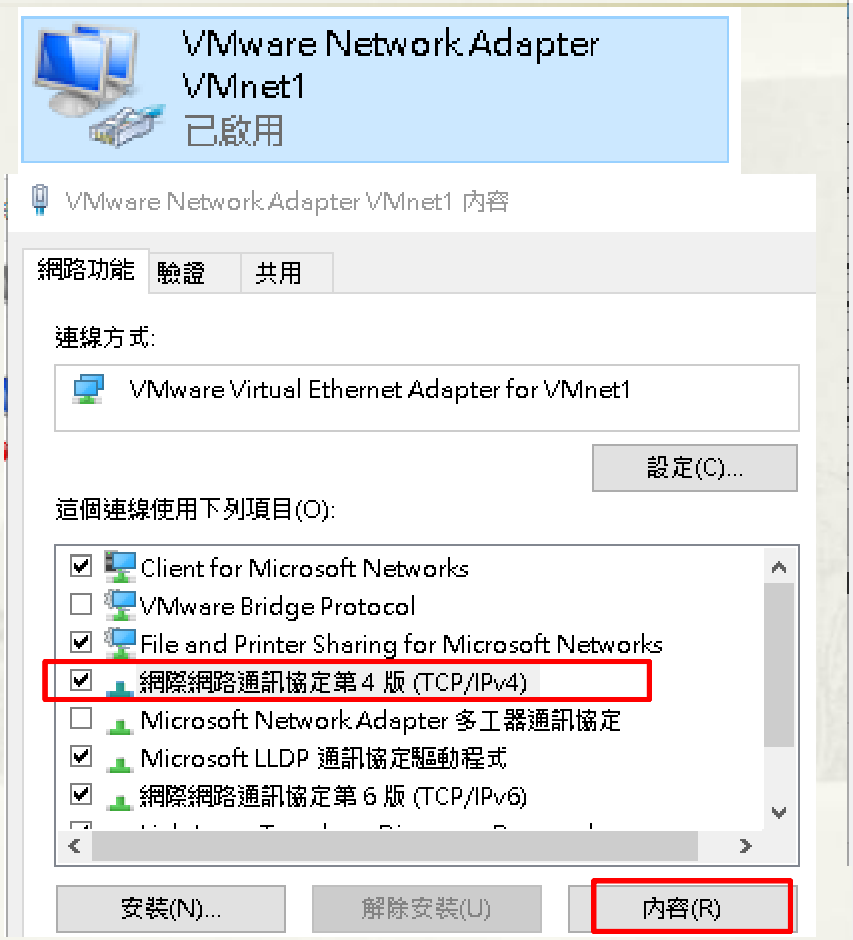
Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	512 MB
Processors	1
Hard Disk (SCSI)	8 GB
CD/DVD (IDE)	Auto detect
Network Adapter	Custom (VMnet2)
Network Adapter 2	Host-only
USB Controller	Present
Display	Auto detect

LAN_2

本機 Host 連線 LAN_1 設定



VMware Network Adapter
VMnet1
已啟用

VMware Network Adapter VMnet1 內容

網路功能 | 驗證 | 共用

連線方式:

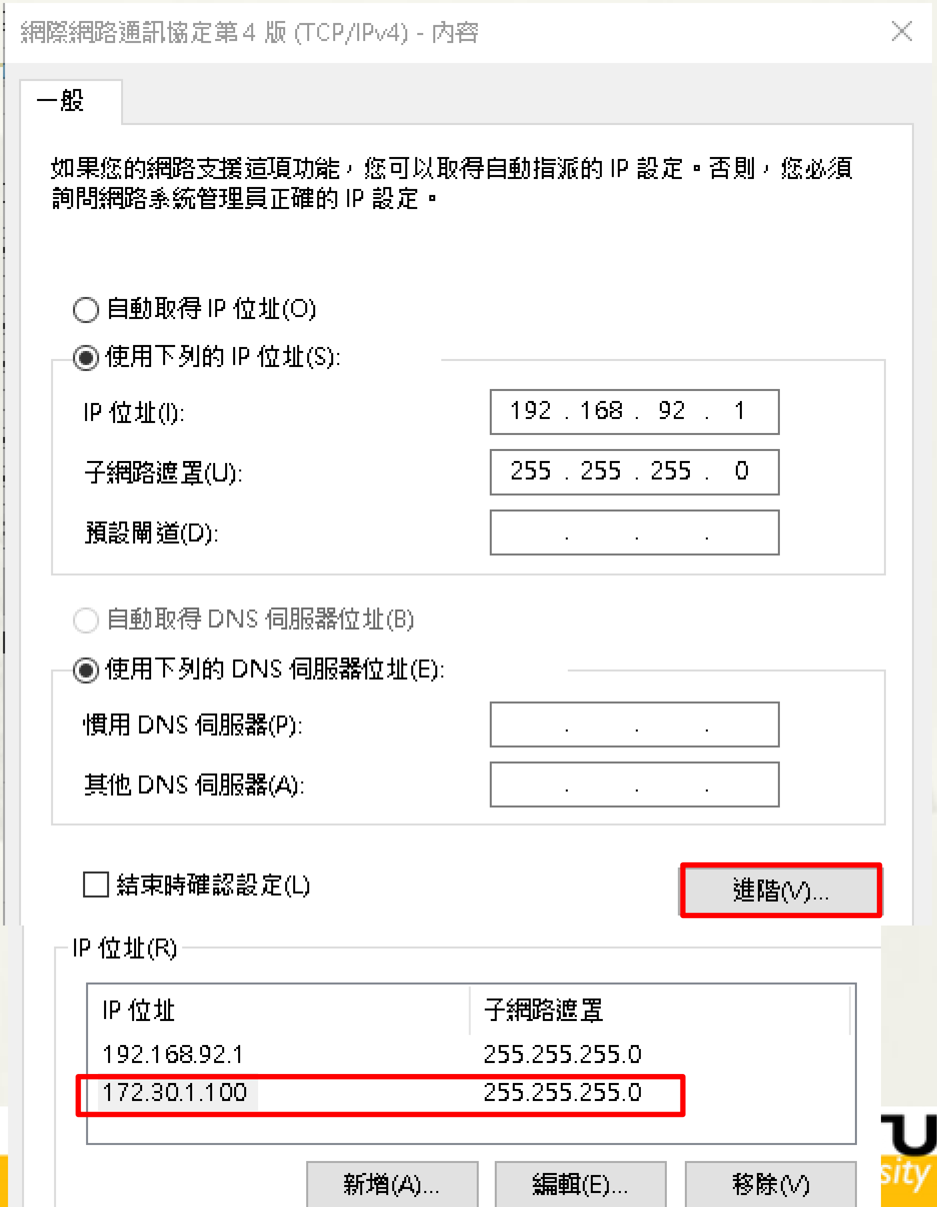
VMware Virtual Ethernet Adapter for VMnet1

設定(C)...

這個連線使用下列項目(O):

- ☑ Client for Microsoft Networks
- ☐ VMware Bridge Protocol
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ 網際網路通訊協定第 4 版 (TCP/IPv4)
- ☐ Microsoft Network Adapter 多工器通訊協定
- ☑ Microsoft LLDP 通訊協定驅動程式
- ☑ 網際網路通訊協定第 6 版 (TCP/IPv6)

安裝(N)... | 解除安裝(U) | 內容(R)



網際網路通訊協定第 4 版 (TCP/IPv4) - 內容

一般

如果您的網路支援這項功能，您可以取得自動指派的 IP 設定。否則，您必須詢問網路系統管理員正確的 IP 設定。

○ 自動取得 IP 位址(O)
● 使用下列的 IP 位址(S):

IP 位址(I): 192 . 168 . 92 . 1
子網路遮罩(U): 255 . 255 . 255 . 0
預設閘道(D): . . .

○ 自動取得 DNS 伺服器位址(B)
● 使用下列的 DNS 伺服器位址(E):

慣用 DNS 伺服器(P): . . .
其他 DNS 伺服器(A): . . .

☐ 結束時確認設定(L)

進階(V)...

IP 位址(R)

IP 位址	子網路遮罩
192.168.92.1	255.255.255.0
172.30.1.100	255.255.255.0

新增(A)... | 編輯(E)... | 移除(V)

攻擊 - Kali

- SSH
  - Login: root
  - Passwd: toor
- VMWare VM
  - https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/
- 工具
  - Nmap
  - Metasploit
  - Netcat

攻擊方 - Kali Metasploit

- 初始化
  - systemctl start postgresql
  - systemctl enable postgresql
  - msfdb init
- 開啟
  - msfconsole -q

Meterpreter Shell

- 常用語法
  - getuid
  - sysinfo
  - keyscan_start 鍵盤側錄開始
  - keyscan_stop 鍵盤側錄結束
  - screenshot
    - 若出現錯誤:
      - [-] stdapi_ui_desktop_screenshot: Operation failed: Access is denied.
    - 原因:
      - Windows 目前正使用 RDP 連線. 僅支援 Console 登入之下擷取螢幕.

攻擊方
OpenVAS

- OpenVAS
  - http://172.30.1.3/
  - Login: admin
  - Passwd: admin_openvas
  - Virtual Appliance Version: 6.0.0
    - https://www.greenbone.net/en/install_use_gce

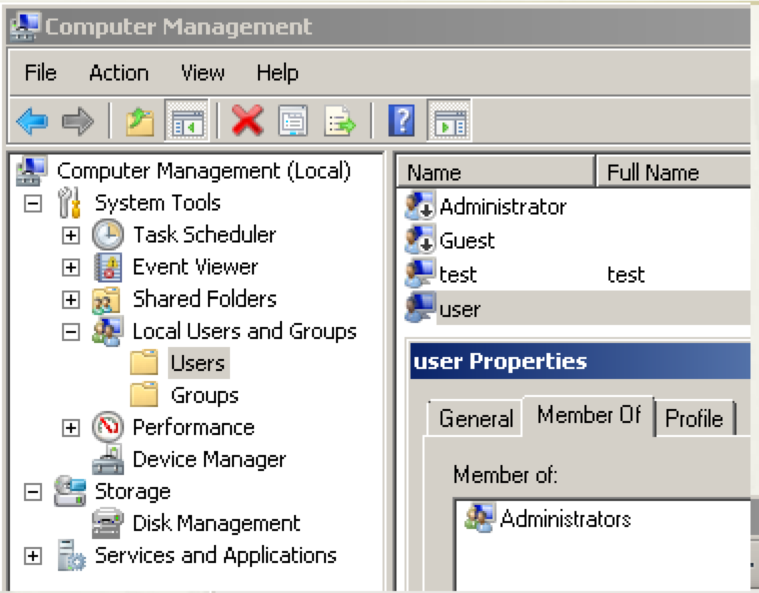
受害方
Metasploitable

- Metasploitable2
  - SSH
    - Login: msfadmin
    - Passwd: msfadmin
  - https://sourceforge.net/projects/metasploitable/
  - https://metasploit.help.rapid7.com/docs/metasploitable-2-exploitability-guide
- Metasploitable3 參考用
  - https://github.com/rapid7/metasploitable3
  - https://metasploit.help.rapid7.com/docs/setting-up-a-vulnerable-target

受害方
Windows 7

- Win7
  - 最初版本無任何 Patch
  - Console Login
    - Administrator Group
      - Login: user
      - Passwd: user
    - Not in Administrator Group
      - Login: test
      - Passwd: test
- Firefox v28

受害方
Windows 7



Computer Management

File Action View Help

- Computer Management (Local)
  - System Tools
    - Task Scheduler
    - Event Viewer
    - Shared Folders
    - Local Users and Groups
      - Users
      - Groups
    - Performance
    - Device Manager
  - Storage
    - Disk Management
  - Services and Applications

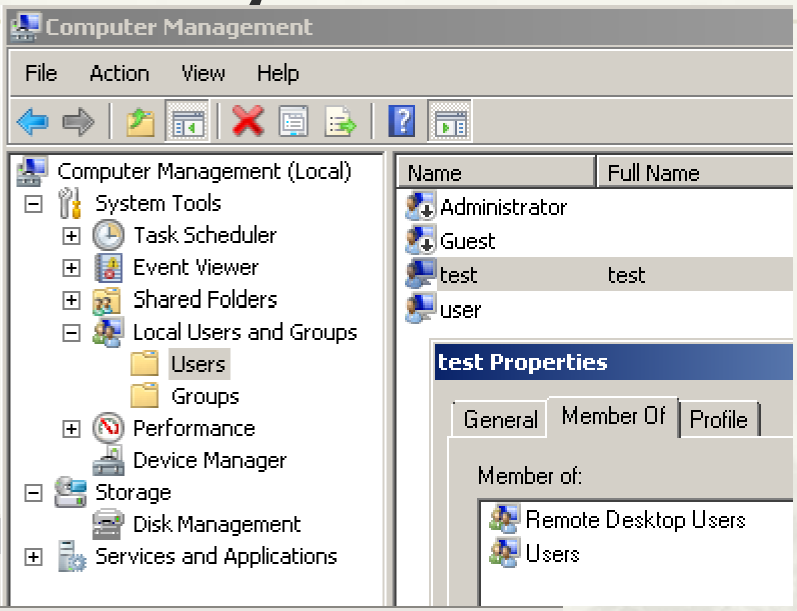
Name	Full Name
Administrator	
Guest	
test	test
user	

user Properties

General | Member Of | Profile

Member of:

- Administrators



Computer Management

File Action View Help

- Computer Management (Local)
  - System Tools
    - Task Scheduler
    - Event Viewer
    - Shared Folders
    - Local Users and Groups
      - Users
      - Groups
    - Performance
    - Device Manager
  - Storage
    - Disk Management
  - Services and Applications

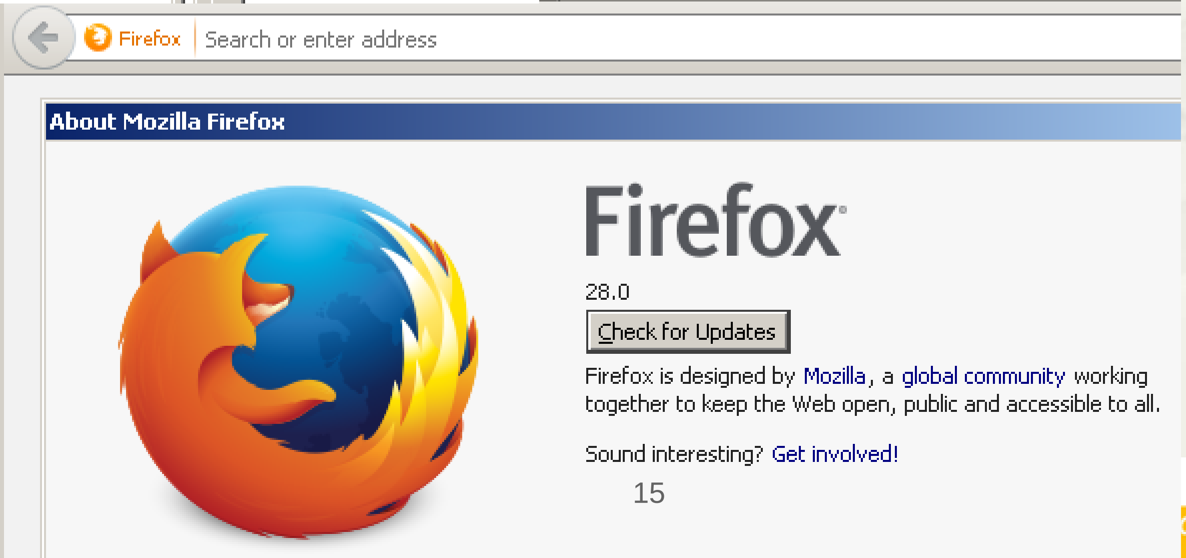
Name	Full Name
Administrator	
Guest	
test	test
user	

test Properties

General | Member Of | Profile

Member of:

- Remote Desktop Users
- Users



Firefox | Search or enter address

About Mozilla Firefox

Firefox

28.0

Check for Updates

Firefox is designed by Mozilla, a global community working together to keep the Web open, public and accessible to all.

Sound interesting? Get involved!

弱點偵察
Scan

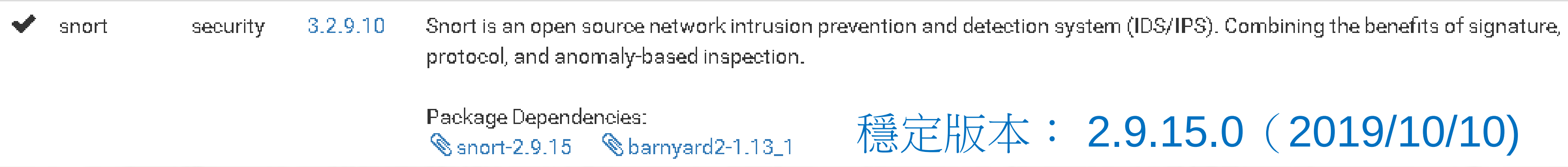
- nmap
  - nmap -Pn -A 172.30.2.100
  - 結果: nmap_Metaspliable2.TXT
  - nmap -Pn -sC -sV -p 445 172.30.2.101
    - -Pn Treat all hosts as online (skip host discovery), 若目的ip 無法回應 ping
    - -A OS detection + script scanning
    - -sV Service version scanning
    - -sC Scan using default safe scripts must be run with -sV switch in order for the NSE scripts (--script default)
- OpenVAS
- Metasploit

防守

- Firewall
  - Pfsense v2.4.4 p3
  - http://172.30.1.1/
    - Login: admin
    - Passwd: pfsense
  - https://www.pfsense.org/

防守 – IDS/IPS
Snort in pfsense

- System > Package Manager
  - 安裝 snort package



✓ snort security 3.2.9.10 Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.

Package Dependencies:
snort-2.9.15 barnyard2-1.13_1

穩定版本： 2.9.15.0（2019/10/10)

- Services > Snort > Global Settings
  - Enable Snort VRT= Check
  - Snort Oinkmaster Code=
- Services > Snort > Update Rules
  - Update Rules

Snort in pfsense
Install & Setup

- Services > Snort > Interfaces
  - Interface= LAN_2
  - Home Net= HomeNet_Pass
  - External Net= default
- Firewall > Aliases > IP
  - Name= HomeNet
  - Type= Network
  - Network= 172.30.2.0/24
- Services > Snort > Pass Lists
  - Name= HomeNet_Pass
  - Assigned Alias= HomeNet

Snort in pfsense

- /usr/local/etc/snort/snort.conf
- /usr/local/etc/snort/rules/*.rules

簡報完畢

謝謝